FACULTAD DE CIENCIA Y TECNOLOGÍA.

ESCUELA DE INGENIERÍA ELECTRÓNICA.

Análisis y diseño de un sistema de video asistencia y control de accesos basados en normas ISO 27000 para ETAPA EP.

Trabajo de graduación previo a la obtención del título de:

INGENIERO ELECTRÓNICO.

Autores:

YOLANDA JAQUELINE ORTEGA URGILÉS.

FRANKLIN EDUARDO CUMBE ALVARADO.

Director:

EDGAR RODRIGO PAUTA ASTUDILLO.

CUENCA, ECUADOR.

2016

Dedicatoria

Años van, años vienen, y el tiempo pasar sin cesar…….

He dejado pasar mucho tiempo para poder ver cristalizados sueños en realidades, pero aquí estoy, caí y supe levantarme con la bendición de Papá Diosito quien nunca me soltó de la mano. Hoy al finalizar este duro trabajo, quiero dedicar con todo mi corazón a Papi Diego y mi Mami Yoli, ejemplo de padres que siempre estuvieron allí, apoyándome e impulsándome para seguir adelante y no morir en el intento. A mis hermanos Diego y Cris, Janeth y Pacho, Diana y Johan, José y Liz, a mis sobrinas y sobrinos a quienes amo y les agradezco por esa mano siempre extendida que tuvieron para levantarme e impulsarme.

Pasaron los años y llegaron a mi vida Christian Avecillas, amor de esposo quien tomó mi mano para continuar este camino junto con el amor más tierno que existe sobre la faz de esta tierra y que se convirtió en la razón de mi ser, mi pequeño hijo Sebastián; a quienes los sacrifiqué con mi tiempo para poder realizar este sueño.

Dios les pague familia por ese amor que me tienen, y que a veces no creo merecer. Por ustedes y para ustedes….

Yolanda Jaqueline Ortega Urgilés

Dedicatoria

La vida es una incógnita a medida que pasa el tiempo la vamos descifrando. Cuando somos pequeños añoramos con crecer y terminar nuestros estudios lo más pronto posible, pero a medida que crecemos vamos dejando de tener esos sueños para convirtiéndolos en dulces realidades, el único problema es que no nos damos cuenta de que nuestros seres queridos también van creciendo y que los sueños que de niños compartimos a veces ellos no los van a poder disfrutar porque no se encuentran ya con nosotros, no sabes cuánto me hubiese gustado que Tú me hubieras puesto la capa para ir a recibir mi título pero sé que de allá arriba me vas a mirar y decir "ya vez que si pudiste lograrlo", todo esto es para ti mi Ñañita Pastoriza y lo que se viene será mucho mejor no voy a dejar de soñar.

Franklin Eduardo Cumbe Alvarado.

Agradecimientos

No habría podido conseguir nada sin ti Diosito, pues contigo todo y sin ti nada, has sido la luz que guía mi camino. A mi familia que siempre me apoyaron, e impulsaron gracias infinitas por ser ese motor que inspira mi vida.

De igual manera quiero expresar mi más profundo agradecimiento a ETAPA EP, empresa que nos abrió las puertas representada por el Ingeniero Ricardo Urgilés como coordinador del proyecto y al Magister Edgar Pauta, dilecto catedrático y Director del trabajo de titulación quienes con sus conocimientos y experiencia nos supieron guiar y apoyar en nuestro trabajo. Un especial agradecimiento al Magister Luis Felipe Sexto, catedrático de la Unidad de Posgrados quien con su paciencia y sus conocimientos nos guio en este arduo trabajo. Finalmente a todo el cuerpo docente y administrativo de la Facultad de Ciencia y Tecnología, gracias por todo.

Yolanda Jaqueline Ortega Urgilés

Al finalizar mi tesis quiero agradecer con todo mi corazón a mi familia que ha sido un soporte muy importante en la consecución de este título, yo sé que ha pasado tiempo pero gracias por siempre darme su apoyo, a mis hermanos que desde la distancia siempre me brindaron su mano, y a mi ángel de la guarda que siempre me va a guiar K2-146.

Un agradecimiento muy especial al Magister Edgar Pauta, Director del Trabajo de Titulación de la Universidad del Azuay, y al Ingeniero Ricardo Urgilés, Coordinador del Proyecto en ETAPA EP, quienes con sus valiosos conocimientos nos apoyaron y guiaron para poder obtener mi tan ansiado título.

Franklin Eduardo Cumbe Alvarado.

INDICE CONTENIDOS.

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

Anexo XII: Alcance del proyecto para la implementación del sistema de gestión de seguridad de la información dirigido al control de accesos a las salas de telecomunicaciones

Anexo XIII: Política de seguridad del sistema de gestión de seguridad de la información dirigido al control de accesos a las salas de telecomunicaciones

Anexo XIV: Metodología de evaluación y tratamiento del riesgo para la implementación del sistema de gestión de seguridad de la información dirigido al control de accesos a las salas de telecomunicaciones**.**

Anexo XV: Declaración de aplicabilidad del sistema de gestión de seguridad de la información dirigido al control de accesos a las salas de telecomunicaciones**.**

Anexo XVI: Plan de tratamietno del riesgo del sistema de gestión de seguridad de la información dirigido al control de accesos a las salas de telecomunicaciones

Anexo XVII: NTE INEN/ISO-IEC 27001:2011

ANÁLISIS Y DISEÑO DE UN SISTEMA DE VIDEO ASISTENCIA Y CONTROL DE ACCESOS BASADO EN NORMAS ISO 27000 PARA ETAPA EP

RESUMEN

El presente trabajo de titulación desarrollado en ETAPA EP, inicia con una introducción a las normas de estándares nacionales e internacionales para el manejo de los Sistemas de Gestión de Seguridad de la Información, unificados en la ISO 27000.

Utilizando metodologías de evaluación del estado actual de la organización, se obtuvo como resultado las vulnerabilidades a las que se encuentra expuesta la organización, por lo que, haciendo uso de una normativa internacional encargada de dar los lineamientos para incrementar los niveles de seguridad en la empresa obtuvimos como resultado el diseño de un nuevo sistema de seguridad para las Salas de Telecomunicaciones junto con un manual de procesos que les permitirá dar los primeros pasos hacia una certificación ISO 27000.

Palabras Claves: SGSI, ISO 27000, Sistema de Video Asistencia, Vulnerabilidad, Salas de Telecomunicaciones.

Edgar Rodrigo Pauta Astudillo
Director de Trabajo de Titulación

Hugo Marcelo Torres Salamea
Director de Escuela

Yolanda Jaqueline Ortega Urgilés

Franklin Eduardo Cumbe Alvarado

Autores

ANALYSIS AND DESIGN OF A VIDEO ASSISTANCE AND ACCESS CONTROL SYSTEM FOR *ETAPA EP* BASED ON ISO 27000 STANDARDS

ABSTRACT

This graduation work developed in ETAPA EP, starts with an introduction to the rules of national and international standards for the management of Information Security Management Systems, unified under the ISO 27000, through methods for assessing the current state of the organization. The results demonstrated the vulnerabilities to which the organization is exposed; therefore, by using an international standard responsible for giving guidelines to increase safety levels in the Company, it was possible to obtain as a result the design of a new security system for telecommunications rooms along with the development of a processes handbook that will help to take the first steps towards the achievement of ISO 27000 certification.

Keywords: ISMS, ISO 27000, Video Assistance System, Vulnerability, Telecommunications Rooms

Edgar Rodrigo Pauta Astudillo
Thesis Director

Hugo Marcelo Torres Salamea
School Director

Yolanda Jaqueline Ortega Urgilés

Franklin Eduardo Cumbe Alvarado

Authors

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

Ortega Urgilés Yolanda Jaqueline

Cumbe Alvarado Franklin Eduardo

Trabajo de Titulación

Ing. Pauta Astudillo Edgar Rodrigo

Septiembre, 2016.

ANÁLISIS Y DISEÑO DE UN SISTEMA DE VIDEO ASISTENCIA Y CONTROL DE ACCESOS BASADO EN NORMAS ISO 27000 PARA ETAPA EP

INTRODUCCIÓN

En años anteriores las organizaciones no han priorizado el tema de la seguridad de la información, siendo éste un activo invaluable y de vital importancia para un normal funcionamiento y desempeño del sistema productivo, pues, podría encontrarse sujeta a innumerables vulneraciones en sus seguridades como por ejemplo: adulteraciones, mal manejo de sus bienes por parte de personal interno o tercerizado, quienes al tener acceso directo a las instalaciones, y específicamente a las Salas de Telecomunicaciones, podrían efectuar actividades ajenas a la empresa e inclusive podrían utilizar su información para ejecutar fraudes, engaños, etc; provocando daños económicos o perjudicando el buen nombre de la organización.

Siendo ETAPA EP, una empresa que brinda servicios con calidad, no se encuentra exenta de ser víctima de ataques y vulneraciones en sus seguridades, por lo que al contar con un sistema de seguridad junto con procesos adecuados que permitan realizar

un control de los trabajos que se ejecutan en dichas salas, mismos que basados en las normas ISO 27000 le permitirán incrementar los niveles de seguridad.

Este proceso se da con:

- Una evaluación de la situación actual de las Salas de Telecomunicaciones involucradas en el estudio: Central Totoracocha, Concentrador de Baños y Nodo Externo 24 de Mayo.
- La aplicación de una técnica adecuada para la evaluación del riesgo, de esta manera se podrá tener una visión más clara de las necesidades y procesos basados en normas ISO 27000 que se requieren en la organización.
- El diseño de las nuevas Salas de Telecomunicaciones, que contarán con nuevos dispositivos para el control de acceso a las mismas.

Lo expuesto en esta introducción, se desarrollan en los 4 capítulos que contiene este trabajo.

CAPÍTULO 1

MARCO TEÓRICO

1. Introducción

En el desarrollo de este trabajo utilizaremos términos cuyos conceptos deberemos tenerlos muy claros, por lo que en este marco teórico citaremos definiciones, normas o estándares, seguridad, entidades encargadas de la normalización nacional e internacional y sus objetivos principales.

1.1. Definiciones

1.1.1 Estándar: Viene del inglés *Standard* y cuya definición más general que conocemos es la dada por la Real Academia Española, que nos dice "Que sirve como tipo, modelo, norma, patrón o referencia", o su sinónimo norma que se define como "Regla que se debe seguir o a que se debe ajustar las conductas, tareas, actividades, etc." (Española, 2015) En este contexto y haciendo referencia a nuestro tema de estudio, diremos que las normas son documentos que proporcionan requisitos, especificaciones, directrices o características que pueden ser utilizadas consistentemente para asegurar que los materiales, productos, procesos y servicios son adecuados para su propósito. (ISO, ISO, 2015) Es decir son un conjunto de herramientas prácticas que ayudan al crecimiento y apertura a los mercados mundiales, facilitan el comercio, reducen los riesgos y garantizan que los países en desarrollo compartan los beneficios. Las normas ayudan a construir asociaciones a aumentar la satisfacción del cliente y asegurar la calidad haciendo del mundo un lugar más productivo, creativo y seguro.

1.1.2. Seguridad de la Información: Se define como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

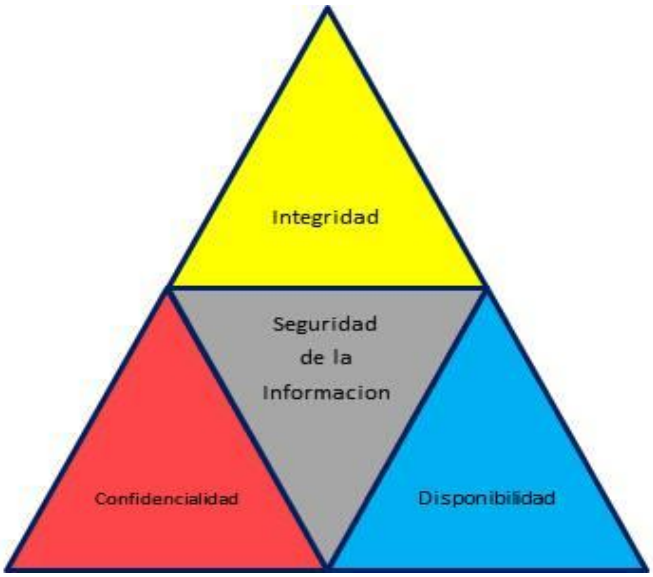


Figura 1. 1: Seguridad de la Información.

La información que manejan las empresas u organizaciones existen de muchas formas (impresa, almacenada electrónicamente, transmitida por medios electrónicos) y como todo recurso es un activo que tiene valor y por ende se debe proteger de amenazas con la finalidad de evitar se produzcan daños económicos, adulteraciones, malos manejos o fraudes. (M, 2005)

Una vez definida Seguridad de la Información, debemos aclarar y no confundirla con Seguridad Informática, pues ésta hace referencia a la vulneración y amenazas técnicas que se dan a la información a través de virus, spam, violación de contraseñas, irrupciones a los equipos, etc. (Meyer, 2012)

1.1.3 SGSI: Sistema de Gestión de la Seguridad de la Información o su acrónimo en inglés ISMS (*Information Security Management System*), de acuerdo a ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (27000, 2012)

1.1.4 Gestión de Riesgos: Se define como riesgo a la posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.

Por su parte la Gestión de Riesgos es la necesidad de garantizar el correcto funcionamiento de la tecnología de la empresa protegiéndola de crecientes amenazas que aprovechándose de mínimas posibilidades de efectuar una vulneración (fraude, espionaje, sabotaje o vandalismo) se coloca en peligro los activos de la organización, pero se debería considerar también dentro de los riesgos a los incidentes causados voluntaria o involuntariamente por el personal tanto interno como terciado o aquellos provocados accidentalmente por la naturaleza como son las catástrofes.

Gestión de Riesgos tiene como desafío proteger unos de los más importantes activos de la organización: la información, consiguiendo mantener o hasta incrementar la reputación de la empresa, implementando controles acordes a la actividad a la que se dedique la misma, promoviendo acciones correctivas y preventivas, garantizando el cumplimiento de reglamentaciones y procesos de gestión de seguridad de la información. (Stefanini, 2015)

1.1.5 Dominios de Control: Previenen los accesos no autorizados a los servicios de la red, por lo que la normativa NTE INEN/ISO-IEC 27001:2011 toma en cuenta aspectos organizativos, lógicos, físicos y legales que llevaron a establecer 11 Dominios de Control que abarcan 39 objetivos de control y 133 controles, no siendo todos aplicables a la empresa sino adaptables a las necesidades de la misma, detallándolos a continuación:

1. **Políticas de Seguridad**:
    - ✓ Dirigir y dar soporte a la gestión de seguridad de la información.

2. **Aspectos Organizativos de la Seguridad de la Información:**

   - ✓ Gestionar la seguridad de la información dentro de la organización.
   - ✓ Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.
   - ✓ Mantener la seguridad de la información cuando la responsabilidad de su tratamiento sea externalizado a otra organización (empresas contratistas).

3. **Clasificación y Control de Activos (Gestión de Activos):**

   - ✓ Mantener una protección adecuada sobre los activos involucrados de la organización.
   - ✓ Asegurar un nivel de protección adecuado a los activos de la información.

4. **Seguridad del Recurso Humano:**

   - ✓ Reducir los riesgos de errores humanos como robos, fraudes o mal uso de las instalaciones y los servicios.
   - ✓ Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de seguridad de la información y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.
   - ✓ Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

5. **Seguridad Física y del Entorno:**

   - ✓ Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

- ✓ Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
- ✓ Prevenir la exposición a riesgos o robo de la información y de sus recursos de tratamiento de información.

6. Gestión de las Comunicaciones y Operaciones:

- ✓ Asegurar la operación correcta y segura de los recursos de tratamiento de la información.
- ✓ Minimizar el riesgo de fallo en los sistemas.
- ✓ Proteger la integridad del software y de la información.
- ✓ Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- ✓ Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- ✓ Evitar daños a los activos e interrupciones de actividades de la organización.
- ✓ Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

7. Control de Accesos:

- ✓ Controlar los accesos a la información.
- ✓ Evitar accesos no autorizados a los sistemas de información.
- ✓ Evitar el acceso de usuarios no autorizados.
- ✓ Protección de los servicios en red
- ✓ Evitar accesos no autorizados a ordenadores.
- ✓ Evitar el acceso no autorizado a la información contenida en los sistemas.

- ✓ Detectar actividades no autorizadas.
- ✓ Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

8. Adquisición de Sistemas de Información, Desarrollo y Mantenimiento:

- ✓ Asegurar que la seguridad está incluida dentro de los sistemas de información.
- ✓ Evitar pérdidas, modificaciones o mal uso de los datos de usuarios en las aplicaciones.
- ✓ Proteger la confidencialidad, autenticidad e integridad de la información.
- ✓ Asegurar que los proyectos de tecnología de la información y las actividades complementarias son llevadas a cabo de una forma segura.
- ✓ Mantener la seguridad del software y la información de la aplicación del sistema.

9. Gestión de Incidentes de Seguridad de la Información:

- ✓ Gestionar los incidentes de seguridad de la información y corregir errores.

10. Gestión de la Continuidad del Negocio:

- ✓ Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres.

11. Conformidad (Marco Legal y Buenas Prácticas):

- ✓ Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.

- ✓ Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.
- ✓ Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas. (27000, 2012) (Rico, S.A.) (Huerta, GRUPO S2, 2004)

Figura 1. 2: Dominios de control *(Huerta, s/a)*

1.2. Entidades Encargada de la Normalización.

Las entidades encargadas de la Normalización o Estandarización son organismos que tienen como objetivo desarrollar estándares con la finalidad de crear y compartir información en la industria tanto pública como privada.

1.2.1. UIT (UNION INTERNACIONAL DE TELECOMUNICACIONES).

La UIT o su acrónimo en inglés ITU (*International Telecommunication Union*), es una organización especializada en telecomunicaciones a nivel mundial, perteneciente a la ONU, con sede en Ginebra-Suiza y de mayor antigüedad. Fue creada con la finalidad de regular los primeros sistemas de interconexión mundial.

La normativa generada por la UIT se encuentra contenida en un documento de recomendaciones y agrupado por series referentes a un mismo tema, como por ejemplo tarificación, mantenimiento, etc. Al ser sólo recomendaciones, no es un documento vinculante pero suele cumplirse como mandatorio al garantizar la interconectividad de las redes y permitir la prestación de servicios de telecomunicaciones a escala mundial. (ITU, 2015)

1.2.2. IEC (*International Eletrotechnical Commission*).

La IEC es una organización no gubernamental sin fines de lucro, fundada en 1906, que cuenta con un 97% de miembros a nivel mundial. Su objetivo es desarrollar normas internacionales aplicables a sistemas eléctricos y electrónicos sirviendo como base para la estandarización nacional y como referencia en la elaboración de licitaciones y contratos internacionales. Está conformado por expertos y delegados procedentes de las industrias de todo el mundo, funcionarios de gobierno, asociaciones e instituciones académicas reconocidas; designados por los miembros que conforman los comités nacionales que defienden los intereses electrotécnicos de las entidades a las que representan.

La IEC por su alta credibilidad y confiabilidad, se ha asociado con varias organizaciones internaciones como ISO para producir normas conjuntas, promover la importancia de la normalización y corregir posibles superposiciones de trabajos similares.

¿Pero cómo funciona la IEC?:

- El Consejo de Administración de Normalización, es responsable de la gestión global de los trabajos técnicos.
- La elaboración de las normas se lleva a cabo a través de los Comités y Subcomités Técnicos, integrados por los representantes de los Comités Nacionales dedicados a un tema en particular.

- Los Comités Técnicos son creados o disueltos por el Consejo de Administración de Normalización.
- Cada Comité Técnico tiene su presidente y una secretaria, elegidos entre los representantes de los Comités Nacionales y designados por el Consejo de Administración de Normalización.
- Son responsables de la elaboración de normativas tales como: Biometría, Identificación Automática y Datos Técnicos, La Interconexión de Equipos de Tecnología de la Comunicación, Codificación de Audio, Foto, Multimedia e Información Hipermedia, entre otras. (IEC, 2015)

1.2.3. ISO (*International Standarization Organization*).

ISO fue creada en febrero de 1947 cuando un grupo de 25 países se reunieron en Londres con la finalidad de crear una nueva organización internacional que facilite la coordinación internacional, simplificación, orientación y la unificación de las normas industriales. En la actualidad su sede se encuentra en Ginebra, Suiza.

Como una organización independiente, no gubernamental, ISO en la actualidad se encuentra integrado por 162 países miembros de los organismos nacionales de normalización, y con publicaciones de más de 20500 Normas Internacionales que cubren casi todas las industrias. Se reúnen una vez al año en Asamblea General en su sede para la revisión, actualización y aprobación de nuevos estándares. (ISO, ISO, 2015) Los miembros que forman parte de la ISO son categorizados en tres grupos:

I. **Organismo Miembro:** Formando por un representante de cada país.
II. **Miembros Correspondientes:** No tienen derecho a voto pero son informados de los trabajos de su interés.
III. **Miembros Suscriptores:** Pagan membresías para mantenerse en contacto con la normalización internacional. (INEN, 2009)

ISO crea foros basándose en experiencias y conocimientos, se desarrollan en colaboración de gobiernos, empresas y consumidores, y están integrados por quienes necesitan las normas, las implementan y se ven afectadas por ellas proporcionando herramientas para que aumenten la satisfacción del cliente haciendo de su entorno un lugar más seguro.

Trabaja en colaboración con dos organizaciones internacionales reconocidas en el desarrollo de normas que son la IEC y la UIT o ITU, quienes formaron la Cooperación Mundial de Normalización con la finalidad de fortalecerse en el ámbito normativo y promover la adopción y aplicación basadas en el consenso internacional en todo el mundo (ISO, ISO, 2015)

¿Cómo se desarrollan normas ISO?

Las normas ISO no son desarrolladas de manera arbitraria por la organización, las mismas responden a necesidades generalmente de las industrias. Se reúne a un grupo de expertos en el tema dentro de un comité técnico quienes serán los encargados de evaluar la factibilidad de la norma, de ser positiva la respuesta se procede a elaborar un marco que es compartido con los miembros de ISO quienes a su vez harán comentarios y votarán por ella, de llegarse a un consenso el proyecto se convierte en norma ISO, caso contrario regresa al comité técnico para su revisión y edición como lo expone la figura 1.3.

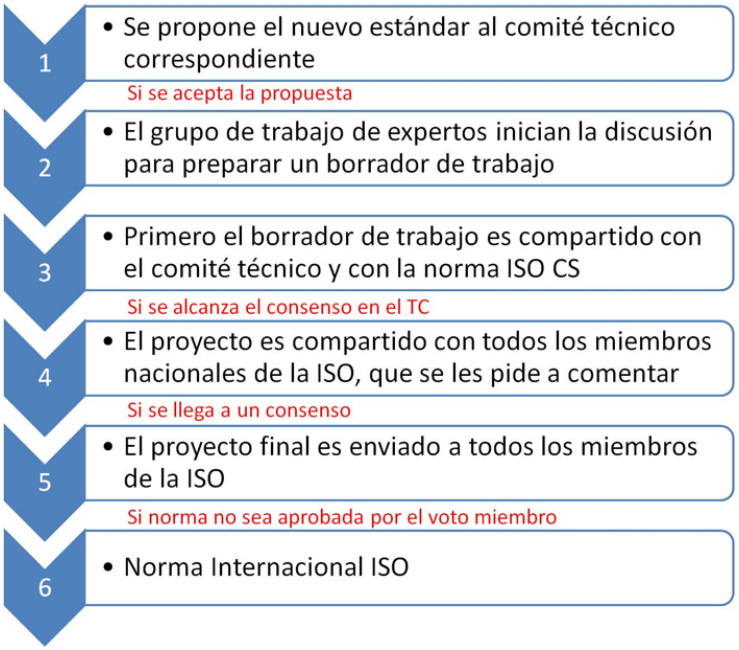


Figura 1. 3: Principios claves para el desarrollo de una Norma. *(ISO, 2015)*

Como mencionamos anteriormente, en estos más de 60 años de vida de la organización, se han desarrollado aproximadamente 20500 estándares reunidos en los siguientes grupos de Sistemas de gestión ISO:

- ✓ Calidad
- ✓ Seguridad y Protección
- ✓ Administración
- ✓ Salud y Medicina
- ✓ Medio Ambiente y Energía
- ✓ Industria
- ✓ Servicios
- ✓ Tecnología de la Información

Las Normas que abarcan los SGSI (Sistemas de Gestión de Seguridad de la Información) están dentro del grupo de Tecnología de la Información y se encuentran en la serie 27000

Proporciona una visión general de las normas que componen la serie 27000, indicando su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de estas normas y aporta las bases de:

- Por qué es importante la implantación de un SGSI.
- Una introducción a los SGSI.
- Una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI

Este grupo de normas permiten disminuir de forma significativa el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal. Las publicaciones datan del 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición del 14 de Enero de 2014. (Agustin López Neira, Javier Ruiz Spoh, 2012)

1.2.3.1. Familia de Normas ISO 27000.

La familia de normas 27000 está distribuida de la siguiente manera:

27000: Contiene una descripción general y vocabulario utilizado en la serie de normas 27000. Aporta con las bases del por qué es importante la implementación del SGSI y los pasos a seguir para el establecimiento, monitorización, mantenimiento y mejora de un SGSI. La versión de la norma a utilizarse en nuestro trabajo es la 27000: 2011 disponible y adaptada a las necesidades de nuestro país.

27001: Contiene los requisitos del Sistema de Gestión de Seguridad de la Información. Es la norma principal de la familia de la serie 27000. En su contenido cita los controles y sus objetivos de control.

27002: Norma no certificable que proporciona la guía de buenas prácticas en donde se describe los controles y sus objetivos recomendables en cuanto a seguridad de la información. Es una adopción de la norma ISO 17799:2005

27003: Norma no certificable que se centra en proporcionar una guía dirigida a cubrir los aspectos críticos para el diseño e implementación del SGSI.

27004: Norma no certificable que proporciona los lineamiento para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficiencia de un SGSI y de los controles implementados.

27005: Norma no certificable diseñada para brindar apoyo en la aplicación satisfactoria de la Seguridad de la Información en la gestión de riesgos.

27006: Norma que proporciona los requisitos para la acreditación de entidades de auditorías y certificación de los Sistemas de Gestión de Seguridad de la Información.

27007: Norma no certificable que proporciona las directrices para las auditorías de los Sistemas de Gestión de Seguridad de la Información.

27009: Norma no certificable que proporciona una guía sobre el uso y aplicación de los principios de ISO 27001 para servicios específicos en emisión de certificaciones acreditadas de terceras partes.

27010: Es una guía para los SGSI cuando se comparte información entre organizaciones o sectores, es decir es aplicable al intercambio de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados o naciones.

27011: Guía que contiene las directrices para la SGSI en organizaciones del sector de telecomunicaciones basada en la norma 27002.

27013: Es guía de implementación que integra las normas ISO 27001 e ISO 20000-1 (Gestión de Servicios TI).

27014: Guía de gobierno corporativo de la Seguridad de la Información.

27015: Conocida como TR27015, es un complemento de la norma ISO 27002 pero orientada a organizaciones del sector financiero y seguros.

27016: Es una guía para la valoración de los aspectos financieros de la Seguridad de la Información.

27017: Es una guía para Cloud Computing con ISO 27002 y con controles adicionales específicos para estos entornos de nubes.

27018: Es un código de buenas prácticas en control de protección de datos para servicios de computación en Cloud Computing

27019: Guía que contiene las directrices para la SGSI en organizaciones del sector de telecomunicaciones basada en la norma 27002.

27023: Norma no certificable es una guía de apoyo para la transición entre versiones de las normas 27001 y 27002 del 2005 a la versión del 2013.

27031: Norma no certificable que proporciona una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio.

27032: Proporciona una guía para la mejora de la seguridad cibernética.

27033: El estado de esta norma es parcialmente desarrollada, está dedicada a la seguridad en redes y se encuentra dividida en siete partes.

27034: Su estado es parcialmente desarrollada. Está dirigida a la seguridad en aplicaciones informáticas y consta de seis partes.

27035: Es una guía sobre la gestión de incidentes de seguridad de la información. Consta de tres partes que se encuentran en desarrollo.

27036: Norma en desarrollo que consta de cuatro partes dedicadas a la seguridad en las relaciones con proveedores.

27037: Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

27038: Es una norma que proporciona una guía de especificaciones para la seguridad en la redacción digital.

27039: Esta norma es una guía para la selección, despliegue y operatividad de sistemas de detección y prevención de intrusos (IDS/IPS)

27040: Norma que proporciona una guía para la seguridad en medios de almacenamiento.

27041: Norma dirigida a proporcionar una guía para garantizar la idoneidad y adecuación de los métodos de investigación.

27042: Es una guía que contiene directrices para el análisis e interpretación de las evidencias digitales.

27043: Norma que desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

27044: Norma en fase de desarrollo encargada de gestionar los eventos y la seguridad de la información (*Security Information and Event*).

27799: Es una norma que proporciona directrices para apoyar la interpretación y aplicación de ISO 27002 en el sector sanitario. (27000, 2012)

1.2.4. INEN (Instituto Ecuatoriano de Normalización).

Es una entidad técnica estatal de derecho público rectora de la normalización, reglamentación y metrología que actúa bajo régimen de ley de nuestro país, entre sus funciones está:

1. Capacitación y entrenamiento en normalización técnica, Calidad Total, entre otras.
2. Calibración de aparatos.
3. Certificación de cumplimiento con norma o reglamentos técnicos.
4. Análisis y ensayos físicos, químicos y microbiológicos.
5. Auditoría y consultoría para las empresas.
6. Información sobre normas técnicas INEN y catálogos de normas de otros países.

> "El INEN representa a la República del Ecuador ante los Organismos Internacionales, Regionales y Subregionales de Normalización, Certificación y metrología, siendo Organismo miembro de la Organización Internacional de Normalización, ISO; miembro pleno de la Comisión Panamericana de Normas Técnicas, COPANT, del Comité Andino de Normalización, CAN y miembro corresponsal de la Organización Internacional de Metrología Legal, OIML, miembro pleno del Sistema Interamericano de Metrología, SIM y de la Interamerican Acreditation Corporation, IAAC". (INEN, 2009)

INEN, forma parte de los Organismos Miembros con derecho a participar con su voto en cualquier Comité Técnico y en los Comités de Políticas de la ISO.

CAPÍTULO 2

EVALUACIÓN DE LAS SALAS DE TELECOMUNICACIONES

2. Introducción.

En este capítulo, se procederá a definir las Salas de Telecomunicaciones que intervendrán en nuestro proyecto, seguido de un análisis de las políticas internas básicas de seguridad de la empresa, las cuales nos servirán como punto de partida para el desarrollo de un checklist que no es más que un indicador de posibles fallas que se pueden estar dando en los sistemas ya existentes, obteniendo sugerencias o recomendaciones del personal que labora en dichas Salas, pues ellos son quienes están en contacto directo y reconocen las falencias existentes.

En este punto se ha visto la necesidad de contar con la valiosa colaboración del personal de ETAPA EP: Ing. Manuel Ricardo Urgilés Ortiz, Coordinar del Proyecto desde ETAPA EP, y del Mgs. Edgar Rodrigo Pauta Astudillo, Director de Tesis y Colaborador de ETAPA EP, quienes nos facilitarán el acceso a las instalaciones instruyéndonos cómo es el manejo de la seguridad en las Salas de Telecomunicaciones.

Ya en la investigación de campo se deberá distinguir dos puntos a considerarse: El primero y que servirá como punto de partida es la visita de las Centrales, Concentradores, Nodos, Nodos Externos y Radio Bases en de donde con debidas técnicas de documentación recopilaremos información valiosa de las falencias que se encuentren en las Salas para luego proceder a desarrollar un conversatorio con los representantes de los departamentos involucrados en la investigación de nuestro trabajo, con quienes mediante una exposición se llegará a un consenso de las necesidades más urgentes desde el punto de vista del área a la que representan, dándoles una perspectiva de la finalidad del proyecto y cómo va a interactuar con las normas ya existentes, proponiendo dar una mejora incluyendo un seguimiento con la finalidad de que se cumplan los procesos de seguridad de la organización.

2.1. Definición de Salas de Telecomunicaciones.

Para definir las Salas de Telecomunicaciones que intervendrá, se efectuó una reunión con los coordinadores del proyecto en ETAPA EP, en donde se establecieron las Salas tipo, siendo éstas las siguientes:

- Central Telefónica Totoracocha.
- Concentrador Baños.
- Nodo Externo 24 de Mayo.

Proporcionando adicionalmente al proyecto una evaluación complementaria mediante la aplicación del checklist a la Radio Base de Misicata y los Nodos de El Arenal y La Laguna con la finalidad de aportar a ETAPA EP con una idea del estado y manejo de las Salas de Telecomunicaciones de los lugares indicados.

2.2. Checklist.

La función para la que se crea un checklist es la de analizar la situación actual de la empresa, permitiendo cuantificar los resultados obtenidos en las Salas evaluadas, pudiéndose incluir al momento de aplicarlo aspectos necesarios que no se cubrió en el documento elaborado. (Empresarios., 2008)

Tabla 2. 1: Checklist Sistemas de Seguridad ETAPA EP

SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.			
FECHA:			
HORA:			
LUGAR:			
TIPO DE SALA:			
	SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?			
Los exteriores poseen cercado eléctrico?			
El área periférica cuenta con sistemas de video seguridad?			
En las instalaciones existe personal de seguridad?			
El personal de seguridad es el encargado de registrar los ingresos a la ST?			
En la puerta de ingreso a la Ss existe un sistema biométrico?			
La puerta de ingreso a la ST es blindada?			
En el interior de la ST existe sistemas de video seguridad?			
La ST cuenta con sistema de climatización?			
Existe sistema de control de humedad en la ST?			
Cuenta la ST con sistema contra incendios?			
Tiene la ST extintores?			
Existe una salida de emergencia en la ST?			
Cuenta con señalización adecuada para la ST?			
Existe un botiquín en la ST?			
Cuenta con Batería Sanitaria la ST?			
La iluminación es adecuada en la ST?			
Cuenta con instrumentación para el uso del personal que ingresa en la ST?			
Los equipos son de fácil acceso para el personal que acude a la ST?			

OBSERVACIONES						
Responsable:			Firma:			

La aplicación de esta herramienta de evaluación nos ayudará posteriormente en el capítulo 4 para el análisis y evaluación de riesgos.

2.2.1. Aplicación de Checklist.

2.2.1.1. Central Telefónica Totoracocha.

Central de gran importancia por el tamaño de sus instalaciones, cantidad de equipos y servicios que brinda, encargada de dar soporte y cobertura en Telefonía Fija, Internet y Fibra Óptica. Está ubicada en la calle Rumi-Urco y Río Cutucú en la parroquia urbana Totoracocha. En la aplicación del checklist, se pudo observar que la Sala de Telecomunicaciones estaba dividida en 4 subsalas, aplicándose el formato a cada una de ellas, adicionalmente a lo expuesto se puede indicar que es la Sala que menos falencias presentó, detallándose las mismas en el checklist aplicado.

Figura 2. 1: Central de Totoracocha (Fuente Google Maps)

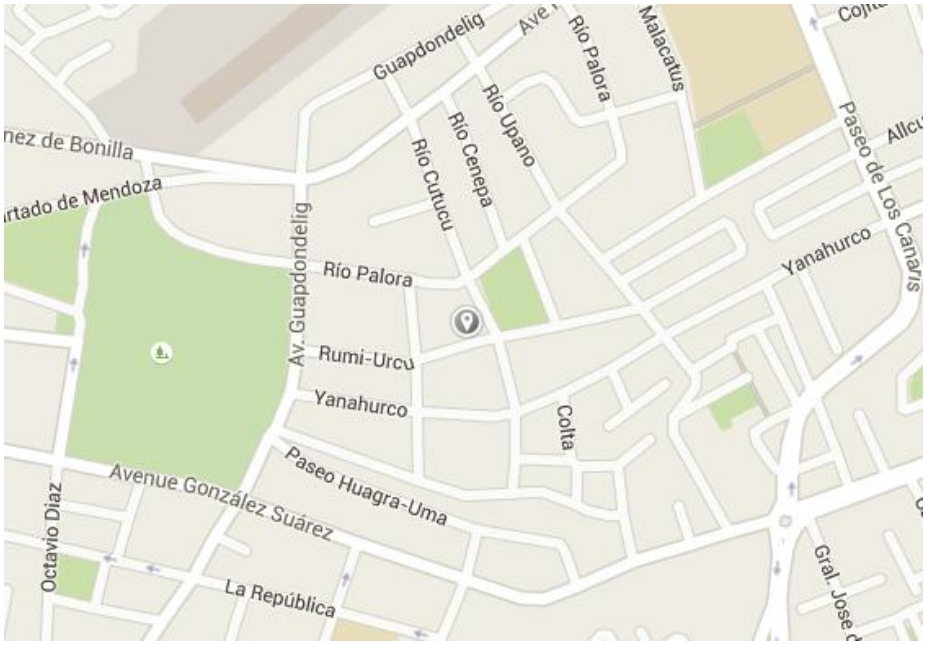


Figura 2. 2: Ubicación Central Totoracocha

Sala de Equipos.

Tabla 2. 2: Checklist Equipos, Central Totoracocha

					Formulario 1-1		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	8h42						
LUGAR:	Central Totoracocha						
TIPO DE SALA:	Sala de Equipos						
					SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?							1
Los exteriores poseen cercado eléctrico?							X
El área periférica cuenta con sistemas de video seguridad?					2		
En los exteriores de las instalaciones existe personal de seguridad?					X		
El personal de seguridad es el encargado de registrar los ingresos a la ST?							3
En la puerta de ingreso a la ST existe un sistema biométrico?					X		
La puerta de ingreso a la ST es blindada?					X		
En el interior de la ST existe sistemas de video seguridad?							X
La ST cuenta con sistema de climatización?					X		
Existe sistema de control de humedad en la ST?					X		
Cuenta la ST con sistema contra incendios?					X		
Tiene la ST extintores?					X		
Existe una salida de emergencia en la ST?							4
Cuenta con señalización adecuada para la ST?							X
Existe un botiquín en la ST?							X
Cuenta con Batería Sanitaria la ST?					5		
La iluminación es adecuada en la ST?					6		
Cuenta con instrumentación para el uso del personal que ingresa en la ST?							7
Los equipos son de fácil acceso para el personal que acude a la ST?					X		
OBSERVACIONES							
1. Posee sistema de puerta abierta, pero no se encuentra funcional.							
2. En el exterior del edificio no cuenta con cámaras de video vigilancia. En el interior posee cámaras pero no se encuentran funcionales							
3. La persona encargada de dar la autorización de ingreso es el Ing. Ricardo Urgilés.							
4. No cuenta con salida de emergencia.							
5. En el exterior de la Sala.							
6. El encendido de las luminarias se encuentran dispersas.							
7. La instrumentación es personal.							
Responsable:			Firma:				

Figura 2. 3: C. Totoracocha. Cámaras

Figura 2. 4: Totoracocha. Puertas

Figura 2. 5: C. Totoracocha. S. Contrafuego

Figura 2. 6: Totoracocha Sanitarios

Figura 2. 7: Totoracocha. Equipos

Figura 2. 8: C. Totoracocha. Equipos

Figura 2. 9: Totoracocha. Equipos

Figura 2. 10: C. Totoracocha. Equipos

Figura 2. 11: C. Totoracocha. Extintor

Figura 2. 12: C. Totoracocha. Contrafuego

Figura 2. 13: C. Totoracocha. A. Incendio

Figura 2. 14: C. Totoracocha. Rociadores

Figura 2. 15: C. Totoracocha. Equipos

Figura 2. 16: C. Totoracocha. Equipos

Figura 2. 17: C. Totoracocha. Equipos

Figura 2. 18: C. Totoracocha. Equipos

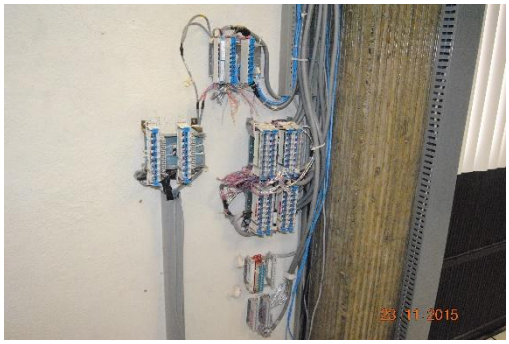


Figura 2. 19: C. Totoracocha. Equipos

Figura 2. 20: C. Totoracocha. Escalerillas

Figura 2. 21: C. Totoracocha. Documentos

Figura 2. 22: C. Totoracocha. Equipos

Figura 2. 23: C. Totoracocha. Equipos

Figura 2. 24: C. Totoracocha. Equipos

Sala de Energía 1

Tabla 2. 3: Checklist Sala de Energía. C. Totoracocha

				Formulario 1-2			
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	9h00						
LUGAR:	Central Totoracocha						
TIPO DE SALA:	Sala de Energía 1						
				SI		**NO**	
Las instalaciones cuenta con sistemas de alarmas?						X	
Los exteriores poseen cercado eléctrico?						X	
El área periférica cuenta con sistemas de video seguridad?				1			
En los exteriores de las instalaciones existe personal de seguridad?				X			
El personal de seguridad es el encargado de registrar los ingresos a la ST?						2	
En la puerta de ingreso a la ST existe un sistema biométrico?						X	
La puerta de ingreso a la ST es blindada?						X	
En el interior de la ST existe sistemas de video seguridad?						X	
La ST cuenta con sistema de climatización?				X			
Existe sistema de control de humedad en la ST?						X	
Cuenta la ST con sistema contra incendios?						X	
Tiene la ST extintores?				3			
Existe una salida de emergencia en la ST?						4	
Cuenta con señalización adecuada para la ST?						X	
Existe un botiquín en la ST?						X	
Cuenta con Batería Sanitaria la ST?				5			
La iluminación es adecuada en la ST?				X			
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						6	
Los equipos son de fácil acceso para el personal que acude a la ST?				X			
OBSERVACIONES							
1. En el exterior del edificio no cuenta con cámaras de video vigilancia. En el interior posee cámaras pero no se encuentran funcionales							
2. No existe registro de ingresos.							
3. En el exterior de la Sala.							
4. No cuenta con salida de emergencia.							
5. En el exterior de la Sala.							
6. La instrumentación es personal.							
Responsable:			Firma:				

Figura 2. 25: C. Totoracocha. Ingreso

Figura 2. 26: C. Totoracocha. Cámaras

Figura 2. 27: C. Totoracocha. Equipos

Figura 2. 28: C. Totoracocha. Equipos

Figura 2. 29: C. Totoracocha. Escalerillas

Figura 2. 30: C. Totoracocha. Equipos

Figura 2. 31: C. Totoracocha. T. Carga

Figura 2. 32: C.Totoracocha.Climatización

Sala de Energía 2

Tabla 2. 4: Checklist Sala de Energía., C. Totoracocha

				Formulario 1-3			
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	9h10						
LUGAR:	Central Totoracocha						
TIPO DE SALA:	Sala de Energía 2						
				SI		**NO**	
Las instalaciones cuenta con sistemas de alarmas?						X	
Los exteriores poseen cercado eléctrico?						X	
El área periférica cuenta con sistemas de video seguridad?				1			
En los exteriores de las instalaciones existe personal de seguridad?				X			
El personal de seguridad es el encargado de registrar los ingresos a la ST?						2	
En la puerta de ingreso a la ST existe un sistema biométrico?						X	
La puerta de ingreso a la ST es blindada?						X	
En el interior de la ST existe sistemas de video seguridad?						X	
La ST cuenta con sistema de climatización?				X			
Existe sistema de control de humedad en la ST?						X	
Cuenta la ST con sistema contra incendios?						X	
Tiene la ST extintores?				3			
Existe una salida de emergencia en la ST?						4	
Cuenta con señalización adecuada para la ST?						X	
Existe un botiquín en la ST?						X	
Cuenta con Batería Sanitaria la ST?				5			
La iluminación es adecuada en la ST?				X			
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						6	
Los equipos son de fácil acceso para el personal que acude a la ST?				X			
OBSERVACIONES							
1. En el exterior del edificio no cuenta con cámaras de video vigilancia. En el interior posee cámaras pero no se encuentran funcionales							
2. No existe registro de ingresos.							
3. En el exterior de la Sala.							
4. No cuenta con salida de emergencia.							
5. En el exterior de la Sala.							
6. La instrumentación es personal.							
Responsable:			Firma:				

Figura 2. 33: C. Totoracocha. Sanitarios

Figura 2. 36: C. Totoracocha. Cámaras

Figura 2. 34: C Totoracocha.Climatización

Figura 2. 37: C. Totoracocha. Equipos.

Figura 2. 35: C. Totoracocha. Ingreso

Figura 2. 38: C. Totoracocha. Generador

Sala de Repartidores.

Tabla 2. 5: Checklist Sala de Repartidores, C. Totoracocha

				Formulario 1-4			
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	9h20						
LUGAR:	Central Totoracocha						
TIPO DE SALA:	Sala Repartidores.						
				SI		**NO**	
Las instalaciones cuenta con sistemas de alarmas?						X	
Los exteriores poseen cercado eléctrico?						X	
El área periférica cuenta con sistemas de video seguridad?				1			
En los exteriores de las instalaciones existe personal de seguridad?				X			
El personal de seguridad es el encargado de registrar los ingresos a la ST?						2	
En la puerta de ingreso a la ST existe un sistema biométrico?						X	
La puerta de ingreso a la ST es blindada?						X	
En el interior de la ST existe sistemas de video seguridad?						X	
La ST cuenta con sistema de climatización?						X	
Existe sistema de control de humedad en la ST?						X	
Cuenta la ST con sistema contra incendios?						X	
Tiene la ST extintores?				3			
Existe una salida de emergencia en la ST?						4	
Cuenta con señalización adecuada para la ST?						X	
Existe un botiquín en la ST?						X	
Cuenta con Batería Sanitaria la ST?				5			
La iluminación es adecuada en la ST?				X			
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						6	
Los equipos son de fácil acceso para el personal que acude a la ST?				X			
OBSERVACIONES							
1. En el exterior del edificio no cuenta con cámaras de video vigilancia. En el interior posee cámaras pero no se encuentran funcionales							
2. No existe registro de ingresos.							
3. En el exterior de la Sala.							
4. No cuenta con salida de emergencia.							
5. En el exterior de la Sala.							
6. La instrumentación es personal.							
Responsable:			Firma:				

Figura 2. 39: C. Totoracocha. Cámaras

Figura 2. 41: C.Totoracocha. Repartidores

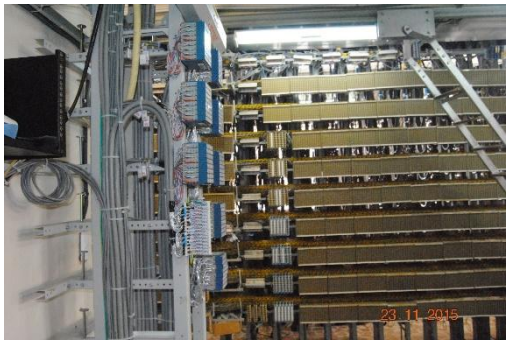


Figura 2. 40: C. Totoracocha. Repartidores

Figura 2. 42: C. Totoracocha. Equipos

2.2.1.2. Concentrador Baños.

Los concentradores por su infraestructura y equipamiento son los segundos en la escala de jerarquía en las Salas de Telecomunicaciones, a su cargo también está el cubrir el servicio de Telefonía Fija e Internet de la zona. Está ubicada en la Parroquia Rural de Baños en la calle sin nombre y Av. Ricardo Durán, encontrándose las siguientes observaciones.

Figura 2. 43: Concentrador Baños (Fuente: Google Maps).

Sala de Equipos.

Tabla 2. 6: Checklist Sala de Equipos, Concentrador Baños

				Formulario 2-1		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.						
FECHA:	Cuenca, 23 de noviembre de 2015					
HORA:	11h02					
LUGAR:	Parroquia Baños					
TIPO DE SALA:	Concentrador Baños - Equipos					
				SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?						X
Los exteriores poseen cercado eléctrico?						X
El área periférica cuenta con sistemas de video seguridad?						X
En los exteriores de las instalaciones existe personal de seguridad?				X		
El personal de seguridad es el encargado de registrar los ingresos a la ST?				X		
En la puerta de ingreso a la ST existe un sistema biométrico?						X
La puerta de ingreso a la ST es blindada?						X
En el interior de la ST existe sistemas de video seguridad?						X
La ST cuenta con sistema de climatización?				X		
Existe sistema de control de humedad en la ST?						X
Cuenta la ST con sistema contra incendios?						X
Tiene la ST extintores?				X		
Existe una salida de emergencia en la ST?						X
Cuenta con señalización adecuada para la ST?				1		
Existe un botiquín en la ST?						X
Cuenta con Batería Sanitaria la ST?				2		
La iluminación es adecuada en la ST?				X		
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						3
Los equipos son de fácil acceso para el personal que acude a la ST?				4		
OBSERVACIONES						
1. Cuenta con una sóla señalización de salida						
2. Las baterias sanitarias son de uso del guardia de seguridad y no tienen agua más de 1 año.						
3. La instrumentación es personal.						
4. Disposición inadecuada, poco espacio.						
Espacio reducido que dificulta el normal desempeño en el trabajo.						
Responsable:			Firma:			

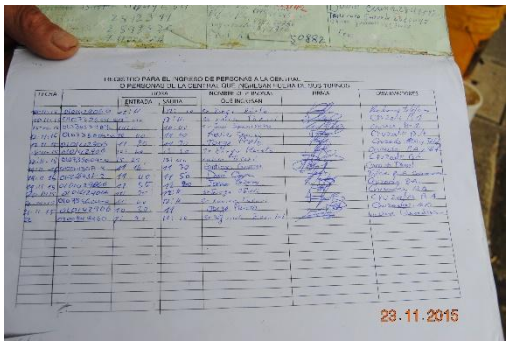


Figura 2. 44: C. Baños. Bitácoras

Figura 2. 45: C. Baños. Instalaciones

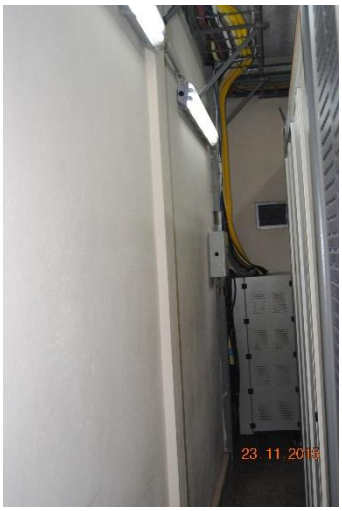


Figura 2. 46: C. Baños. Iluminación

Figura 2. 47: C. Baños. Escalerillas

Figura 2. 48: C. Baños. Equipos

Figura 2. 49: C. Baños. Equipos

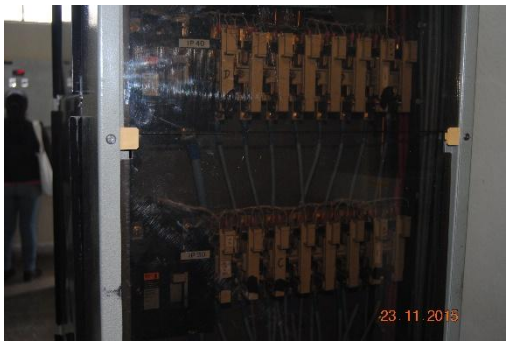


Figura 2. 50: C. Baños. Equipos

Figura 2. 51: C. Baños. S Contrafuego

Figura 2. 52: C. Baños. A. Incendio

Figura 2. 53: C. Baños. Señalización

Figura 2. 54: C. Baños. Escalerillas

Figura 2. 55: C. Baños. Baterías

Figura 2. 56: C. Baños. Baterías

Figura 2. 57: C. Baños. Esquemas

Sala Repartidores.

Tabla 2. 7: Checklist Sala de Repartidores, C. Baños.

				Formulario 2-2		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.						
FECHA:	Cuenca, 23 de noviembre de 2015					
HORA:	11h14					
LUGAR:	Parroquia Baños					
TIPO DE SALA:	Concentrador Baños - Repartidores.					
				SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?						X
Los exteriores poseen cercado eléctrico?						X
El área periférica cuenta con sistemas de video seguridad?						X
En los exteriores de las instalaciones existe personal de seguridad?				X		
El personal de seguridad es el encargado de registrar los ingresos a la ST?				X		
En la puerta de ingreso a la ST existe un sistema biométrico?						X
La puerta de ingreso a la ST es blindada?						X
En el interior de la ST existe sistemas de video seguridad?						X
La ST cuenta con sistema de climatización?				X		
Existe sistema de control de humedad en la ST?						X
Cuenta la ST con sistema contra incendios?						X
Tiene la ST extintores?				X		
Existe una salida de emergencia en la ST?						X
Cuenta con señalización adecuada para la ST?				1		
Existe un botiquín en la ST?						X
Cuenta con Batería Sanitaria la ST?				2		
La iluminación es adecuada en la ST?						3
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						4
Los equipos son de fácil acceso para el personal que acude a la ST?						5
OBSERVACIONES						
1. Cuenta con una sóla señalización de salida						
2. Las baterias sanitarias son de uso del guardia de seguridad y no tienen agua más de 1 año.						
3. Baja iluminación.						
4. La instrumentación es personal.						
5. Disposición inadecuada, poco espacio.						
Espacio reducido que dificulta el normal desempeño en el trabajo.						
Responsable:			Firma:			

Figura 2. 58: C. Baños. Documentos

Figura 2. 61: Baños. Repartidores

Figura 2. 59: Baños. Repartidores

Figura 2. 62: C. Baños. Basura

Figura 2. 60: Baños. Repartidores

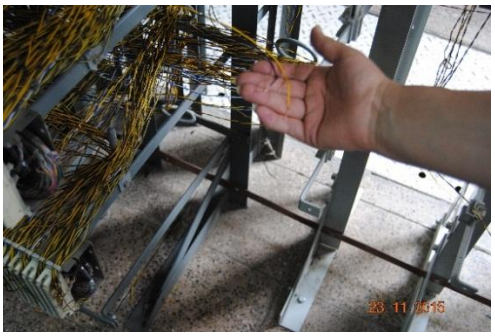


Figura 2. 63: C. Baños. Repartidores

Figura 2. 64: C. Baños. Repartidores

Figura 2. 65: C. Baños. Repartidor

2.2.1.3. Radio Base Misicata.

Sus instalaciones están adecuadas para brindar servicio de Internet, Telefonía Fija y Telefonía CDMA, está ubicada en la parroquia Rural Baños en el Barrio Antenas de Misicata a 10 minutos de la Av. Carlos Arízaga Toral.

Figura 2. 66: Radio Base Misicata (Fuente: Google Maps)

Figura 2. 67: Exteriores Radio Base Misicata

Salas de Equipos y Energía.

Tabla 2. 8: Checklist Radio Base Misicata sala de Equipos y Energía

					Formulario 3-1		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 1 de diciembre de 2015						
HORA:	10h00						
LUGAR:	Barrio Antenas de Misicata						
TIPO DE SALA:	Radio Base Misicata						
					SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?							X
Los exteriores poseen cercado eléctrico?							X
El área periférica cuenta con sistemas de video seguridad?							X
En los exteriores de las instalaciones existe personal de seguridad?							1
El personal de seguridad es el encargado de registrar los ingresos a la ST?							X
En la puerta de ingreso a la ST existe un sistema biométrico?							X
La puerta de ingreso a la ST es blindada?							X
En el interior de la ST existe sistemas de video seguridad?							X
La ST cuenta con sistema de climatización?					2		
Existe sistema de control de humedad en la ST?							X
Cuenta la ST con sistema contra incendios?							X
Tiene la ST extintores?							X
Existe una salida de emergencia en la ST?							X
Cuenta con señalización adecuada para la ST?							X
Existe un botiquín en la ST?							X
Cuenta con Batería Sanitaria la ST?							X
La iluminación es adecuada en la ST?							3
Cuenta con instrumentación para el uso del personal que ingresa en la ST?							4
Los equipos son de fácil acceso para el personal que acude a la ST?					X		
OBSERVACIONES							
1. No cuenta con guardia de seguridad, vecino del sector hace las veces de guardia (Sr. Mario Morocho)							
2. Filtro de ventilación es una esponja rosada.							
3. El exterior de las instalaciones se encuentra totalmente sin iluminación y sin ningún tipo de mantenimiento.							
4. La instrumentación es personal.							
Se ofreció iluminación al sector sin cumplirse hasta la fecha, vecinos molestos manifiestan que prohibirán el acceso a las instalaciones puesto que la vía es privada.							
Existe libre acceso de personal ajeno a la empresa.							
Conectores de Alta Tensión sin protección y oxidados.							
Sin limpieza.							
Responsable:			Firma:				

Figura 2. 68: R.B. Misicata. Ubicación

Figura 2. 71: R.B. Misicata. Antenas

Figura 2. 69: R.B. Misicata. Ingreso

Figura 2. 72: R.B. Misicata. Ingreso

Figura 2. 70: R.B. Misicata. Instalaciones

Figura 2. 73: R.B. Misicata. Generador

Figura 2. 74: R.B. Misicata. Escalerillas

Figura 2. 75: R.B. Misicata. Puertas

Figura 2. 76: R.B. Misicata. Equipos

Figura 2. 77: R.B. Misicata. T. Carga

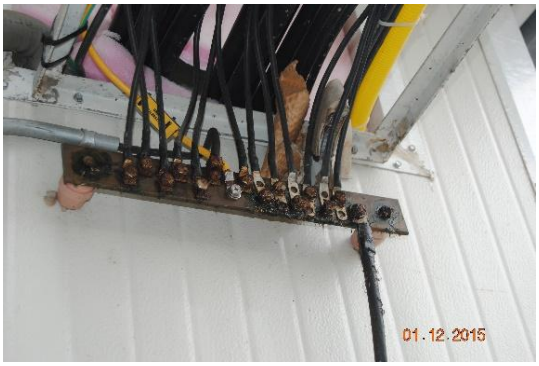


Figura 2. 78: R.B. Misicata. Conectores

Figura 2. 79: R.B. Misicata. Equipos

Figura 2. 80: R.B. Misicata. T. Carga

Figura 2. 81: R.B. Misicata. Conductores

.

Figura 2. 82: R.B. Misicata. Equipos

Figura 2. 83: R.B. Misicata. Instalaciones

Figura 2. 84: R.B. Misicata. Equipos

2.2.1.4. Nodos la Laguna y El Arenal.

Los Nodos por la cantidad y capacidad de equipos que se encargan de brindar el servicio de Telefonía Fija e Internet en el sector, son los terceros en jerarquía de Salas de Telecomunicaciones en la empresa. Para nuestro estudio se han tomado como referencia dos lugares diferenciados por la existencia o no de guardianía de seguridad, siendo éstos: Nodo La Laguna y Nodo El Arenal.

Nodo la Laguna.

Está ubicado en el sector conocido como La Laguna en la Calle Jacaranda entre Av. Ordóñez Lazo y Paseo 3 de Noviembre en la Parroquia Urbana San Sebastián.

Figura 2. 85: Nodo la Laguna (Fuente: Google Maps)

Sala de Equipos.

Tabla 2. 9: Checklist Sala de Equipos, Nodo la Laguna

				Formulario 4-1			
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	11H52						
LUGAR:	Jacaranda, entre Paseo 3 de Noviembre y Av. Ordóñez Lasso.						
TIPO DE SALA:	Nodo La Laguna - Sala Equipos						
				SI		**NO**	
Las instalaciones cuenta con sistemas de alarmas?						**X**	
Los exteriores poseen cercado eléctrico?						**X**	
El área periférica cuenta con sistemas de video seguridad?						**X**	
En los exteriores de las instalaciones existe personal de seguridad?				**X**			
El personal de seguridad es el encargado de registrar los ingresos a la ST?				**1**			
En la puerta de ingreso a la ST existe un sistema biométrico?						**X**	
La puerta de ingreso a la ST es blindada?						**X**	
En el interior de la ST existe sistemas de video seguridad?						**X**	
La ST cuenta con sistema de climatización?				**X**			
Existe sistema de control de humedad en la ST?						**X**	
Cuenta la ST con sistema contra incendios?						**X**	
Tiene la ST extintores?						**X**	
Existe una salida de emergencia en la ST?						**X**	
Cuenta con señalización adecuada para la ST?						**X**	
Existe un botiquín en la ST?						**X**	
Cuenta con Batería Sanitaria la ST?				**2**			
La iluminación es adecuada en la ST?				**3**			
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						**4**	
Los equipos son de fácil acceso para el personal que acude a la ST?				**X**			
OBSERVACIONES							
1. No existe registro de ingreso del personal a las Salas.							
2. Las baterias sanitarias son de uso exclusivo del guardia de seguridad.							
3. Ventalenres grandes que facilitan ilumoncaión en el día, en la noche se dificulta.							
4. La instrumentación es personal.							
No se lleva adecuadamente los reguistros de ingresos a las Salas.							
Responsable:			Firma:				

Figura 2. 86: N. Laguna. Puertas

Figura 2. 89: N. Laguna. Equipos

Figura 2. 87: N. Laguna. Escalerillas

Figura 2. 90: N. Laguna. Climatización

Figura 2. 88: N. Laguna. Equipos

Figura 2. 91: N. Laguna. Equipos

Figura 2. 92: N. Laguna. Equipos

Figura 2. 95: N. Laguna. T. Carga

Figura 2. 93: N. Laguna. Equipos

Figura 2. 96: N. Laguna. T. Carga

Figura 2. 94: N. Laguna. Baterías

Figura 2. 97: N. Laguna. Escalerillas

Sala Repartidores.

Tabla 2. 10: Nodo la Laguna. Sala de Repartidores

				Formulario 4-2		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.						
FECHA:	Cuenca, 23 de noviembre de 2015					
HORA:	12H00					
LUGAR:	Jacaranda, entre Paseo 3 de Noviembre y Av. Ordóñez Lasso.					
TIPO DE SALA:	Nodo La Laguna - Sala Repartidores.					
				SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?						**X**
Los exteriores poseen cercado eléctrico?						**X**
El área periférica cuenta con sistemas de video seguridad?						**X**
En los exteriores de las instalaciones existe personal de seguridad?				**X**		
El personal de seguridad es el encargado de registrar los ingresos a la ST?				**1**		
En la puerta de ingreso a la ST existe un sistema biométrico?						**X**
La puerta de ingreso a la ST es blindada?						**X**
En el interior de la ST existe sistemas de video seguridad?						**X**
La ST cuenta con sistema de climatización?				**X**		
Existe sistema de control de humedad en la ST?						**X**
Cuenta la ST con sistema contra incendios?						**X**
Tiene la ST extintores?						**X**
Existe una salida de emergencia en la ST?						**X**
Cuenta con señalización adecuada para la ST?						**X**
Existe un botiquín en la ST?						**X**
Cuenta con Batería Sanitaria la ST?				**2**		
La iluminación es adecuada en la ST?				**3**		
Cuenta con instrumentación para el uso del personal que ingresa en la ST?						**4**
Los equipos son de fácil acceso para el personal que acude a la ST?				**X**		
OBSERVACIONES						
1. No existe registro de ingreso del personal a las Salas.						
2. Las baterias sanitarias son de uso exclusivo del guardia de seguridad.						
3. Ventalenres grandes que facilitan ilumoncaión en el día, en la noche se dificulta.						
4. La instrumentación es personal.						
Escalera en malas condiciones en Sala de Repartidores.						
Responsable:			Firma:			

Figura 2. 98: N. Laguna. Ingreso

Figura 2. 99: N. Laguna. Basura

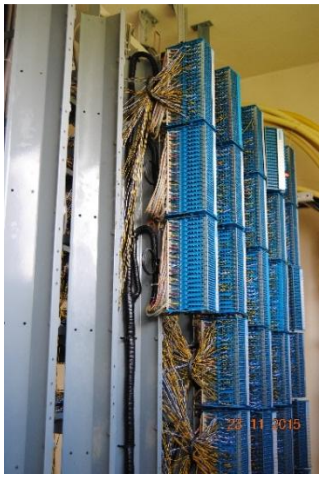


Figura 2. 100: N. Laguna. Repartidores

Figura 2. 101: N. Laguna. Documentos

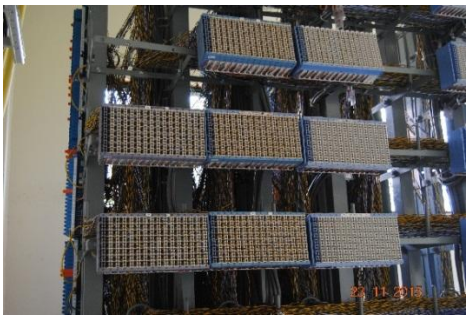


Figura 2. 102: N. Laguna. Repartidores

Figura 2. 103: N. Laguna. Documentos

Figura 2. 104: N. Laguna. Repartidores

Figura 2. 105: N. Laguna. Escaleras

Nodo El Arenal.

Está ubicado en el sector del Arenal, Parroquia Urbana El Batán en la calle S/N entre Av. Carlos Arízaga Vega y Francisco Cisneros, junto a la Iglesia Cristo del Consuelo.

Figura 2. 106: Nodo el Arenal (Fuente: Google Maps)

Figura 2. 107: Exteriores Nodo el Arenal. Instalaciones

Sala Repartidores

Tabla 2. 11: Checklist Sala de Repartidores, Nodo El Arenal

					Formulario 5-1		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	10h35						
LUGAR:	Junto a parroquia Cristo del Consuelo						
TIPO DE SALA:	Nodo El Arenal						
					SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?							X
Los exteriores poseen cercado eléctrico?							X
El área periférica cuenta con sistemas de video seguridad?							X
En los exteriores de las instalaciones existe personal de seguridad?							X
El personal de seguridad es el encargado de registrar los ingresos a la ST?							1
En la puerta de ingreso a la ST existe un sistema biométrico?							X
La puerta de ingreso a la ST es blindada?							X
En el interior de la ST existe sistemas de video seguridad?							X
La ST cuenta con sistema de climatización?					2		
Existe sistema de control de humedad en la ST?							X
Cuenta la ST con sistema contra incendios?							X
Tiene la ST extintores?					X		
Existe una salida de emergencia en la ST?							X
Cuenta con señalización adecuada para la ST?							X
Existe un botiquín en la ST?							X
Cuenta con Batería Sanitaria la ST?							X
La iluminación es adecuada en la ST?							X
Cuenta con instrumentación para el uso del personal que ingresa en la ST?							3
Los equipos son de fácil acceso para el personal que acude a la ST?					X		
OBSERVACIONES							
1. No existe guardia de Seguridad.							
2. Sala dividida por puerta de vidrio. En Sala de equipo existe climatización pero en Sala de Repartidores no existe.							
3. La instrumentación es personal.							
Instalación de gran superficie, compartida con la división de agua potable. Totalmente descuidada en aseo, mantenimiento de equipos y zonas de acceso.							
Todas las cuadrillas que acceden a las intalaciones poseen duplicado de llaves.							
De acuerdo a funcionario terciado que nos permitió el acceso, los puertos no se encuentran funcionales aproximadamente 15%.							
Responsable:			Firma:				

Figura 2. 108: N. Arenal. Puertas

Figura 2. 109: N. Arenal. Repartidores

Figura 2. 110: N. Arenal. Repartidores

Figura 2. 111: N. Arenal. Documentos

Figura 2. 112: Arenal. Repartidores

Figura 2. 113: N. Arenal. Extintores

Figura 2. 114: N. Arenal. Basura

Figura 2. 115: N. Arenal. Escalerillas

Figura 2. 116: N. Arenal. Escalerillas

Figura 2. 117: N. Arenal. Repartidores

2.2.1.5. Nodo Externo 24 de Mayo.

En Salas de Telecomunicaciones es la más pequeña en tamaño, equipamiento y cobertura de servicios. Está ubicado en la Av. 24 de Mayo y El Comercio Esquina de la Parroquia Urbana Monay.

Figura 2. 118: Nodo externo 24 de Mayo (Fuente: Google Maps)

Figura 2. 119: Nodo externo 24 de Mayo, Instalaciones

Salas Equipos y Repartidores.

Tabla 2. 12: Checklist Nodo Externo 24 de Mayo

					Formulario 6-1		
SISTEMAS DE SEGURIDAD EN SALAS DE TELECOMUNICACIONES DE ETAPA EP.							
FECHA:	Cuenca, 23 de noviembre de 2015						
HORA:	8h20						
LUGAR:	Av. 24 de Mayo y El Comercio Esq.						
TIPO DE SALA:	Nodo Externo Multiplataforma 24 de Mayo						
					SI		**NO**
Las instalaciones cuenta con sistemas de alarmas?							X
Los exteriores poseen cercado eléctrico?							X
El área periférica cuenta con sistemas de video seguridad?							X
En los exteriores de las instalaciones existe personal de seguridad?							X
El personal de seguridad es el encargado de registrar los ingresos a la ST?							1
En la puerta de ingreso a la ST existe un sistema biométrico?							X
La puerta de ingreso a la ST es blindada?							X
En el interior de la ST existe sistemas de video seguridad?							X
La ST cuenta con sistema de climatización?					X		
Existe sistema de control de humedad en la ST?					X		
Cuenta la ST con sistema contra incendios?							X
Tiene la ST extintores?							X
Existe una salida de emergencia en la ST?							2
Cuenta con señalización adecuada para la ST?							X
Existe un botiquín en la ST?							X
Cuenta con Batería Sanitaria la ST?							3
La iluminación es adecuada en la ST?					4		
Cuenta con instrumentación para el uso del personal que ingresa en la ST?							5
Los equipos son de fácil acceso para el personal que acude a la ST?					X		
OBSERVACIONES							
1. Nodo externo de insfraestructura pequeña sin guardia de seguridad.							
2. De acuerdo a información proporcionada por facilitador, no aplica para infraestructuras pequeñas							
3. De acuerdo a información proporcionada por facilitador, no aplica para infraestructuras pequeñas							
4. Insuficiente.							
5. La instrumentación es personal.							
Nota: Al momento de realizar la toma de datos se encontró que personal terciado realizaba trabajos en repartidores, manifestando que en sus labores se requiere asistencia.							
Responsable:			Firma:				

Figura 2. 120: N. 24 Mayo. Equipos

Figura 2. 123: N. 24 Mayo. Equipos

Figura 2. 121: N. 24 Mayo. Equipos

Figura 2. 124_ N. 24 Mayo. Instalaciones

Figura 2. 122: N. 24 Mayo. Repartidores

Figura 2. 125: N. 24 Mayo. Escalerillas

2.3. Compromiso con Áreas Involucradas en Proyecto.

Partiendo de la información recopilada a través de los checklist aplicados y con el apoyo de las imágenes obtenidas en las Salas Tipo, se ha podido verificar las falencias existentes en las Salas, las mismas que se dieron a conocer en un conversatorio desarrollado el día marte 24 de noviembre de 2015, al cual acudieron los representantes de los departamentos involucrados en el desarrollo de este trabajo, siendo éstos:

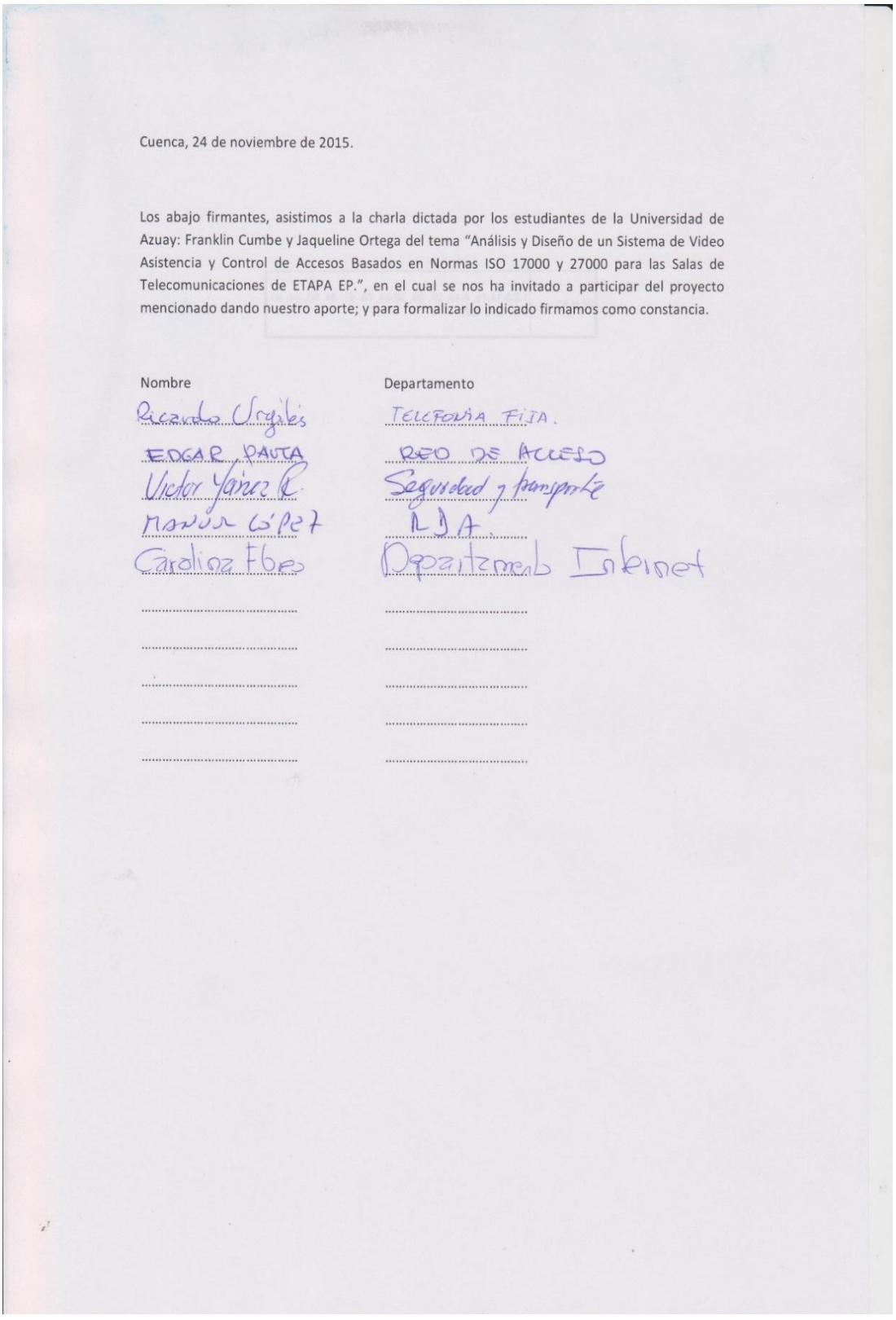
- Departamento de Seguridad y Transporte, Ingeniero Víctor Yánez
- Departamento de Internet, Ingeniera Carolina Flores.
- Departamento de Red de Accesos (RDA), Ingeniero Manuel López.
- Coordinador del proyecto en ETAPA EP, Ingeniero Ricardo Urgilés.
- Director de Tesis y funcionario del RDA, Magister Edgar Pauta.

Figura 2. 126: Reunión con los representantes de los departamentos involucrados de ETAPA EP

.

Figura 2. 127: Reunión con los Representantes de los Departamentos Involucrados de ETAPA EP

En la reunión se pudo obtener el apoyo al proyecto desde su área de trabajo, ya que sin su colaboración se verá comprometida la ejecución de todos los objetivos, dejando constancia de ello en la carta compromiso que adjuntamos.



Cuenca, 24 de noviembre de 2015.

Los abajo firmantes, asistimos a la charla dictada por los estudiantes de la Universidad de Azuay: Franklin Cumbe y Jaqueline Ortega del tema "Análisis y Diseño de un Sistema de Video Asistencia y Control de Accesos Basados en Normas ISO 17000 y 27000 para las Salas de Telecomunicaciones de ETAPA EP.", en el cual se nos ha invitado a participar del proyecto mencionado dando nuestro aporte; y para formalizar lo indicado firmamos como constancia.

Nombre	Departamento
Ricardo Urgilés	TELEFONIA FIJA.
EDGAR PAUTA	RED DE ACCESO
Victor Yanez R.	Seguridad y transporte
[illegible]	[illegible]
Carolina Fbo	Departamento Internet

Figura 2. 128: Carta Compromiso participantes del Proyecto en ETAPA EP

2.4. Resultados.

En este apartado de nuestro trabajo, exponemos los resultados obtenidos gráficamente para una mejor visualización de la evaluación realizada en las Salas.

Tabla 2. 13: Resultados de Checklist aplicado a las STs

CONSOLIDADO CHECKLIST					
		SI	NO	SI CON OBSERVACIÓN	NO CON OBSERVACIÓN
1	Las instalaciones cuenta con sistemas de alarmas?	0	11	0	1
2	Los exteriores poseen cercado eléctrico?	0	11	0	0
3	El área periférica cuenta con sistemas de video seguridad?	4	7	5	0
4	En los exteriores de las instalaciones existe personal de seguridad?	8	3	0	1
5	El personal de seguridad es el encargado de registrar los ingresos a la ST?	4	7	2	6
6	En la puerta de ingreso a la ST existe un sistema biométrico?	1	10	0	0
7	La puerta de ingreso a la ST es blindada?	1	10	0	0
8	En el interior de la ST existe sistemas de video seguridad?	0	11	0	0
9	La ST cuenta con sistema de climatización?	10	1	2	0
10	Existe sistema de control de humedad en la ST?	2	9	0	0
11	Cuenta la ST con sistema contra incendios?	1	10	0	0
12	Tiene la ST extintores?	7	4	4	0
13	Existe una salida de emergencia en la ST?	0	11	0	5
14	Cuenta con señalización adecuada para la ST?	2	9	2	0
15	Existe un botiquín en la ST?	0	11	0	0
16	Cuenta con Batería Sanitaria la ST?	8	3	9	1
17	La iluminación es adecuada en la ST?	8	3	4	0
18	Cuenta con instrumentación para el uso del personal que ingresa en la ST?	0	11	0	0
19	Los equipos son de fácil acceso para el personal que acude a la ST?	10	1	1	0

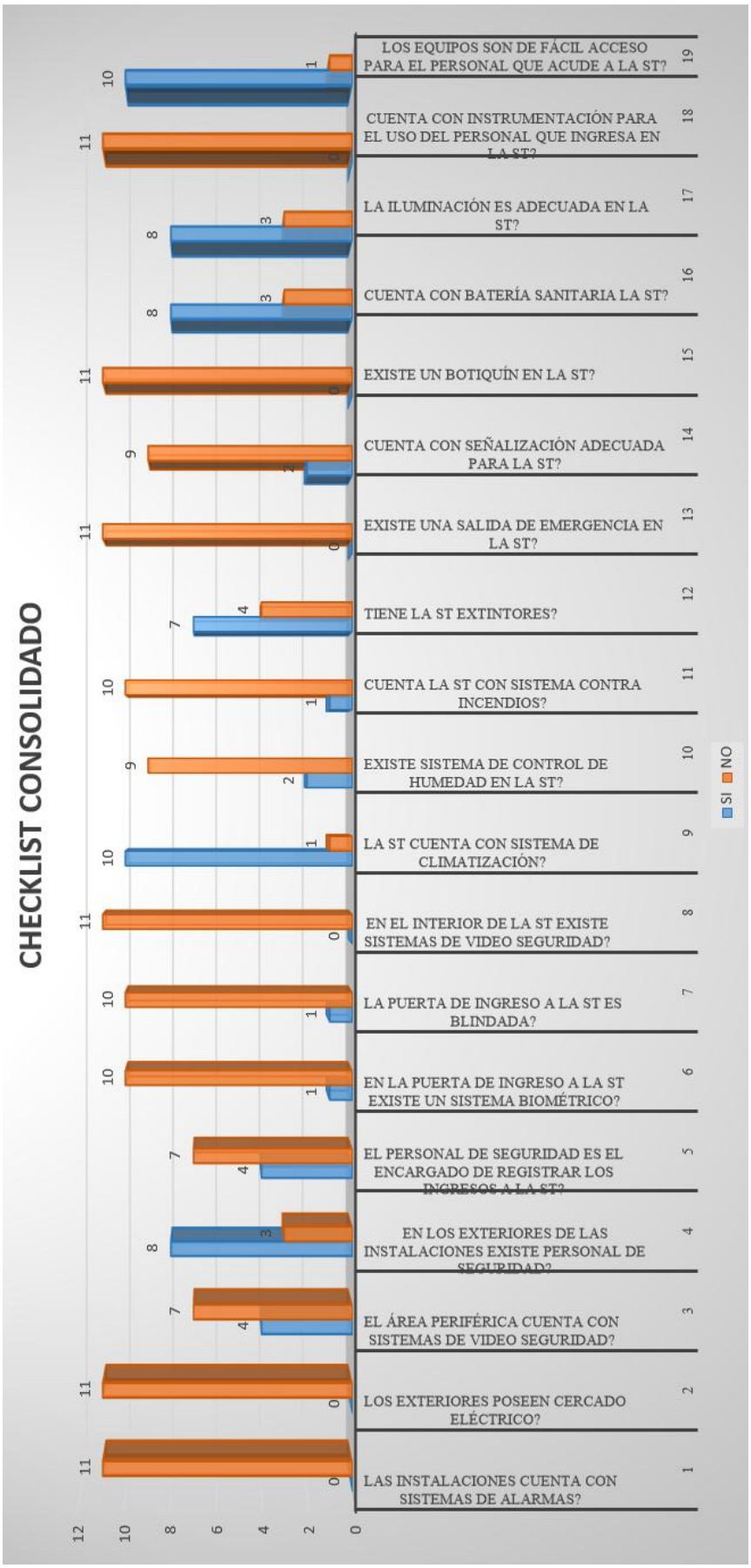


Figura 2. 129: Consolidado Checklist aplicado a STs

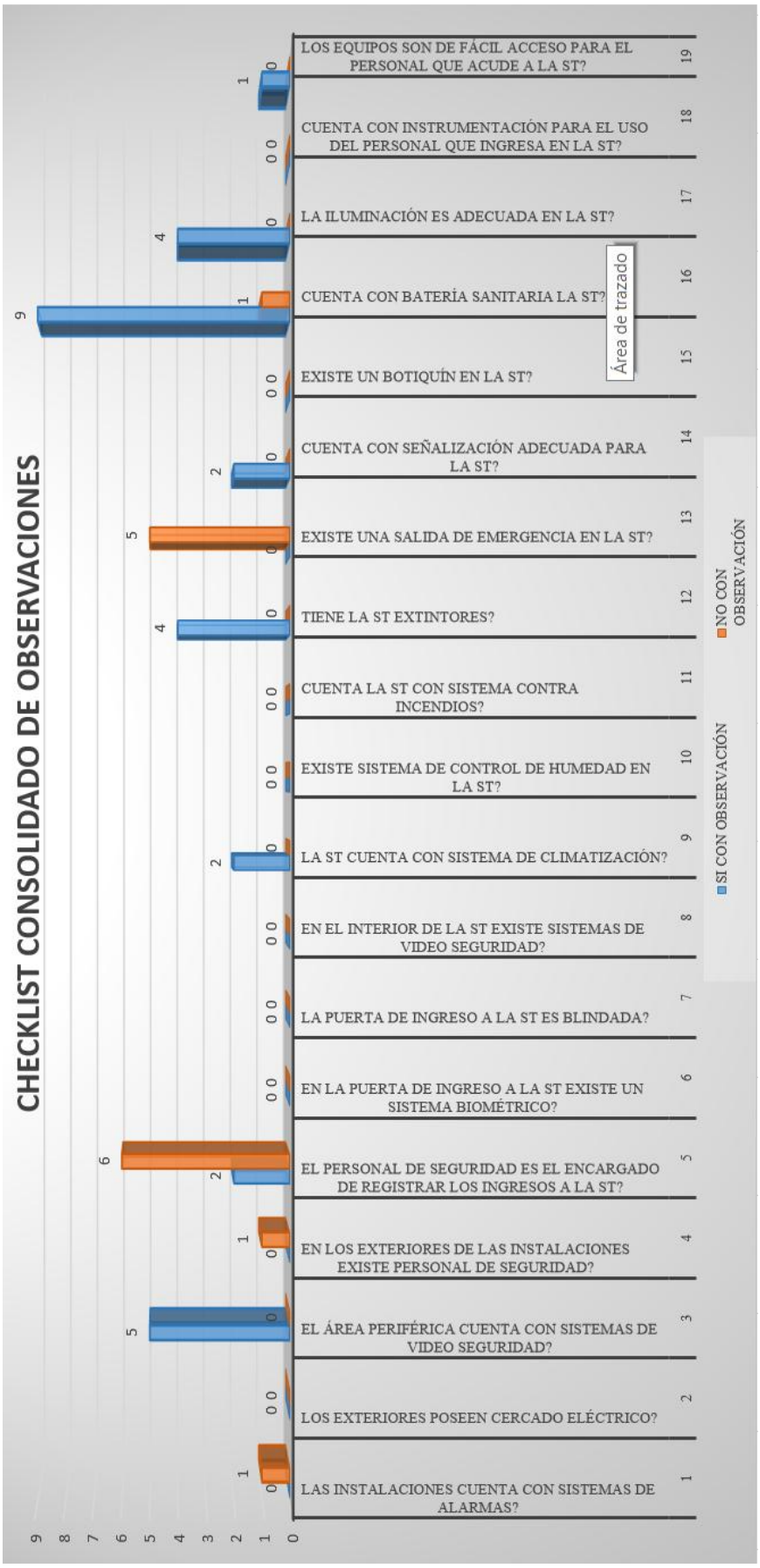


Figura 2. 130: Observaciones en STs

Figura 2. 131: Sistema de Alarmas en STs

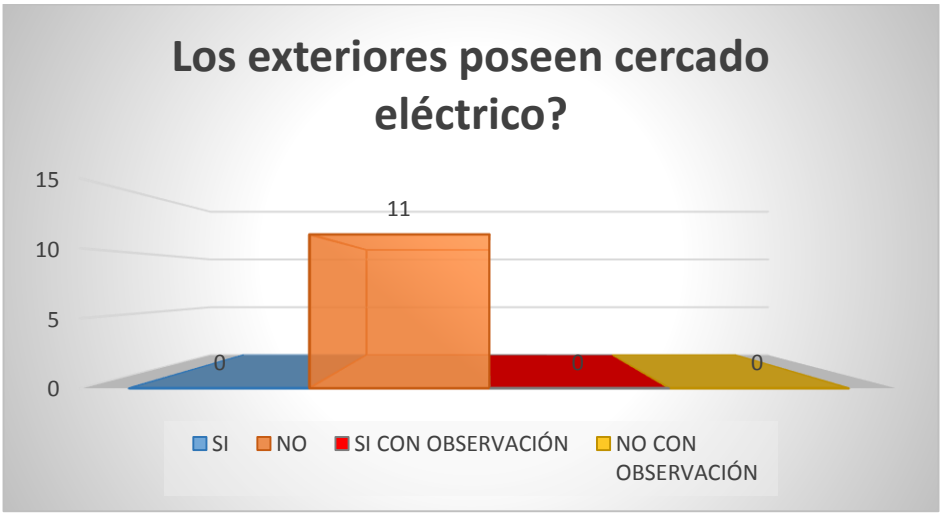


Figura 2. 132: Cercas Eléctricas en STs

Figura 2. 133: Sistema de Video en Periferia en STs

Figura 2. 134: Personal de Seguridad en STs

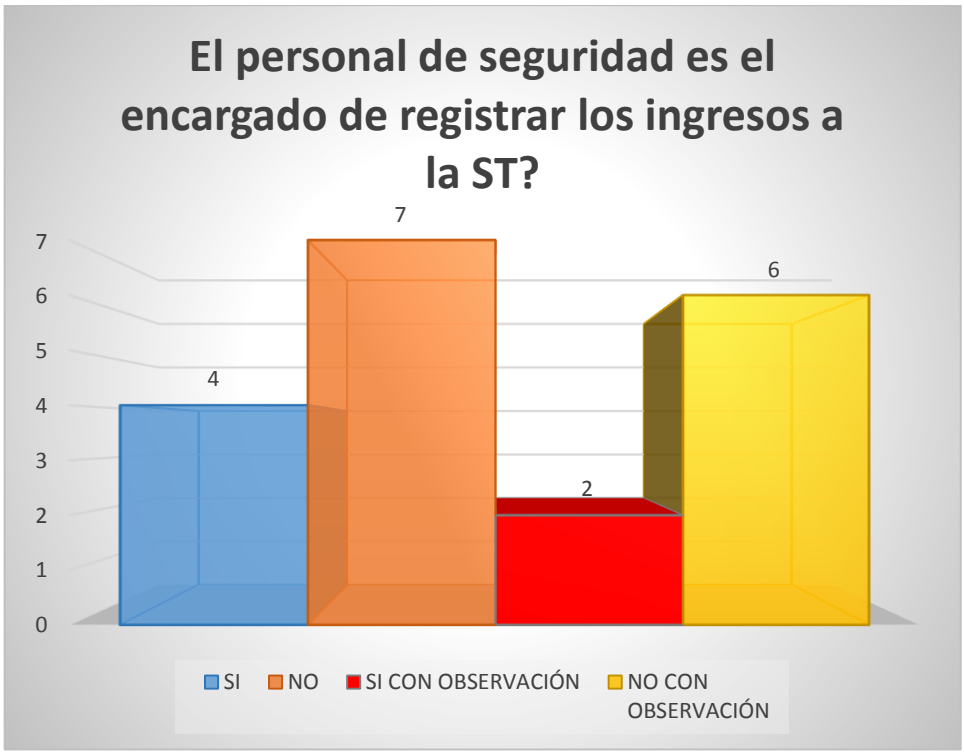


Figura 2. 135: Registro de Ingresos en STs

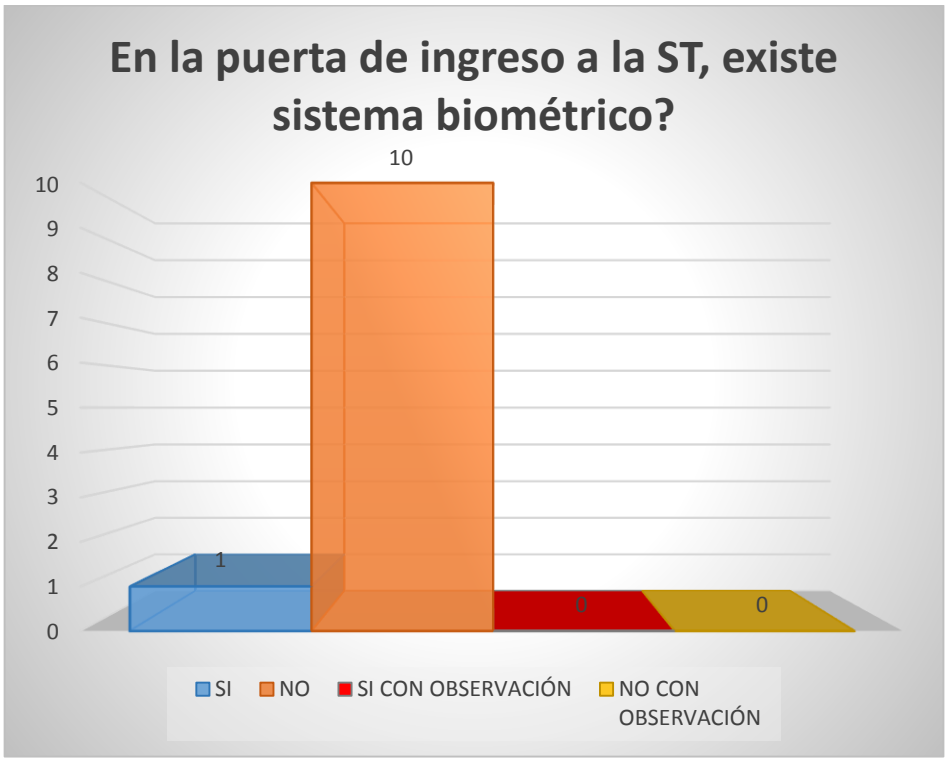


Figura 2. 136: Sistema Biométrico en STs

Figura 2. 137: Puertas Blindadas en STs

Figura 2. 138: Sistemas de Video en Interiores en STs

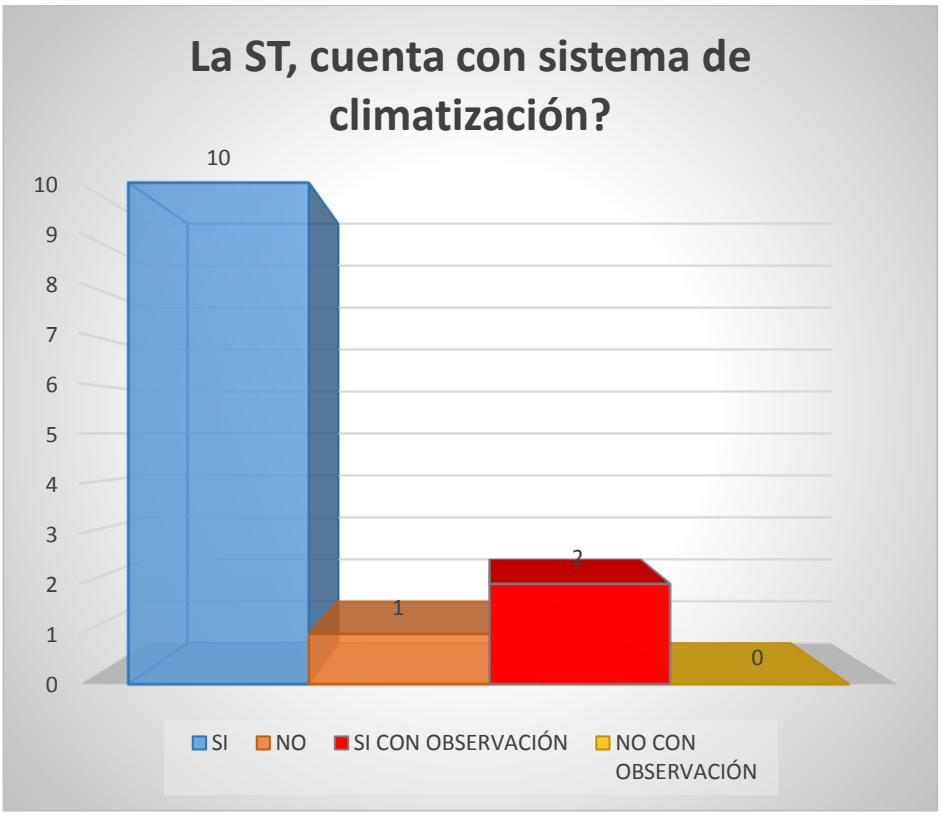


Figura 2. 139: Climatización en STs

Figura 2. 140: Control de Humedad en STs

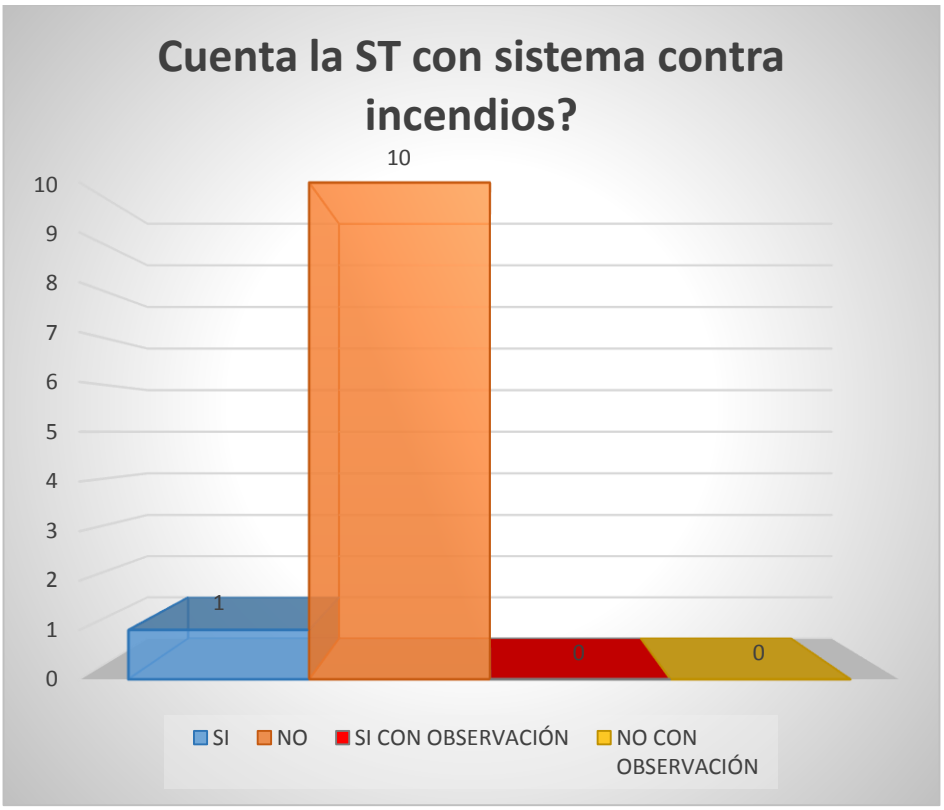


Figura 2. 141: Sistemas Contra Incendios en STs

Figura 2. 142: Extintores en STs

Figura 2. 143: Salidas de Emergencia en STs

Figura 2. 144: Señalización Adecuada en STs

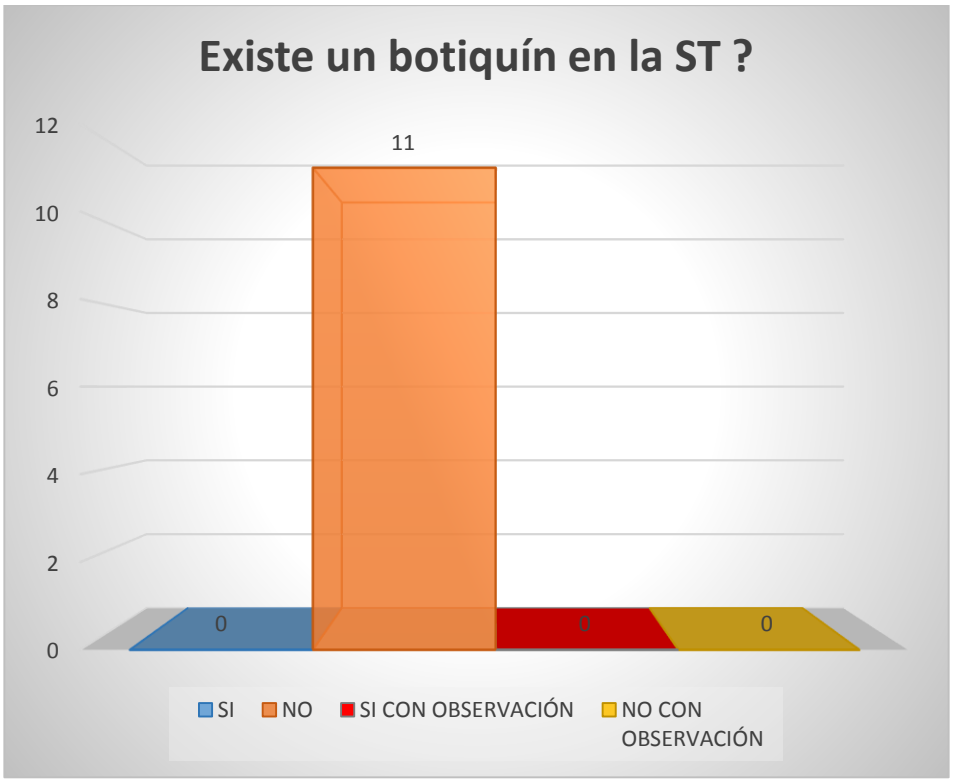


Figura 2. 145: Botiquines en STs

Figura 2. 146: Baterías Sanitarias en STs

Figura 2. 147: Iluminación en STs

Figura 2. 148: Instrumentación en STs

Figura 2. 149: Equipos de fácil Acceso en STs

CAPÍTULO 3

DISEÑO Y PRESUPUESTO DE LOS EQUIPOS Y SISTEMAS A UTILIZARSE

3. Introducción.

Este capítulo iniciará con una introducción básica de la norma ISO 27001 en lo que respecta a la seguridad física y los parámetros que esta nos indica para que las instalaciones permanezcan seguras, dichos parámetros se encuentran en el Apartado # 9 de la Norma.

Área Segura: Como objetivo, es evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

3.1. Perímetro de la Seguridad Física.

En el apartado A9.1.1 del Anexo A de la norma NTE INEN-ISO/IEC 27001: 2011 se hace referencia a los puntos que deben considerarse en las instalaciones para hacerlas seguras, tales como:

Definir el perímetro a proteger, es decir:

- Que las edificaciones sean seguras, sus accesos puertas y ventanas protegidas.
- Establecer un área de recepción u otro mecanismo para el control de acceso.
- La construcción de barreras físicas.
- Instalación de sistemas adecuados de detección de intrusos (Alarmas) según normas nacionales, regionales, internacionales, y puestas a pruebas.
- Los servicios de procesamiento de información de propiedad de la organización deberían estar físicamente separados de aquellos que se encuentran a cargo de terceras partes.

Basado en lo que dice el apartado anterior se necesitarán de:

1. Cercas eléctricas y barreras físicas para el control de la periferia.
2. Biométricos para el control de acceso.
3. Identificaciones o credenciales para el personal.
4. Alarmas, sensores de movimiento, sensores magnéticos para puertas y ventanas para la detección contra intrusos.
5. Alarmas contra incendios, sus sensores y dispositivos en casos de emergencia.
6. La información física y magnética separada de la organización de la de terceros.

3.2. Equipos Existentes en el Mercado.

Tener una referencia de los equipos y sistemas que se emplean en la actualidad con la finalidad de escoger el adecuado para el proyecto, esta información fue recopilada de los proveedores que fueron visitados.

3.3. Presupuesto.

Existe una amplia gama de equipos en el mercado por lo que el presupuesto también es variado, dependiendo de la marca, calidad, garantía, robustez, eficiencia y obviamente el costo, pero en su mayoría son equipos independientes es decir no requieren funcionar en conjunto, lo que conlleva a incorporar un sistema que permita la integración de los equipos antes descritos para ETAPA EP.

3.4. Comparativo.

Aquí se detallará una comparación respecto a que sistema es el más eficaz para los requerimientos de ETAPA EP. Es por ello que para el proyecto se ha buscado sistemas que engloben las necesidades que se precisa en la organización optando por el sistema GENETEC que es un sistema que enlaza estos sistemas en una sola plataforma.

3.5. Clasificación de Cámaras.

Esta clasificación se la hace tomando en cuenta las características particulares de las instalaciones a las que se van a dar protección, lo cual es importante al momento de elegir las cámaras de video vigilancia para la organización.

3.5.1. Tipos de Cámaras que se Encuentran en el Mercado.

3.5.1.1. Cámara Interior.

Las cámaras más sencillas que podemos encontrar son las de interior. No necesitan una carcasa estanca o visión nocturna ya que suele haber iluminación permanente durante las horas que se necesita supervisión.

Figura 3. 1: Cámara Interior. (INTPLUS, 2016)

Cámara con sonido diseñada especialmente para instalaciones de CCTV. Su alta calidad y pequeño formato es perfecto para instalarla en locales, salas, comercios, pasillos y allí donde queremos que se "vea" la existencia de cámaras, pero que a la vez no rompan la estética del entorno. Incluye soporte para su colocación en paredes y techos óptica de 4mm y transformador de 12V estabilizado. Posibilidad de cambiar de ópticas.

3.5.1.2. Cámaras con Infrarrojos.

Si la cámara va a estar colocada en un lugar con poca iluminación o se necesita vigilancia 24 horas la mejor opción es colocar cámaras con visión nocturna. Estas

cámaras graban durante el día a todo color y cuando hay poca iluminación enciende de forma automática sus infrarrojos para seguir grabando en blanco y negro.

Figura 3. 2: Cámara con Infrarrojos. (INTPLUS, 2016)

Cámara tipo domo para exteriores. Como se muestra en la figura 3.2, cuenta con una protección (carcasa anti vandálica), lente vari focal 2,8-12 mm Sony Effio 1/3" y visión nocturna de 30 metros de alcance. Esta cámara de altísima resolución (800 líneas) le ofrecerá imágenes claras y nítidas cuando hay iluminación exterior e imágenes en blanco y negro cuando la cámara detecta un nivel bajo de luz. Manteniendo su negocio vigilado y protegido las 24 horas del día.

3.5.1.3. Cámaras Anti Vandálicas.

Las zonas transitadas por mucho público o locales que son especialmente vulnerables a robos y agresiones son las indicadas para las cámaras anti vandálicas, siendo perfectas para parkings, almacenes, discotecas, bares o exteriores de tiendas. En la figura 3.3 se ilustra una cámara que cuenta con la protección de una carcasa resistente a golpes y que tiene la propiedad de mantenerse fija para seguir grabando todo lo que ocurre.

Figura 3. 3: Cámara Anti Vandálicas. (INTPLUS, 2016)

Su tamaño compacto en formato de domo y carcasa anti vandálica, de alta resolución (800 líneas) que incluye un sensor Sony Effio 1/3", lente vari focal de 2.8-12 mm, con visión nocturna de 30 metros que garantiza imágenes claras y nítidas; hacen que esta cámara prácticamente se la puede utilizar en cualquier parte.

3.5.1.4. Cámaras IP.

Las cámaras IP son sistemas completos que se conectan directamente a Internet y muestran la imagen del lugar donde está colocada. Con una cámara IP puede utilizar su móvil para ver su casa desde cualquier parte del mundo, sin necesidad de otros equipos.

Figura 3. 4: Cámara IP. (INTPLUS, 2016)

En la figura 3.4 se ilustra una cámara para exterior de alta calidad que incorpora un sensor 1/3" Sony Exmor de 1.3 Megapíxel y lente vari focal de 5 a 50 mm que junto a

las 1000 líneas de televisión le aseguran una imagen correcta, y nítida de todo lo que ocurre en su casa o negocio. Esta cámara de alta calidad incorpora también visión nocturna por infrarrojos que le permiten captar imágenes en oscuridad total en una distancia de hasta 100 metros.

3.5.1.5. Cámaras con Movimiento y Zoom.

Las cámaras con zoom y movimiento son idóneas para instalaciones de CCTV que tienen a una persona monitorizando las cámaras o para grandes superficies que se vigilan siguiendo una ruta de movimiento.

Figura 3. 5: Cámara con Movimiento y Zoom. (INTPLUS, 2016)

El tipo de cámara que se ilustra en la figura 3.5, es una cámara mini domo de exterior con movimiento horizontal y vertical de alta velocidad, visión nocturna de 50 metros de alcance y zoom óptico de 10 aumentos perfecta para cualquier solución de video vigilancia. Incorpora un sensor 1/3” Sony 960H Súper HAD CCD II con 650 líneas de televisión que garantiza una visión amplia, clara y nítida de todo lo que ocurre en los exteriores de las instalaciones.

3.5.1.6. Cámaras Ocultas.

Son útiles en ambientes en los casos en los que se requiere vigilar con discreción. Estas cámaras se colocan dentro de algún objeto (detectores de humo, sensores de movimiento, espejos, tornillos, enchufes) y pasan 100% desapercibidas a todas las personas que pasen por delante.

Figura 3. 6: Cámaras Ocultas. *(*INTPLUS*, 2016)*

En la figura 3.6 se muestra un ejemplo de una cámara oculta en un espejo panorámico resultando perfecta para vigilar de forma discreta y elegante todo lo que ocurre en interiores. El espejo se coloca en cualquier pared orientándolo hacia el lugar que se quiere controlar. El espejo panorámico ofrece una visión global de toda la habitación donde esté colocado y todas las personas tenderán a mirarse en él, de forma que sus caras quedan grabadas en el disco del grabador con total calidad. (INTPLUS, 2016)

3.6. Biométricos.

A diferencia de los sistemas que utilizan llaves, tarjetas de identificación que pueden perderse o ser sustraídas de sus propietarios o de los sistemas que utilizan paswords y códigos en donde el ser humano puede olvidarlos o ser sustraídas o duplicadas, la biometría es una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como la huella digital, el reconocimiento del patrón venoso del dedo, el reconocimiento facial, etc. “Es un excelente sistema de identificación de la persona que se aplica en muchos procesos debido a dos razones fundamentales, la seguridad y la comodidad.”

Se podría decir que se trata del mismo sistema que utiliza el cerebro humano para reconocer y distinguir una persona de otra.

3.6.1. Técnicas Biométricas:

3.6.1.1. Huella Dactilar.

En la figura 3.7 se muestra el equipo biométrico que utiliza la huella dactilar como método de identificación, siendo en la actualidad uno de los sistemas más conocidos y utilizados por su comodidad de adquisición y las numerosas fuentes posibles para su recolección (dedos).

Figura 3. 7: Huella Dactilar. (Biometría, 2013)

3.6.1.2. Características del Ojo: Iris y Retina.

Este método de identificación que se ilustra en la figura 3.8 es relativamente joven desarrollándose con fuerza por los años 90; se basa en el reconocimiento del ojo humano a través del iris o de la retina.

Figura 3. 8: Características del Ojo: iris y Retina. (Biometría, 2013)

3.6.1.3. Geometría de la Mano e Imagen Vascular.

En combinación con otras técnicas, es el sistema de identificación más utilizado en el control físico de acceso. Toma un conjunto de características geométricas (el ancho de los dedos, la localización, ancho de la palma, longitud de los dedos, etc…) convirtiéndose en uno de los más rápidos dentro de su grupo y con una probabilidad de error aceptable. En aproximadamente un segundo son capaces de determinar si una persona es quien dice ser (figura 3.9).

Figura 3. 9: Geometría de la mano e Imagen Vascular. (EcuRed, 2016)

3.6.1.4. Características Faciales.

Esta técnica de identificación que se muestra en la figura 3.10 recurre a los grandes avances que ha dado la computación en las últimas décadas, utilizando algoritmos de reconocimiento facial mediante el empleo de sofisticadas representaciones matemáticas y procesos de coincidencia que permiten reconocimientos similares de individuos de forma automática.

Figura 3. 10: Características Faciales. (Biometría, 2013)

3.6.1.5. Composición Química del Olor Corporal

La técnica de identificación que se ilustra en la figura 3.11 utiliza sensores que detectan a las personas autenticándolas en función de su olor corporal, este sistema biométrico es el más reciente en las industrias desarrollada por investigadores de la Universidad de Madrid junto con Ilía Sistemas dando una efectividad del 85%.

Figura 3. 11: Composición Química del Olor Corporal. *(*Madrid, 2016*)*

3.6.1.6. Líneas de la Mano.

Esta técnica utiliza una combinación de dos sistemas de identificación: la huella palmar y la huella dactilar que son representadas a través de la información de la impresión de surcos de fricción, esta información combina la información de surcos, las características de los surcos y la estructura de los surcos de la porción de la epidermis expuesta (figura 3.12). Dado que las huellas palmares y dactilares son únicas y permanentes, han sido utilizadas por más de un siglo como una forma confiable de identificación.

Figura 3. 12: Líneas de la Mano. (Biometría, 2013)

3.6.1.7. Escritura Manuscrita.

Figura 3. 13: Escritura Manuscrita. (Certicámara, 2016)

3.6.1.8. Voz.

La técnica de identificación que se muestra en la figura 3.14, utiliza un proceso que permite reconocer la voz a través de las características de la estructura física del tracto vocal de un individuo así como también de sus características de comportamiento, este reconocimiento por voz es una elección popular de reconocimiento biométrico remoto.

Figura 3. 14: Voz. (Biometría, 2013)

3.6.1.9. Tecleo.

Este sistema utiliza la técnica de identificación de índice numérica (figura 20) establecida para cada persona de la organización. Es uno de los más comunes por su sencillez pero también de los más inseguros puesto que sus passwords pueden ser olvidados, sustraídos o duplicados.

Figura 3. 15: Tecleo. (SAS, 2015)

3.6.1.10. Gesto y Movimiento Corporal.

Figura 3. 16: Gesto y Movimiento Corporal. (Parra, 2016)

3.7. Cercas Eléctricas.

Son dispositivos de seguridad perimetral muy utilizados en la actualidad y de gran demanda que están constituidos por un conjunto de alambres electrificados con alta tensión (8000 a 10000 volt), un equipo de control y detección y dispositivos de aviso de intentos de intrusión (figura 3.17).

El objetivo de la cerca eléctrica es proteger el perímetro delimitado por el tendido de alambres electrificados, detectando el corte o toque de los mismos por un posible intruso, dando aviso al propietario mediante sirenas, llamado telefónico, encendido de focos, etc.

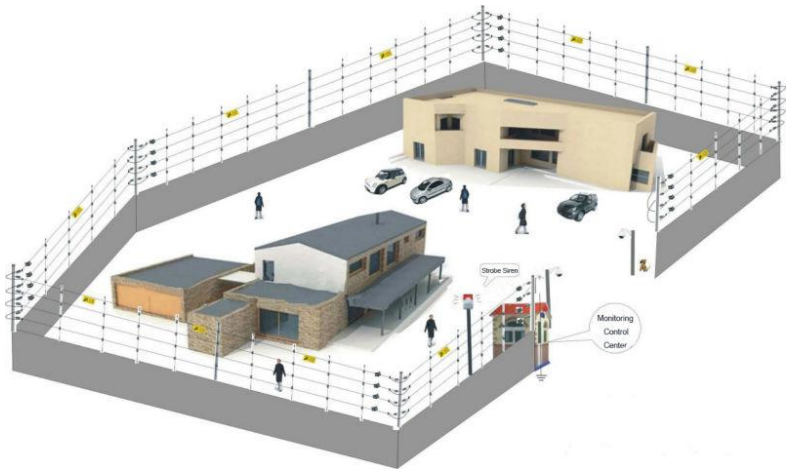


Figura 3. 17: Cercas Eléctricas. (FullCar, 2016)

3.8. Alarmas.

Son señales o avisos que advierten la proximidad de un peligro. El aviso de alarma informa que se debe seguir ciertas instrucciones de emergencia ante la presencia inminente de una amenaza.

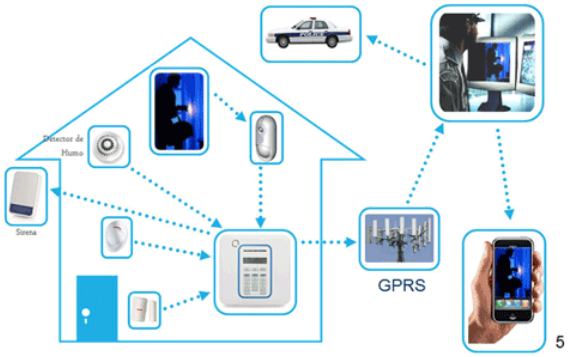


Figura 3. 18: Alarmas.

3.9. Diseño.

Nuestro diseño incluye un sistema de video asistencia que permite la comunicación interactiva entre el operario y el personal que se encuentra en la Sala de Control y Monitoreo.

Luego de un análisis resultado de las visitas realizadas a las instalaciones y de reuniones mantenidas con los coordinadores del proyecto, se ha llegado a la conclusión de que la asistencia mediante dispositivos adicionales que permitan la comunicación, no es viable, puesto que en las STs se genera ruido en los equipos, existe interferencia y retraso en las comunicaciones (*delay*) por lo que se ha decido reutilizar recursos ya existentes dentro de la misma, contando ETAPA EP con el sistema de telefonía CDMA que han sido distribuidos a todo el personal que labora dentro de la organización dándose de esta manera la asistencia propuesta en este trabajo.

3.9.1. Diseño de un SGSI Para la Central de Totoracocha.

Debido a su importancia y jerarquía estas Salas de Telecomunicaciones son las que encabezan la lista de prioridades y a las cuales se les debe dar mayor resguardo al momento de una implementación de seguridad. Estas instalaciones cuentan con gran cantidad de equipos y sistemas que permiten el desempeño normal de ETAPA EP, una falla de seguridad en estas instalaciones significaría la pérdida de recursos y de información que se puedan suscitar en el resto de STs, dejando a la organización desprotegida y con vulnerabilidades en su infraestructura.

En las Centrales se verá la necesidad de instalar los siguientes equipos y sistemas que ayudaran a que las instalaciones no sufran algún ataque de tipo físico:

- Protección del área periférica: esto se lo conseguirá con la colocación de cercas eléctricas en los muros de las instalaciones.
- Guardias de seguridad: los cuales van a controlar el flujo del personal que ingresa a las instalaciones.

- Cámaras de video vigilancia: estos equipos ayudaran a los guardias en su labor de vigilar las periferias y así como del interior de las instalaciones quedando estas registradas en el sistema para posterior revisión y corrección de algún error cometido por ellos.
- Alarmas y sensores: tanto para la periferia como para las STs u oficinas en las que se maneje información importante y a la que el resto del personal de la organización no debería ingresar.
- Controles Biométricos: ayudaran a los guardias a un control más efectivo al momento del ingreso de personal perteneciente a la organización. Cada persona que ingrese deberá contar con una credencial, pasword, huella etc siendo estos dispositivos de control o claves de uso individual y no debería estar sujeto a ningún tipo de préstamo.

3.9.1.1. Planos de Diseño de la Central de Totoracocha

Para el diseño del sistema de seguridad y control de acceso se solicitó los planos digitales de las instalaciones de la Central de Totoracocha de ETAPA EP, información que se reforzó con la visita técnica realizada a las instalaciones permitiéndonos tener una perspectiva más clara de la ubicación de los equipos que se requieren en éste sistema (Anexo I).

Los criterios de ubicación de las 20 cámaras distribuidas en 3 para la sala de repartidores, 4 para la salas de energía, 3 en pasillos y graderíos y 10 para la sala de equipos, responden a la necesidad de una ubicación estratégica para cubrir el área física de la sala tomando en cuenta la iluminación existente, la altura y ubicación de los equipos, los pasillo y corredores, ingresos y salidas de emergencia; elevando así el control del personal que accede a las salas a realizar trabajos. Las cámaras manejan tecnología de video trickling con almacenamiento local en memoria SD de 64 GB, y a su vez se almacenará centralizadamente en el servidor RAID 5. El tiempo de almacenamiento, NTE INEN/ISO-IEC 27001/2011 recomienda como mínimo un almacenamiento 3 meses, pudiendo la organización incrementar el tiempo si lo cree necesario.

Se colocaron 20 sensores de movimiento distribuidos en 4 para la sala de energía, 3 para la sala de repartidores, 3 para los pasillos y graderíos, y 10 para la sala de equipos, siguiendo un criterio similar al de la ubicación de las cámaras que permiten a estos dispositivos tener una mayor cobertura.

Se incluyeron 5 sensores magnéticos que se distribuyeron de la siguiente manera: 1 para la sala de equipos, 1 para la sala de repartidores, 2 en las salas de energía y 1 en la puerta de acceso al edificio en donde se encuentran las salas anteriormente mencionadas.

En cuanto al equipo biométrico para el control de acceso, es un Bioscryp caracterizado por su durabilidad y alta resolución en el lector óptico, incluye teclado, tarjeta, una lámpara y controladores de puertas que mostrará en pantalla un aviso de apertura con la opción de efectuarlo de manera remota desde la sala encargada de la gestión y supervisión. Se ha colocado este equipo al ingreso del edificio, puesto que el acceso a las salas es compartido (Diseño de ubicación de dispositivos se incluyen en Anexos II, III y IV).

Para lograr una mayor protección y seguridad de las instalaciones en las que se encuentran las STs se ha dispuesto un cerco eléctrico RAPTOR compuesto por 5 líneas de alambrado, un kit electrificador, cable de bujía y cable gemelo que ayudarán a evitar el acceso de intrusos (Diseño se incluye en Anexos I).

3.9.1.2. Presupuesto Requerido en Central.

- ✓ Los costos detallados no incluyen IVA.
- ✓ El presupuesto tiene una validez de 45 días a partir de la fecha de la elaboración de este documento.
- ✓ Si se elevan los impuestos a importaciones e IVA, se incrementaría los valores.

- ✓ El presupuesto no incluye materiales no descritos de manera explícita en esta proforma.

Tabla 3. 1: Presupuesto de Equipos para la Central de Totoracocha.

Cant	Descripción	Marca	Modelo	Valor Unit.	Valor Total
1	1 Servidor con 12 TB con Raid de 5.2, fuentes de poder, 16GB Memoria, Xeon de procesador y Servicio SMTP configurado.	HP	HP ProLiant DL 380 Gen 9	16128.75	16128.75
100 MB	Ancho de banda requerido para enlace vía fibra óptica (2mb por cada dispositivo)			400.00	40000.00
3	Switch 24 Puertos POE Capa 3	HP	HP 1910-24 POE	783.07	2349.21
2	Transmisores de fibra multimodo.	HP		308.64	617.28
2	Patch cord de fibra multimodo			123.46	246.92
1	Monitor heavy duty 32”	PELCO	PMCL532BL	2249.21	2249.21
1	Licencia de Servidor de video	GENETEC	Om-s-Base	1855.60	1855.60
1	Licencia de Servidor de acceso.	GENTEC	GSC-Sy-S	2624.07	2624.07
1	Licencia de integración de cámaras IP	GENTEC	Om-S-1C	314.89	314.89
46	Licencia de integración de acceso.	GENTEC	SMA-RDR-S-1Y	33.74	1552.04

1	Licencia de integración de alarma	GENTEC		400.00	400.00
1	Licencia de integración de cerca eléctrica	GENTEC		380.00	380.00
20	Cámara fija 1080p Full HD, con SD de 64 GB y video trickling para interiores.	AXIS	P1355	2349.12	46982.4
1	Control de acceso de huella, tarjeta y código.	BYOSCRIPT	L1 4GSTSH	2998.94	2998.94
5	Controlador de accesos.	HID	EDGE EVO EH400-K	890.31	4451.55
5	Luz de Emergencia.			88.18	440.90
5	Cierra puertas.			84.66	423.30
5	Cerradura eléctrica.			141.09	705.45
5	Cerradura electromagnética 600lb.			222,22	1111.10
1	Instalación, configuración y puesta en marcha del sistema de CCTV y accesos para cada ST.			670.19	670.19
1	Instalación, configuración y puesta en marcha del servidor y monitores en la central.			529..10	529.10
1	Kit de Alarma (1 sensor de movimiento. 1 sensor magnético, una sirena de 30 W y una batería de 7 A)	DSC CLASSIC	PC-585	275.00	275.00
20	Sensores de movimiento			22.00	440.00
5	Sensores magnéticos			5.00	25.00

1 mt	Cable UTP Cat. 5			0.75	0.75
25	Instalación, configuración y funcionamiento			20.00	500.00
1 mt.	Kit Electrificador (batería, sirena y electrificador)	RAPTOR		200.00	200.00
1 mt.	Cable bujía			0.65	0.65
1	Cable gemelo 2x18			0.70	0.70
1 mt.	5 líneas de cable galvanizado acerado, templadores o aisladores, tapón, cartel, tubo de 1m de alto y 1" de diámetro	RAPTOR		12	12.00
				TOTAL	128485.0

3.9.2. Diseño de un SGSI Para el Concentrador Baños.

En estas Salas de Telecomunicaciones tenemos un menor número de equipos pero que no deja de ser importantes para la organización. Su implementación de sistemas de seguridad seguirá la misma disposición que la de las centrales su diferencia radica en el área física más no en los equipos que en ella se encuentra.

En los Concentradores se verá la necesidad de instalar los siguientes equipos y sistemas que ayudaran a que las instalaciones no sufran algún ataque:

- Protección del área periférica: esto se lo conseguirá con la colocación de cercas eléctricas en los muros de las instalaciones.
- Guardias de seguridad: los cuales van a controlar el flujo del personal que ingresa a las instalaciones.
- Cámaras de video vigilancia: estos equipos ayudaran a los guardias en su labor de vigilar las periferias y así como del interior de las instalaciones quedando

estas registradas en el sistema para posterior revisión y corrección de algún error cometido por ellos.

- Alarmas y sensores: tanto para la periferia como para las STs u oficinas en las que se maneje información importante y a la que el resto del personal de la organización no debería ingresar.
- Controles Biométricos: ayudaran a los guardias a un control más efectivo al momento del ingreso de personal perteneciente a la organización. Cada persona que ingrese deberá contar con una credencial, pasword, huella etc siendo estos dispositivos de control o claves de uso individual y no debería estar sujeto a ningún tipo de préstamo

3.9.2.1. Planos de Diseño del Concentrador Baños.

Para el diseño del sistema de seguridad y control de acceso del Concentrador de Baños, al igual que en la Central de Totoracocha se solicitó el plano digital de las instalaciones a ETAPA EP, información que se reforzó con la visita técnica realizada al Concentrador y que nos permitió tener una amplia perspectiva de la ubicación de los equipos que se requieren para este recinto (Anexo V).

Se ubicaron 10 cámaras distribuidas en 3 para la sala de repartidores, 2 para la salas de energía y 5 para la sala de equipos, que responden a la necesidad de una ubicación estratégica para cubrir el área física de la sala tomando en cuenta la iluminación existente, la altura y ubicación de los equipos, los pasillo y corredores, ingresos y salidas de emergencia; elevando así el control del personal que accede a las salas a realizar trabajos. Las cámaras manejan tecnología de video trickling con almacenamiento local en memoria SD de 64 GB, y a su vez se almacenará centralizadamente en el servidor RAID 5 ubicado en la Sala de Control. El tiempo de almacenamiento, NTE INEN/ISO-IEC 27001/2011 recomienda como mínimo un almacenamiento 3 meses, pudiendo la organización incrementar el tiempo si lo cree necesario.

Se diseñó la colocación de 6 sensores de movimiento distribuidos en 2 para la sala de repartidores, 2 en la sala de energía y 4 en la sala de equipos, siguiendo un criterio

similar al de la ubicación de las cámaras que permiten a estos dispositivos tener una mayor cobertura.

Se incluyeron 5 sensores magnéticos que se distribuyeron de la siguiente manera: 2 para la sala de equipos, 1 para la sala de repartidores y 2 en las salas de energía.

En cuanto al equipo biométrico para el control de acceso, es un Bioscryp caracterizado por su durabilidad y alta resolución en el lector óptico, incluye teclado, tarjeta, una lámpara y controladores de puertas que mostrará en pantalla un aviso de apertura con la opción de efectuarlo de remota desde la sala encargada de la gestión y supervisión. Se ha colocado 2 equipos, uno para el ingreso a la sala de repartidores y otro que es compartido en la sala de equipos y energía (Diseño de ubicación de dispositivos se incluye en Anexo VI y VII).

Para lograr una mayor protección y seguridad de las instalaciones en las que se encuentran las STs se ha dispuesto un cerco eléctrico RAPTOR compuesto por 5 líneas de alambrado, un Kit electrificado y cables de bujía y gemelo que ayudarán a evitar acceso a intrusos. (Diseño se incluye en Anexos V).

3.9.2.2. Presupuesto Requerido Concentrador.

- ✓ Los costos detallados no incluyen IVA.
- ✓ El presupuesto tiene una validez de 45 días a partir de la fecha de la elaboración de este documento.
- ✓ Si se elevan los impuestos a importaciones e IVA, se incrementaría los valores.
- ✓ El presupuesto no incluye materiales no descritos de manera explícita en esta proforma.

Tabla 3. 2: Presupuesto de Equipos para el Concentrador de Baños

Cant	**Descripción**	**Marca**	**Modelo**	**Valor Unit.**	**Valor Total**
60 MB	Ancho de banda requerido para enlace vía fibra óptica (2mb por cada cámara)			400.00	24000.00
2	Switch 24 Puertos POE Capa 3	HP	HP 1910-24 POE	783.07	1566.14
2	Transmisores de fibra multimodo.	HP		308.64	617.28
2	Patch cord de fibra multimodo			123.46	246.92
1	Monitor heavy duty 32”	PELCO	PMCL532BL	2249.21	2249.21
1	Licencia de Servidor de video	GENETEC	Om-s-Base	1855.60	1855.60
1	Licencia de Servidor de acceso.	GENTEC	GSC-Sy-S	2624.07	2624.07
1	Licencia de integración de cámaras IP	GENTEC	Om-S-1C	314.89	314.89
25	Licencia de integración de acceso.	GENTEC	SMA-RDR-S-1Y	33.74	843.50
1	Licencia de integración de alarma	GENTEC		400.00	400.00
1	Licencia de integración de cerca eléctrica	GENTEC		380.00	380.00
10	Cámara fija 1080p Full HD, con SD de 64 GB y video trickling para interiores.	AXIS	P1355	2349.12	23491.20

2	Control de acceso de huella, tarjeta y código.	BYOSCRIPT	L1 4GSTSH	2998.94	5997.88
4	Controlador de accesos.	HID	EDGE EVO EH400-K	890.31	3561.24
4	Luz de Emergencia.			88.18	352.72
4	Cierra puertas.			84.66	423.30
2	Cerradura eléctrica.			141.09	282.18
2	Cerradura electromagnética 600lb.			222,22	444.44
1	Instalación, configuración y puesta en marcha del sistema de CCTV y accesos para cada ST.			670.19	670.19
1	Instalación, configuración y puesta en marcha del servidor y monitores en la central.			529..10	529.10
1	Kit de Alarma	DSC CLASSIC	PC-585	275.00	275.00
6	Sensores de movimiento			22.00	132.00
5	Sensores magnéticos			5.00	25.00
1 mt	Cable UTP Cat. 5			0.75	0.75
11	Instalación, configuración y funcionamiento			20.00	220.00
1 mt.	Kit Electrificador (batería, sirena y electrificador)	RAPTOR		200.00	200.00
1 mt.	Cable bujía			0.65	0.65
1	Cable gemelo 2x18			0.70	0.70
1 mt.	5 líneas de cable galvanizado acerado,	RAPTOR		12	12.00

	templadores o aisladores, tapón, cartel, tubo de 1m de alto y 1” de diámetro				
				TOTAL	71715.96

3.9.3. Diseño de un SGSI Para el Nodo 24 Mayo.

Estas Salas de Telecomunicaciones son pequeñas con respecto a los Concentradores y Centrales en ellas se encuentra un limitado número de equipos por lo que se ha estableciendo que para ellas se verá la necesidad de utilizar solo algunos de los sistemas citados en las anteriores salas. (Anexo VIII)

En los Nodos se verá la necesidad de instalar los siguientes equipos y sistemas que ayudaran a que las instalaciones no sufran algún ataque de tipo físico:

- Cámaras de video vigilancia: estos equipos ayudaran a los guardias en su labor de vigilar las periferias y así como del interior de las instalaciones quedando estas registradas en el sistema para posterior revisión y corrección de algún error cometido por ellos, controladas remotamente.
- Alarmas y sensores: para las STs en caso de que alguien quiera ingresar sin previa autorización, también controlada vía remota.
- Controles Biométricos: ayudaran a los guardias a un control más efectivo al momento del ingreso de personal perteneciente a la organización. Cada persona que ingrese deberá contar con una credencial, pasword, huella etc siendo estos dispositivos de control o claves de uso individual y no debería estar sujeto a ningún tipo de préstamo.

3.9.3.1. Planos de Diseño del Nodo Externo 24 de Mayo.

El Nodo Externo 24 de Mayo por su tamaño varía en su diseño con respecto a los anteriores, puesto que el mismo consta de un solo cuarto con accesos independientes para equipo y energía, y otro para repartidores.

ETAPA EP nos proporcionó el plano digital que se reforzó con la visita técnica realizada al Nodo y que nos permitió tener una amplia perspectiva de la ubicación de los equipos que se requieren para este recinto.

El nodo cuenta con 4 cámaras distribuidas en 1 para la sala de repartidores y 3 para la salas de equipos y energía, y que responden a la necesidad de una ubicación estratégica para cubrir el área física de la sala tomando en cuenta la iluminación existente, la altura y ubicación de los equipos, los pasillo y corredores, ingresos y salidas de emergencia; elevando así el control del personal que accede a las salas a realizar trabajos. La tecnología de las cámaras utilizadas en éste nodo es la mima de la Central y Concentrador. El tiempo de almacenamiento, NTE INEN/ISO-IEC 27001/2011 recomienda como mínimo un almacenamiento 3 meses, pudiendo la organización incrementar el tiempo si lo cree necesario.

Se ubicaron 2 sensores de movimiento, uno por cada sala, siguiendo un criterio similar al de la ubicación de las cámaras que permiten a estos dispositivos tener una mayor cobertura.

Se incluyeron 2 sensores magnéticos, uno por cada ingreso a las salas.

En cuanto al equipo biométrico empleado para el Nodo tiene las mismas características y tecnología utilizada en las Salas anteriores. Se ha colocado 1 equipo biométrico en el ingreso a la sala de equipos y energía. La sala de repartidores, por el tamaño del nodo no surge la necesidad de la colocación de otro sistema de control de acceso (Diseño de ubicación de dispositivos se incluye en Anexo VIII y IX).

No se ve la necesidad en este nodo de coloca un cerco eléctrico, como lo hemos venido indicando el tamaño del nodo es muy reducido y adicionalmente la estructura de la edificación no amerita.

3.9.3.2. Presupuesto Requerido Nodo Externo

- ✓ Los costos detallados no incluyen IVA.
- ✓ El presupuesto tiene una validez de 45 días a partir de la fecha de la elaboración de este documento.
- ✓ Si se elevan los impuestos a importaciones e IVA, se incrementaría los valores.
- ✓ El presupuesto no incluye materiales no descritos de manera explícita en esta proforma.

Tabla 3. 3: Presupuesto de Equipos para el Nodo Externo 24 de Mayo.

Cant	Descripción	Marca	Modelo	Valor Unit.	Valor Total
25 MB	Ancho de banda requerido para enlace vía fibra óptica (2mb por cada cámara)			400.00	10000.00
1	Switch 24 Puertos POE Capa 3	HP	HP 1910-24 POE	783.07	783.07
2	Transmisores de fibra multimodo.	HP		308.64	617.28
2	Patch cord de fibra multimodo			123.46	246.92
1	Monitor heavy duty 32”	PELCO	PMCL532BL	2249.21	2249.21
1	Licencia de Servidor de video	GENETEC	Om-s-Base	1855.60	1855.60
1	Licencia de Servidor de acceso.	GENTEC	GSC-Sy-S	2624.07	2624.07
1	Licencia de integración de cámaras IP	GENTEC	Om-S-1C	314.89	314.89

10	Licencia de integración de acceso.	GENTEC	SMA-RDR-S-1Y	33.74	337.40
1	Licencia de integración de alarma	GENTEC		400.00	400.00
1	Licencia de integración de cerca eléctrica	GENTEC		380.00	380.00
4	Cámara fija 1080p Full HD, con SD de 64 GB y video trickling para interiores.	AXIS	P1355	2349.12	9396.48
1	Control de acceso de huella, tarjeta y código.	BYOSCRIPT	L1 4GSTSH	2998.94	2998.94
1	Controlador de accesos.	HID	EDGE EVO EH400-K	890.31	890.31
2	Luz de Emergencia.			88.18	176.36
1	Cierra puertas.			84.66	84.66
1	Cerradura eléctrica.			141.09	141.09
1	Cerradura electromagnética 600lb.			222,22	222.22
1	Instalación, configuración y puesta en marcha del sistema de CCTV y accesos para cada ST.			670.19	670.19
1	Instalación, configuración y puesta en marcha del servidor y monitores en la central.			529..10	529.10
1	Kit de Alarma	DSC CLASSIC	PC-585	275.00	275.00
2	Sensores de movimiento			22.00	44.00
2	Sensores magnéticos			5.00	10.00
1 mt	Cable UTP Cat. 5			0.75	0.75

4	Instalación, configuración y funcionamiento			20.00	80.00
1	Cable gemelo 2x18			0.70	0.70
				TOTAL	35328.24

3.10. Costos.

Existe una amplia gama de equipos, marcas y calidades en el mercado; sin embargo se detallan los más convenientes para la organización.

Hay que tener en cuenta que en nuestro mercado local no existen muchos sistemas que engloben las necesidades que buscamos para ETAPA EP, más bien son sistemas independientes lo cual nos generaría un problema por la comunicación que debe existir entre dichos dispositivos.

Existen sistemas de seguridad física que se manejan en una única plataforma:

- Video.
- Controles de Acceso.
- Incendios.
- Alarmas.
- Biométricos.

Genetec es una marca que engloba e integra los sistemas de seguridad física incluyendo en sus equipos seguridades lógicas mediante la encriptación en la transmisión de la información recopilada por los dispositivos utilizados (cámaras, alarmas), contando con garantía de respaldo en los equipos requeridos para los sistemas de seguridad y con representantes de marca en nuestro país.

CAPÌTULO 4

PROCESOS ISO

4. Introducción.

Para que ETAPA EP pueda iniciar el proyecto de obtener una certificación ISO 27001 de Gestión de Seguridad de la Información (SGSI) como paso inicial debe existir el apoyo claro y decidido de la Gerencia General y de la Gerencia de Telecomunicaciones, quienes generarán una planificación conformando un grupo de trabajo de personal de las áreas involucradas, que estarán comprometidos con el proyecto asignando roles, acordando fechas, definiendo responsabilidades ligadas a los lineamientos del Estándar 27001.

La norma ISO para los sistemas de gestión están definidos por un proceso de 4 etapas que deben cumplirse para llegar a alcanzar el objetivo de la norma como son: PLAN (Planificar) – DO (Implementar) – CHECK (Medir) – ACT (Mejorar), y habiendo definido al inicio de este proyecto el alcance del presente trabajo, en este capítulo nos centraremos en la primera etapa: PLAN.

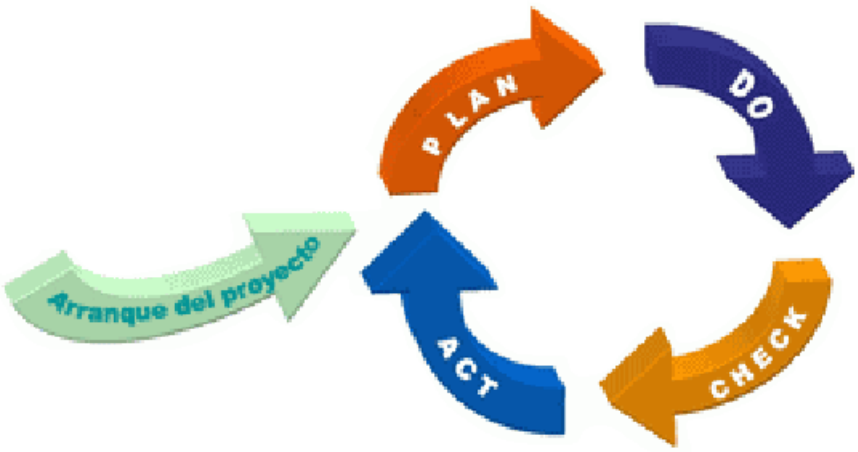


Figura 4. 1: Proceso Iso de Gestión. (PriteshGupta.com, 2012)

Iniciamos nuestro proyecto con la redacción de un documento en el que detallaremos los requisitos necesarios que deberá cumplir la empresa previo a solicitar a las entidades pertinentes la certificación ISO 27001 de SGSI para las Salas de Telecomunicaciones. En estos documentos utilizaremos plantillas didácticos de Academy 27001, debiendo realizar esta aclaración, puesto que para que ETAPA EP pueda hacer uso de dichos documentos, tendrá que adquirir los derechos de uso.

La aplicación de la Norma ISO 27001 es Universal, permitiendo de una manera general establecer requisitos para gestionar un SGSI aplicable a todo tipo de organización (empresas comerciales, agencias de gobierno, organizaciones sin fines de lucro), dejando la posibilidad abierta de que ETAPA EP pueda aplicarla a sus otras divisiones realizando las adaptaciones necesarias.

4.1. Sistema de Gestión de Seguridad de la Información (SGSI) Para Las Salas De Telecomunicaciones de ETAPA EP.

4.1.1. Antecedentes.

ETAPA tiene sus inicios como EMALT (Empresa Municipal de Electricidad, Agua Potable y Teléfonos) creada en 1948 con la finalidad de proveer los servicios de luz y energía eléctrica, agua potable y telefonía, para luego de 16 años asumir estas responsabilidades la Dirección Financiera de la Municipalidad de Cuenca. Sin embargo, el rápido crecimiento de la ciudad, creó la necesidad de la existencia de una empresa pública, independiente a la Municipalidad, y es así que en "Enero de 1968 cuando ejercía la Alcaldía el Dr. Ricardo Muñoz Chávez, el Concejo de Cuenca de acuerdo al Art. 194 de la Ley de Régimen Municipal, que facultaba a las Municipalidades construir Empresas Públicas para garantizar una adecuada prestación de servicios públicos, aprobó la Ordenanza de Creación de la Empresa Pública Municipal de Teléfonos, Agua Potable y Alcantarillado –ETAPA- con atribuciones, funciones, autonomía financiera y personería jurídica, designando como su primer Gerente, al Ing. Fernando Malo Cordero.".

Es así que desde su creación, ETAPA se ha ido fortaleciendo y creciendo acorde al ritmo de la Ciudad y el desarrollo de la tecnología, llegando hoy en día a constituirse en un referente a nivel nacional e internacional por la alta calidad y eficiencia en la prestación de sus servicios de telecomunicaciones, agua potable, alcantarillado y gestión ambiental. (ETAPA, ETAPA EP, 2016)

Objetivos Estratégicos Corporativos.

- Garantizar eficiencia y sostenibilidad.
- Mejorar la satisfacción del cliente.
- Mejorar el clima laboral.
- Diversificar los productos y servicios.

Misión Corporativa: "Somos una empresa pública municipal, ambiental y socialmente responsable, que mejora la calidad de vida de las personas y contribuye al desarrollo de las organizaciones, con un portafolio de productos y servicios innovadores y sostenibles de telecomunicaciones y servicios de agua potable y saneamiento manteniendo los más altos estándares de calidad.".

Visión en Telecomunicaciones: "Al 2019, se la empresa que proporciona soluciones integrales, innovadoras y sostenibles, basadas en las tecnologías de la información y comunicación, liderando la trasformación de Cuenca hacia una ciudad digital; con presencia nacional a través de un portafolio de productos y servicios que permitan fortalecer su desarrollo empresarial.". (ETAPA, ETAPA EP, 2016)

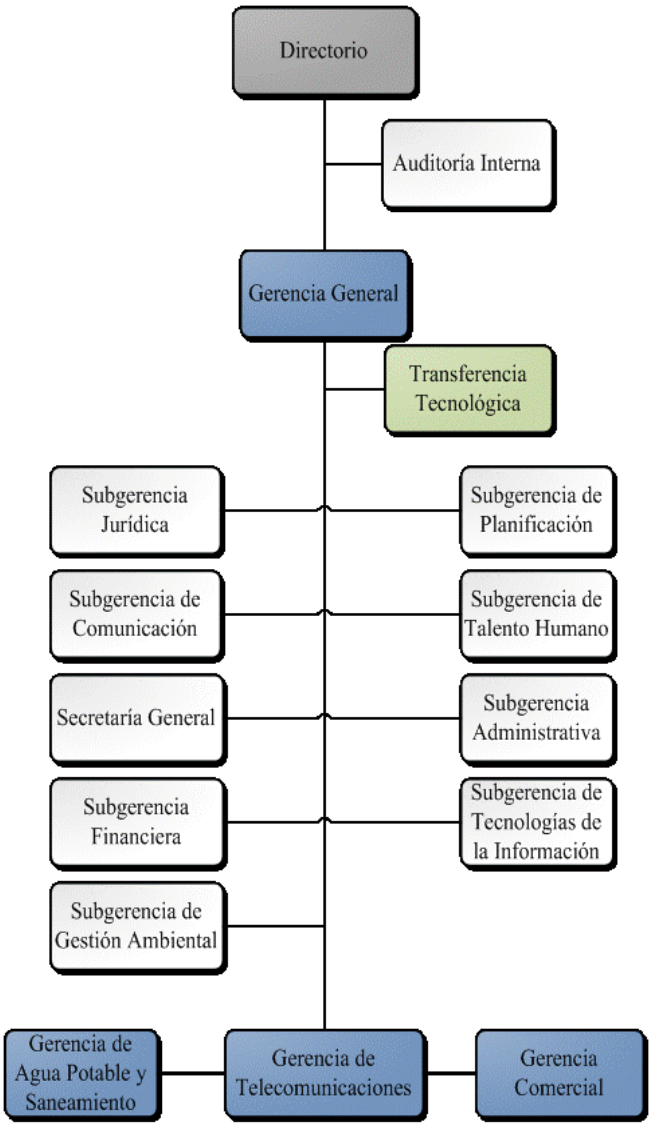


Figura 4. 2: Organigrama ETAPA EP. (ETAPA, ETAPA EP, 2016)

4.1.2. Creación y Gestión del SGSI.

La creación de un Sistema de Gestión de Seguridad de la Información, involucra la creación de una serie de documentos que encaminan a la organización a una certificación ISO 27001, parte de estos documentos son obligatorios para poder alcanzar la certificación y otros sirven de soporte, más no son obligatorios.

Tabla 4. 1: Documento ISO 27000 (Academy, 2016)

DOCUMENTO	**OBLIGATO_ RIEDAD**	**PUNTOS IMPORTANTES DE LA NORMA.**
Procedimiento para Control de Documentos y Registros		NTE INEN-ISO/IEC 27001:2011 apartado 4.3.2
Plan del proyecto		
Identificación de Requisitos		NTE INEN-ISO/IEC 27001:2011 apartado 4.3.1 c) y A.15.1.1
Lista de Requisitos Legales, normativos, contractuales y otros	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.3.1 c) y A.15.1.1
Alcance del SGSI	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.2.1 a)
Política de Seguridad de la Información	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.2.1 b) y 5.1 a)
Metodología de Evaluación y Tratamiento del Riesgo	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.2.1 c)
Cuadro de Evaluación de Riesgos	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.2.1 d) y e)
Cuadro de Tratamiento de Riesgos	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.2.1 f) y g)
Informe de Evaluación y Tratamiento de Riesgos	✓	NTE INEN-ISO/IEC 27001:2011 apartado 8.2 y 8.3
Declaración de Aplicabilidad		NTE INEN-ISO/IEC 27001:2011 apartado 4.2.1 j)

Plan de Tratamiento del Riesgo	✓	NTE INEN-ISO/IEC 27001:2011 apartado 4.2.2 a) y b)
Anexo A. Controles	✓	NTE INEN-ISO/IEC 27001:2011 Anexo A. Controles señalados como aplicables en la Declaración de Aplicabilidad.
Plan de Capacitación y Concienciación	✓	NTE INEN-ISO/IEC 27001:2011 apartado 5.2.2
Procedimiento para Auditoría Interna	✓	NTE INEN-ISO/IEC 27001:2011 apartado 6
Programa Anual de Auditoría		NTE INEN-ISO/IEC 27001:2011 apartado 6
Informe de Auditoría Interna	✓	NTE INEN-ISO/IEC 27001:2011 apartado 6
Lista de Apoyo de Auditoría Interna		NTE INEN-ISO/IEC 27001:2011 apartado 6
Minuta de Revisión de la Dirección	✓	NTE INEN-ISO/IEC 27001:2011 apartado 7.2 y 7.3
Procedimiento para Medidas Correctivas		NTE INEN-ISO/IEC 27001:2011 apartado 8.2
Formulario para Medidas Correctivas	✓	NTE INEN-ISO/IEC 27001:2011 apartado 8.2

En esta etapa del proyecto para la elaboración de los documentos que involucran el alcance de nuestro trabajo, utilizaremos plantillas obtenidas de la página web Academy 27000, aclarando que estos documentos empleados tienen fines meramente académicos y que para su uso comercial; ETAPA EP deberá adquirir los derechos de uso.

4.2. Plantilla de Documentos ISO 27000

El documento consta de:

1. Logo de la organización: Se incluye el logo de la organización.
2. Nombre de la organización: Incluir el nombre de la Persona jurídica.
3. Título del documento: De acuerdo al documento que se redacte.
4. Datos del documento: En este apartado se incluye
    1. Código: Codificación de la organización que consta de 3 partes:
        - FP: Ficha de Proceso.
        - CST: Control de Salas de Telecomunicaciones.
        - 001: Número de Versión de documento.
    2. Versión: Número de versión del documento.
    3. Fecha: Fecha en la que se elabora el documento.
    4. Creado por: Consta el nombre de la o las personas que redactan el documento.
    5. Aprobado por: Consta el nombre de la o las personas que aprueban el documento.
    6. Nivel del Confidencialidad: Se cataloga al documento de acuerdo al nivel de confidencialidad que va a tener como Alto, Medio y Bajo
5. Historial de Modificaciones: En un cuadro en el que se incluya la fecha, versión, el nombre de la o las personas y la descripción de la modificación, se registra cada modificación efectuada al documento.
6. Tabla de contenido: Se incluye el detalle del documento, en el mismo de incluirá siempre:
    1. Objetivo, Alcance y Usuarios del documento.
    2. Documentos de Referencia: Se detalla todos los documentos que sirvieron de referencia para la elaboración del presente documento.

3. Abreviaturas y Definiciones: Se incluye las abreviaturas utilizadas, así como definiciones de terminología básica.
4. Validez y Gestión del documento. Se detalla la fecha de validez del documento redactado, así como los períodos de gestión que se dará al mismo.
5. Apéndices: Documentos derivados del principal.
6. Firmas: Constancia de participación y aprobación del documento.

EMPRESA PÚBLICA MUNICIPAL DE TELECOMUNICACIONES, AGUA POTABLE, ALCANTARILLADO Y SANEAMIENTO "ETAPA EP"

[TÍTULO DEL DOCUMENTO]

Código:	XXXXX- VERSIÓN
Versión:	000000
Fecha de la Versión:	Día / mes / año
Creado por:	XXXXXXXXXX
Aprobado por:	XXXXXXXXXXXXX
Nivel de Confidencialidad:	Alto – Medio o Bajo

Historial de Modificaciones.

Fecha	Versión	Creado Por	Descripción de la modificación.

Tabla de contenido

4.3. Documentos Para el SGSI.

4.3.1. Plan de Proyecto.

El Plan de proyecto es un documento no obligatorio dedicado a describir generalidades del proyecto.

En este se incluye informaciones adicionales a la obligatoria dada en la plantilla general, tales como: (Se incluye en Anexo X: Plan De Proyecto Para La Implementación Del Sistema De Gestión De Seguridad De La Información Dirigido Al Control De Accesos A Las Salas De Telecomunicaciones)

- Objetivo del proyecto.
- Resultado esperados del proyecto
- Organización del proyecto: Incluye el detalle de las personas y los cargos que ejercen cada uno en el proyecto (promotor, gerente, coordinador, equipo de proyecto)
- Cuadro de participantes del proyecto
- Principales riesgos del Plan
- Herramientas para la implementación del proyecto y generación de informes.
- Gestión de registros guardados en base al documento.

4.3.2. Identificación de Requisitos.

Documento no obligatorio en el que se aborda dos aspectos: El primero es definir los documentos legales, normativos, contractuales y documentos de otra índole que estén involucrados con la Seguridad de la Información en el Control de Accesos a la Salas de Telecomunicaciones; y en el segundo punto se determina las partes inmersas en el SGSI, es decir Gerencias, Subgerencias, Direcciones Departamentales, áreas y/o personal relacionado directa o indirectamente con la administración y manejo de las Salas.

En este apartado se incluye la siguiente información adicional a la puntualizada en la plantilla utilizada: (Se incluye como ANEXO XI: Procedimiento Para la Identificación de Requisitos en el Proceso de Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones)

- Identificación de requisitos.

- Responsabilidades.
- Revisión y evaluación.
- Gestión de registros guardados en base al documento
- Y como apéndice se incluye un listado de los requisitos legales, normativos, contractuales y de otra índole que se utilizan en la elaboración del documento. Aclaramos en este punto que la información que se debe llenar en este apéndice lo debe hacer la organización, dejándoles el formato listo para su uso (Se incluye como ANEXO XI: Procedimiento Para La Identificación De Requisitos En El Proceso De Implementación Del Sistema De Gestión De Seguridad De La Información Dirigido Al Control De Accesos A Las Salas De Telecomunicaciones, Apéndice A).

4.3.3. Alcance del SGSI.

Documento habilitante que se redacta al inicio y en el que se detalla los límites del proyecto en términos de las características de la actividad comercial de la organización, ubicación, activos y tecnología. Incluye en su contenido (Se incluye en ANEXO XII: Alcance del Proyecto Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones)

- Definición del Alcance, en donde se hace una presentación breve de la organización, seguido de una justificación clara y concisa de los límites, identificando los procesos que se ven inmersos en el control de Accesos a las Salas de Telecomunicaciones, la ubicación exacta y las exclusiones del SGSI.

4.3.4. Política de Seguridad.

El establecimiento de este documento es de vital importancia para la implantación del SGSI en la organización. Es de acceso público, redactado y aprobado por la Alta Dirección. En su contenido adicional al detallado en la plantilla utilizada se incluye: (Se detalla en el ANEXO XIII: Política de Seguridad del Sistema de Gestión de

Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones)

- Fijar el o los objetivos generales para el SGSI.
- Determinar roles y responsabilidades para la revisión y establecimiento de nuevos objetivos del SGSI.
- Fijar quien o quienes son los responsables en la determinación de los controles de seguridad individuales o grupales agregados en la Declaración de Aplicabilidad.
- Determinar la periodicidad de las revisiones de los objetivos (se recomienda de por lo menos una vez al año).
- La organización medirá el cumplimiento de todos los objetivos, asignando un responsable, quien se encargará de definir el método a utilizarse para medir el cumplimiento de los objetivos. Las revisiones métricas se las deben efectuar por lo menos una vez al año con la redacción de un reportar de novedades para la dirección.
- Crear programas de capacitación y concienciación en el tema de Seguridad de la Información para el control de accesos a las Salas de Telecomunicaciones.
- Crear un sistema de comunicación de la Política a implementarse.
- Se determina el apoyo a brindar para la implementación del SGSI.

4.3.5. Evaluación y Tratamiento del Riesgo.

Existe una amplia gama de metodologías para la gestión del riesgo, y todas siguen una misma secuencia. Se inicia con la identificación y valoración de los activos de la organización en cuanto a la confidencialidad, disponibilidad e integridad, seguido de la identificación de las amenazas a las que pueden estar expuestos dichos activos y que podrían desembocar en una vulnerabilidad a la seguridades de la organización, y finalmente se realiza una evaluación de los controles existentes haciendo un comparativo con los que proponen implementar en el Plan de Tratamiento de Riesgos con miras a mejorar los sistemas de seguridad ya existentes (Se incluye como ANEXO

XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones)

4.3.5.1. Identificación de Activos.

Magerit es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica dirigida a tecnología de la información, dividida en tres libros que contienen en su Tomo I el Método de Análisis y Gestión de Riesgos, en el Tomo II el Dimensionamiento de Activos, Criterios de Valoración, Amenazas y Salvaguardas; en su Tomo III las Técnicas de Medición del Riesgo.

Para nuestro trabajo Magerit nos ha proporcionado en su libro II un catálogo conformado por un grupo de 12 tipos de activos definiendo en cada grupo a los activos específicos no siendo estos fijos sino pudiendo variar de acuerdo a la actividad económica, características y servicios de la organización. Para nuestro fin se ha determinado que los tipos de activos involucrados son cinco y un total de 22 activos específicos. En esta etapa del trabajo con la ayuda del personal de ETAPA EP se logró identificar a los propietarios o responsables de cada uno de los activos a su cargo. (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice A).

4.3.5.2. Dimensionamiento de Activos.

El dimensionamiento de los activos nos da una idea de las características o atributos que hacen valioso al activo en cuanto a su confidencialidad, disponibilidad e integridad utilizando el criterio de valoración que va desde 1 como bajo y 3 como alto (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice B).

Tabla 4. 2: Dimensionamiento de Activos en cuanto a su Confidencialidad. (Dirección General de Modernización Administrativa, 2012)

CONFIDENCIALIDAD BAJA	1	Cuando el activo es de acceso público sin que se vea afectada la información que en éste se maneje.
CONFIDENCIALIDAD MEDIA	2	Cuando el activo es de acceso privado, teniendo acceso el personal (interno, contratado y terceras partes) de la empresa. En este caso, si la información es revelada a personas ajenas a la organización, las operaciones de la empresa no se ven afectadas considerablemente.
CONFIDENCIALIDAD ALTA	3	Cuando el activo es de acceso restringido al que tienen acceso personal o departamentos específicos. Si la información manejada por el activo es revelada causaría graves daños a la organización.

Tabla 4. 3: Dimensionamiento de Activos en cuanto a su Disponibilidad. (Dirección General de Modernización Administrativa, 2012)

DISPONIBILIDAD BAJA	**1**	Cuando el desempeño de la organización no se ve afectado si el activo no se encuentra disponible.
DISPONIBILIDAD MEDIA	2	Cuando el activo no se encuentra disponible, pudiendo afectar el desempeño normal de la organización, pero pueden existir acciones de contingencia que permitan continuar el desarrollo normal de la empresa o podría esperar a que se reestablezca el activo.
DISPONIBILIDAD ALTA	3	Cuando el activo es de gran valor y es afectado provocando consecuencias graves a las operaciones de la organización.

Tabla 4. 4: Dimensionamiento de Activos en cuanto a su Integridad. (Dirección General de Modernización Administrativa, 2012)

INTEGRIDAD BAJA	**1**	Activo de información en donde los datos modificados carecen de valor apreciable, es decir al ser alterados no suponen preocupación alguna.
INTEGRIDAD MEDIA	2	Activo de información que requiere integridad, pero si los datos son modificados las operaciones en la organización no se ven afectadas gravemente.
INTEGRIDAD ALTA	3	Activo de información que al ser modificado, alterado o falsificado su contenido de manera voluntaria, intencionada o accidental, las operaciones de la organización se ven afectadas gravemente.

4.3.5.3. Amenazas.

Las amenazas o también denominadas en múltiples bibliografías como riesgos, se podría definir como la causa potencial de la materialización de un incidente de seguridad que puede causar daños a un sistema de información o a la organización. Se podría decir que es la parte medular de la Evaluación de Riesgos.

Las amenazas específicas las obtenemos del mismo libro de Magerit donde se nos proporciona un catálogo de amenazas clasificadas por su origen en 4 grupos: (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice C)

- Amenazas de Origen Natural
- Amenazas de Origen Industrial
- Amenazas causadas por las personas de manera accidental, y
- Amenazas caudadas por las personas de manera deliberada.

Ya con las amenazas identificadas, y una vez establecido que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo en dos sentido:

- ***Consecuencia:*** Mide el daño causado por un incidente en el supuesto que ocurriera, es decir cuán perjudicado resultaría el activo.

Tabla 4. 5: Dimensionamiento de la Consecuencia de la Amenaza. (Dirección General de Modernización Administrativa, 2012)

CONSECUENCIA BAJA	**1**	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, la obligación legal o contractual o el prestigio de la organización (activo no se afecta gravemente).
CONSECUENCIA MEDIA	2	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización (activo se afecta regularmente).
CONSECUENCIA ALTA	3	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización (activo se afecta gravemente).

- ***Frecuencia de Ocurrencia:*** Expresa cuán frecuente se puede materializar la amenaza. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia.

Tabla 4. 6: Dimensionamiento de la Frecuencia de ocurrencia de la Amenaza. (Dirección General de Modernización Administrativa, 2012)

FRECUENCIA BAJA	**1**	Los controles existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. La frecuencia de ocurrencia es de una vez al año o menos.
FRECUENCIA MEDIA	2	Los controles existentes son moderados y en general han suministrado un adecuado nivel de protección. La frecuencia de ocurrencia de incidentes es de una vez cada 6 meses o menos.
FRECUENCIA ALTA	3	Los controles existentes son bajos o deficientes. La frecuencia de ocurrencia de incidentes es de al menos una vez al mes.

4.3.5.4. Vulnerabilidades.

Vulnerabilidad refiere al impacto y riesgo al que estarían expuestos los activos si no se protegieran adecuadamente, es decir son aquellos procedimientos o mecanismos tecnológicos que incrementan el riesgo en la organización. Frente a cada amenaza se puede presentar una o varias vulnerabilidades, pudiendo ser sus propietarios o causantes de las mismas agentes externos a la organización o las personas o entidades a cargo del activo.

De similar manera que se procedió en los apartados que anteceden a este punto, existe un catálogo de vulnerabilidades que nos sirven de base para poder identificar las que afectan a nuestros activos, no pudiendo ser exactamente las mismas que actúen a ETAPA EP, pues éstas dependen de las características que presenta cada organización, por lo que para este caso particular nosotros las hemos definido. (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice D)

Como referencia, podemos valorar las vulnerabilidades para ETAPA EP utilizando los criterios de valoración expuestos a continuación.

Tabla 4. 7: Dimensionamiento de Controles Existentes. (Dirección General de Modernización Administrativa, 2012) (ISO, NTE INEN-ISO/IEC 27005/2012, 2012)

BAJO CONTROL DE SEGURIDAD	**3**	No cuentan con ningún control de seguridad.
CONTROL DE SEGURIDAD MEDIO	2	Cuentan con controles de seguridad medios que ayudan a prevenir la ocurrencia de algunas amenazas.
ALTO CONTROL DE SEGURIDAD	**1**	Cuentan con controles de seguridad funcionales y adecuados para evitar la ocurrencia de amenazas.

4.3.5.5. Estimación del Riesgo.

En las metodologías para la estimación del riesgo se utiliza el método cualitativo, el cuantitativo o lo que muy frecuentemente es empleado la combinación de las dos dependiendo de las circunstancias. Nosotros hemos venido utilizando la valoración cuantitativa, pues el riesgo al que se ve expuesta la organización se expresa como el producto de la consecuencia con la frecuencia de ocurrencia.

$$R = A * B$$

R ⟹ Estimación de Riesgo

A ⟹ Consecuencia (cuan perjudicado se vería el activo)

B ⟹ Frecuencia de ocurrencia.

Es así que una vez determinada la metodología de evaluación, se reunió a todos los departamentos o áreas involucradas en este proyecto con el objetivo de que siendo ellos quienes están inmersos en la realidad del día a día, sean quienes nos proporcionen los datos requeridos en ésta evaluación. (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice E)

Figura 4. 3: Proceso de Evaluación de Riesgos

Figura 4. 4: Procesos de Evaluación de Riesgos

Figura 4. 5: Proceso de Evaluación de Riesgos

4.3.5.6. Criterios para Tratamiento del Riesgo.

Con la revisión de los datos obtenidos en la evaluación o estimación del riesgo, se puede observar que los valores de los resultados fluctúan entre 1 y 9, por lo que se determina la escala de catalogación de riesgos para nuestros activos de la siguiente manera:

- El valor de 1 será catalogado como un nivel de riesgo muy bajo (MB).
- Los valores de 2 y 3 serán catalogados como riesgos bajos (B).
- Los valores de 4 y 5 serán catalogados como riesgos bajos (M).
- Los valores de 6 y 7 serán catalogados como riesgos bajos (A).
- Los valores de 8 y 9 serán catalogados como riesgos bajos (MA).

Se detalla a continuación la matriz de riesgos establecida para poder proceder con la etapa de tratamiento del riesgo.

Tabla 4. 8: Matriz Cuantitativa del Riesgo. (Dirección General de Modernización Administrativa, 2012) (ISO, NTE INEN-ISO/IEC 27005/2012, 2012) (FERMA, 2002)

		FRECUENCIA		
		1	**2**	**3**
CONSECUENCIA	**1**	1	2	3
	2	2	4	6
	3	3	6	9

Tabla 4. 9: Matriz Cualitativa del Riesgo. (Dirección General de Modernización Administrativa, 2012) (ISO, NTE INEN-ISO/IEC 27005/2012, 2012) (FERMA, 2002)

		FRECUENCIA		
		B	**M**	**A**
CONSECUENCIA	**B**	MB	B	B
	M	B	M	A
	A	B	A	MA

Se define conjuntamente con los coordinadores del proyecto que para el caso particular de ETAPA EP, los riesgos aceptables serán los que hayan obtenido valores entre 1 y 3; mientras que los riesgos no aceptables serán los que hayan obtenido valores entre 4 y 9. En el caso en el que el riesgo es considerado como no aceptable, la organización debe elegir entre cuatro opciones de tratamiento del riesgo para cada uno de las amenazas (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice F):

1. ***Reducir el Riesgo***: ETAPA EP toma la decisión de reducir el riesgo mediante la selección e implementación de controles tomados del Anexo A de la norma NTE INEN-ISO/IEC 27001:2011 u otros controles de seguridad. Al seleccionar esta opción, es necesario evaluar en nuevo valor de vulnerabilidad en el Cuadro de Tratamiento de Riesgos con la finalidad de evaluar la efectividad de los controles planificado.

2. ***Aceptar o Retener el Riesgo***: En la norma NTE INEN-ISO/IEC 27001:2011 se cita "asumir los riesgos de manera consciente y objetiva, conforme a las políticas de la organización y a los criterios de aceptación de riesgo" (apartado 4.2.1 literal f.2). Es así que ETAPA toma la decisión de aceptar el riesgo basándose en los resultados de la evaluación del riesgo, y si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.

3. ***Evitar el Riesgo:*** La organización decide evitar las actividades o acciones que dan origen al riesgo, retirándolas de las operaciones ya planificadas, o mediante el cambio en las condiciones bajo las cuales se efectúa. Esta decisión por lo general se toma en los casos en los que los costos para la implementación son más elevados que los que causarían la materialización del riesgo.

4. ***Transferir el Riesgo***: Se debe transferir el riesgo a terceras partes que puedan gestionarlo de manera más eficaz (compañías de seguridad, seguros o proveedores). (ISO, NTE INEN-ISO/IEC 27005/2012, 2012)

4.3.5.7. Resultados de Evaluación de Riesgo.

A partir de los datos obtenidos en el proceso de evaluación, y ya establecida la metodología para el tratamiento del riesgo, podemos interpretar los resultados en varios aspectos.

4.3.5.8. Expresión Gráfica del Riesgo Global.

Tabla 4. 10: Resultado de Activos Evaluados

TOTAL ACTIVOS CON RIESGO = 14	TOTAL ACTIVOS SIN RIESGO = 5	TOTAL ACTIVOS NO EXISTENTES = 3
Equipo Biométrico	Credenciales	Cercas Eléctricas
Sistemas de Video	Datos de Validación de Credenciales	Documentos Internos
Alarmas y Sensores	Registros de Actividades	Bases de Datos
Ficheros	Reglamento Interno de Trabajo	
Copias de Respaldo	Usuarios Externos	
Datos de Gestión Interna		
Datos de Control de Acceso		
Contratos		
Manuales		
Documentos de Capacitaciones		
Planificaciones		
infraestructura		
Visitas		
Usuarios Internos		

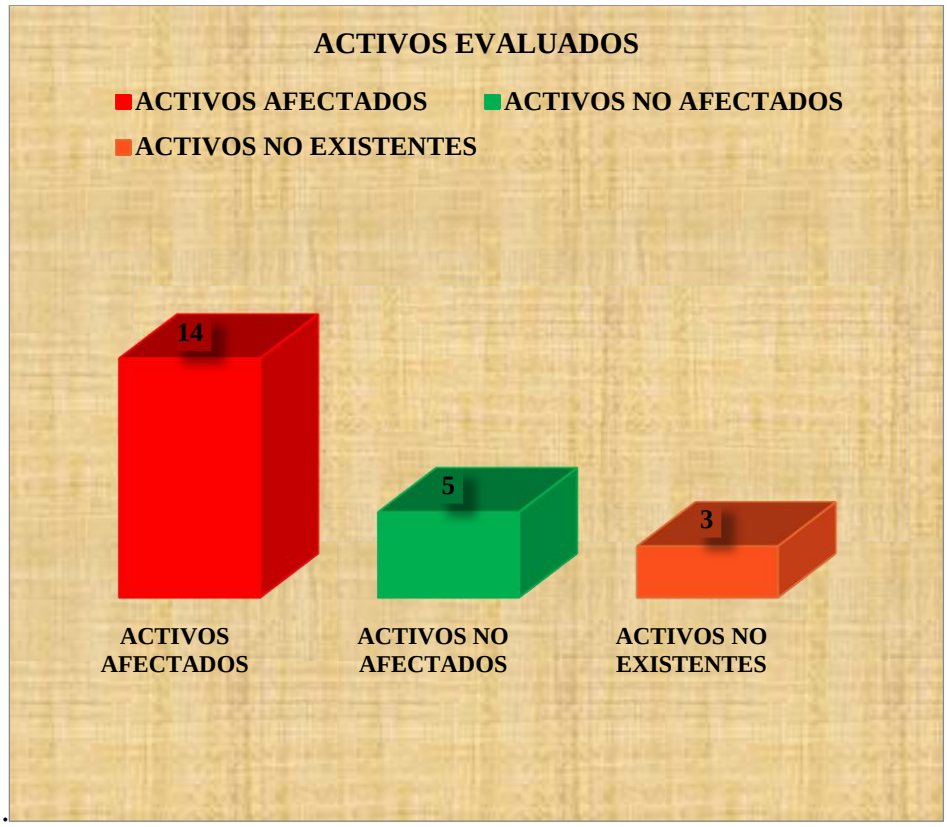


Figura 4. 6: Resultados de Evaluación de Riesgos

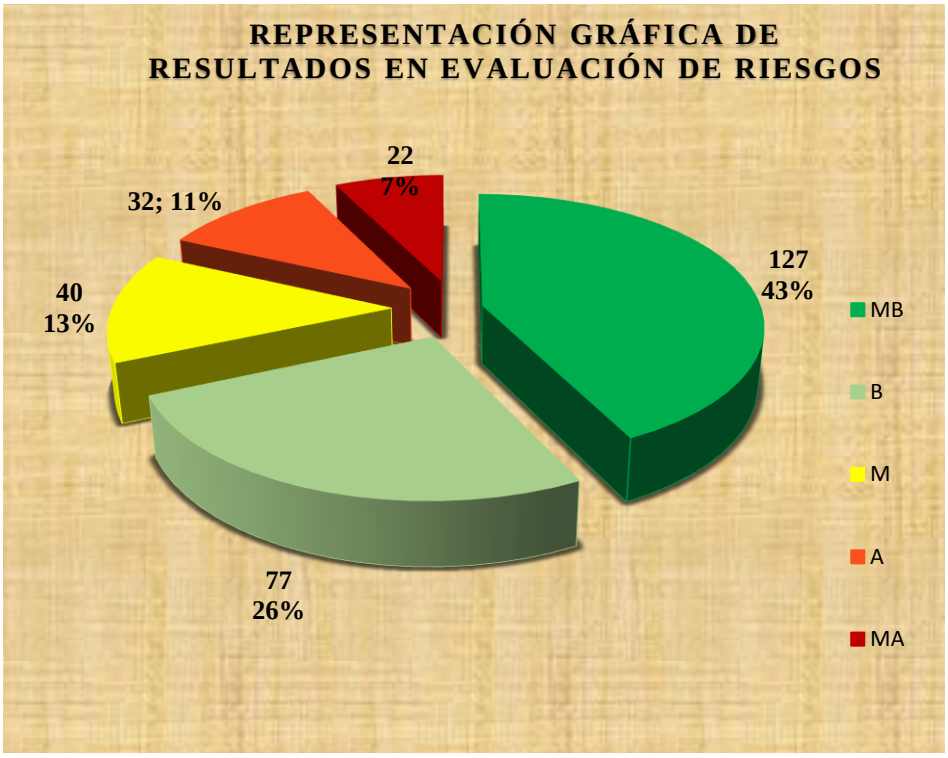


Figura 4. 7: Resultado de Evaluación de Riesgos: Amenazas

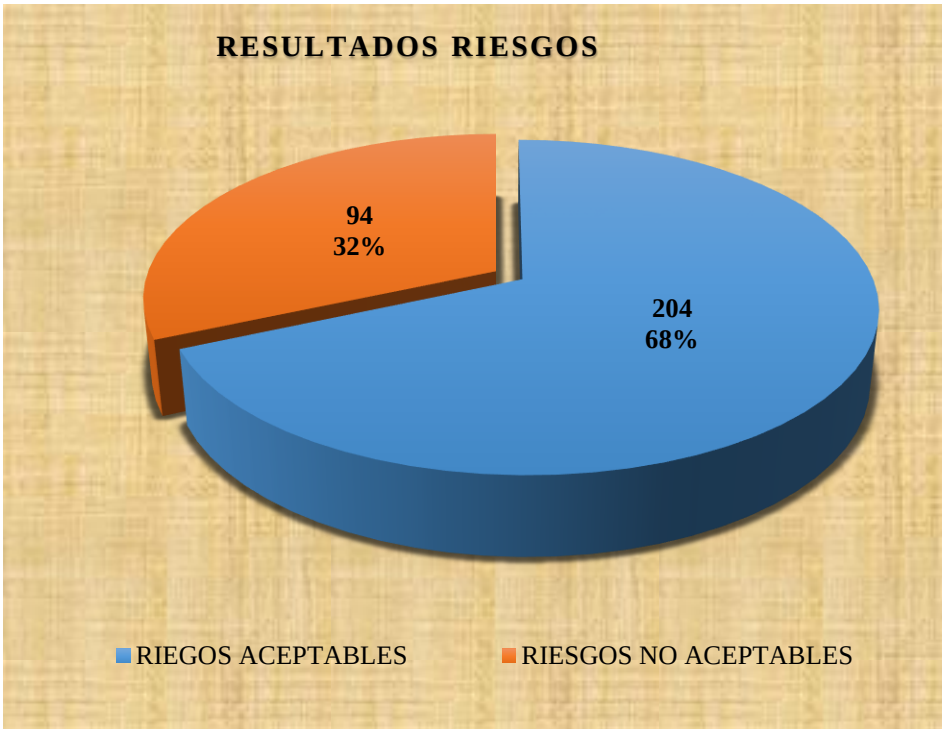


Figura 4. 8: Resultado de Riesgos: Criterio de Tratamiento

4.3.5.9. Resultados Evaluación Activo Equipo Biométrico.

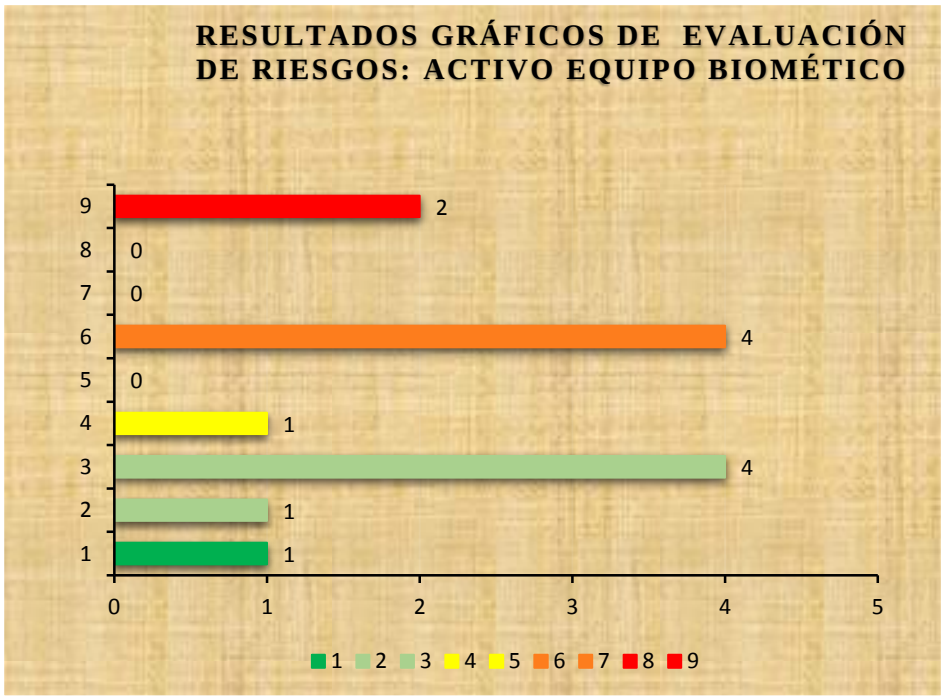


Figura 4. 9: Resultado de Riesgos: Equipo Biométrico

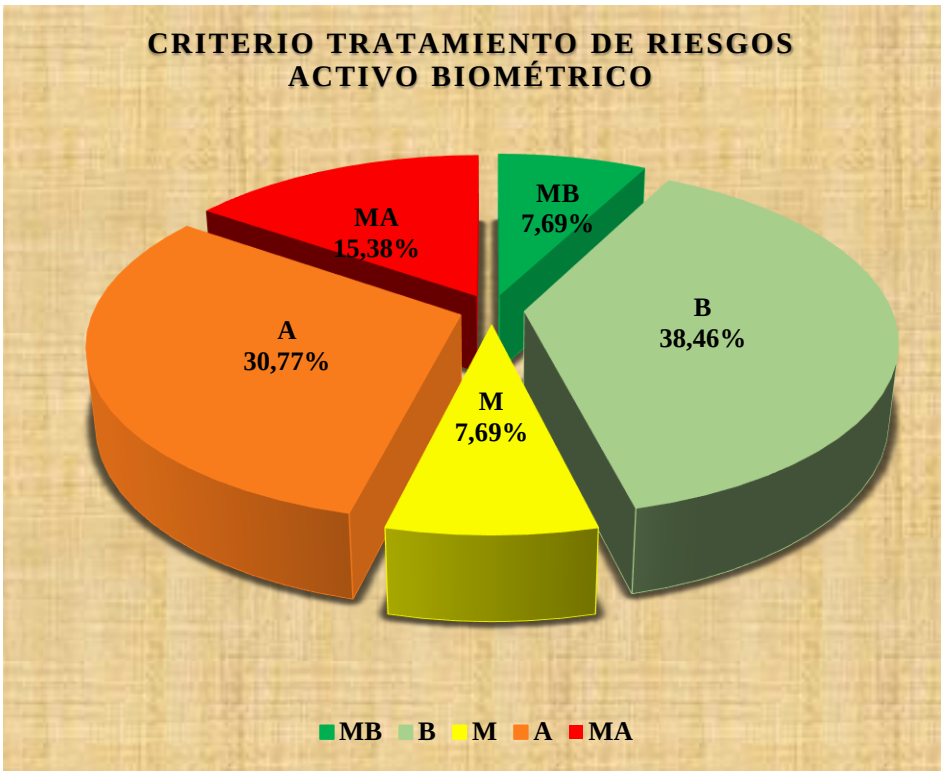


Figura 4. 10: Criterio de Tratamiento de Riesgo: Equipo Biométrico

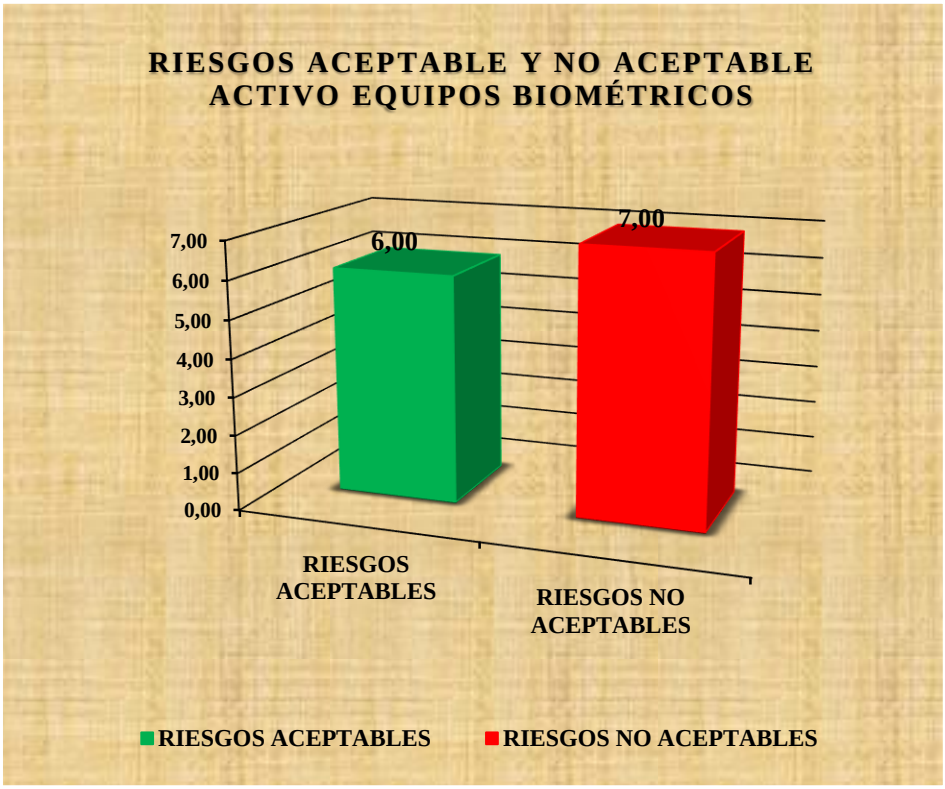


Figura 4. 11: Riesgo Aceptable y no Aceptable: Equipo Biométrico

4.3.5.10. Resultados Evaluación Activo Sistemas de Video

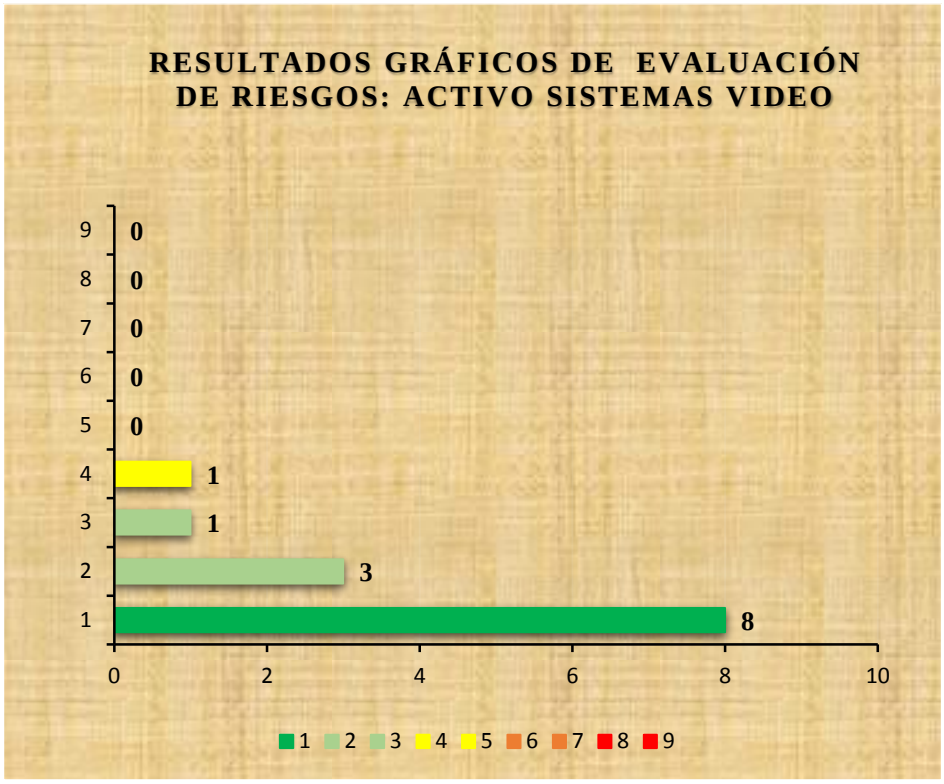


Figura 4. 12: Resultado de Riesgo: Sistemas de Video

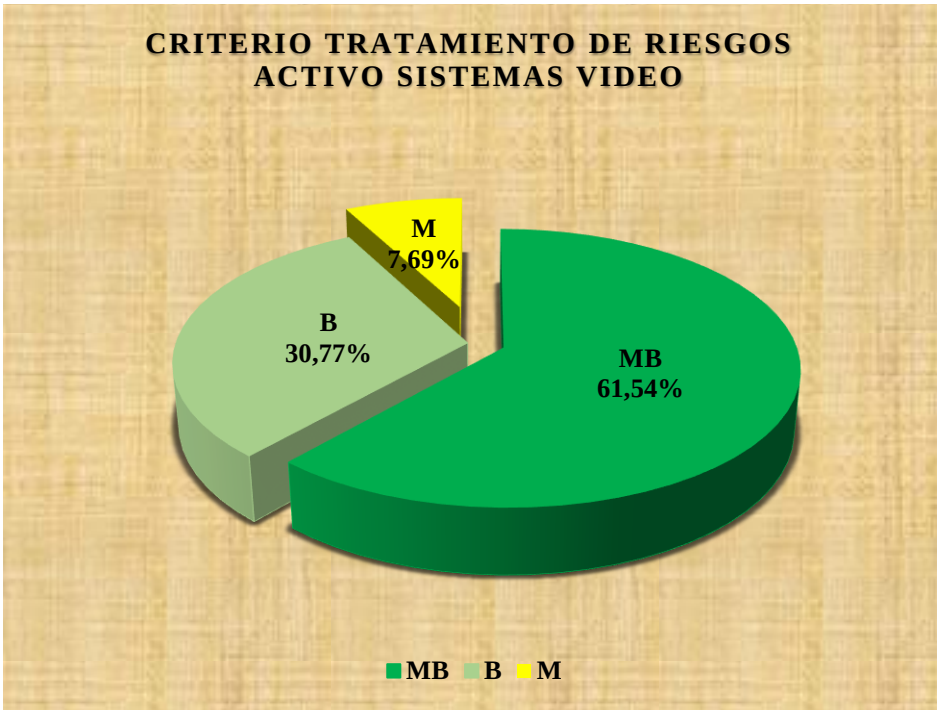


Figura 4. 13: Criterio de Tratamiento de Riesgos: Sistemas de Video

Figura 4. 14: Riesgos Aceptables y no Aceptable: Sistemas de Video

4.3.5.11. Resultados Evaluación Activo Alarmas y Sensores

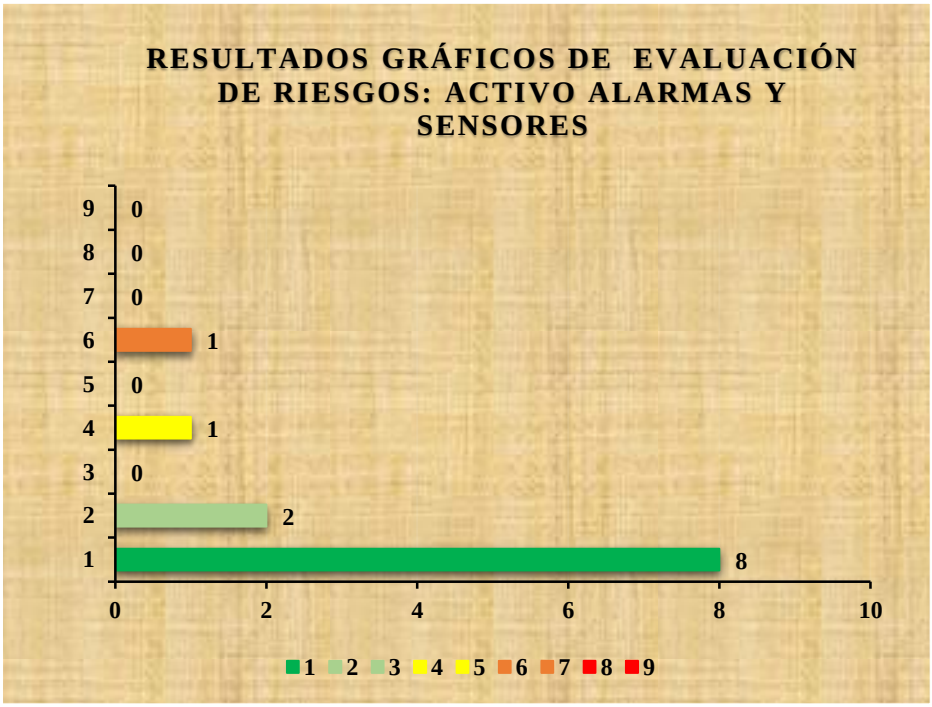


Figura 4. 15: Resultado de Riesgos: Alarmas y Sensores

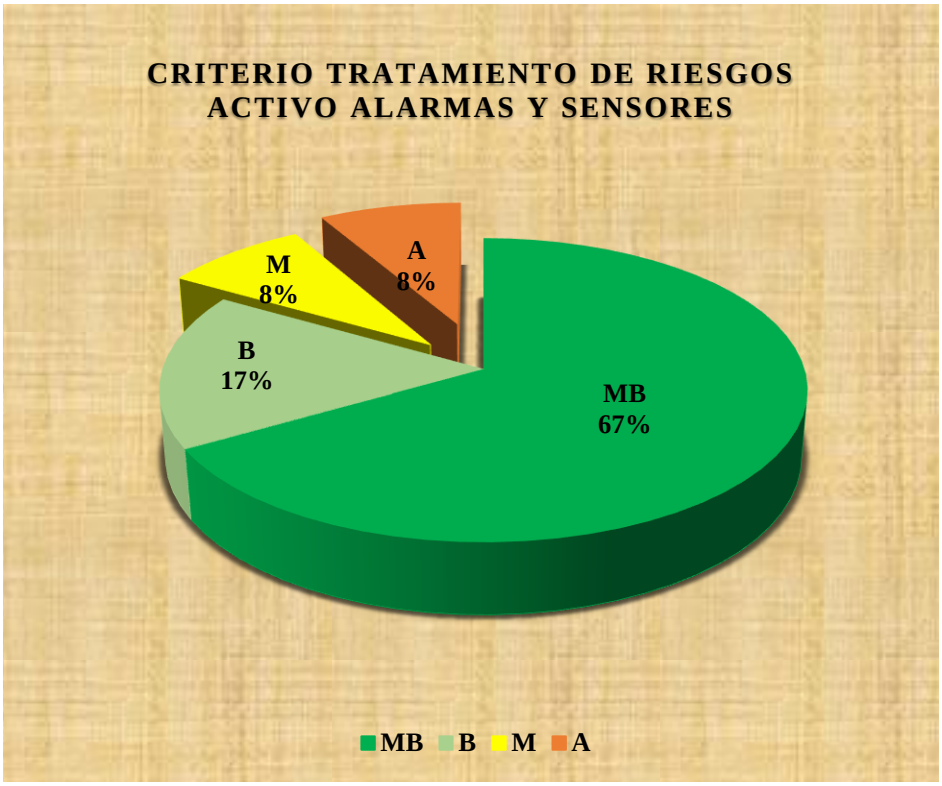


Figura 4. 16: Criterio de Tratamiento de Riesgos: Alarmas y Sensores

.

Figura 4. 17: Riesgos Aceptables y no Aceptables: Alarmas y Sensores

4.3.5.12. Resultados Evaluación Activo Ficheros

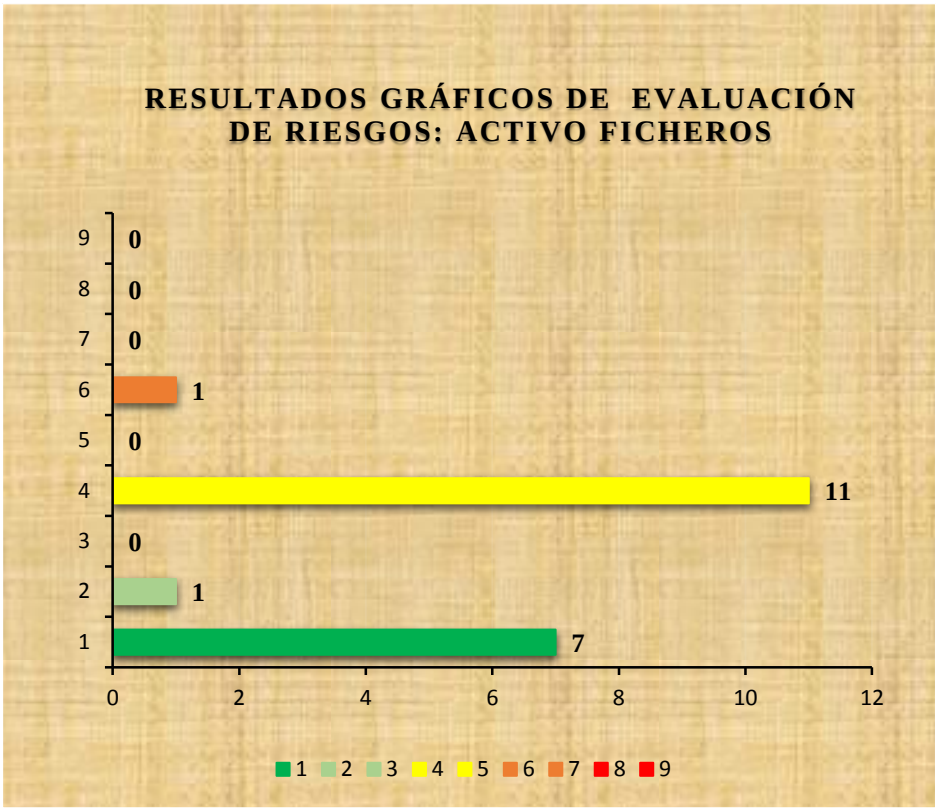


Figura 4. 18: Resultados de Riesgo: Ficheros

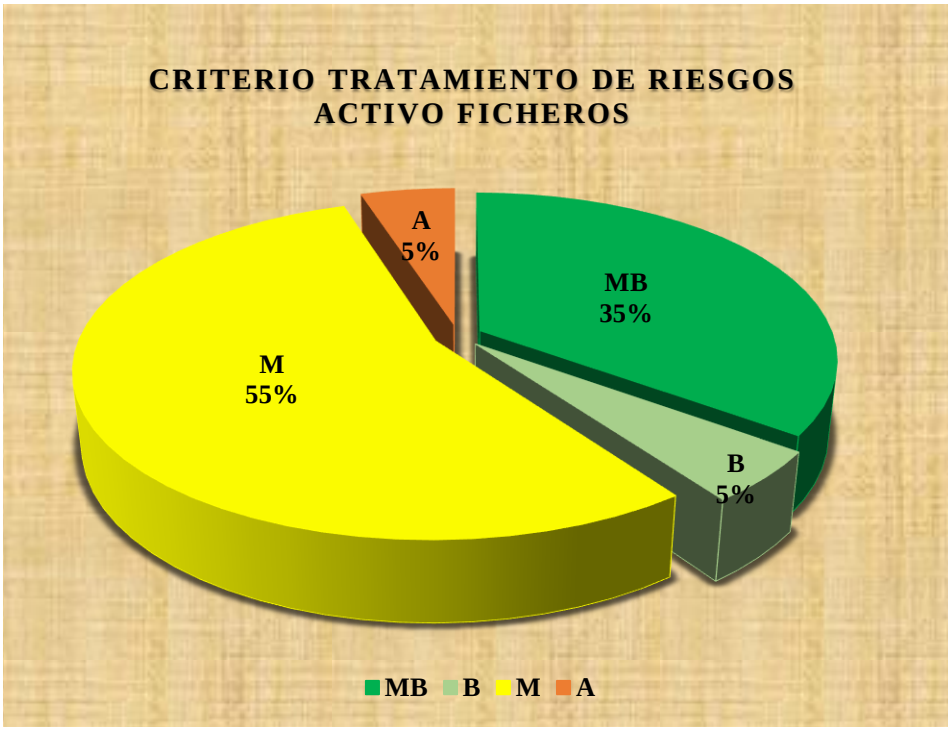


Figura 4. 19: Criterio de Tratamiento de Riesgo: Ficheros

Figura 4. 20: Riesgos Aceptables y no Aceptables. Ficheros

.

4.3.5.13. Resultados Evaluación Activo Copias de Respaldo

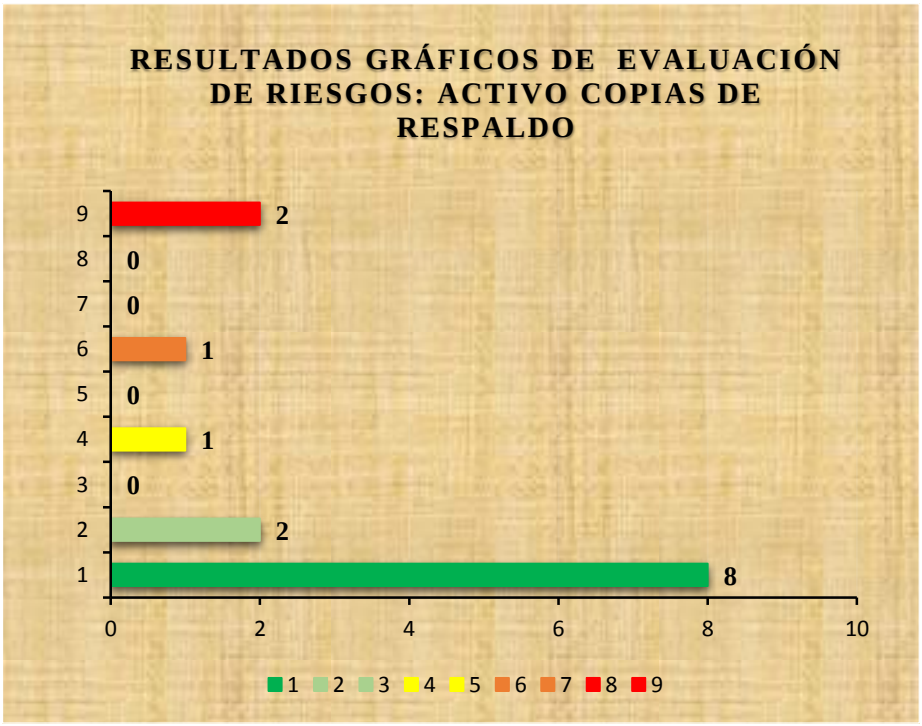


Figura 4. 21: Resultados de Riesgo: Copias de Respaldo

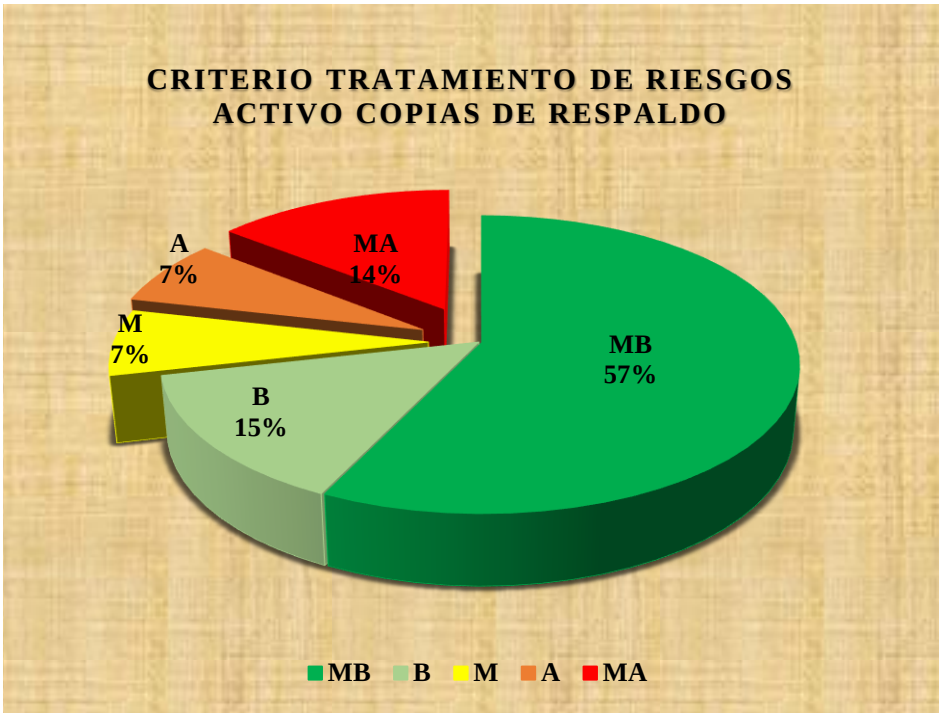


Figura 4. 22: Criterio de Tratamiento de Riesgo: Copias de Respaldo

Figura 4. 23: Riesgos Aceptables y no Aceptables: Copias de Seguridad

4.3.5.14. Resultados Evaluación Activo Datos de Gestión Interna

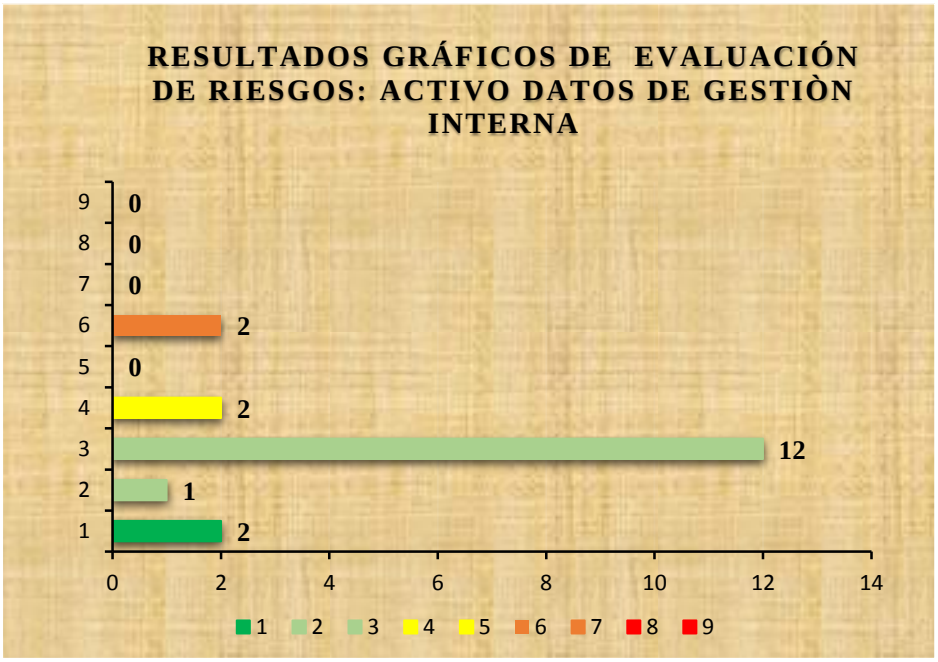


Figura 4. 24: Resultado de Riesgo: Datos de Gestión Interna

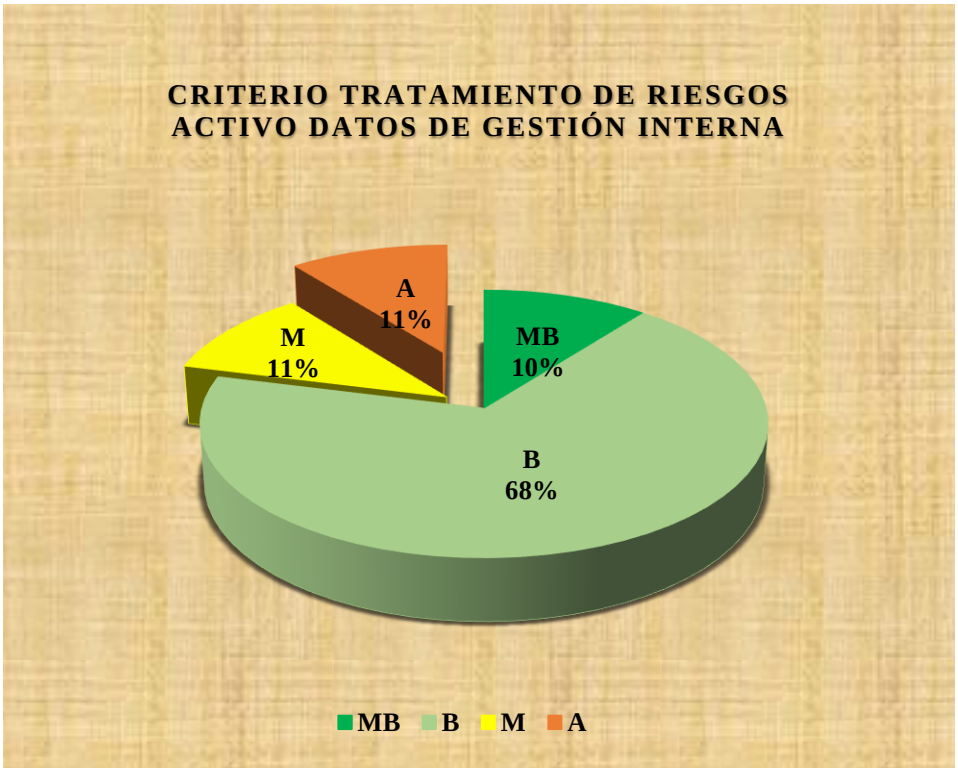


Figura 4. 25: Criterio de Tratamiento de Riesgo: Datos de Gestión Interna

Figura 4. 26: Riesgos Aceptables y no Aceptables: Datos de Gestión Interna

4.3.5.15. Resultados Evaluación Activo Credenciales

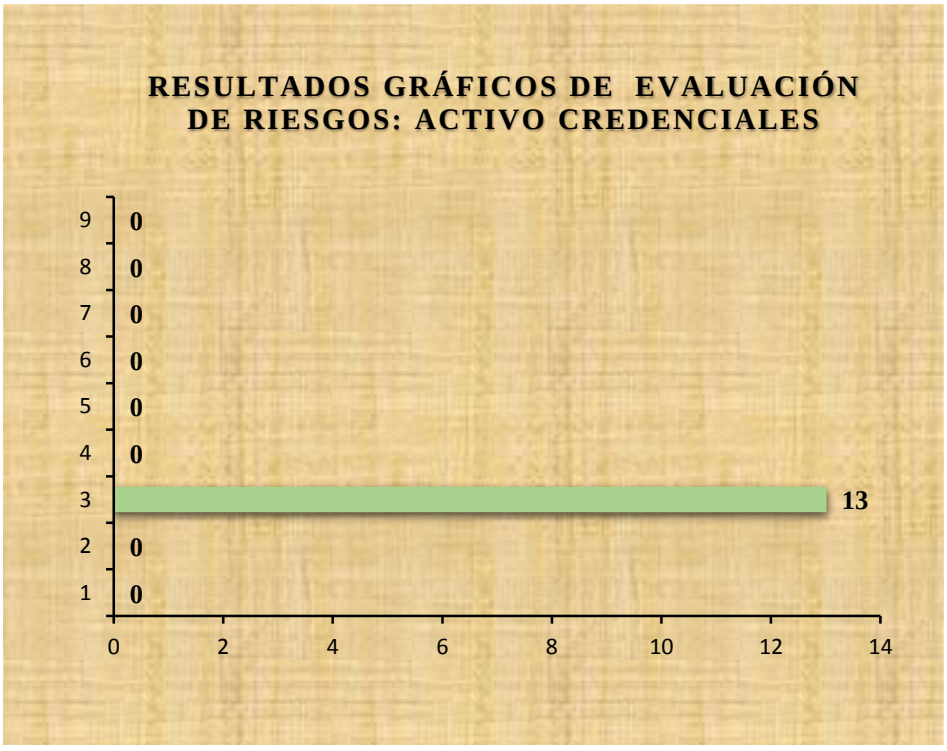


Figura 4. 27: Resultados de Riesgo: Credenciales

Figura 4. 28: Criterio de Tratamiento de Riesgos: Credenciales

Figura 4. 29: Riesgos Aceptables y no Aceptables: Credenciales

4.3.5.16. Resultados Evaluación Activo Datos de Validación de Credenciales

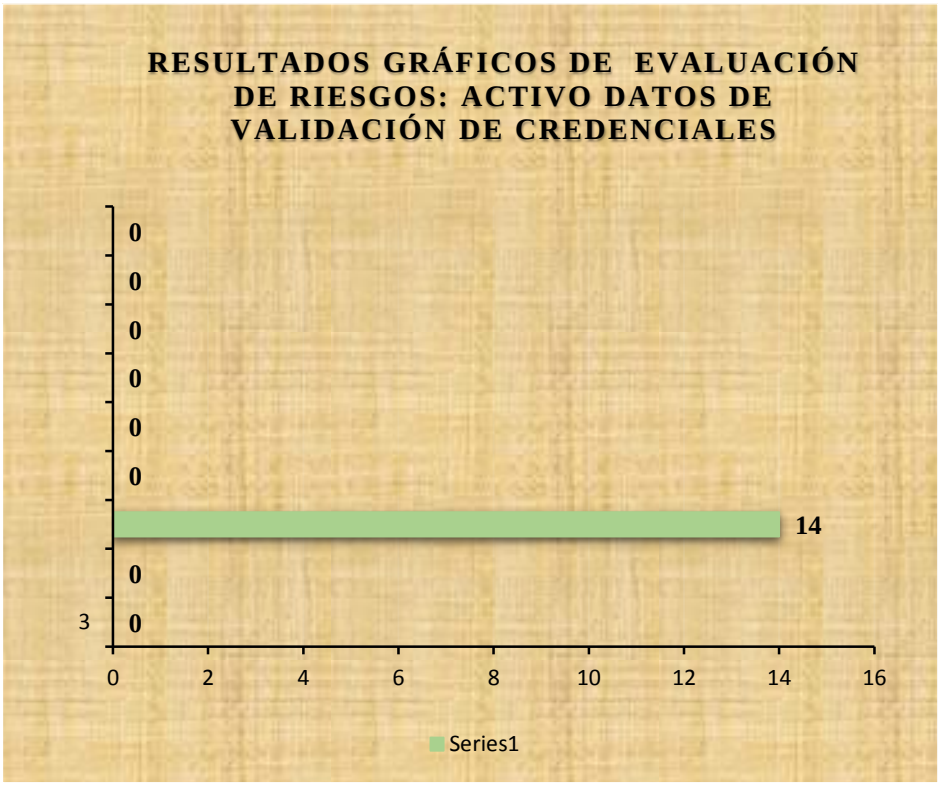


Figura 4. 30: Resultados de Riesgo: Validación de Credenciales

Figura 4. 31: Criterio de Tratamiento de Riesgo: Validación de Credenciales

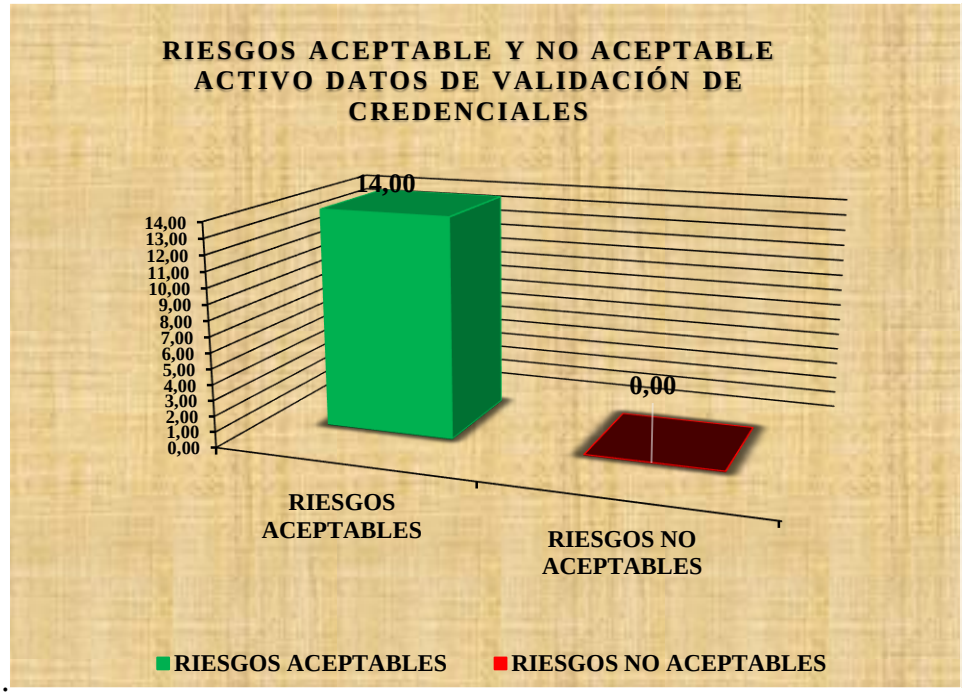


Figura 4. 32 Riesgos Aceptables y no Aceptables: Validación de Credenciales:

4.3.5.17. Resultados Evaluación Activo Datos de Control de Acceso

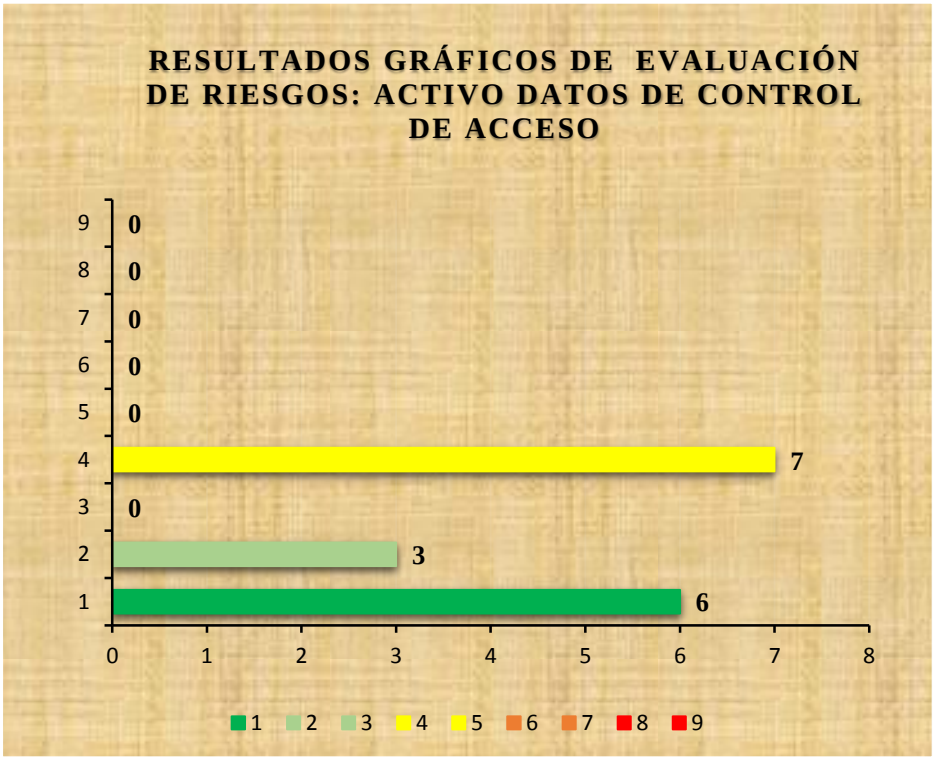


Figura 4. 33: Resultados de Riesgo: Datos de Control de Acceso

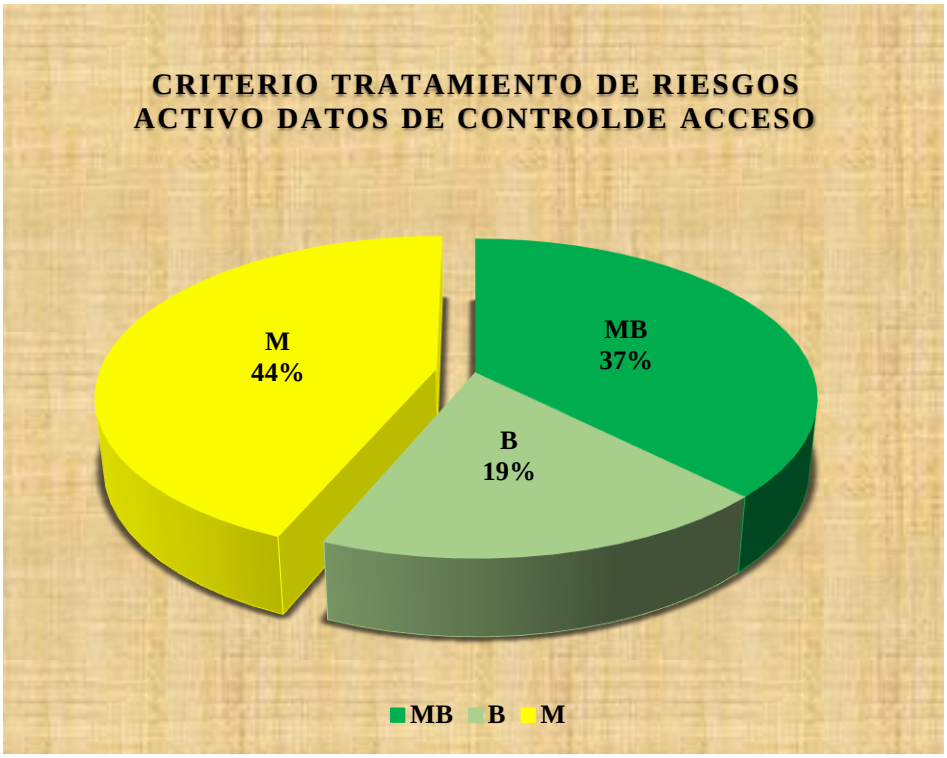


Figura 4. 34: Criterio de Tratamiento de Riesgo: Datos de Control de Acceso

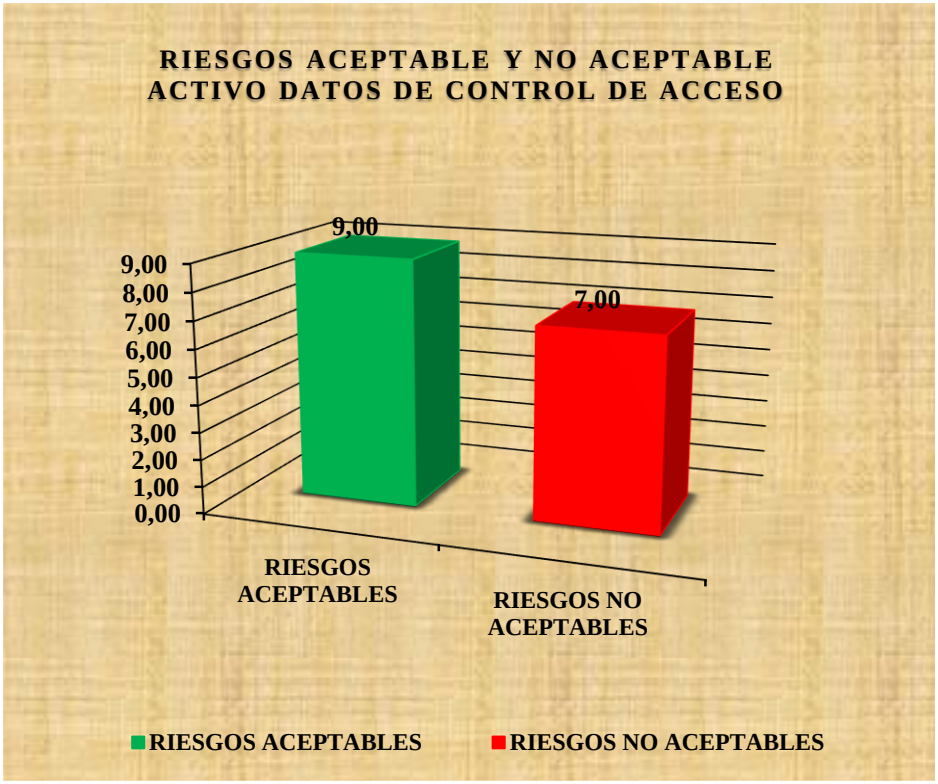


Figura 4. 35: Riesgos Aceptables y no Aceptables: Datos de Control de Acceso

4.3.5.18. Resultados Evaluación Activo Registros de Actividades

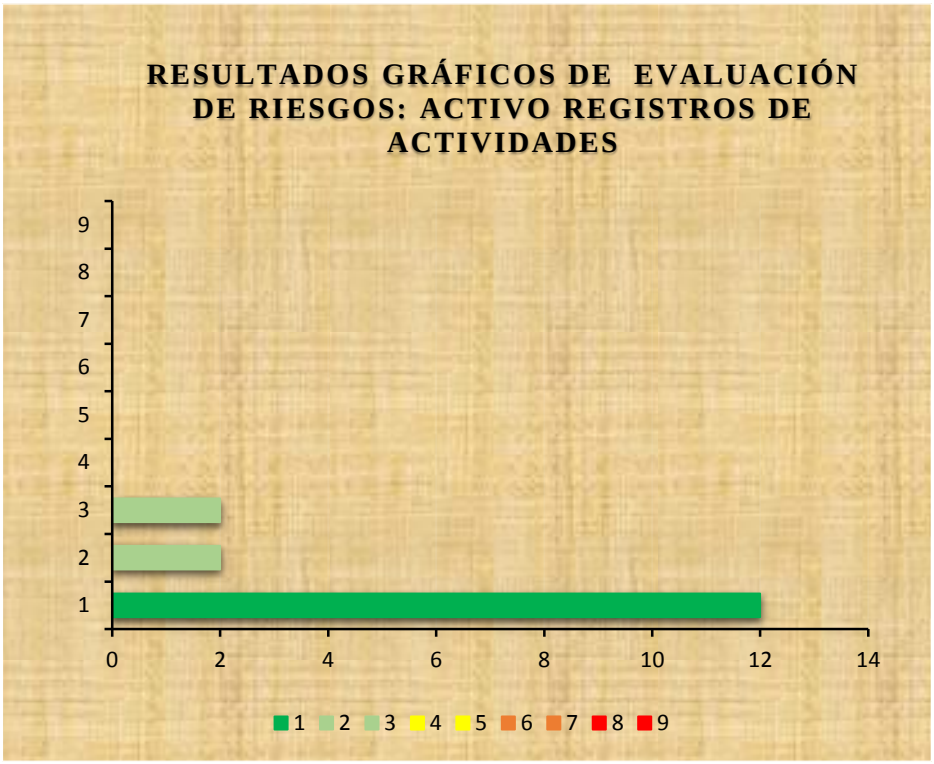


Figura 4. 36: Resultado de Riesgo: Registro de Actividades

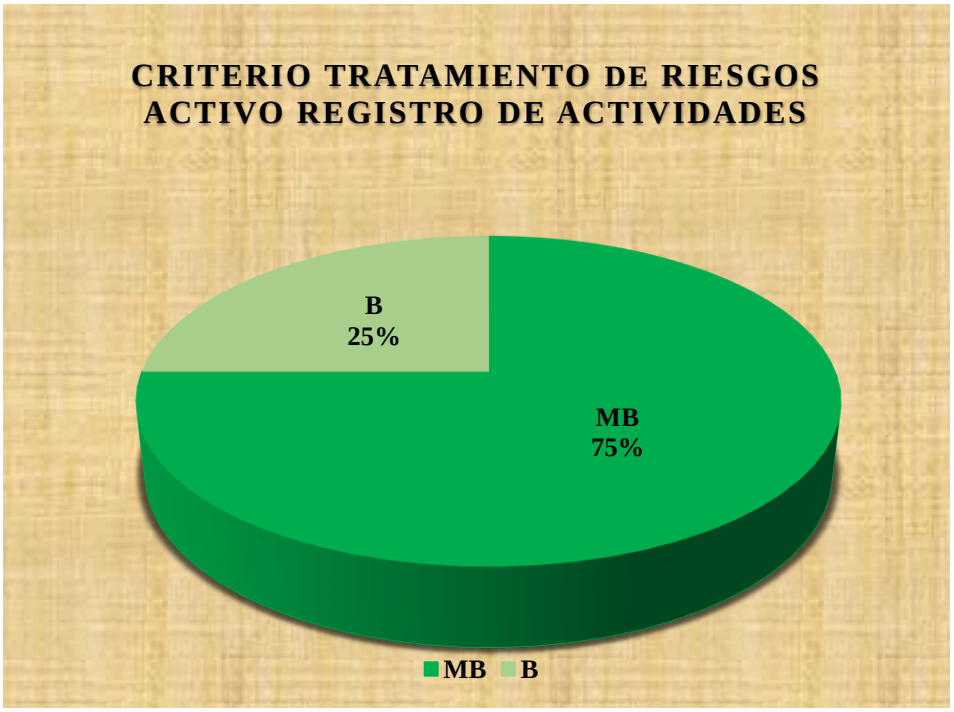


Figura 4. 37: Criterio de Tratamiento de Riesgo: Registro de Actividades

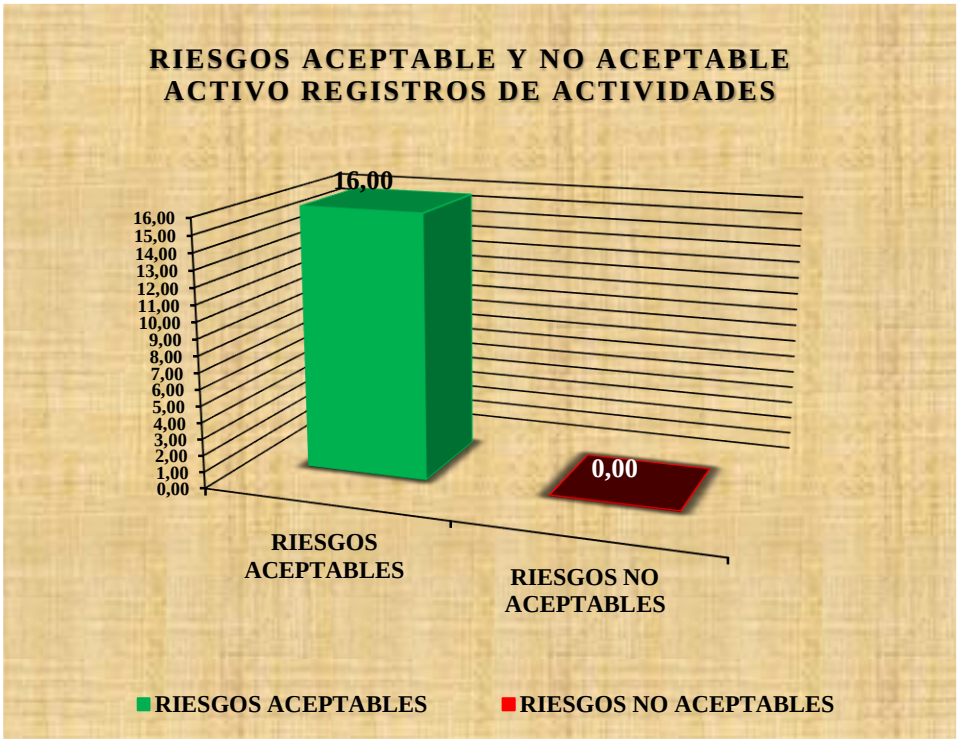


Figura 4. 38: Riesgos Aceptables y no Aceptables: Registro de Actividades

.

4.3.5.19. Resultados Evaluación Activo Contratos

Figura 4. 39: Resultado de Riesgo: Contratos

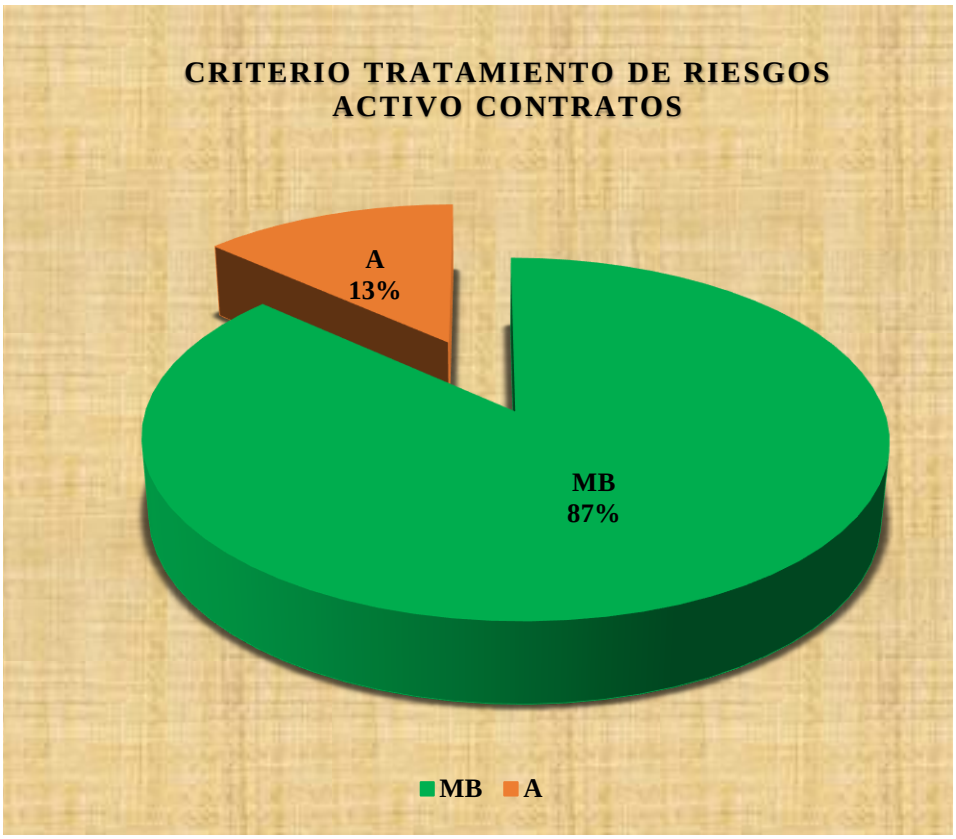


Figura 4. 40: Criterio de Tratamiento de Riesgo: Contratos

Figura 4. 41: Riesgos Aceptables y no Aceptables. Contratos

4.3.5.20. Resultados Evaluación Activo Manuales

Figura 4. 42: Resultados de Riesgo: Manuales

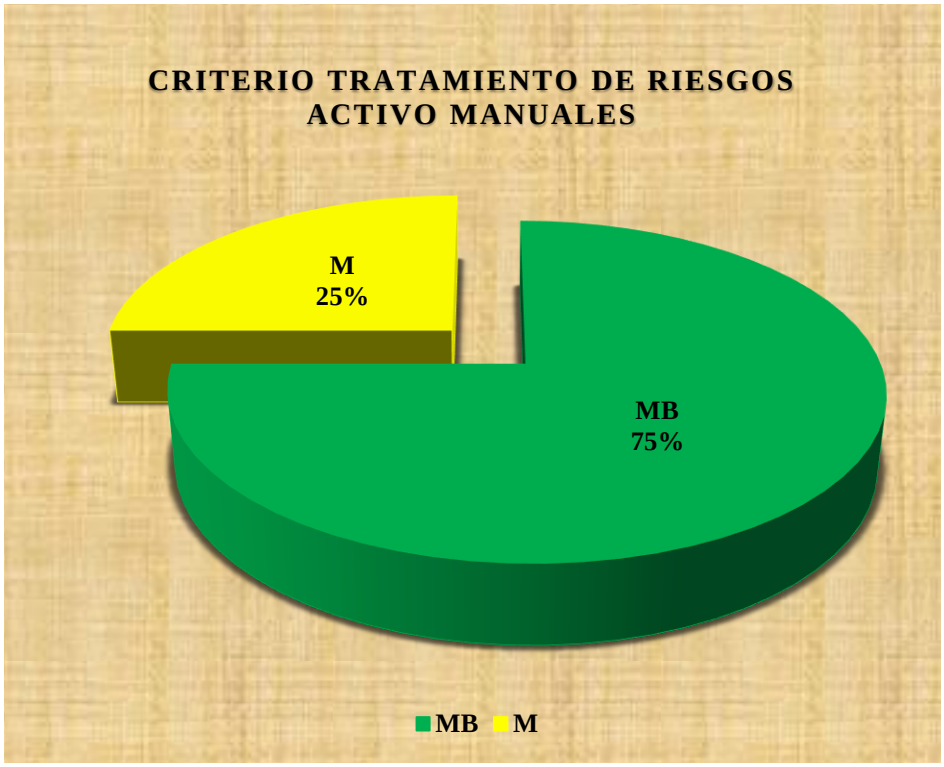


Figura 4. 43: Criterio de Tratamiento de Riesgo: Manuales

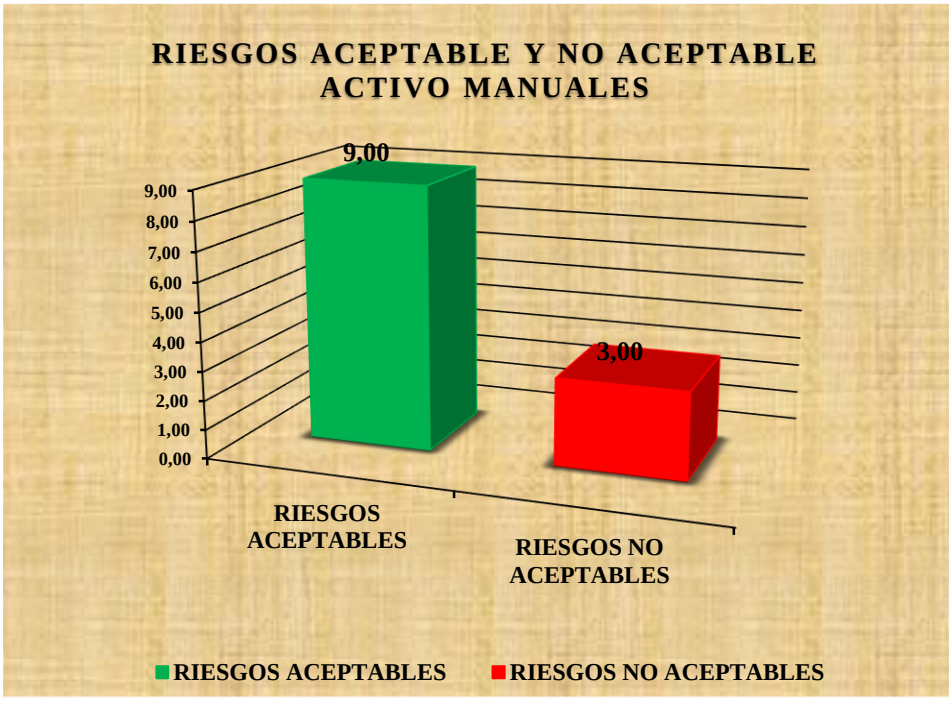


Figura 4. 44: Riesgos Aceptables y no Aceptables: Manuales

.

4.3.5.21. Resultados Evaluación Activo Reglamento Interno de Trabajo

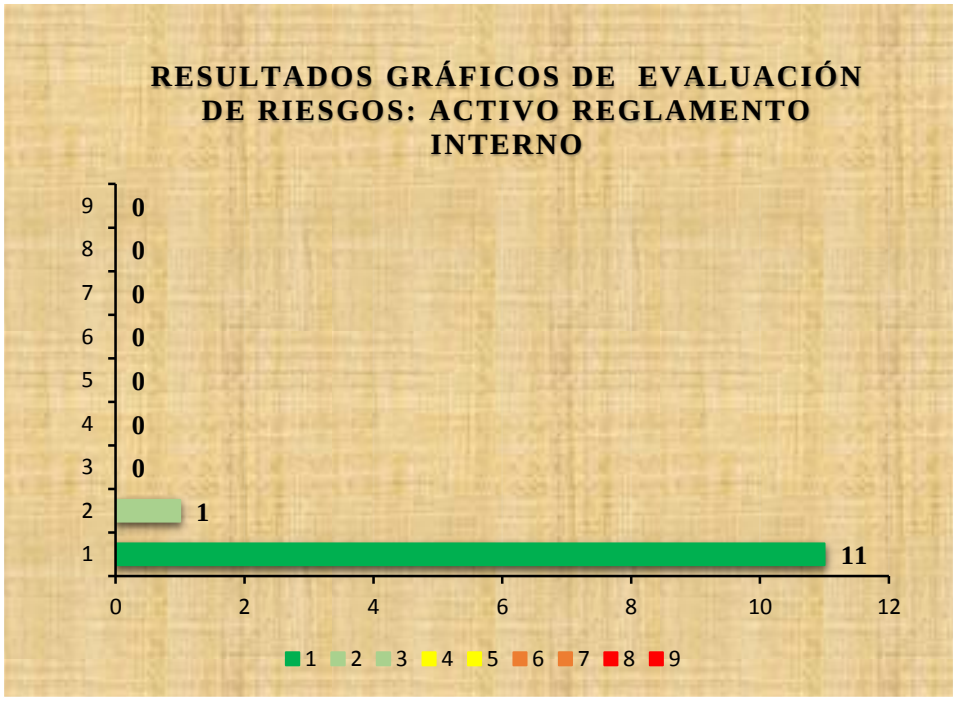


Figura 4. 45: Resultados de Riesgo: Reglamento Interno de Trabajo

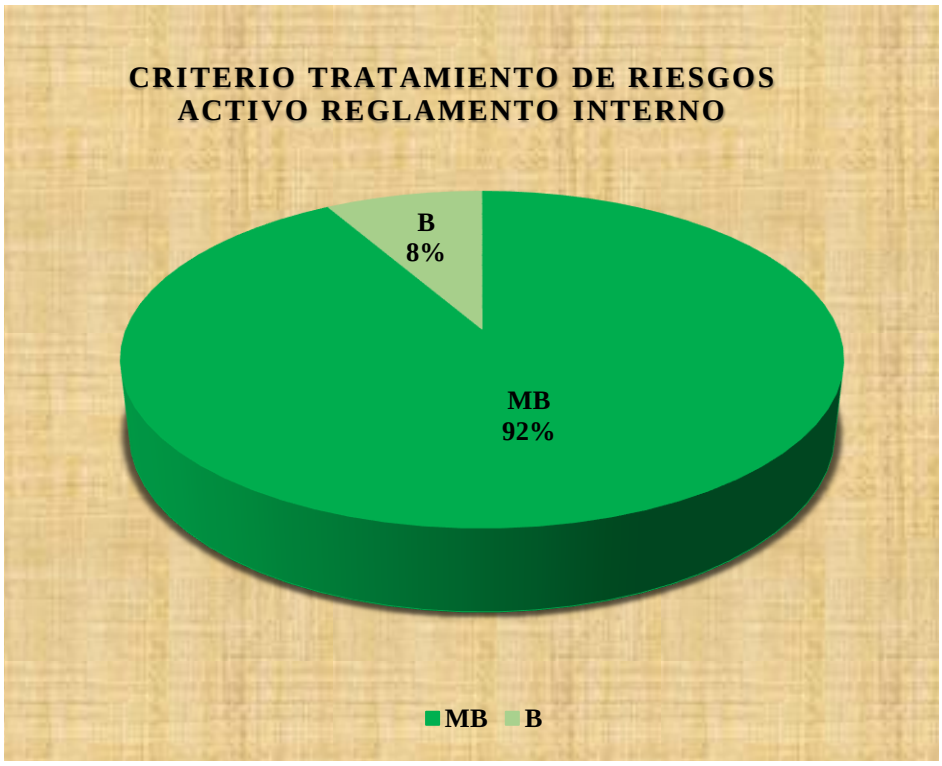


Figura 4. 46: Criterio de Tratamiento de Riesgo: Reglamento Interno de Trabajo

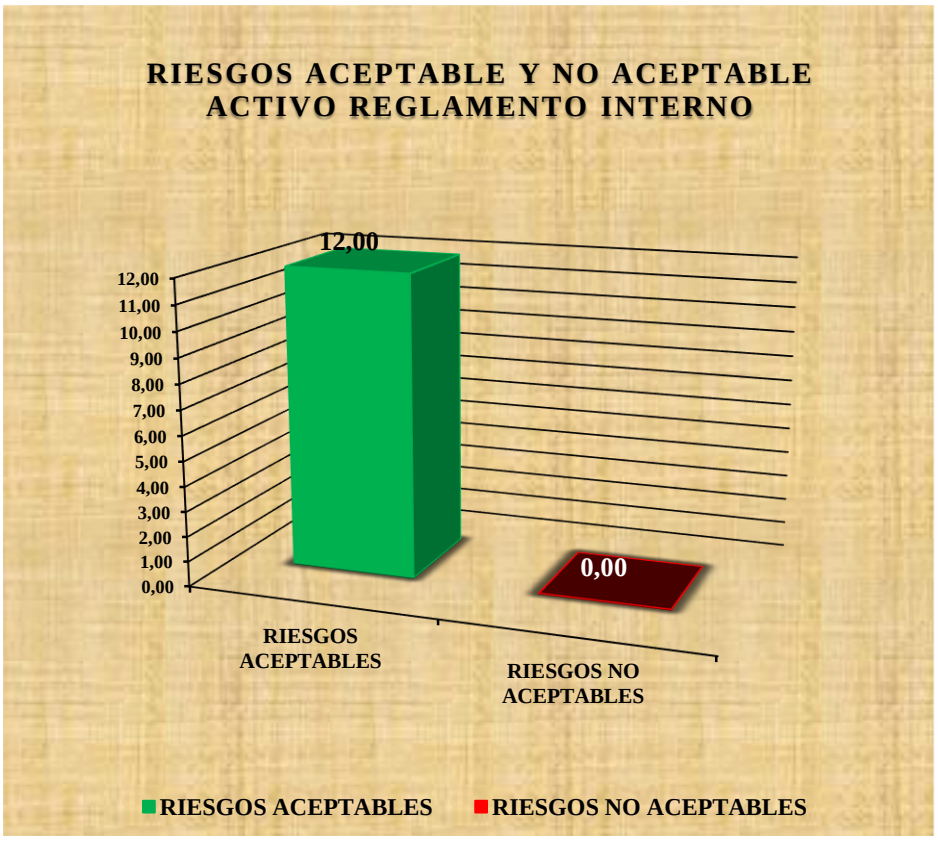


Figura 4. 47: Riesgos Aceptables y no Aceptables: Reglamento Interno de Trabajo

4.3.5.22. Resultados Evaluación Activo Documentación de Capacitación

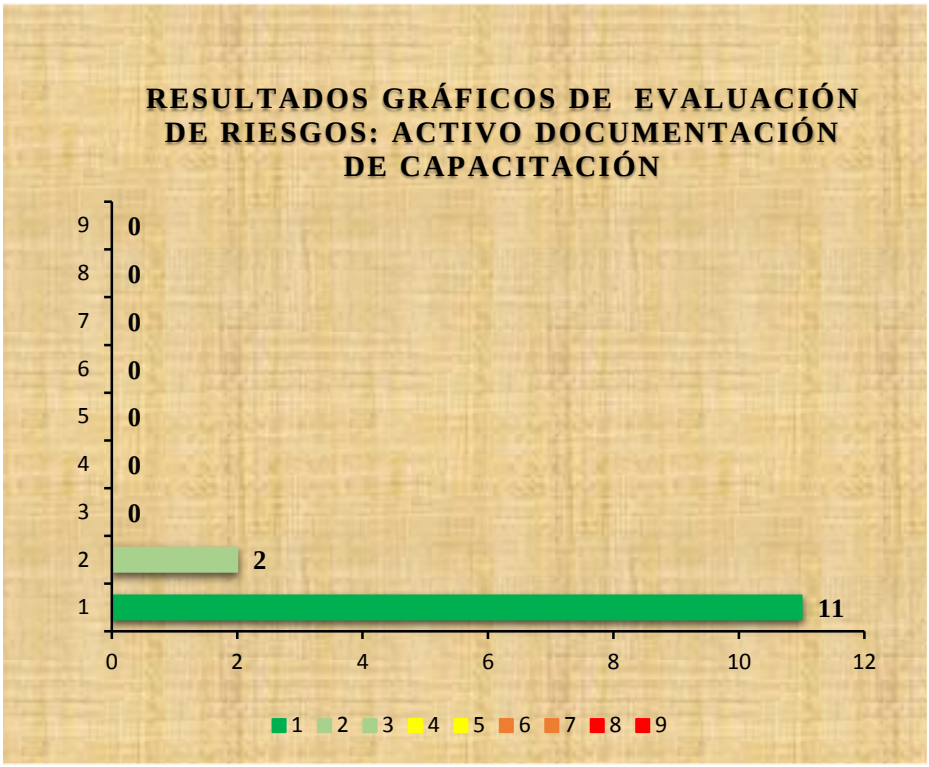


Figura 4. 48: Resultados de Riesgo: Documentos de Capacitación

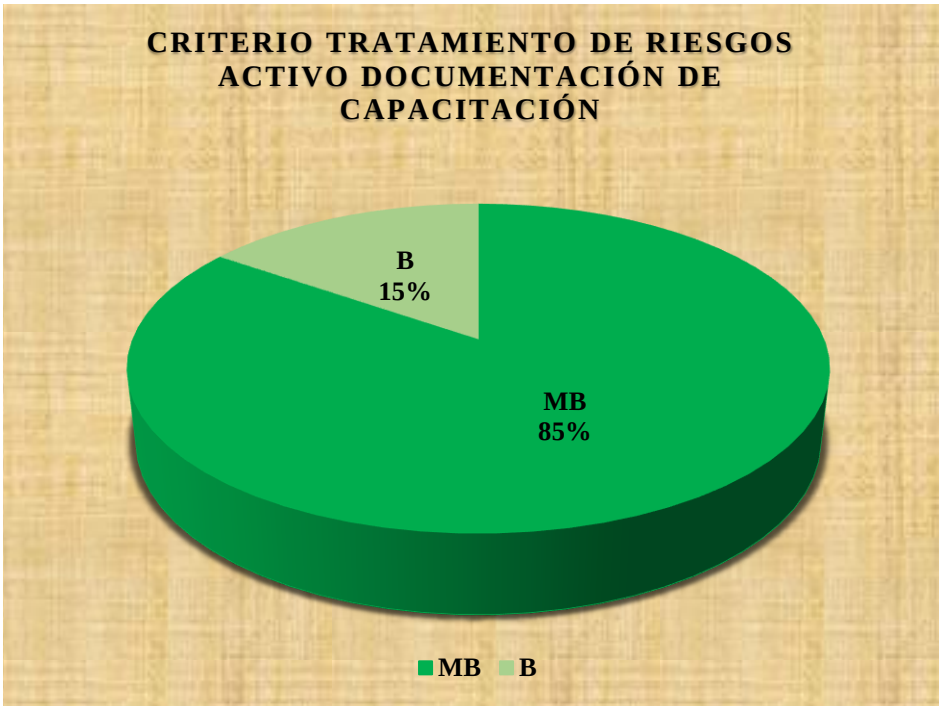


Figura 4. 49: Criterio de Tratamiento de Riesgo: Documento de Capacitación

Figura 4. 50: Riesgos Aceptables y no Aceptables: Documento de Capacitación

4.3.5.23. Resultados Evaluación Activo Planificaciones

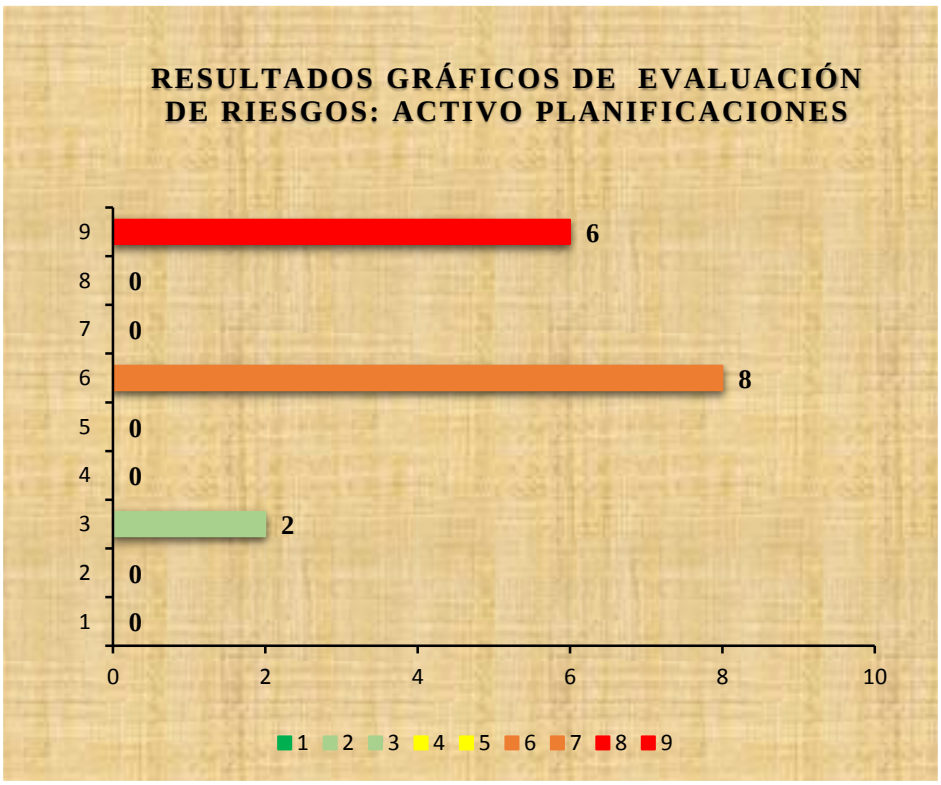


Figura 4. 51: Resultados de Riesgo: Planificación

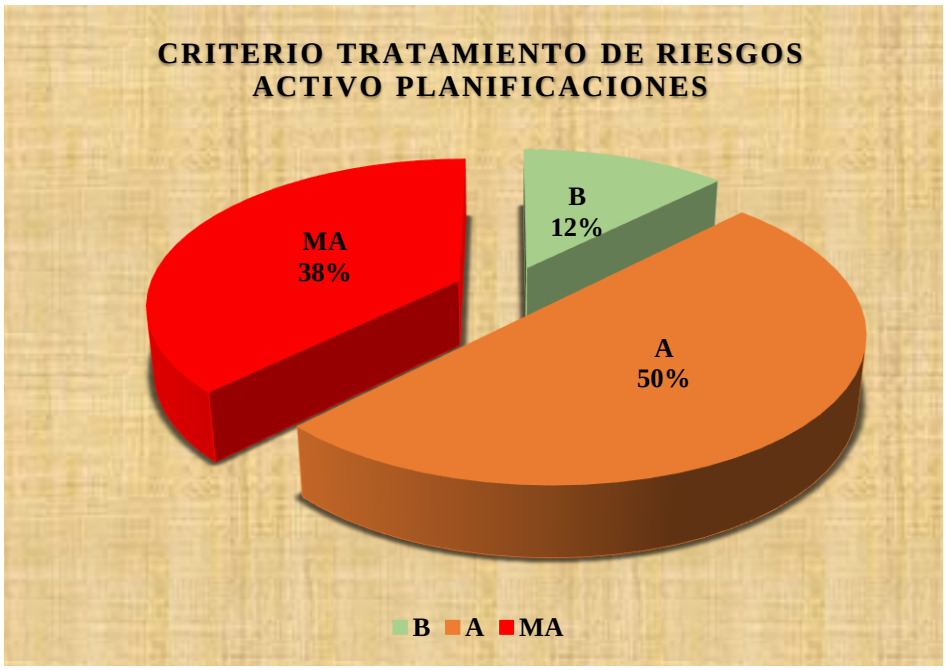


Figura 4. 52: Criterio de Tratamiento de Riesgo: Planificación

Figura 4. 53: Riesgos Aceptables y no Aceptables: Planificación

4.3.5.24. Resultados Evaluación Activo Infraestructura

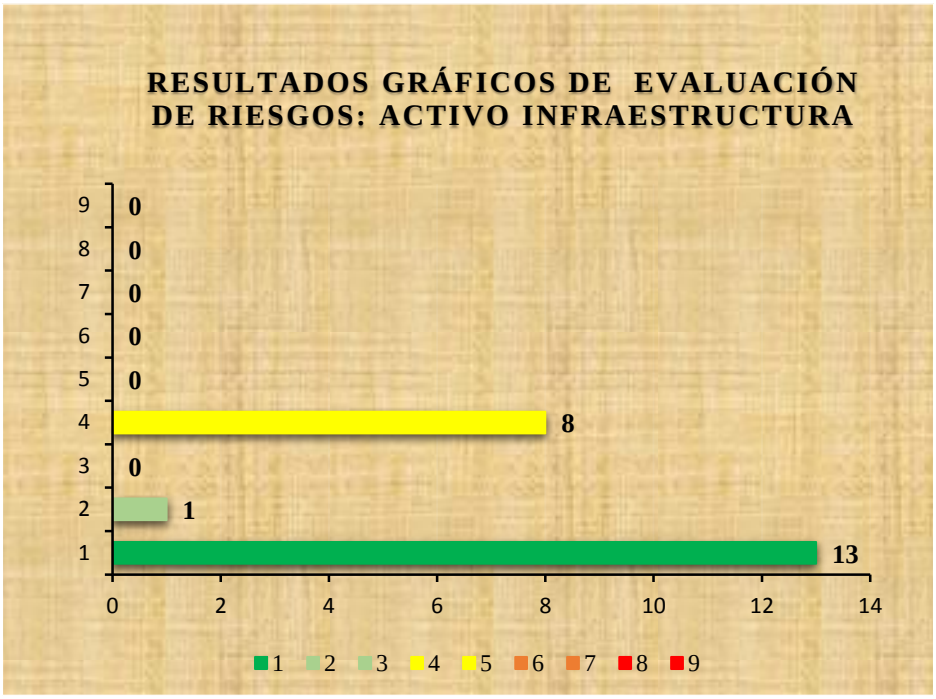


Figura 4. 54: Resultados de Riesgo: Infraestructura

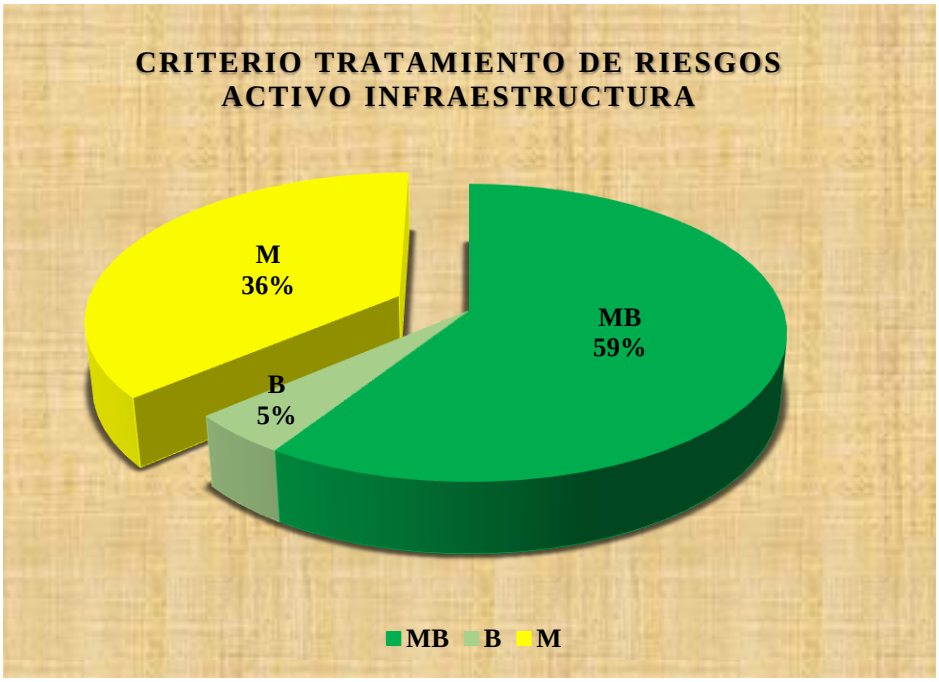


Figura 4. 55: Criterio de Tratamiento de Riesgo: Infraestructura

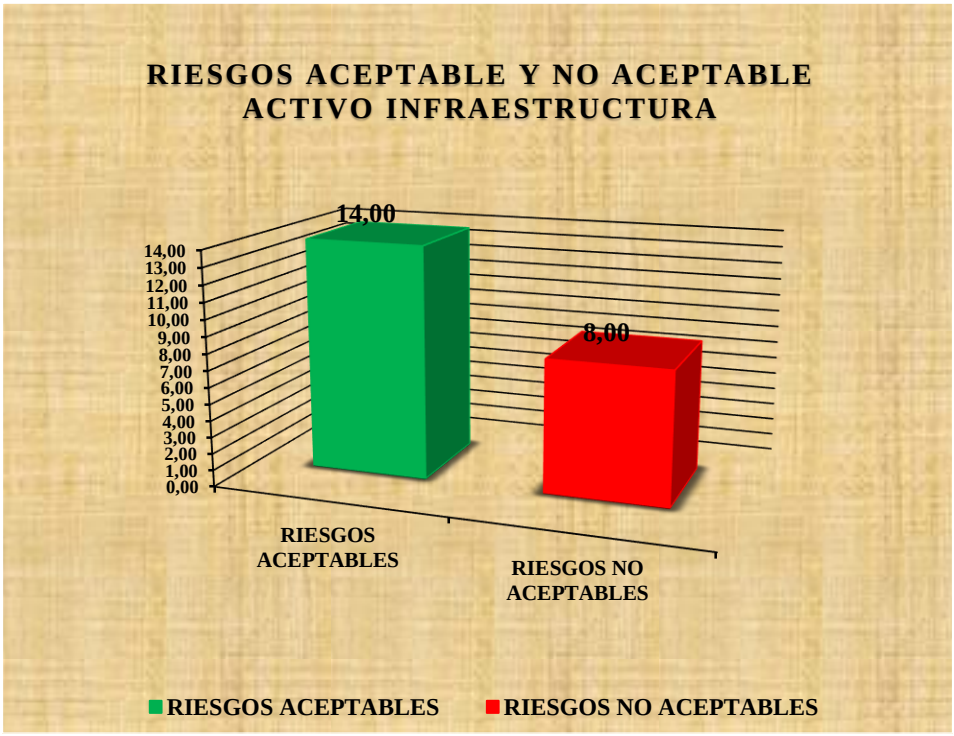


Figura 4. 56: Riesgos Aceptables y no Aceptables: Infraestructura

4.3.5.25. Resultados Evaluación Activo Visitas

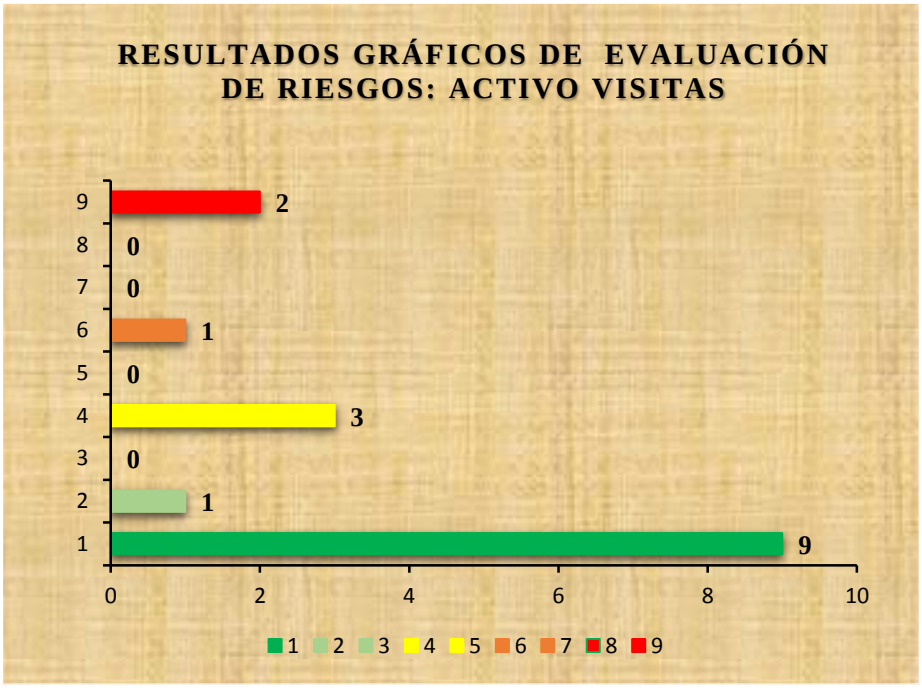


Figura 4. 57: Resultado de Riesgo: Visitas

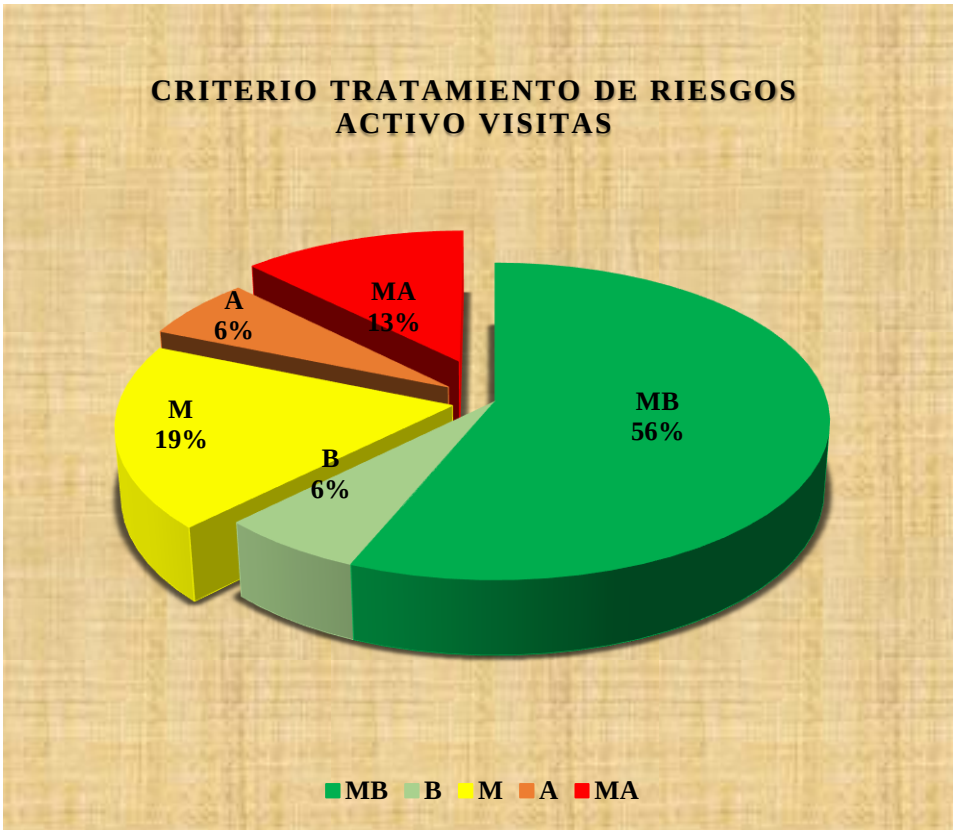


Figura 4. 58: Criterio de Tratamiento de Riesgo: Visitas

Figura 4. 59: Riesgos Aceptables y no Aceptables: Visitas

4.3.5.26. Resultados Evaluación Activo Usuarios Externos

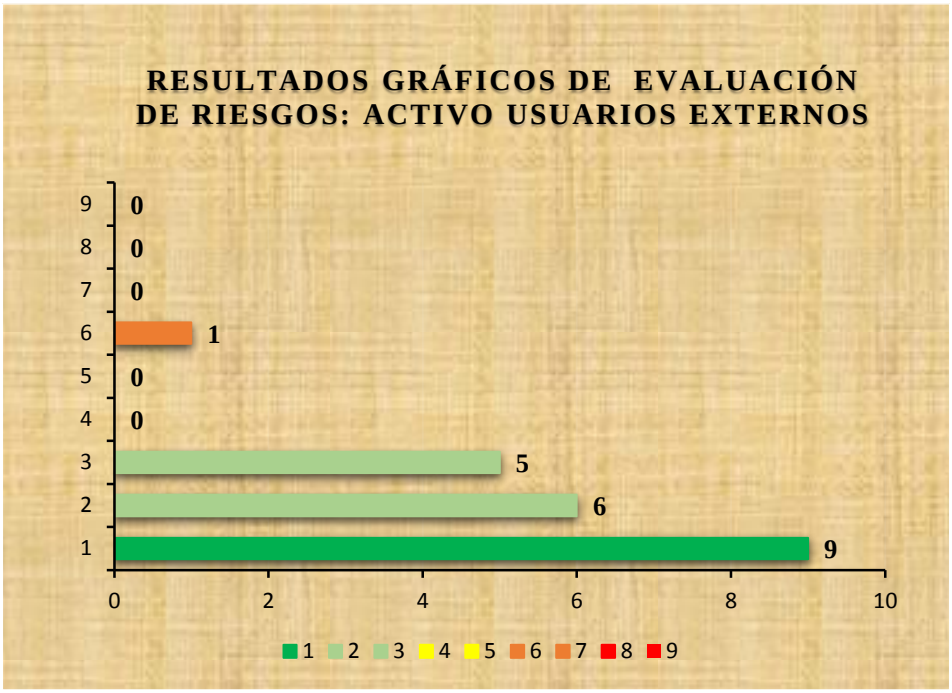


Figura 4. 60: Resultados de Riesgo: Usuarios Externos

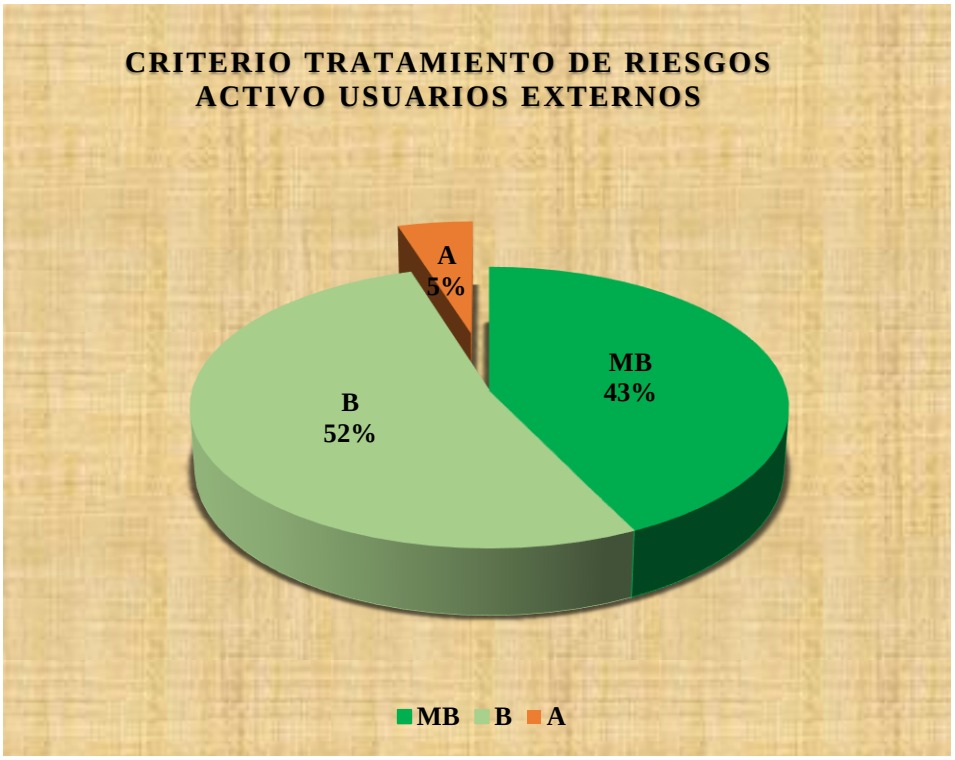


Figura 4. 61: Criterio de Tratamiento de Riesgo: Usuarios Externos

Figura 4. 62: Riesgos Aceptables y no Aceptables: Usuarios Externos

4.3.5.27. Resultados Evaluación Activo Usuarios Internos

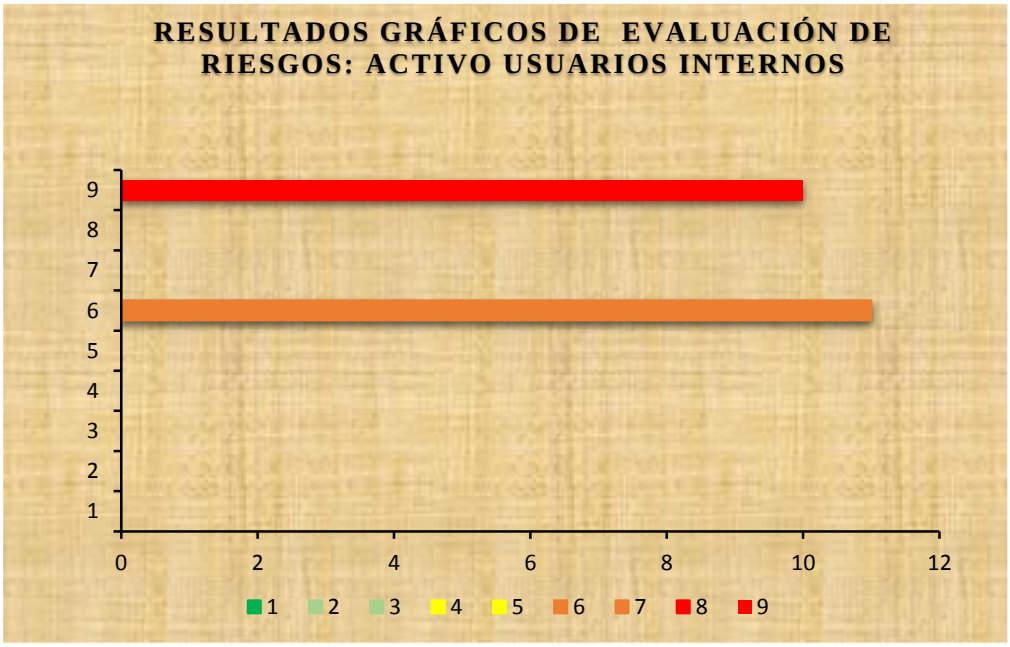


Figura 4. 63: Resultados de Riesgo: Usuarios Internos

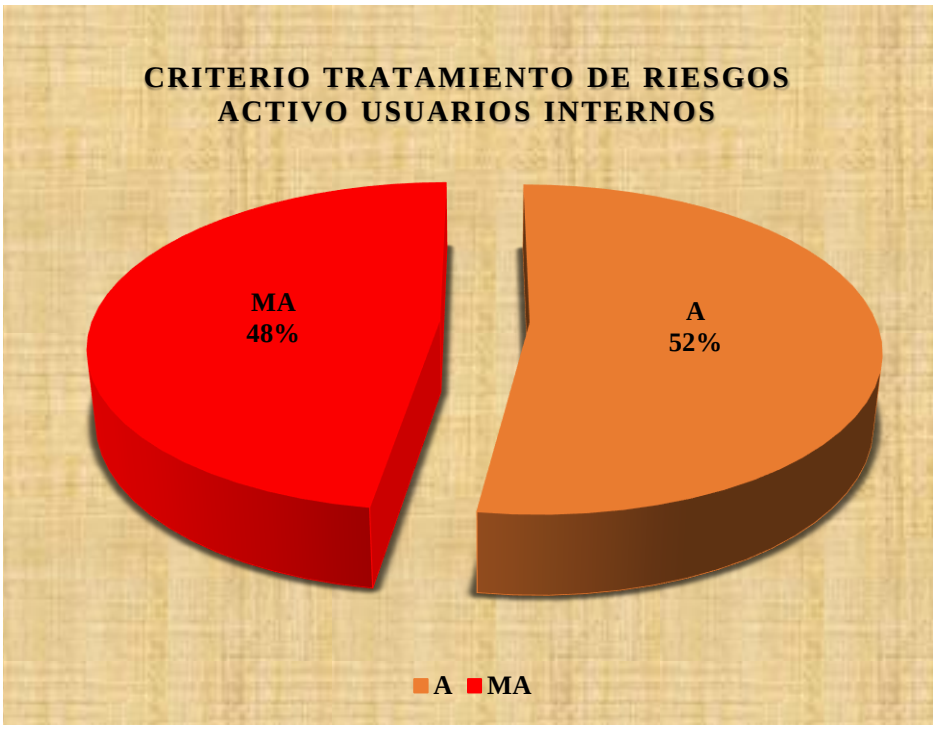


Figura 4. 64: Criterio de Tratamiento de Riesgo: Usuarios Internos

.

Figura 4. 65: Riesgos Aceptables y no Aceptables: Usuarios Internos

4.3.5.28. Informe de Evaluación y Tratamiento de Riesgos.

El Informe es un apéndice del proceso de Evaluación y Tratamiento de Riesgos que detalla mediante un resumen los pasos o procedimientos seguidos junto con los documentos utilizados durante este proceso. Se lo redacta una vez realizada la Evaluación y Tratamiento de Riesgos, en su contenido se citan puntos similares a los documentos anteriores, adicionándose (ANEXO XIV: Metodología de Evaluación y Tratamiento del Riesgo Para la Implementación del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, Apéndice G):

- Objetivo de la Gestión de Riesgos: Describe el objetivo de la evaluación y tratamiento de riesgos, indicando la importancia de la identificación de los activos y los parámetros de cuantificación.
- Alcance de la Evaluación y Tratamiento de Riesgos: Especifica hasta donde se llegará con la evaluación y tratamiento, haciendo una breve descripción de los lugares que intervinieron en el proceso.
- Período de Tiempo: Refiere al tiempo empleado en el proceso de evaluación y tratamiento del riesgo
- Participantes en el Proceso y Recolección de Información: Identifica a todo el personal participante en la recolección de información, en la evaluación de los activos involucrados en el SGSI y en las soluciones propuestas en el tratamiento de riesgos.
- Resumen de la Metodología Aplicada: Es un resumen de la metodología utilizada durante todo el proceso. Se detallará qué metodología fue empleada, los criterios de evaluación y tratamiento de riesgos.
- Resumen de los documentos utilizados: Se enlista todos los documentos redactados durante el proceso de evaluación y tratamiento de riesgos.

4.3.6. Declaración de Aplicabilidad.

Se redacta de acuerdo a los resultados obtenidos en el tratamiento del riesgo; es un documento clave dentro del Sistema de Gestión de Seguridad de la Información en el

que se incluye una descripción de los controles del Anexo A proporcionados en la normas NTE INEN-ISO/IES 27001:2011. En su contenido adicional al ya establecido en el formato se abordan los siguientes puntos: (Anexo XV: Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones)

- Aplicabilidad de los controles del SGSI para el control de acceso a las Salas de Telecomunicaciones de ETAPA EP: En este apartado se trabaja con el ANEXO A de la norma NTE INEN-ISO/IES 27001:2011, en la cual encontramos los 11 Dominios de control con sus objetivos de control y los controles específicos. Con ayuda del tratamiento del riesgo en el que la organización determinó los controles que será necesarios implementar, se justifica con fundamento su aplicación o no dentro de la organización, proporcionando además las recomendaciones de la norma para su implementación.
- Aceptación de los riesgos residuales: En un cuadro que se ajunta como apéndice (ANEXO XV: Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones, APENDICE A), se enlista todos los riesgos específicos que nos son aceptables, y que la organización tomó la decisión de no implementar controles de seguridad, es decir que los activos mantendrán el riesgo.

4.3.7. Plan de Tratamiento del Riesgo.

Es básicamente un plan de acción sobre cómo implementar los controles definidos en la Declaración de Aplicabilidad, se utiliza y actualiza activamente a lo largo de la implementación del SGSI. (ANEXO X: Plan de Tratamiento del Riesgo del Sistema de Gestión de Seguridad de la Información Dirigido al Control de Accesos a las Salas de Telecomunicaciones)

A partir de este punto en adelante, son documentos que se redactan paralelamente con la implementación del SGSI, por lo que definiremos lo que se debe tratar en cada uno de ellos sin profundizar en su contenido.

4.3.8. Anexo A

Contiene todos los controles que corresponden al Sistema de Gestión de Seguridad de la Información que detallamos a continuación. (ANEXO XVII: NTE INEN/ISO-IEC 27001:2011)

4.3.8.1. A.6 Organización de la Seguridad de la Información.

Objetivos:

- ***Organización Interna:*** Gestionar la seguridad de la información dentro de la organización.
- ***A Terceros***: Mantener la seguridad de la información de la organización y de los dispositivos de tratamiento de la información que son accesados, procesados, comunicados o gestionados por terceros.

Políticas Sugeridas:

- Política trae tu propio dispositivo
- Política sobre dispositivos móviles y tele-trabajo.

4.3.8.2. A.7 Gestión de Activos.

Objetivos:

- ***Responsabilidad sobre los activos:*** Conseguir y mantener una protección adecuada de los activos de la organización.
- ***Clasificación de la información:*** Asegurar que la información recibe un nivel adecuado de protección.

Políticas Sugeridas:

- Política de uso aceptable.

- Política de Clasificación de la Información.
- Inventario de Activos

4.3.8.3. A.8 Seguridad Ligada al Recurso Humano.

Objetivos:

- ***Previo al empleo:*** Asegurar que los empleados, los contratistas y los terceros conocen y comprenden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o uso indebido de los recursos.
- ***Durante el empleo:*** Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo y para reducir el riesgo de error humano.
- ***Cese del empleo o cambio de puesto de trabajo:*** Asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.

Políticas Sugeridas:

- Declaración de confidencialidad
- Declaración de Aceptación de Documentos.

4.3.8.4. A.9 Seguridad Física y Ambiental.

Objetivos*:*

- ***Áreas seguras:*** Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.

- ***Seguridad de los equipos:*** Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.

Políticas Sugeridas:

- Procedimientos para trabajo en áreas seguras.
- Política de pantalla y escritorio limpios.
- Política de eliminación y destrucción.

4.3.8.5. A.10 Gestión de Comunicaciones y Operaciones.

Objetivos:

- ***Responsabilidades y procedimientos de operación:*** Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información.
- ***Gestión de la provisión de servicios por terceros:*** Implementar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.
- ***Planificación y aceptación del sistema:*** Minimizar el riesgo de fallos de los sistemas.
- ***Protección contra código malicioso y descargable:*** Proteger la integridad el software y de la información.
- ***Copias de seguridad:*** Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.
- ***Gestión de la seguridad de las redes:*** Asegurar la protección de la información en las redes y a la protección de la infraestructura de soporte.
- ***Manipulación de los soportes:*** Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización

- ***Intercambio de información:*** Mantener la seguridad de la información y del software intercambiado dentro de una organización y con un tercero.
- ***Servicio de comercio electrónico:*** Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos.
- ***Supervisión:*** Detectar las actividades de tratamiento de la información no autorizadas.

Políticas Sugeridas:

- Política de creación de copias de seguridad.
- Política de gestión de cambios.
- Procedimientos operativos para TI y comunicaciones.
- Política de transferencia de información.

4.3.8.6. A.11 Control de Acceso.

Objetivos:

- ***Requisitos de negocio para el control de acceso:*** Controlar el acceso a la información.
- ***Gestión de acceso de usuarios:*** Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información**.**
- ***Responsabilidades de usuarios:*** Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de información o de recursos de tratamiento de la información.
- ***Control de acceso a la red:*** Prevenir el acceso no autorizado a los servicios en red.
- ***Control de acceso al sistema operativo:*** Prevenir el acceso no autorizado a los sistemas operativos.

- ***Control de acceso a las aplicaciones y a la información:*** Prevenir el acceso no autorizado a la información que contienen las aplicaciones.
- ***Equipos portátiles y teletrabajo:*** Garantizar la seguridad de la información cuando se utilizan equipos portátiles y servicios de teletrabajo.

Políticas Sugeridas:

- Política de claves.
- Política de control de acceso.

4.3.8.7. A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

Objetivos:

- ***Requisitos de seguridad de los sistemas de información:*** Garantizar que la seguridad está integrada en los sistemas de información.
- ***Tratamiento correcto de las aplicaciones:*** Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones.
- ***Controles criptográficos:*** Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.
- ***Seguridad de los archivos se sistema:*** Garantizar la seguridad de los archivos de sistema.
- ***Seguridad en los procesos de desarrollo y soporte:*** Mantener la seguridad del software y de la información de las aplicaciones.
- ***Gestión de la vulnerabilidad técnica:*** Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas o identificadas.

Políticas Sugeridas:

- Política de desarrollo seguro.
- Apéndice de especificaciones de requisitos de seguridad.

4.3.8.8. A.13 Gestión de Incidentes de Seguridad de la Información.

Objetivos:

- ***Notificación de eventos y puntos débiles de seguridad de la información:*** Asegurarse de que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.
- ***Gestión de incidentes de seguridad de la información y mejoras:*** Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.

Políticas Sugeridas:

- Procedimiento para gestión de incidentes.
- Apéndice Registro de incidentes.

4.3.8.9. A.14 Gestión de la Continuidad del Negocio.

Objetivos:

- ***Aspectos de seguridad de la información en la gestión de la continuidad del negocio:*** Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.

Políticas Sugeridas:

- Política de Gestión de continuidad del negocio.

4.3.8.10. A.15 Cumplimiento.

Objetivos:

- ***Cumplimiento de los requisitos legales:*** Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad.
- ***Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico:*** Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización.
- ***Consideraciones sobre la auditoría de los sistemas de información:*** Lograr que el proceso de auditoría de los sistemas de información alcancen la máxima eficacia con las mínimas interferencias.

Políticas Sugeridas:

- Política de Gestión de continuidad del negocio.

CONCLUSIONES:

- ✓ Al finaliza este trabajo, hemos podido establecer que una organización sea cual fuere la actividad económica a la que se dedica o el tamaño de la misma, poseen activos que representan su desarrollo, crecimiento y proyección. Es así que protegiéndolos conseguiremos mantener esas características que toda organización pretende.

- ✓ El Sistema de Gestión de Seguridad de la Información SGSI que nos proporciona ISO 27000 nos da las directrices para poder proteger la información, que es uno de los activos de gran importancia pues en ella se refleja sus actividades financieras, administrativas y técnicas, es decir toda la organización en sí, pero no de manera arbitraria seleccionando controles que pueden afectar a otros activos o que pueden sobrecargar los sistemas de seguridad ya existentes en la organización. Es por eso que existe una serie de pasos que se han llevado a cabo en este trabajo y que han determinado las posibles amenazas y vulnerabilidades que pueden suscitarse en los accesos a las Salas de Telecomunicaciones y que van de la mano con métodos adecuados de evaluación de riesgos en la organización; herramientas que nos han llevado a determinar los controles idóneos para evitar al máximo la ocurrencia de eventos que afecten la confidencialidad, integridad y disponibilidad de la información en la organización.

- ✓ Esta tarea implica una interacción entre los propietarios de los riesgos, los coordinadores del proyecto y los promotores (autores), teniendo ETAPA EP, un rol protagónico dentro de este trabajo, al proporcionarnos datos reales y confidenciales para la organización que nos dieron una visión de las posibles amenazas y vulnerabilidades de las que puede ser víctima, y participando activamente de evaluaciones con resultados analizados y presentados al equipo de trabajo, quienes han tomado la decisión de implementar futuros controles de seguridad que le permitirá a la organización proyectar altos estándares de

seguridad y calidad en sus servicios, pues al proteger sus bienes está garantizando la protección de la información y por ende un servicio continuo, eficaz y de calidad que influirá en su crecimiento económico y financiero.

- ✓ Los controles seleccionados, constituyeron una herramienta clave en este trabajo, estos nos llevaron a diseñar los nuevos sistemas de seguridad y control de accesos a las Salas de Telecomunicaciones de ETAPA EP, pues nos proporcionaron una amplia visión de las medidas correctivas que se deben implementar con el objetivo de proteger sus bienes.

RECOMENDACIONES:

Se recomienda:

- ✓ La implementación de los controles seleccionados en la fase de tratamiento de riesgos incluyendo al personal involucrado en las áreas para que se les capacite y cumplan con las políticas establecidas en estos puntos.

- ✓ Establecer un nivel jerárquico para la implementación de los controles seleccionados utilizando el criterio de los riesgos con niveles más altos hasta los más bajos recurriendo como herramienta al Anexo XIV: Plan de tratamiento de riesgos.

- ✓ Realizar controles periódicos al personal o entidad a la que la organización tomó la decisión de transferir el riesgo con la finalidad de verificar que la decisión tomada fue la idónea, o caso contrario someter a una nueva evaluación del riesgo con la finalidad de seleccionar controles adecuado que permita reducir las amenazas suscitadas.

- ✓ Dar seguimiento a los riesgos con niveles mayores a 4 puntos en los que la organización aceptó o evitó el riesgo y en el caso de materializarse la amenaza efectuar una nueva evaluación del riesgo tomando en cuenta los posibles controles a implementarse en cada caso.

- ✓ Como meta, ETAPA EP debería tender a implementar y aplicar el SGSSI en todos sus niveles de seguridad a toda la organización.

- ✓ Finalmente, se recomienda a la organización la designación de un departamento o área específica dentro de la empresa que se encargue de la

supervisión, revisión y de reportar posibles falencias que se pueden suscitar en el proceso de monitoreo para corregirlas inmediatamente y siguiendo los lineamiento establecidos por ISO 27000.

BIBLIOGRAFÍA

27000, I. (2012). *ISO 27000 EN ESPAÑOL*. (GUÍA DE CONTROLES ISO 27002:2013) Recuperado el 9 de 11 de 2015, de www.iso27000.es

Academy, 2. (2016). *Academy 27001*. Recuperado el 16 de Marzo de 2016, de www.27001academy.com

Agustin López Neira, Javier Ruiz Spoh. (2012). *ISO 27000 EN ESPAÑOL*. (ACERCA DE) Recuperado el 5 de 11 de 2015, de www.iso20000.es

Biometría. (2013). *Biometría*. Recuperado el 16 de Marzo de 2016, de www.biometria.gov.ar

Certicámara. (2016). *Carticamara. Validez y seguridad jurídica electrónica.* Recuperado el 17 de Marzo de 2016, de www.certicamara.com

Dirección General de Modernización Administrativa, P. e. (2012). *Metodología de Análisis y Gestión de Riesgos de los Ssitemas d Información.* Madrid: Edición digital: Subdirección General de Información, Documentación y Publicaciones (Jesús González Barroso).

EcuRed. (2016). *EcuRed Conocimiento con todos y para todos*. Recuperado el 16 de Marzo de 2016, de www.ecured.cu

Empresarios., C. G. (2008). *CGE.* Recuperado el 25 de 11 de 2015, de www.cge.es

Española, R. A. (2015). *Real Academia Española*. Recuperado el 04 de 11 de 2015, de dle.rae.es

ETAPA. (2016). *ETAPA EP*. Recuperado el 26 de Enero de 2016, de www.etapa.net.ec

ETAPA. (2016). *ETAPA EP*. Recuperado el 26 de Enero de 2016, de www.etapa.net.ec

FERMA, F. O. (2002). ESTÁNDARES DE GERENCIA DE RIESGOS. BRUSELAS: AIRMIC_ALARM, IRM.

FullCar. (2016). *FullCar Sistemas de Seguridad & Audio.* Recuperado el 17 de MArzo de 2016, de www.fullcar.com

Huerta, A. V. (30 de 09 de 2004). *GRUPO S2*. (Código de Buenas Prácticas de Seguridad UNE- ISO/IEC 17799) Recuperado el 9 de 11 de 2015, de www.shutdown.com.es

Huerta, A. V. (s/a). *S2 Grupo.* Recuperado el 19 de 11 de 2015, de GRUPO SEC: http://www.shutdown.es

IEC. (2015). *IEC*. (About the IEC - Standars Development) Recuperado el 6 de 11 de 2015, de www.iec.ch

INEN. (2009). *INEN*. (La Institución.) Recuperado el 4 de 11 de 2015, de www.normalizacion.gob.ec

INTPLUS. (2016). *Video Vigilancia*. Recuperado el 15 de Marzo de 2016, de www.videovigilancia.com

ISO. (2012). *NTE INEN-ISO/IEC 27005/2012.* Quito: Instituto Ecuatoriano de Normalización, INEN.

ISO. (2015). *ISO*. (Standars - About us - Standars Development) Recuperado el 1 de 11 de 2015, de www.iso.org

ITU. (2015). *UIT - ITU*. (About ITU - Standaritation) Recuperado el 6 de 11 de 2015, de www.itu.int

kimaldi. (2016). *Kimaldi*. Recuperado el 15 de Marzo de 2016, de www.kimaldi.com

M, M. (15 de 6 de 2005). *Tecnología de la Información Beta.* Recuperado el 7 de 11 de 2015, de mmujica.files.wordpress.com

Madrid, U. P. (2016). *Universidad Politécnica de Madrid*. Recuperado el 16 de Marzo de 2016, de www.upm.es

Meyer, I. C. (2012). *ISO 27000*. (Artículos y Podcast / Artículo Seguridad Informática y Seguridad de la Inormación) Recuperado el 7 de 11 de 2015, de www.iso27000.es

Parra, I. M. (2016). *Wikimedia Foundation.* Recuperado el 17 de Marzo de 2016, de upload.wikimedia.org

PriteshGupta.com. (2012). *ISO 27000 EN ESPAÑOL*. Recuperado el 20 de Enero de 2016, de www.iso27000.com

Rico, J. C. (S.A.). *S21SEC*. Recuperado el 9 de 11 de 2015, de www.fundaciondedalo.org

SAS, S. y. (2015). *SEAT. sEGURIDAD Y EQUIPOS DE ALTA TECNOLOGÍA*. Recuperado el 17 de Marzo de 2016, de www.seguridadseat.com

Stefanini. (2015). *Stefanini Powering Your Business*. (Gestión de Riesgo y Seguridad de la Información) Recuperado el 9 de 11 de 2015, de www.stefanini.com/es