FACULTAD DE ARQUITECTURA E INGENIERÍAS

TRABAJO DE INVESTIGACIÓN DE FIN DE CARRERA

TITULADO:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27002:2013 PARA EL CONTROL DE ACCESO A LA INFRAESTRUCTURA DE RED DE AXXIS HOSPITAL."

REALIZADO POR:

Ing. María Fernanda Palma Agama

DIRECTOR DEL PROYECTO:

Ing. Edison Estrella, MBA.

COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD Y REDES

Quito, diciembre 2019

DECLARACIÓN JURAMENTADA

Yo, MARÍA FERNANDA PALMA AGAMA, con cédula de identidad # 0502477649, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

María Fernanda Palma Agama

C.C.: 0502477649

DECLARATORIA

El presente trabajo de investigación titulado:

“DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27002:2013 PARA EL CONTROL DE ACCESO A LA INFRAESTRUCTURA DE RED DE AXXIS HOSPITAL.”

Realizado por:

MARÍA FERNANDA PALMA AGAMA

como Requisito para la Obtención del Título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD Y REDES

Ha sido dirigido por el profesor

Ing. Edison Estrella, MBA

quien considera que constituye un trabajo original de su autor

Ing. Edison Estrella, MBA

DIRECTOR

Los Profesores Informantes:

MSC. CHRISTIAN PAZMIÑO

ING. VERÓNICA RODRÍGUEZ, MBA.

Después de revisar el trabajo presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador

Msc. Christian Pazmiño. Ing. Verónica Rodríguez, MBA.

Quito, octubre de 2019

DEDICATORIA

Galo David mi compañero, mi inspiración y guía, es hermoso regresar y ver el recorrido de nuestras vidas, el saber que nos quedan muchos más retos a nivel profesional y muchas nuevas aventuras como familia, siempre eres esa mano que me llena de aliento y me impulsa a conseguir nuevos triunfos. Te amo…

Esteban y Emilia… Mis chiquitos, cada dedito de cada día fue mi entera inspiración, al mirar sus ojitos ventanitas de sus corazones y esas sonrisas que llenan el alma, me motivan a ser mejor cada día y saber que esas pequeñas fuertes personitas son el mayor motor que Dios puso en mi vida.

Mis papitos Estela y Elpidiun por ser mi raíz y ejemplo de perseverancia, aunque no estemos siempre juntos, son esa semilla implantada en mi corazón para alcanzar cada sueño y cada meta propuesta.

Mis hermanas Patricia y Paola, mis amigas y mis cómplices cada una en su modo son mi ejemplo.

A todos ustedes dedico este trabajo, que se ha marcado por dos años de esfuerzo en los que cada uno ha aportado a su modo para que hoy pueda lograr terminar con esta etapa profesional y este trabajo de titulación, mis chiquitos por sus noches sin mamá, mi esposo por su apoyo y empuje, mis papitos y hermanas ahí siempre para velar por mi familia.

AGRADECIMIENTO

Quiero agradecer de manera especial a:

AXXIS Hospital que ha sido verdaderamente un aliado estratégico. El poder trabajar y agregar valor a la institución es algo enriquecedor y además es gratificante pertenecer a la familia AXXIS.

A la Universidad Internacional SEK, por contar con excelentes docentes quienes en cada módulo aportaron con su experiencia para poder aplicarla en nuestras actividades profesionales.

Ing. Edison Estrella, por el tiempo y dedicación al desarrollo de este documento, su valioso aporte para poder presentar este trabajo, bajo sus claras directrices se pudo llegar a cumplir los objetivos.

Ing. Christian Pazmiño, su asistencia y guía para completar el proyecto han sido de valiosa ayuda.

Ing. Verónica Rodríguez, por compartir sus enseñanzas y conocimientos los cuales me han servido de norte en la elaboración del documento.

Índice de Contenido

Índice de Figuras

Índice de Tablas

Resumen

AXXIS Hospital es una organización de Salud, tiene más de 10 años de trayectoria institucional, en los cuales su crecimiento y cobertura no sólo a pacientes de Quito, sino a pacientes a nivel nacional refiere un servicio con altos estándares de calidad, uno de estos es la certificación SGC ISO9001 2015. En línea con los procesos de calidad del hospital se ve la necesidad de implementar políticas encaminadas a la seguridad y control de acceso a la infraestructura de red aplicando la norma ISO/IEC 27002:2013 para el presente trabajo se realizó el levantamiento de la información de los equipos que conforman la infraestructura de red mediante el análisis de la situación actual de cada unidad médica; según los hallazgos encontrados, se diseñó la política de seguridad de la información para el control de acceso a la infraestructura de red. En la red de la institución, tanto a nivel físico como lógico, se debe precautelar su seguridad ante la presencia de intrusos, incidentes o eventos que puedan presentarse provocando y evidenciando las vulnerabilidades existentes en AXXIS. Con la política de seguridad se establecieron controles que permiten anticipar y reaccionar a la presencia de amenazas que alteren la integridad, disponibilidad, y confidencialidad de la información, se evaluaron los dominios de la norma que son aplicables a la organización y que deben ser adoptados para precautelar la seguridad física y lógica de la misma, finalmente se documenta la política para poder socializarla y aplicarla dentro de la institución, obteniendo controles que mejoran la manera de acceder a los recursos mediante la infraestructura de red.

Palabras clave: Amenazas, infraestructura de red, riesgo, política de seguridad, ISO/IEC 27002:2013, Vulnerabilidad.

ABSTRACT

AXXIS Hospital is a Health organization, with more than 10 years of institutional trajectory, in which its growth and coverage not only to Quito patients, but to patients nationwide refers to a service with high quality standards, one of these is The SGC ISO9001 2015 certification. In line with the hospital's quality processes, there is a need to implement policies aimed at the security and control of access to the network infrastructure based at the standard ISO/IEC 27002:2013 for the present work the equipment information was collected. that make up the network infrastructure by analyzing the current situation of each medical unit; According to the findings found, the information security policy was designed to control access to the network infrastructure. In the institution's network, both physically and logically, its security must be guarded in the presence of intruders, incidents or events that may occur causing and evidencing the existing vulnerabilities in AXXIS. With the security policy, controls were established that allow anticipating and reacting to the presence of threats that alter the integrity, availability, and confidentiality of the information, the domains of the standard that are applicable to the organization and that must be adopted to evaluate Precautionary physical and logical security of the same, finally the policy is documented to be able to socialize and apply it within the institution, obtaining controls that improve the way to access resources through the network infrastructure.

Keywords: Threats, network infrastructure, risk, security policy, ISO/IEC 27002:2013, vulnerability.

CAPÍTULO I

INTRODUCCIÓN

El desarrollo e incremento de centros médicos y hospitales a nivel nacional es la base de nuevas oportunidades y crecimiento del país e institucional, ahora la medicina va muy de la mano con diferentes avances tecnológicos, y no puede quedarse atrás la información y la digitalización de la misma. Esto ha convertido a los hospitales en un referente clave vanguardistas en equipos médicos, como AXXIS Hospital, Hospital de los Valles, Hospital Metropolitano. Que transmiten información digital en tiempo real, y así, disponer de la información de historias clínicas en cualquier parte del mundo, resultados de exámenes, costos de servicios, entre otros; lo que implica el invertir en tecnología para ahorrar el recurso más valioso, el tiempo (El Comercio, 2019).

La seguridad a nivel físico permite identificar vulnerabilidades, amenazas y las medidas correctivas que se deben utilizar para proteger físicamente la información y los recursos vinculados a la organización. En el campo o grupo de los recursos constituyen el personal, las estaciones de trabajo, datos, información, equipos y dispositivos de comunicación con los cuales los usuarios de red interactúan diariamente, es decir, los activos que se asocian al mantenimiento y procesamiento de datos e información.

Ahora, al hablar de desarrollo tecnológico y transferencia de información en el ciberespacio para que esté al alcance del usuario final, no se puede dejar a un lado o dar menor prioridad a la seguridad física que resguarda la información compartida y prever que sólo pueda acceder personal autorizado o descargar un contenido, y los cambios generados o la información nueva ingresada sea confiable generada por fuentes autenticadas; y además, la disponibilidad de la misma para que el usuario final acceda a

la información de manera rápida, sencilla y que se contemple la solución inmediata ante posibles incidentes.

1.1. PLANTEAMIENTO DEL PROBLEMA

El continuo crecimiento tecnológico de centros médicos, hospitales y demás instituciones de salud, hacen que la tendencia sea digitalizar la información, ya sea de historias clínicas de los pacientes que debe ser estrictamente confidencial y los datos propios del giro de negocio, por lo que es primordial garantizar y precautelar la integridad, confidencialidad y disponibilidad para cumplir con estándares de calidad y servicio (Mosquera, Saravia, & Pacheco, 2016).

El acceso de personas a clínicas y hospitales es el común denominador, muchas de estas son pacientes propios de las unidades médicas que dispone el hospital, pero, qué sucede si entre este tránsito diario de personas, se infiltran atacantes, ladrones y personas que se infiltran con el fin de perjudicar el servicio hospitalario (AXXIS,2019).

Los daños que se pretende mitigar están desde hurtos, hasta afectaciones severas a los diferentes servicios que el hospital ofrece a los pacientes, la infraestructura de red de AXXIS interconecta los diferentes sistemas y al presentarse un incidente de seguridad, las unidades médicas asociadas se ven directamente afectadas, así como transmisión de datos en tiempo real en áreas críticas.

El hospital cuenta con un sistema de cableado estructurado, cada piso dispone de su cuarto de Rack y un switch de acceso para la distribución de los servicios de red (Internet, Historia Clínica, RisPAC, Correo Electrónico, etc.); todos los Racks están interconectados al Data Center mediante topología tipo estrella a través de enlaces de fibra óptica brindando conectividad a toda la organización. En la inspección se revisa la ubicación de racks y equipos, ya que el departamento de TICs indica que se encuentran instalados en los ductos del edificio y otros con acceso directo sin seguridades, la vulnerabilidad de estas instalaciones permite que posibles atacantes tengan fácil acceso

a la infraestructura de red, haciendo que un evento de inseguridad pueda ocurrir en cualquier momento.

Las instalaciones de consultorios y algunas áreas comunes han tenido varios cambios afectando la integridad física de la red, en el pasar de los años estas modificaciones arquitectónicas han provocado que se encuentren puntos en pasillos comunes, que continúan conectados a los equipos de red de piso en donde los puertos no se han bloqueado haciendo que un atacante pueda conectarse y tener acceso a la red del hospital.

Los equipos médicos implementados en AXXIS, se interconectan a las diferentes unidades médicas como Laboratorio, Imagen, Gastroenterología, entre otros servicios que ofrece el hospital, la información que envían estos equipos a través de la red de datos en tiempo real permite el oportuno diagnóstico de pacientes, al tener puertos lógicos y físicos abiertos, hace que la infraestructura sea susceptible a presentar fuga de información, fácil acceso a bases de datos de pacientes, proveedores, o alianzas estratégicas del hospital afectando seriamente a la continuidad del negocio.

Es por estas razones, que se pretende implementar una política de seguridad para el acceso a la infraestructura de red, para precautelar la integridad de los datos, intentos de ataques a la red, robo de información del hospital y de esta manera minimizar los riesgos y maximizar los procesos que permitan tener un adecuado manejo de la información, información, mantener controles para un correcto registro de ingreso de personal autorizado a cada segmento de la red del hospital.

1.1.1. Diagnóstico del Problema.

AXXIS Hospital es una institución que está conformada por Unidades Médicas, entre las que se encuentran Emergencia, Hospitalización, Consulta externa, Farmacia, Laboratorio, Imagen, Cirugía, Rehabilitación, Gastro, UCI (Unidad de Cuidados Intensivos), Docencia, Materno Infantil; adicionalmente maneja Servicios

Administrativos, lo que hace que este hospital disponga de un servicio integral para los pacientes a nivel nacional (AXXIS, 2019).

El crecimiento progresivo que el Hospital ha experimentado en los últimos años, ha desencadenado en que cada unidad o área busque independientemente sus herramientas tecnológicas para cubrir las necesidades presentadas, al tener un crecimiento desordenado y que el control de los procesos llevados en cada una de estas sea cada vez más difícil de tomar, provocando, pérdidas económicas significativas, que el tiempo de funcionarios tanto médicos como administrativos sea prolongado por lo que la atención al cliente final, en este caso el paciente, se vea afectada de manera significativa; y más aún, si se pone énfasis a la información médica digital que se maneja en el hospital, es decir Historias Clínicas, Contabilidad, Resultados de Exámenes Médicos y Exámenes Complementarios; la continuidad del negocio depende de la correcta gestión que se dé a los resultados obtenidos de la información ingresada por las diferentes unidades tomando las decisiones acertadas manteniendo un control de riesgos.

Se programan entrevistas y encuestas dirigidas al personal de AXXIS, con la finalidad de evidenciar que las medidas de seguridad a la información implementadas, validar si son o no suficientes ó en otros son prácticamente nulas, además de verificar el conocimiento por parte de los usuarios sobre la infraestructura misma de la red. Estudiar las acciones preventivas y correctivas del personal del departamento de TI para evaluar si requiere capacitación acerca de seguridad informática y en caso de encontrar deficiencias en seguridad puedan tomar correcciones oportunas ante eventos que ocasionan que la institución se encuentre vulnerable ante:

- Control de acceso en áreas restringidas.
- Control de personal no autorizado en áreas donde se encuentran equipos de red.
- Acciones a tomar en caso de realizar trabajos en la infraestructura de red o cerca a esta, y el personal se encuentre sin identificaciones de trabajadores o proveedores.
- Control sobre los periféricos de las computadoras.

1.1.2. Pronóstico

La estructura administrativa de AXXIS tiene como base un modelo matricial, es decir, todas las Unidades y servicios administrativos, dependen uno de otro, por lo que, si un incidente de seguridad se lleva a cabo en cualquiera de ellas, afectaría directamente desempeño de toda la organización, es aquí que se tiene la necesidad de realizar la política de seguridad de acceso a la infraestructura de red, para que se garantice que los servicios del hospital cuenten con una estructura de seguridad robusta y se pueda disponer de información veraz en el menor tiempo para mejorando su disponibilidad.

Como departamento de TIC, se debe realizar el correcto manejo y control de uso de datos para no acarrear con consecuencias como se detallan a continuación:

Al no contar con controles de acceso a la infraestructura de red, puede acarrear riesgos como desconexión de los servicios y esto afectar significativamente la operación del hospital o fuga de información.

No se evidencian procesos claros para el manejo de incidentes como: acceso no autorizado a recursos de la red de AXXIS, daños físicos, robo de equipos, manipulación de conexiones en cualquier unidad que conforma el hospital.

No se podría proporcionar información veraz y oportuna para una correcta toma de decisiones.

1.1.2.1. Control del Pronóstico

Minimizar los riesgos de acceso de personal no autorizado a la información que usan como puente la infraestructura de red, mediante la creación de controles que permitan la correcta administración y otorgue seguridades a los equipos de comunicación.

Mediante el análisis de una matriz de riesgos, se determina la criticidad de los eventos que pueden afectar al hospital, la probabilidad de que estos ocurran y en consecuencia las acciones que se deben tomar, con la evaluación del estado de la red, se establecen controles para mitigar las amenazas que se presenten.

En base a la probabilidad de ocurrencia e impacto de los riesgos evaluados, se diseña una política de seguridad para el control de acceso a la infraestructura de red basada en la norma ISO/IEC 27002:2013, para determinar controles específicos ante la presencia de incidentes de seguridad.

Las diferentes áreas y unidades médicas del Hospital, deberán aplicar los controles que se definen en la política se seguridad con carácter obligatorio, esto permitirá la optimización de procesos.

1.1.2.2. Formulación del Problema

AXXIS actualmente cuenta con una infraestructura de TI en donde se interconectan dos torres, la primera consta de 14 pisos incluido 3 subsuelos, en donde se encuentran los consultorios médicos para medicina ocupacional. La segunda torre es Hospitalización, tenemos los servicios dedicados al desarrollo de Hospital, abarca de igual manera 14 pisos, incluyendo 3 subsuelos; y como proyecto a largo plazo, se integrará la torre materno infantil en donde se proyecta que la interconexión sea al Data Center ubicado en la torre de Hospital.

Toda la institución que conforma el hospital, no cuenta con controles para salvaguardar la infraestructura de red, y al no mantener procesos claros, podría resultar en eventos de gran criticidad para las comunicaciones del hospital y la disponibilidad de la información.

El crecimiento institucional, debe ser llevado bajo estrictos parámetros de control para un manejo ordenado de la información, tanto de los sistemas de Salud, como los sistemas, administrativos/contables de la misma. El precautelar el acceso a la red de tres torres debe ser considerado como un eje fundamental para el correcto manejo de la información de este complejo médico.

1.1.3. Objetivo General.

Diseñar una política de seguridad de control de acceso a la infraestructura de red basada en la ISO 27002:2013, mediante el estudio de los diferentes controles de la norma, garantizando así la integridad, confidencialidad y disponibilidad de la información.

1.1.4. Objetivos Específicos.

- Determinar la situación actual de la infraestructura de red de AXXIS Hospital, mediante la elaboración de una matriz de riesgos para la identificación de vulnerabilidades, amenazas e impacto en la seguridad de red.
- Asociar la norma ISO/IEC 27002:2013 mediante la selección de controles necesarios mitigando así los riesgos de seguridad de la información de la infraestructura de red.
- Estructurar una política de seguridad de la información en base a los controles seleccionados de la norma ISO/IEC 27002:2013 estableciendo medidas de protección a la infraestructura.

1.1.5. Justificación

La información empresarial de los sistemas médicos de las diferentes unidades que componen AXXIS, convergen en el Data Center del Hospital, el principal problema es el manejo del acceso a la infraestructura de red sin llevar registros de ingreso y el desconocimiento de los activos de comunicación de la institución por parte del personal.

La infraestructura de la red de datos se ha visto vulnerable en varias oportunidades ya que hay libre acceso en áreas de equipos de comunicaciones, que transmiten en tiempo real información de pacientes y en especial de áreas críticas, la pérdida de conexión por un evento de seguridad física puede desencadenar una serie de errores que pondrían en peligro la vida de los pacientes.

Es por esto que, al desarrollar la política de seguridad de TI, se apuntará a cubrir necesidades de control en el manejo de su infraestructura, así como de la información almacenada en la misma.

1.2. ESTADO DEL ARTE

Sobre el desarrollo de políticas de seguridad de infraestructuras de red de empresas o instituciones públicas como privadas, se han realizado varias investigaciones, se valora los aportes de estudios existentes para que mediante un análisis comparativo se pueda seguir un modelo que con el fin cumplir con las necesidades que actualmente presenta el hospital, a continuación, se presentan trabajos de varios autores y tener una gama amplia del enfoque que tendrá esta investigación.

Según Sahibudin & Ayat (2018) diferentes marcos de trabajo, herramientas y estándares han sido incluidos en los sistemas de gestión de TI, en diferentes organizaciones.

Por lo que se requiere administrar, dirigir y controlar una o más personas o entidades con la finalidad de coordinar el cumplimiento de un objetivo general.

La gestión de TI, abarca varios puntos como recursos humanos, recursos financieros, recursos tecnológicos y en donde convergen todos estos es en la gestión de

las tecnologías de la información fusionando así la gestión administrativa con la gestión de TI.

Para Disterer (2013) La información y los sistemas de información están expuestos a riesgos cada vez más altos, esto por los crecientes procesos de negocios proporcionados por la tecnología de la información, así como un mayor manejo de información digital en redes dentro de las empresas y también con proveedores externos a las mismas.

Un eficaz SGSI ayuda a reducir los riesgos y prevenir las brechas de seguridad. Las normas ISO 27000, 27001 y 27002 forman un marco para diseñar y operar un SGSI, basado en experiencias duraderas de desarrollo. Con estas empresas se ofrece la oportunidad de alinear sus procedimientos de TI, además de métodos para garantizar un nivel adecuado de seguridad de la información alineados a un estándar internacional.

Certificación de un SGSI según ISO 27001 también proyecta una imagen positiva a través de la verificación de una gestión sistemática de la seguridad de la información, demuestra una "prestación de servicios de vanguardia" en relación con seguridad de información. Las organizaciones pueden demostrar que son "lo suficientemente robustas" para proporcionar servicios de TI de forma segura.

Por otro lado, Năstase, Năstase, & Ionescu (2009) indica que cada proceso, decisión de gestión y el presupuesto representan un factor clave, los gerentes deben evitar implementaciones costosas y desenfocadas de estándares y mejores prácticas priorizando dónde y cómo usar los estándares y prácticas. La empresa debe tener un plan de acción efectivo que se adapte a sus circunstancias y necesidades particulares. Primero, es importante que la junta directiva se haga cargo del gobierno de TI y establezca la dirección que debe seguir la gerencia. La gestión debe ser guiada por la manera de alinear las iniciativas de TI con las necesidades comerciales reales y asegurar que la administración entienda sobre el impacto potencial en el negocio de los riesgos relacionados con la TI. La junta debe también enfatizar en que el rendimiento de TI se mida y se informe al directorio y debe establecer un consejo de gobierno de TI con la

responsabilidad de comunicar los problemas de TI entre el consejo y la dirección. Y, por último, pero no menos importante, el consejo debería insistir en el uso de un marco de gestión para el gobierno de TI basado en un enfoque común y de un marco de mejores prácticas para la gestión de servicios de TI y seguridad basada en un estándar global como ISO/IEC 27002.

Otro punto de vista es el de Nicolás (2015) quien en su trabajo de investigación indica que los sistemas de información, sus datos y la información en sí, representan para cada organización los activos más valiosos, por lo que otorgar las protecciones necesarias para precautelar su integridad es sumamente necesario. Para descubrir vulnerabilidades y amenazas se realizan diferentes tipos de diagnósticos estableciendo de esta manera el estado actual de la organización empresarial en el marco de la seguridad, tomando como referencia la evaluación de riesgos, procesos de análisis y la normativa vigente. Para establecer el estado actual de las diferentes instituciones, se parte del análisis y evaluación de riesgos, verificación de controles existentes, pruebas de software y monitoreo de los sistemas instalados; así, identificar las causas probables de incidentes y proponer soluciones para mitigarlas.

Para Gehrmann (2012) la gestión de la tecnología de la información (TI) propone guiar y controlar un grupo de recursos con la finalidad de lograr un objetivo particular. Esta gestión abarca varias dimensiones dentro de una organización, entre las que se pueden citar los recursos humanos, los recursos financieros y los recursos tecnológicos como dimensiones clave relacionadas con la Gestión de TI.

Existen varias metodologías, estándares, herramientas, marcos y buenas prácticas para gestionar tecnologías de la información. Los más aplicables y utilizados hoy en día son ISO / IEC 27002, COBIT e ITIL. Cada uno tiene sus aspectos positivos y sus limitaciones. El uso eficiente de TI por parte de las organizaciones es un objetivo que debe alcanzarse y ha sido buscado por muchas compañías. Algunas de estas empresas ya han alcanzado el nivel de complejidad requerido por el uso de estas tecnologías, adquiriendo una ventaja competitiva en el mercado al que pertenecen. Este nivel puede ser alcanzado a través de la gestión de TI, sin embargo, la gestión de TI

tiene un enfoque mucho más amplio y es extremadamente complejo. Contiene acciones mucho más integrales que la administración de tecnología de la información, para los usuarios de estas tecnologías y procesos.

Un área de administración de TI hoy debe estar compuesta por la combinación de dos directrices, la tecnología de la información en sí misma y, en consecuencia, la gestión empresarial. Esto se debe a que la TI puede asumir diferentes aspectos dentro de la organización, dependiendo de la perspectiva existente. Esto puede asumir aspectos de las aplicaciones e infraestructura de TI que forman parte de los procesos y servicios de la empresa cuya responsabilidad y soporte técnico son proporcionados por los proveedores.

En otros aspectos, la organización puede tener su propio conjunto de habilidades y recursos para respaldar la aplicación y TI. Implementando y aplicando una gestión informática.

Según Álvarez & Fernández (2012) establecen en su investigación que la Norma ISO/IEC 27002 es el conjunto de directrices orientados al inicio, implementación, control y mejora de la gestión de la seguridad de la información en cada institución. Muestra un catálogo de buenas prácticas que, a partir de la experiencia y participación de varios colaboradores, quienes previamente han sido informados y comunicados acerca de los objetivos que de manera común han sido aceptados para facilitar, agilizar y obtener gestión de la seguridad de la información.

Para Franco & Guerrero (2013) presentan un análisis en donde señalan que la competitividad de hoy en día de las empresas independientemente de su giro de negocio tiene como un factor determinante a la gestión de la seguridad de la información, indican que "La gestión del riesgo y el aseguramiento de la información se apoyan en la aplicación de normas internacionales como el estándar ISO/IEC 27002".

Ahora, para Cárdenas (2018) en su estudio realizado sobre el desarrollo del diseño de una política de seguridad de la información, enfocada a los sistemas médicos

de AXXIS Hospital, analiza la importancia de manejar procesos eficientes ante la presencia de incidentes de seguridad en los sistemas informáticos en donde se encuentra alojada la información de Historias Clínicas de los pacientes, abarca un abanico de controles y normas diseñadas para que la información sea confiable, esté disponible en las diferentes unidades manteniendo la confidencialidad de la misma. En este trabajo se evalúan los diferentes sistemas que manejan cada unidad y la vinculación de la información de los diferentes sistemas que intercambian datos, sin embargo, aún no se establecen normas y controles para el área de la infraestructura de red. Además, analiza las leyes vigentes en la República del Ecuador en el marco regulatorio del COIP en cuanto a la divulgación de datos e información confidencial de pacientes, para enfocar su estudio en este tipo de vulnerabilidades.

El trabajo complementario de la política desarrollada es ahora el diseño de la política de seguridad enfocada en la infraestructura de red, el resguardo de la integridad física de los equipos y que el personal de la comunidad AXXIS pueda estar en la competencia de reconocer riesgos y vulnerabilidades para minimizarlos al máximo y contar con un sistema de red con protecciones robustas limitando perímetros de seguridad y controlando el acceso físico del mismo.

Otro trabajo realizado sobre políticas de seguridad en base a la ISO / IEC 27002:2013 es el de Mosquera, Sarabia y Pacheco en el Hospital Regional José David Padilla Villafañe Ese, en donde se describe la importancia de la seguridad de la infraestructura de red, las consecuencias de no tenerla, el cambio y buenas prácticas al aplicarla dentro de la institución, el tener la estructura clara de la red y donde se concentran las actividades de gestión de los sistemas de información, con la finalidad de manejar controles que la Norma ISO/IEC 27002:2013 otorga para la administración de los activos de red es vital para un correcto desarrollo en las actividades diarias del negocio.

Se toma como referencia el criterio de Álvarez y Fernández, que se alinean con este trabajo en conservar los dominios de la norma ISO/IEC 27002:2013 y los controles que esta exige para la adecuada gestión de la información de AXXIS, dentro de cada

organización es importante garantizar que los datos y la infraestructura de red por donde cursan, tengan estrictos estándares de control para garantizar la integridad, confidencialidad y disponibilidad de la misma; en este contexto, si se trata de instituciones de Salud, como AXXIS Hospital, la no divulgación de la información es prioritario ya que al tener historias clínicas, resultados de exámenes y facturación en tiempo real, y perder uno u otro parámetro, la continuidad del negocio va a verse afectada seriamente, por lo que, con los controles de la norma seleccionados, se tiene una directriz para un correcto manejo de la red y la estructura de su estudio es muy similar al desarrollado en esta institución de salud.

CAPÍTULO II

MARCO TEÓRICO

La necesidad de crear en una organización una política de seguridad se debe a que continuamente se trata de mitigar vulnerabilidades, las mismas que podrían desencadenar una serie de problemas que causarían un alto impacto en la continuidad del negocio, para Guerrero, Lasso, & Legarda (2015) el concepto de vulnerabilidad es la existencia de una amenaza ya sea de forma premeditada o de manera accidental, en un sistema informático, dando como resultado la pérdida y hurto de la información, a este concepto se podría agregar suplantación, modificación o alteración de la misma, todo esto siendo contraproducente para una organización.

En este contexto, qué se puede considerar como riesgo, ya que según Solarte et al. (2015) define como riesgo a "problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas." (p.498)

Las amenazas informáticas para Solarte et al. (2015) se relacionan con la posibilidad de que un evento se pueda presentar, no se puede premeditar y en estos eventos provocan un daño material o inmaterial sobre los activos, elementos informáticos y sistemas de información. Una amenaza se considera como ataques cometidos por personal interno o externo, ocasionando daños a la infraestructura tecnológica, a los sistemas de información o a la misma información de la organización. (p.498)

En el campo de las amenazas, se encuentran también las amenazas físicas, en donde un atacante tiene acceso físicamente a los dispositivos de la organización ocasionando problemas, que pueden identificarse a tiempo para evitar daños significativos en las organizaciones.

Para Aguilera (2010) Una de las medidas para mitigar riesgos y amenazas de infraestructuras de red e información, es establecer una disciplina que permita diseñar las normas, procedimientos, métodos y técnicas orientadas a precautelar la infraestructura física y así conseguir un sistema de información seguro y confiable.

En base a esta consideración, se deben determinar parámetros para tener el correcto dimensionamiento de los sistemas que se van a proteger la infraestructura de red y como consecuencia la seguridad de la información.

2.1.1. Seguridad de la Información.

2.1.2.

Para García (2009), la seguridad de la información, son todas las medidas enfocadas a la prevención y corrección de incidentes de seguridad de las organizaciones y de los sistemas tecnológicos para la protección y resguardo de datos e información para mantener su confidencialidad, integridad y disponibilidad.

2.1.3. Infraestructura de red

Según Castro, Devis & Olivera (2011) es un conjunto de equipos y dispositivos informáticos conectados entre sí, para transmitir datos compartiendo recursos e información. Si bien existen diversas clasificaciones de redes informáticas, la más reconocida es aquella que las distingue de acuerdo a su alcance.

2.1.4. Sistemas de Información

Las observaciones de Aguilera (2010) es que en un Sistema de Información se relacionan y coordinan entre sí para contar con elementos organizados para facilitar de

manera eficaz la funcionalidad o actividad global de una empresa para alcanzar sus objetivos.

Los elementos que se toman en consideración son:

• Recursos. Equipamiento o instalaciones físicas como: conexiones, componentes, conectores, periféricos, ordenadores, componentes; y lógicos, como sistemas operativos y aplicaciones informáticas.

• Equipo humano. Directamente el personal contratado por la organización.

• Información. Son los datos creados u organizados y transmitidos que tienen importancia y validez. La información puede estar contenida en cualquier tipo de soporte.

• Actividades que la organización realiza en la empresa, relacionadas o no con la informática.

2.1.5. Análisis de riesgos

Para Aguilera (2010), analizar el nivel de vulnerabilidad de cada evento que pueda presentarse en la empresa permite determinar amenazas para así valorar el impacto que un ataque causaría sobre todo o parte de la infraestructura de red.

Una de las metas del análisis de riesgos es mitigarlos o controlarlos así poder determinar y dimensionar cuáles serán los servicios y requerimientos para conseguir un sistema de información y su infraestructura de red seguros.

Para Paredes (2006) todo se enmarca dentro de un análisis para garantizar la integridad, confidencialidad y disponibilidad de la información, en donde se determine como integridad al modelo en donde la información se crea o modifica por el personal autorizado para hacerlo. Confidencialidad, que la información no sea divulgada y finalmente y por último disponibilidad, que la información esté disponible en cualquier momento que los usuarios lo requieran.

2.1.6. Perímetro de seguridad

Según Sarubbi (2008) la defensa perimetral es reforzar los puntos de acceso de la red privada con la red externa, evaluando y planeando los requerimientos del sistema, implementando seguridades para bloquear el tráfico no deseado, ubicar sistemas de monitoreo y detección de intrusos mediante alertas para la ejecución de acciones de protección y defensa oportunas.

Según Chiu (2006), es necesario mantener un control de acceso a la infraestructura de red, lo cual se logra a través de identificaciones, autenticaciones y autorizaciones para el ingreso confiable.

Para la elección de un control que permita realizar una medición del estado actual de la red en cuanto a seguridad, es necesario adoptar una metodología de evaluación de riesgos y vulnerabilidades, entre las cuales se puede destacar a Magerit y Cramm, para el estudio y clasificación por niveles de afectación en el momento de presentarse un evento de seguridad.

2.2.METODOLOGÍA MAGERIT

Según Abril, Pulido y Bohada (2013) es una metodología creada con la finalidad de cumplir objetivos planteado en torno a la situación actual de seguridad de sistemas de información, mediante la incorporación de medidas de seguridad, así, cubrir todas las necesidades sin dejar elementos fuera del análisis, sino estudiarlos a profundidad, minimizar riesgos, reducir vulnerabilidades, asegurando los sistemas durante toda su implementación o desarrollo.

Es una de las metodologías con mayor aceptación a nivel empresarial, ya que es un soporte para auditorías, acreditaciones o certificaciones que puedan ser alcanzadas por las organizaciones, en la Figura 1, se puede revisar el diagrama de procesos para evaluar los riesgos.

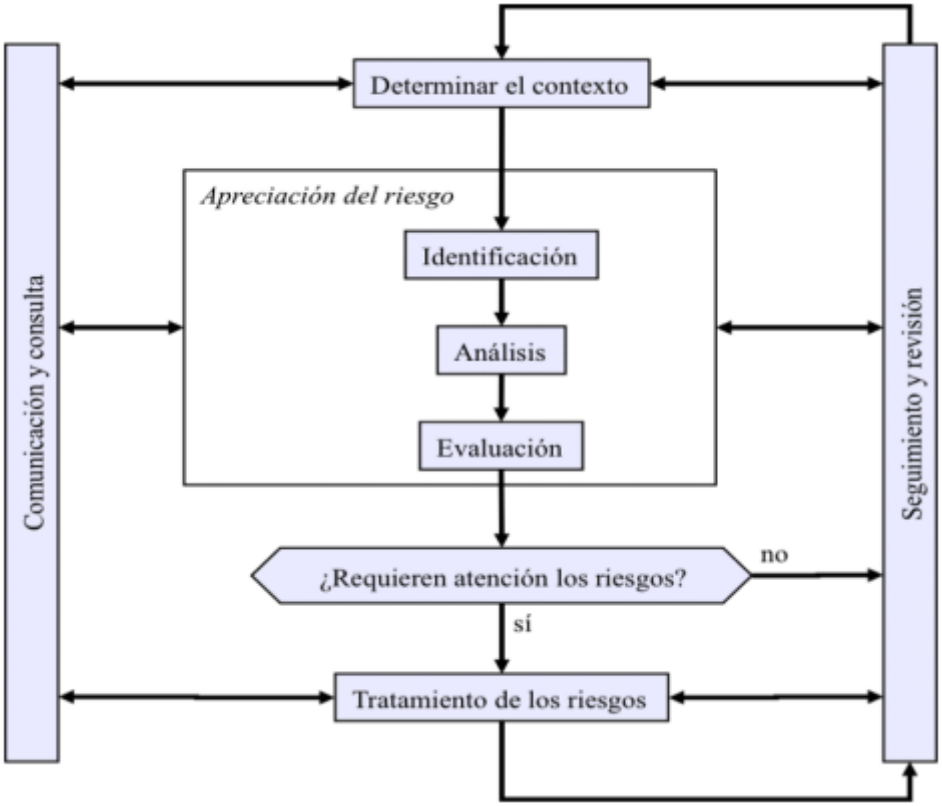


Figura 1 *Proceso de gestión de riesgos*

Fuente: *Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (2012)*

La metodología Magerit, busca los siguientes objetivos:

- Estudiar los riesgos que se presentan en las organizaciones.
- Análisis de cada uno de los riesgos detectados.
- Medidas que se deben adoptar para la prevención, conocimiento, impedimento o control de riesgos detectados en una organización, disminuyendo su impacto.
- Técnicas de evaluación, homologación y certificación de seguridad de los sistemas de información a largo plazo.

En la Figura 2, se observan los elementos del análisis de riesgos para la valoración de la situación actual de la organización.

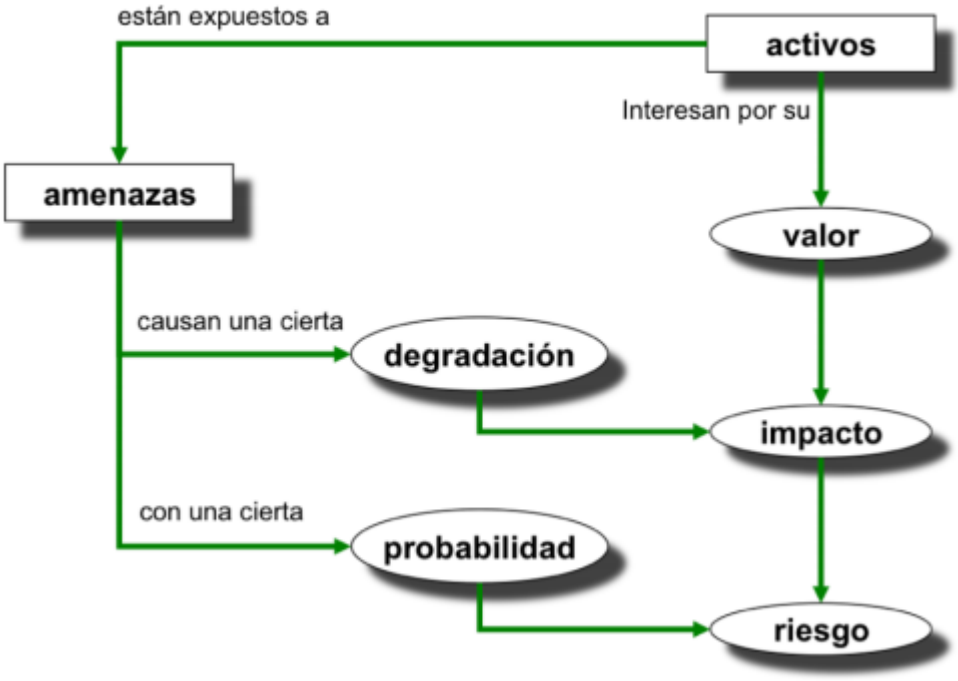


Figura 2 *Elementos del análisis de riesgos potenciales*

Fuente: *Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (2012)*

Una vez realizado el análisis de riesgos, se realiza un estudio de la literatura existente en las políticas de seguridad que puedan cubrir las necesidades detectadas, para que sean adoptadas por la organización y se creen los controles para minimizar su impacto, entre las normas que se destacan está la familia de ISO 27000, COBIT e ITIL, entre otras.

2.3. METODOLOGÍA CRAMM

Según Crespo & Cordero (2016), CRAMM (CCTA Risk Analysis and Management Method), es una metodología de análisis y gestión de riesgos informáticos orientados al entorno de organizaciones empresariales utilizado a nivel internacional.

Metodología desarrollada en 1985 por la Agencia Central de Cómputo y Telecomunicaciones en Reino Unido con el objetivo de proteger la confidencialidad, integridad y disponibilidad de los sistemas y activos de información, para el análisis y control de la gestión de riesgos, que se adapta a cualquier tipo de sistemas y redes de información durante el estudio de factibilidad.

2.4. ISO 27000

Para Montaño (2013) son estándares desarrollados por ISO (*International Organization Standardization*) y por IEC (*International Electrotechnical Commission*) para otorgar una guía sobre gestión de seguridad de la información que pueden ser utilizados en cualquier tipo de organización independientemente del giro de negocio ya sea público o privada.

2.5. ISO 27001

Según Montaño (2013) es una norma que define funciones para un sistema de gestión de seguridad de la información, permite tener una documentación de las necesidades de la organización para la creación, implementación, funcionamiento, y revisión de este sistema.

2.6.ISO 27002:2013

Según Ramos, Urrutia, & Bravo (2017) la Norma ISO 27002:2013, es un grupo de controles que se aplican en la política de seguridad de la información, en el trabajo de investigación titulado “Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002: 2013 para la Cooperativa Codelcauca”, toman como base esta norma ya que proporciona soporte y criterios orientados a garantizar la seguridad de la información, si bien no existe un sistema que brinde el 100% de seguridad de la información, con los dominios y los controles que la

norma provee, se pretende cubrir al máximo posible las vulnerabilidades que se puedan encontrar dentro de las organizaciones y así, con una metodología propia y estricta mantener una adecuada gestión, organización y asegurar la información dentro de procesos cuidadosos, documentados, basados en objetivos y controles de la seguridad informática.

Los controles que la norma provee, se detallan a continuación, de estos se tomarán los más adecuados según los resultados del análisis de riesgos para el giro del negocio:

- **5. Políticas de seguridad.** Se referencia a la creación del documento, el cual debe mantener la formalidad de ser aprobado por la alta gerencia y luego ser socializada en la institución.
  La política debe ser cumplida por los empleados de la organización, se deben revisar los resultados obtenidos con la aplicación de la misma, debe ser actualizada en el tiempo y si existen cambios o modificaciones, para mantener la eficacia de la misma.

- **6. Aspectos organizativos de la seguridad de la información.** Este dominio está enfocado en la parte interna de la organización, se definen responsabilidades de cada representante, con la finalidad de que sólo el personal autorizado pueda tener acceso a los recursos.

- **7. Seguridad ligada a los recursos humanos.** Se definen términos de contratación de los empleados para mantener un formato de análisis previo al ingreso de personal nuevo, capacitaciones al personal existente y así poder entregar técnicas y herramientas a los empleados para poder detectar vulnerabilidades y sean una fuente de apoyo.

- **8. Gestión de activos.** En este dominio se determinan los inventarios de la infraestructura de red y equipos de red y comunicación y cómputo, se entregan los custodios, se parametriza su utilización y devolución.

- **9. Control de accesos.** Se gestiona el acceso a los usuarios de la red, para autenticar y autorizar el uso de la infraestructura. Se establecen privilegios a los usuarios, así como restricciones en áreas de estricta confidencialidad.

- **10. Cifrado.** Utilización de criptografía.

- **11. Seguridad física y ambiental.** Este dominio es el más importante para el desarrollo de este proyecto, ya que específicamente detalla los controles en el perímetro de la red, como manejar los accesos a la misma, las seguridades que se deben implementar para el manejo de equipos, seguridades de instalación del cableado, entre otras.

- **12. Seguridad en la operativa.** Este dominio establece controles para aplicativos o sistemas operativos, prevé de las herramientas para brindar protecciones ante eventuales amenazas. Es importante documentarlo y que sea aprobado por gerencia, si es necesario realizar algún cambio, estos deben ser documentados.

- **13. Seguridad en las telecomunicaciones.** Se establecen diferentes lineamientos de seguridad para asociados a la red, acuerdos de confidencialidad, para quienes utilizan sus recursos.

- **14. Adquisición, desarrollo y mantenimiento de los sistemas de información.** Se basa en requisitos de seguridad para los sistemas de información, aún si estos son parte de un desarrollo, se debe documentar para poder identificarlos y así probarlos, manejar cambios y evaluar sus aplicaciones en la organización.

- **15. Relaciones con suministradores.** Maneja los diferentes controles que deben establecerse con los proveedores de la organización.

- **16. Gestión de incidentes en la seguridad de la información.** Determina responsabilidades, procedimientos y aprendizajes ante la presencia de un evento, el tiempo de respuesta y cómo afrontarlo.

- **17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.** Se establecen parámetros para planificar, implantar y verificar controles de seguridad de la información, para que de esta manera se pueda garantizar la continuidad del negocio. Los planes deben ser sometidos a pruebas, actualizaciones y cambios para ser sometidos a evaluación.

- **18. Cumplimiento.** Se revisará la legislatura, derechos de propiedad intelectual, protecciones y regulaciones para verificar el cumplimiento de la política y poder evaluar el impacto de la misma en la organización.

CAPÍTULO III

ANÁLISIS SITUACIONAL

AXXIS es una organización de salud ubicada en el Distrito Metropolitano de Quito, tiene más de 10 años de crecimiento institucional, actualmente cuenta con dos torres, la primera, dedicada a la medicina ocupacional, tiene el área de consulta externa en la Torre de Consultorios, y es con la que se inicia esta institución.

Figura 3 *Área de Torre Consultorios Hospital AXXIS*

Fuente: *AXXIS Hospital (2019)*

La instalación y ubicación de los racks de comunicación es un punto crítico de la organización, especialmente en la torre de consultorios, en todas las áreas de consulta externa el rack de piso se encuentra junto al puesto de la secretaria clínica, con fácil acceso y sin protecciones, quedando completamente expuestos los activos de red y de fácil acceso, lo que se puede evidenciar en la figura 3 y en las fotografías de pisos diferentes.

Los Racks tienen varios factores de riesgo: el primero es que la conexión a la toma eléctrica, se encuentra por fuera del mismo; el segundo es que los cables de red están expuestos y si un atacante lo requiere, puede desconectarlos, cortarlos o arrancarlos con mucha facilidad.

Otro incidente que puede ocurrir es que, al momento de limpieza, por error humano, se desconecte el cable de luz, quedándose el piso sin conexión a la red, a los servicios de la misma, por lo tanto, se pierde la disponibilidad de la información.

Figura 4 *Rack Piso 1, Torre Consultorios Hospital AXXIS*
Fuente: *AXXIS Hospital (2019)*

Otra de las imágenes que se puede observar, se evidencia la misma vulnerabilidad de acceso físico a la red de datos de la torre consultorio.

Figura 5 *Rack Piso 3, Torre Consultorios Hospital AXXIS*

Fuente: *AXXIS Hospital (2019)*

Situación repetitiva en cada rack de piso de esta torre, uno de los objetivos que se tiene al plantear la política de seguridad, es precautelar la seguridad de la red así no perder disponibilidad de la información garantizando su integridad física.

La segunda torre es Hospitalización, en esta se encuentran las áreas de Emergencia, Hospitalización, Administración, Gastroenterología, Rehabilitación, Restaurante, Consultorios, Docencia, Neonatología, Cirugía y UCI.

Figura 6 *Torre Hospitalización. Hospital AXXIS*

Fuente: *AXXIS Hospital (2017)*

Además, físicamente el Data Center de AXXIS Hospital se encuentra en el Subsuelo 1, haciéndolo vulnerable ante una inundación por fuertes lluvias. La puerta de acceso al mismo no tiene mayor protección y es una puerta de vidrio, considerando además que varios departamentos comparten el área de trabajo para cada una de sus funciones.

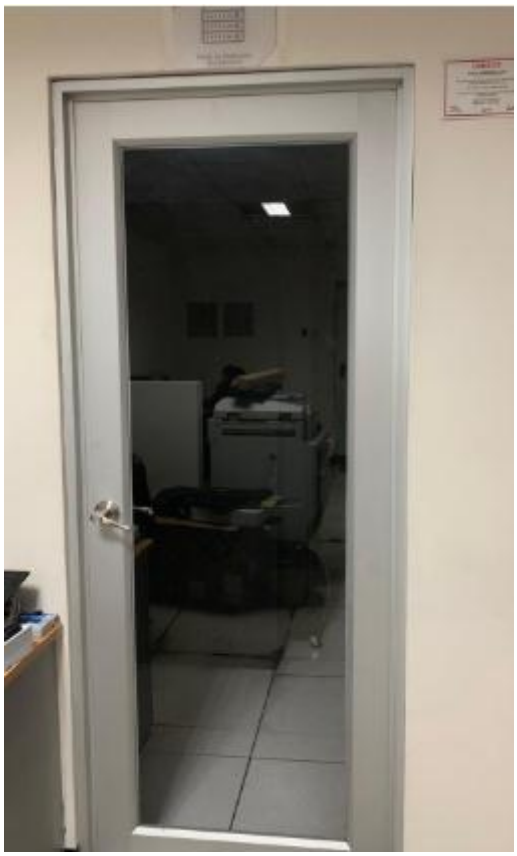


Figura 7 *Ingreso al Data Center*

Fuente: *AXXIS Hospital (2019)*

Al Data Center se interconectan las torres de consultorios y hospitalización, se prevé que se conecte la infraestructura de red del nuevo edificio Materno Infantil. Otra vulnerabilidad detectada es que se ha instalado un rack de piso en un ducto de revisión, como se evidencia en la siguiente fotografía.

Figura 8 *Rack Piso 1, Torre Hospitalización. Hospital AXXIS*

Fuente: *AXXIS Hospital (2019)*

De igual manera, no existe mayor seguridad para acceder a este Rack, siendo un punto vulnerable para la organización, los cables se encuentran con fácil acceso y si personal de mantenimiento ingresa, puede causar daños por error humano.

3.1. ANÁLISIS ORGANIZACIONAL

AXXIS hospital se caracteriza por manejar procesos transversales en sus actividades como institución de salud, la figura 9 muestra el diagrama de funcionalidades de AXXIS, donde se puede observar la distribución de procesos internos desde alta gerencia, hacia las demás unidades que conforman el hospital, encabezadas cada una por sus gerencias y direcciones administrativas, pero la distribución de red de datos es compartida para cada una de estas y es por esto que se necesita fortalecer con un sistema de gestión eficiente, basado en políticas de seguridad que resguarden la información del mismo.

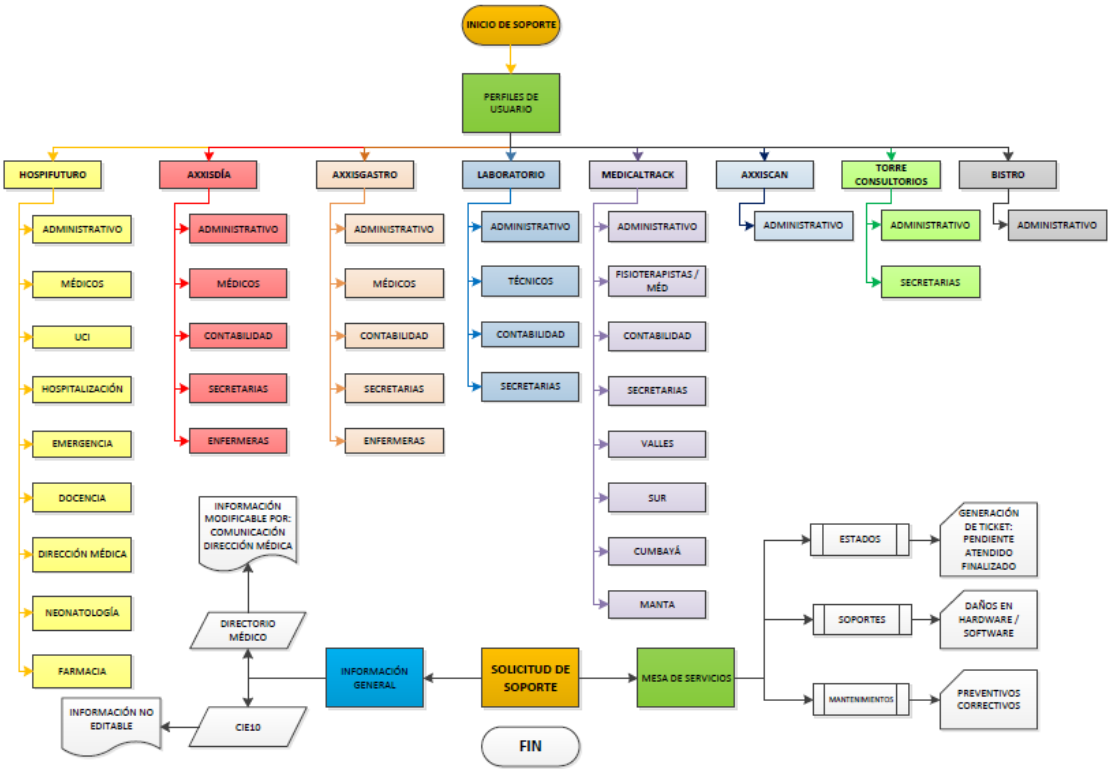


Figura 9 *Diagrama de funcionalidades de TICs.*

Fuente: *AXXIS Hospital (2019), elaborado por la autora*

Bajo este esquema, también se presenta el diagrama de red del Hospital, en donde cada una de las unidades descritas en la Figura 10, se interconectan para acceder a la información que cada una requiera ya sea esta de historias clínicas, resultados de exámenes, información contable, recursos humanos, convenios y comunicación en general.

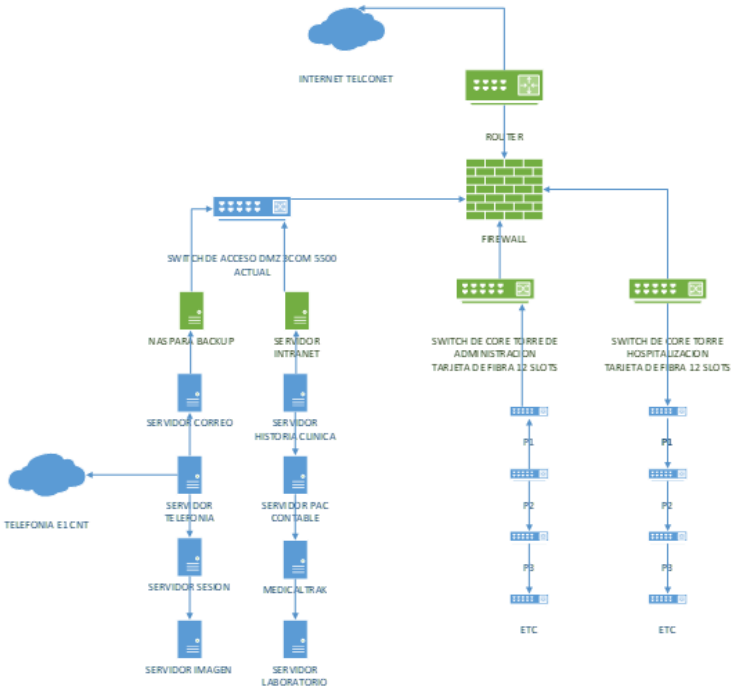


Figura 10 *Diagrama de la red actual del Hospital AXXIS*

Fuente: *AXXIS Hospital (2019), elaborado por la autora*

3.2. ESTIMACIÓN DEL IMPACTO

Una vez que se ha descrito la estructura física del hospital y los edificios que lo componen, se evalúa el personal que trabaja actualmente en la institución, para poder realizar una matriz de riesgo en donde se valoren las vulnerabilidades presentes en la organización con los actores directos y usuarios de red. AXXIS Hospital tiene una nómina comprendida por 185 colaboradores administrativos, como staff de médicos tiene un total de 356 entre accionistas y asociados; es el personal que directamente tiene ingreso y uso a la infraestructura de red, los pacientes del hospital, no serán considerados para el estudio.

Tabla 1 *Personal que conforma la población*

POBLACIÓN	PERSONAS
ADMINISTRATIVOS	185
MÉDICOS	356
TOTAL	**541**

Fuente: *AXXIS Hospital (2019), elaborado por la autora*

En este caso, se realizó una encuesta al 100% de la población, es decir, empleados, médicos, secretarias, administrativos, construcción, entre otros, con el objetivo de determinar el nivel de conocimiento sobre los activos de red del hospital, los procesos que deben acatar para resguardar la seguridad de equipos e información, acorde la perspectiva de cada usuario.

Con la autorización de la dirección administrativa de HOSPIFUTURO S.A., se realizó un banco de preguntas para la elaboración de la encuesta al personal descrito anteriormente, mediante el área de Comunicación, se socializó la aplicación de la encesta a la Gerencia de cada Unidad y se empezó a coordinar los horarios y turnos especialmente del personal rotativo de AXXIS con sus respectivas Jefaturas, logrando cumplir con el objetivo de tener el 100% del personal encuestado.

Adicionalmente se realizó un cuestionario para una entrevista al personal del departamento de TICs del hospital, encabezados por el jefe del área, Ing. Galo Cárdenas; las preguntas se direccionaron para conocer sobre la administración de los recursos de la red y las acciones preventivas y correctivas ante incidentes de seguridad.

En una reunión con el departamento de TICs, se da a conocer el alcance de la investigación, para que se entreguen respuestas lo más cercanas a la realidad con la finalidad de obtener resultados que reflejen el accionar del personal responsable de la infraestructura, activos y servicios de red que maneja el hospital, dimensionar el nivel de conocimientos ante la presencia de accidentes e incidentes en seguridad de la información y las medidas que actualmente se toman para mitigar riesgos y vulnerabilidades.

Dentro de las actividades y responsabilidades del departamento de TICs están:

- Administración de EXMED.
- Administración de Central Telefónica.
- Administración de Correos electrónicos.
- Administración del sistema PAC.
- Soporte a usuario Final.

- Administración, instalación y manejo de Sistema de Control de Incendios.
- Administración, instalación y manejo de Sistema de CCTV.
- Administración, instalación y manejo de Sistema de Control de Accesos.
- Mantenimiento preventivo y correctivo de equipos de red del Hospital y todas las Unidades.
- Desarrollo e implementación de Intranet.
- Administración de Sistemas de respaldos para el Hospital y todas las Unidades.

En base a la información recopilada, se pueden establecer los activos de red que son importantes para la organización y que se debe precautelar su integridad para no poner en riesgo la continuidad del negocio del Hospital.

3.3. ANÁLISIS DE RIESGOS

Se utiliza la matriz de análisis de riesgos para determinar los controles y dominios de la norma ISO/IEC 27002:2013 que pueden aplicarse para el control de acceso a la infraestructura de red enfocados a precautelar la seguridad física y perimetral de la institución.

3.3.1. Matriz de riesgo

Las metodología descritas anteriormente pueden ser aplicables en la organización, ambas brindan un análisis de gestión de riesgos, siguen lineamientos internacionales de control, para el desarrollo de la Política de seguridad de la infraestructura de red basada en la ISO/IEC 27002:2013 se utilizará la metodología Magerit, por ser una de las más utilizadas a nivel empresarial ya que se adapta a procesos de auditorías, acreditaciones y certificaciones y en caso de AXXIS, son procesos de mejora continua dentro de la organización, además de tener un lineamento con la norma ISO/IEC27001, que permite tener una visión global y se enmarca dentro

de los procesos de la familia ISO que es con quienes AXXIS mantiene sus certificaciones de calidad. La matriz de riesgo, permite evaluar los resultados obtenidos en la investigación, para esto se realiza una codificación de identificación de los riesgos detectados de la siguiente manera:

Tabla 2 *Codificación del riesgo*

CODIFICACIÓN DEL RIESGO			
ESTRUCTURA		RX000	
SIGLA	**IDENTIFICACIÓN**		
R	RIESGO		
X	CATEGORÍA	**SIGLA**	**DESCRIPCIÓN**
		I	INTERNO
		E	EXTERNO
		A	ADMINISTRACIÓN
		T	TÉCNICO
		O	OPERACIONAL
000	Asignación de un número secuencial		

Fuente: *Elaborado por la autora*.

Para la valoración del riesgo detectado se maneja las categorías presentadas en la Tabla 3, se utiliza el promedio de la vulnerabilidad detectada, contra el impacto que causaría en el hospital, de esta manera se obtiene la criticidad de que un evento presente pueda llegar a desencadenar, para de esta manera poder contemplarlo en la política de seguridad y saber cómo afrontarlo.

Tabla 3 *RIESGO*

NIVEL DEL RIESGO	INTERVALO
ALTO	4 -5
MEDIO	2.1 – 3.9
BAJO	0 – 2

Fuente: *Elaborado por la autora*.

En la tabla 4 se realiza la recolección y análisis de resultados de la encuesta realizada al personal de AXXIS Hospital, los riesgos encontrados son evidentes y se debe mitigarlos para que un hospital de alto nivel, cuente con una infraestructura confiable (ANEXO 1).

Tabla 4 *Estimación de la criticidad*

ESTIMACIÓN DE LA CRITICIDAD									
TIPIFICACIÓN RIESGO	**RIESGO EVALUADO**	**OBSERVACIÓN**	**CRITICIDAD**	**VULNERABILIDAD**	**IMPACTO**	**VOTO / CARGOS**	**Calificación Funcionario Nro. 1 (Gerente Administrativo)**	**Calificación Funcionario Nro. 2 (Gerente de sistemas)**	**Calificación Funcionario Nro. 3 (Jefe de área médica)**
RT001	Falla de UPS	AXXIS HOSPITAL	Alto	3,7	5,0	VOTO IMPACTO	5,0	5,0	5,0
						VOTO VULNERABILIDAD	2,0	4,0	5,0
RE002	Corte de energía eléctrica	AXXIS HOSPITAL	Medio	2,3	2,5	VOTO IMPACTO	3,0	3,5	1,0
						VOTO VULNERABILIDAD	3,0	3,0	1,0
RA003	Falta de control ambiental	AXXIS HOSPITAL	Medio	3,0	4,0	VOTO IMPACTO	4,0	4,0	4,0
						VOTO VULNERABILIDAD	3,0	3,0	3,0
RA004	Falta de control de acceso físico a oficinas	AXXIS HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	5,0	4,0	4,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0
RA005	Falta de control de acceso a proveedores	AXXIS HOSPITAL	Alto	4,3	4,0	VOTO IMPACTO	5,0	4,0	3,0
						VOTO VULNERABILIDAD	5,0	5,0	3,0
RI006	Usuarios no conocen infraestructura de red	AXXIS HOSPITAL	Medio	3,0	1,7	VOTO IMPACTO	2,0	1,0	2,0
						VOTO VULNERABILIDAD	3,0	3,0	3,0
RA007	No hay control de restricción de accesos	AXXIS HOSPITAL	Alto	4,0	4,3	VOTO IMPACTO	4,0	4,0	5,0
						VOTO VULNERABILIDAD	4,0	4,0	4,0

ESTIMACIÓN DE LA CRITICIDAD									
TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
RT002	Falla en equipos de ventilación	AXXIS HOSPITAL	Medio	3,0	3,0	VOTO IMPACTO	4,0	3,0	2,0
						VOTO VULNERABILIDAD	4,0	4,0	1,0
RE002	Inundaciones	AXXIS HOSPITAL	Medio	1,7	4,0	VOTO IMPACTO	4,0	4,0	4,0
						VOTO VULNERABILIDAD	2,0	1,0	2,0
RE003	Terremotos	AXXIS HOSPITAL	Bajo	2,0	2,0	VOTO IMPACTO	2,0	2,0	2,0
						VOTO VULNERABILIDAD	1,0	3,0	2,0
RI002	Incendios	AXXIS HOSPITAL	Medio	3,3	4,3	VOTO IMPACTO	4,0	4,0	5,0
						VOTO VULNERABILIDAD	3,0	5,0	2,0
RO001	Desconexión física al ISP	AXXIS HOSPITAL	Medio	2,0	3,0	VOTO IMPACTO	4,0	3,0	2,0
						VOTO VULNERABILIDAD	2,0	2,0	2,0
RT003	Corte de servicios a servidores internos	AXXIS HOSPITAL	Alto	3,3	5,0	VOTO IMPACTO	5,0	5,0	5,0
						VOTO VULNERABILIDAD	3,0	3,0	4,0
RE004	Corte del servicio MPLS del proveedor principal	AXXIS HOSPITAL	Medio	3,7	3,7	VOTO IMPACTO	3,0	4,0	4,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0

ESTIMACIÓN DE LA CRITICIDAD									
TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
RT004	Falla del Core de comunicaciones	AXXIS HOSPITAL	Medio	3,3	3,7	VOTO IMPACTO	4,0	4,0	3,0
						VOTO VULNERABILIDAD	3,0	4,0	3,0
RT005	Saturación en el Core de comunicaciones	AXXIS HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	5,0	4,0	4,0
						VOTO VULNERABILIDAD	4,0	3,0	4,0
RO002	Saturación de carga en el enlace	AXXIS HOSPITAL	Bajo	2,0	1,7	VOTO IMPACTO	2,0	2,0	1,0
						VOTO VULNERABILIDAD	3,0	1,0	2,0
RE005	Intermitencia del servicio de Internet	AXXIS HOSPITAL	Bajo	1,0	3,0	VOTO IMPACTO	3,0	2,0	4,0
						VOTO VULNERABILIDAD	1,0	1,0	1,0
RO003	Interrupción del firewall	AXXIS HOSPITAL	Bajo	1,7	2,0	VOTO IMPACTO	2,0	3,0	1,0
						VOTO VULNERABILIDAD	1,0	2,0	2,0
RA005	Acceso no autorizado al Data Center	AXXIS HOSPITAL	Medio	1,3	5,0	VOTO IMPACTO	5,0	5,0	5,0
						VOTO VULNERABILIDAD	1,0	1,0	2,0
RI003	Abuso de privilegios de acceso	AXXIS HOSPITAL	Medio	2,3	5,0	VOTO IMPACTO	5,0	5,0	5,0
						VOTO VULNERABILIDAD	1,0	3,0	3,0

ESTIMACIÓN DE LA CRITICIDAD									
TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
RO004	Errores en mantenimiento de equipos de red	AXXIS HOSPITAL	Medio	3,0	2,3	VOTO IMPACTO	2,0	3,0	2,0
						VOTO VULNERABILIDAD	3,0	4,0	2,0
RO005	Errores en mantenimiento de computadores	AXXIS HOSPITAL	Bajo	1,7	1,7	VOTO IMPACTO	2,0	1,0	2,0
						VOTO VULNERABILIDAD	1,0	1,0	3,0
RI004	Falta de protección de acceso físico a la red	AXXIS HOSPITAL	Bajo	2,0	2,0	VOTO IMPACTO	2,0	1,0	3,0
						VOTO VULNERABILIDAD	2,0	3,0	1,0
RE006	Terrorismo	AXXIS HOSPITAL	Medio	2,3	2,7	VOTO IMPACTO	3,0	2,0	3,0
						VOTO VULNERABILIDAD	3,0	3,0	1,0
RI005	Limpieza del puesto de trabajo	AXXIS HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	4,0	5,0	4,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0
RA006	Inventario de activos	AXXIS HOSPITAL	Medio	4,0	1,0	VOTO IMPACTO	1,0	1,0	1,0
						VOTO VULNERABILIDAD	5,0	3,0	4,0
RI006	Protección a la infraestructura tecnológica	AXXIS HOSPITAL	Medio	3,0	3,0	VOTO IMPACTO	3,0	3,0	3,0
						VOTO VULNERABILIDAD	3,0	4,0	2,0

ESTIMACIÓN DE LA CRITICIDAD									
TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
RA007	Identificación del personal	AXXIS HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	4,0	4,0	5,0
						VOTO VULNERABILIDAD	4,0	3,0	4,0
RI007	Abandono del puesto de trabajo	AXXIS HOSPITAL	Alto	3,0	5,0	VOTO IMPACTO	5,0	5,0	5,0
						VOTO VULNERABILIDAD	3,0	2,0	4,0

Fuente: *Elaborado por la autora.*

En la tabla 4, se pueden observar los riesgos catalogados como críticos para esta investigación, si llegara a ocurrir alguno de estos eventos, se debe tomar en cuenta los considerados como más importantes para el hospital:

- Falla de UPS.
- Falta de control de acceso físico a oficinas.
- Falta de control de acceso a proveedores.
- Falta de control de accesos a ductos.
- Corte de servicios a servidores internos.
- Saturación en el Core de comunicaciones
- Limpieza del puesto de trabajo.
- Identificación del personal.
- Abandono del puesto de trabajo.
- Terrorismo

3.3.2. Estimación del Riesgo.

Se puede observar la representación gráfica de los riesgos con mayor importancia y que significan una gran amenaza para el hospital, el objetivo principal es que con la implementación de la política de seguridad se puedan mitigar al máximo estas amenazas y trabajar en un ambiente confiable y seguro.

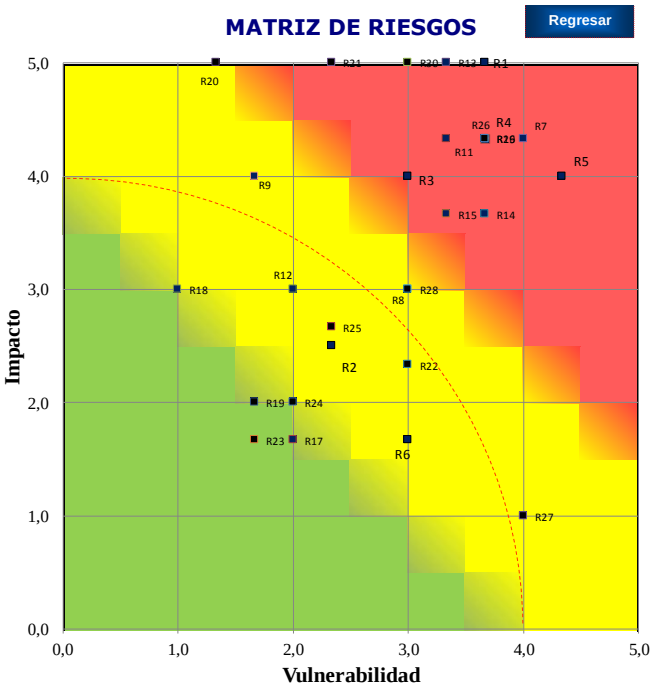


Figura 11 *Matriz de riesgos*

Fuente: Elaborado por la autora

La figura 11, muestra el mapa de calor de la Matriz de riesgo, permite visualizar tres gamas de colores descritos de la siguiente manera:

- Primero: Franja verde, la vulnerabilidad, no representa una gran amenaza y si el evento ocurre, el impacto no es significativo.
- Segundo: Franja amarilla (nivel medio), Las vulnerabilidades van desde improbables hasta probables, pero de llegar a ocurrir el evento, el impacto puede ser aún bajo, es decir se puede controlar.
- Tercero: Franja roja (nivel alto), las vulnerabilidades tienen alta probabilidad de que ocurran en el hospital y con un impacto muy alto que pondrían en riesgo la continuidad del negocio.

En base a estas consideraciones, se presenta la tabla de la norma ISO/IEC 27002:2013, en donde se describen los dominios, los objetivos de control y los controles que la norma determina para mitigar los riesgos detectados.

Tabla 5 *Controles tomados de la Norma ISO/IEC 27002:2013*

NORMA ISO/IEC 27002:2013		
DOMINIO	**OBJETIVO DE CONTROL**	**CONTROLES**
5. POLÍTICAS DE SEGURIDAD.	5.1 Directrices de la Dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información.
		5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la seguridad de la información.
		6.1.2 Segregación de tareas.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7.2 Durante la contratación.	7.2.1 Responsabilidades de gestión.
	7.3 Cese o cambio de puesto de trabajo.	7.3.1 Cese o cambio de puesto de trabajo
8. GESTIÓN DE ACTIVOS.	8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos.
		8.1.2 Propiedad de los activos.
		8.1.3 Uso aceptable de los activos.
		8.1.4 Devolución de activos.
	8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.
		8.3.2 Eliminación de soportes.
		8.3.3 Soportes físicos en tránsito.

NORMA ISO/IEC 27002:2013		
DOMINIO	**OBJETIVO DE CONTROL**	**CONTROLES**
11. SEGURIDAD FÍSICA Y AMBIENTAL.	11.1 Áreas seguras.	11.1.1 Perímetro de seguridad física.
		11.1.2 Controles físicos de entrada.
		11.1.3 Seguridad de oficinas, despachos y recursos.
		11.1.4 Protección contra las amenazas externas y ambientales.
		11.1.5 El trabajo en áreas seguras.
		11.1.6 Áreas de acceso público, carga y descarga.
	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos.
		11.2.2 Instalaciones de suministro.
		11.2.3 Seguridad del cableado.
		11.2.4 Mantenimiento de los equipos.
		11.2.5 Salida de activos fuera de las dependencias de la empresa.
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
		11.2.8 Equipo informático de usuario desatendido.
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

NORMA ISO/IEC 27002:2013		
DOMINIO	**OBJETIVO DE CONTROL**	**CONTROLES**
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
		13.1.2 Mecanismos de seguridad asociados a servicios en red.
		13.1.3 Segregación de redes.
	13.2 Intercambio de información con partes externas.	13.2.1 Políticas y procedimientos de intercambio de información.
		13.2.2 Acuerdos de intercambio.
		13.2.3 Mensajería electrónica.
		13.2.4 Acuerdos de confidencialidad y secreto.
15. RELACIONES CON SUMINISTRADORES.	15.1 Seguridad de la información en las relaciones con suministradores.	15.1.1 Política de seguridad de la información para suministradores.
	15.2 Gestión de la prestación del servicio por suministradores.	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
		15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.1 Responsabilidades y procedimientos.
		16.1.5 Respuesta a los incidentes de seguridad.

Fuente: Norma ISO/IEC 27002:2013

Tomando la norma como referencia, las estrategias y controles a aplicar en cada riesgo detectado son los siguientes:

Tabla 6 *Estrategias y controles*

ESTRATEGIAS Y CONTROLES								
TIPIFICACIÓN RIESGO	**RIESGO EVALUADO**	**OBJETIVO DE CONTROL**	**CRITICIDAD**	**VULNERABILIDAD**	**IMPACTO**	**RESPUESTA AL RIESGO**	**RIESGO**	**CONTROL**
RT001	Falla de UPS	DISPONIBILIDAD	Alto	3,7	5,0	➢ Disponer de conexiones adicionales a UPS. ➢ Conexión directa a tomas normales de energía eléctrica.	Falla de equipos de respaldo de energía eléctrica	11.2.1 Emplazamiento y protección de equipos.
RE001	Corte de energía eléctrica	DISPONIBILIDAD	Medio	2,3	2,5	➢ Mantenimientos frecuentes al Generador	Picos de energía al momento de los cortes, que afecten la electrónica de los equipos	11.2.1 Emplazamiento y protección de equipos.
RA001	Falta de control ambiental	DISPONIBILIDAD	Medio	3,0	4,0	➢ Proteger infraestructura de Racks y Cableado Estructurado.	No existe control de acceso físico en torre consultorios a los Racks de piso	11.2.3 Seguridad del cableado.
RA002	Falta de control de acceso físico a oficinas	INTEGRIDAD DISPONIBILIDAD	Alto	3,7	4,3	➢ Identificaciones mediante carnets y tarjetas de acceso.	Acceso directo a equipos e información. Alteración de conexiones.	11.2.8 Equipo informático de usuario desatendido.
RA003	Falta de control de acceso a proveedores	INTEGRIDAD DISPONIBILIDAD	Alto	4,3	4,0	➢ Identificaciones mediante carnets para proveedores.	Acceso a ductos en el Hospital e infraestructuras de comunicaciones.	11.2.3 Seguridad del cableado.

ESTRATEGIAS Y CONTROLES								
TIPIFICACIÓN RIESGO	**RIESGO EVALUADO**	**OBJETIVO DE CONTROL**	**CRITICIDAD**	**VULNERABILIDAD**	**IMPACTO**	**RESPUESTA AL RIESGO**	**RIESGO**	**CONTROL**
RI001	Usuarios no conocen infraestructura de red	INTEGRIDAD DISPONIBILIDAD	Medio	3,0	1,7	➢ Capacitaciones	Ingreso de personal no autorizado por no conocer el área. Desconexión accidental de equipos.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
RA004	No hay control de restricción de accesos	DISPONIBILIDAD	Alto	4,0	4,3	➢ Mantener identificadas áreas restringidas	Existen áreas de uso común en donde un atacante pasa desapercibido	11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
RT002	Falla en equipos de ventilación	INTEGRIDAD	Medio	3,0	3,0	➢ Mantener soportes periódicos	Calentamiento de equipos del Data Center.	11.2.1 Emplazamiento y protección de equipos.
RE002	Inundaciones	DISPONIBILIDAD	Medio	1,7	4,0	➢ Revisar periódicamente las instalaciones	Data Center ubicado en S1, en lluvias muy fuertes provoca inundaciones	11.1.2 Controles físicos de entrada.
RE003	Terremotos	DISPONIBILIDAD	Bajo	2,0	2,0	➢ Revisar periódicamente sujeciones de Racks	-	11.1.2 Controles físicos de entrada.
RI002	Incendios	DISPONIBILIDAD	Medio	3,3	4,3	➢ Revisar Cableado. ➢ Revisión del sistema de detección de incendios	Destrucción parcial o total de la infraestructura.	13.1.2 Mecanismos de seguridad asociados a servicios en red.
RO001	Desconexión física al ISP	DISPONIBILIDAD	Medio	2,0	3,0	➢ Mantener un enlace de back up con otro proveedor en una acometida diferente del enlace principal	No tener salida a internet y a los servicios externos al hospital	15.2.1 Supervisión y revisión de los servicios prestados por terceros.

ESTRATEGIAS Y CONTROLES								
TIPIFICACIÓN RIESGO	**RIESGO EVALUADO**	**OBJETIVO DE CONTROL**	**CRITICIDAD**	**VULNERABILIDAD**	**IMPACTO**	**ESTRATEGIA**	**RIESGO**	**CONTROL**
RT003	Corte de servicios a servidores internos	DISPONIBILIDAD	Alto	3,3	5,0	➢ Documentar acción de contingencia	Pacientes en alta. Historias clínicas. Exámenes complementarios	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red.
RE004	Corte del servicio MPLS del proveedor principal	DISPONIBILIDAD	Medio	3,7	3,7	➢ Utilizar enlace redundante	Servicios de sucursales fuera de línea. Telemedicina sin conectividad.	13.1.3 Segregación de redes.
RT004	Falla del Core de comunicaciones	DISPONIBILIDAD	Medio	3,3	3,7	➢ Determinar un Core de respaldo ➢ Reemplazar Core	Enlace de red fuera de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.
RT005	Saturación en el Core de comunicaciones	DISPONIBILIDAD	Alto	3,7	4,3	➢ Documentación para activar balanceo de carga	Intermitencia en la conexión	13.1.2 Mecanismos de seguridad asociados a servicios en red.
RO002	Saturación de carga en el enlace	DISPONIBILIDAD	Bajo	2,0	1,7	➢ Balanceo de carga por el enlace redundante	Redes con latencia alta	13.1.2 Mecanismos de seguridad asociados a servicios en red.
RE005	Intermitencia del servicio de Internet	DISPONIBILIDAD CONFIABILIDAD	Bajo	1,0	3,0	➢ Utilizar enlace redundante	Intermitencia en la conexión hacia el ISP	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
RO003	Interrupción del firewall	CONFIABILIDAD INTEGRIDAD	Bajo	1,7	2,0	➢ Conexión a la LAN directamente. ➢ Desconectar el internet	Posibles ataques a la red	13.1.1 Controles de red.

ESTRATEGIAS Y CONTROLES								
TIPIFICACIÓN RIESGO	**RIESGO EVALUADO**	**OBJETIVO DE CONTROL**	**CRITICIDAD**	**VULNERABILIDAD**	**IMPACTO**	**ESTRATEGIA**	**RIESGO**	**CONTROL**
RA005	Acceso no autorizado al Data Center	DISPONIBILIDAD INTEGRIDADD	Medio	1,3	5,0	➢ Identificación de zonas de acceso autorizado ➢ Identificación de personal mediante carnets.	Exposición de Core y servidores.	11.1.1 Perímetro de seguridad física.
RI003	Abuso de privilegios de acceso	INTEGRIDAD	Medio	2,3	5,0	➢ Cambio continuo de credenciales de acceso físico	Falta de capacitación en seguridad perimetral	7.2.2 Concienciación, educación y capacitación en seguridad de la información
RO004	Errores en mantenimiento de equipos de red	INTEGRIDAD CONFIDENCIALIDAD	Medio	3,0	2,3	➢ Documentar el evento para tomar acciones correctivas	Falta de mantenimientos	11.2.4 Mantenimiento de los equipos
RO005	Errores en mantenimiento de computadores	INTEGRIDAD CONFIDENCIALIDAD	Bajo	1,7	1,7	➢ Documentar el evento para tomar acciones correctivas	Falta de mantenimientos	11.2.4 Mantenimiento de los equipos
RI004	Falta de protección de acceso físico a la red	INTEGRIDAD DISPONIBILIDAD	Bajo	2,0	2,0	➢ Revisar instalaciones de cableado estructurado	Continuas remodelaciones en áreas de poco acceso	11.2.3 Seguridad del cableado.
RE006	Terrorismo	DISPONIBILIDAD CONFIDENCIALIDAD INTEGRIDAD	Medio	2,3	2,7	➢ Reducir el impacto del evento	Pérdida de información o daños	11.1.4 Protección contra las amenazas externas y ambientales
RI005	Limpieza del puesto de trabajo	DISPONIBLIDAD	Alto	3,7	4,3	➢ Socialización de la política en cuanto a la ingesta de alimentos	Daños en equipos	11.1.5 El trabajo en áreas seguras.

ESTRATEGIAS Y CONTROLES								
TIPIFICACIÓN RIESGO	**RIESGO EVALUADO**	**OBSERVACIÓN**	**CRITICIDAD**	**VULNERABILIDAD**	**IMPACTO**	**ESTRATEGIA**	**RIESGO**	**CONTROL**
RA006	Inventario de activos	DISPONIBILIDAD	Medio	4,0	1,0	➢ Levantar la documentación de los activos del hospital.	Pérdida o sustracción de equipamiento.	8.1.1 Inventario de activos.
RI006	Protección a la Infraestructura tecnológica	INTEGRIDAD	Medio	3,0	3,0	➢ Asegurar perímetros de seguridad.	Fallas intencionales a los equipos y redes.	11.1.3 Seguridad de oficinas, despachos y recursos.
RA007	Identificación del personal	INTEGRIDAD	Alto	3,7	4,3	➢ Campaña de carnetización.	Ingreso de personal no autorizado a áreas críticas.	11.1.2 Controles físicos de entrada
RI007	Abandono de puesto de trabajo	DISPONIBILIDAD CONFIDENCIALIDAD	Alto	3,0	5,0	• Concientizar al personal sobre exponer los puestos de trabajo.		11.1.3 Seguridad de oficinas, despachos y recursos.

Fuente: Elaborado por la autora.

En la tabla 6 de estrategias y controles, muestra una matriz que determina cada vulnerabilidad, amenaza o riesgo detectado; y, según el nivel de afectación evidenciado, se pueden elegir los dominios de la norma ISO/IEC27002:2013 que aplican a la situación actual de AXXIS Hospital. Al seleccionar los que se acoplan a la infraestructura que actualmente maneja el Hospital, se puede tener una directriz clara sobre la administración de los activos de red y equipos de sistemas de información, para que, en base a esto manejar procesos eficientes para poder crear normas que permitan prevenir y corregir incidentes de seguridad que pudieran presentarse en la institución.

Se procederá a crear la política de seguridad para el control de acceso a la infraestructura de red, con la finalidad de que sea revisada por la Coordinación de Calidad y aprobada por la Gerencia General de AXXIS Hospital.

Los controles seleccionados a partir de la matriz de riesgos tratan de reducir la probabilidad de que un incidente de seguridad ocurra y existan daños o hurtos de activos y equipos de comunicaciones de AXXIS Hospital.

Otro requerimiento que se debe analizar es el desarrollo del presupuesto para trasladar el Data Center desde el Subsuelo 1 hacia pisos superiores, realizar la medición del impacto, cronogramas de trabajo, diseño e implementación y especificaciones técnicas mínimas para la infraestructura del diseño.

En la Planificación de Gerencia General y el Departamento de TICs, se contempla el traslado del Data Center al Piso 4 de la Torre de Hospitalización, se destina un porcentaje del presupuesto de construcción, para el diseño e implementación, por lo que se trasladará el departamento de Sistemas, Monitoreo y Call Center de las torres de Consultorio, Hospitalización y Torre Materno infantil.

CAPÍTULO IV

PROPUESTA

4.1.1. Introducción

Existen varias falencias en el manejo de la seguridad perimetral en la infraestructura de red del hospital que pueden desencadenar en eventos que afecten la continuidad del negocio, es por ello que para el diseño de la política que se propone se han seleccionado los controles de la norma ISO/IEC 27002:2013 que permitirán mitigar los riesgos encontrados.

La Política de Seguridad pretende ser el medio que norme y controle el uso de recursos informáticos, precautelando la integridad de la infraestructura física de red. Todo usuario que utilice los servicios de red e información de AXXIS HOSPITAL, deberá conocer y aceptar el reglamento aprobado previamente por Alta Gerencia y que estará vigente en donde se especifican directrices sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario final, ante cualquier evento que involucre la seguridad de la red institucional y por ende la seguridad de la información que transita por esta.

El cumplimiento de la Política de Seguridad de la Información es de carácter obligatorio para todo el personal que conforma el hospital, independientemente del área en el que desempeñe sus funciones.

La Política de Seguridad de la Información, se enfoca en los procedimientos que son más cercanos a la realidad del hospital, tomando como lineamientos principales ocho criterios seleccionados de la norma ISO/IEC 27002:2013, que se detallan a continuación:

- Política de Seguridad.
- Aspectos organizativos de la seguridad de la información.
- Seguridad ligada a los Recursos humanos.
- Gestión de activos.
- Seguridad Física y ambiental.
- Seguridad en las telecomunicaciones.
- Relaciones con suministradores.
- Gestión de incidentes en la seguridad de la información.

4.1.2. Objetivo

Controlar el acceso a la infraestructura de red de personal no autorizado, evitando daños o robos de activos del hospital, además de interrupciones que puedan afectar a la continuidad del negocio mediante la aplicación de la Política de Seguridad de la Información basada en la norma ISO/IEC 27002:2013.

4.1.3. POLÍTICA DE SEGURIDAD.

Artículo 1. La política y cada uno de sus artículos estarán sujetos a una revisión periódica, con la finalidad de que se realicen ajustes basados en las recomendaciones y se documenten las actualizaciones o modificaciones de la misma bajo un análisis realizado por el departamento de TICs, se recomienda que esta revisión sea semestral en base a un análisis de resultados post aplicación de la política.

Para la implementación de cambios, se regirá al siguiente proceso:

- Creación del comité de revisión de política de seguridad, conformada por (un representante de TICs, Gerente Administrativo, Gerente de Calidad).
- La política de seguridad, deberá revisarse semestralmente, mediante la evaluación de resultados obtenidos en auditoría interna.
- Para realizar un cambio sobre la política, se enviará el documento de Solicitud de Cambio, la cual deberá ser aceptada, analizada y aprobada por la mayoría del comité. (ANEXO 3).

4.1.4. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

Organización Interna.

Artículo 2. AXXIS HOSPITAL mediante su junta directiva asume el compromiso de asignación de responsabilidades, gestión para la seguridad de la información a través del departamento de sistemas. Todos los miembros de AXXIS HOSPITAL independientemente de su jerarquía o tipo de vinculación a la institución, son responsables de la implementación de esta Política de Seguridad de la Información en sus áreas de responsabilidad y del personal bajo su cargo. (ANEXO 4).

Artículo 3. El jefe del área de TICs mediante un documento escrito, está en la facultad de delegar funciones de seguridad perimetral de la red o de la información a uno o varios miembros de su departamento que tengan experiencia en el tema, identificando los activos del hospital y siguiendo procesos definidos en la Política. (ANEXO 5).

Artículo 4. El jefe del área de TICs es el encargado de controlar que todas las actividades de seguridad perimetral y de infraestructura se ejecuten de manera correcta.

Artículo 5. El jefe del área de TICs asignará un responsable para cada tarea que corresponde a su departamento, se mantendrá un estricto control de los activos de información de AXXIS HOSPITAL, evitando así, acceso no autorizados, modificaciones o utilización de activos sin que sean otorgados permisos previamente o que sean indetectables.

Artículo 6. El departamento de TICs se responsabiliza de los controles para monitorear el cumplimiento de las actividades de manera correcta y oportuna.

Artículo 7. Las violaciones o incumplimientos de la Política de Seguridad de la Información para la infraestructura de red, pueden recaer en acciones disciplinarias, que incluye, pero no se limitan a:

- Acciones disciplinarias bajo lineamientos que se reflejan en el Reglamento Interno del Trabajo para las y los Trabajadores, Código de Trabajo, Cláusulas dentro de sus Contratos Laborales y/o todo lo que las leyes ecuatorianas definan como acciones disciplinarias patronales:
- Llamado de atención formal.
- Suspensión o acceso restringido a áreas críticas.
- Reembolso por daños ocasionados.
- Suspensión sin remuneración.
- Finalización del contrato laboral.
- Demanda civil.
- Demanda penal.

4.1.5. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

Antes de la contratación.

Artículo 8. Los integrantes del departamento de TICs deben firmar un compromiso (Anexo 6) de confidencialidad, el personal a cargo de este departamento administra información, equipos, e infraestructura del Core del Hospital.

Durante la contratación.

Artículo 9. AXXIS HOSPITAL mediante el departamento de TICs, ejecutará capacitaciones continuas sobre educación, formación y aplicación de la Política de seguridad de la Información, así como información acerca de la infraestructura de red que pertenece a cada área en donde desempeñan sus funciones diarias.

Artículo 10. Los usuarios de AXXIS HOSPITAL deben asistir regularmente a las capacitaciones y regirse a las disposiciones notificadas en estas.

Artículo 11. Los usuarios de AXXIS HOSPITAL tienen la responsabilidad de dar cumplimiento a los artículos de la Política de Seguridad de la Información detallados en este manual.

Cambio o cese de funciones.

Artículo 12. El departamento de Recursos Humanos de AXXIS HOSPITAL, notificará inmediatamente la desvinculación del personal o cambio de funciones al departamento de TICs, para proceder a cambiar credenciales de acceso a áreas vinculadas a su cargo. Los usuarios que incumplan esta política, son responsables de las acciones generadas por omisión.

Artículo 13. El departamento de Recursos Humanos de AXXIS HOSPITAL, notificará inmediatamente el inicio y finalización del período vacacional del personal al departamento de TICs, para proceder a cambiar credenciales de acceso a áreas vinculadas a su cargo. Los usuarios que incumplan esta política, son responsables de las acciones generadas por omisión.

Artículo 14. El departamento de TICs de AXXIS HOSPITAL, debe realizar modelos de comunicación continua para socializar a todo el personal las obligaciones y responsabilidades sobre seguridad de la información vigentes al ocurrir cambios en el puesto y funciones de trabajo. (ANEXO 7)

Artículo 15. El personal de AXXIS HOSPITAL, que termine su relación laboral, deberá regresar los activos asignados a su cargo y custodia en el estado en que fueron entregados al departamento de control de inventarios. (ANEXO 8)

4.1.6. GESTIÓN DE ACTIVOS.

Responsabilidad sobre los activos.

Artículo 16. El personal de AXXIS Hospital debe tener un inventario de los equipos entregados bajo el rol de custodio de equipos.

Artículo 17. Antes de que cualquier empleado de AXXIS HOSPITAL utilice recursos informáticos de propiedad de la institución, el departamento de TICs proporcionará la información y/o documentación tanto de capacitaciones de uso, como manuales para la correcta utilización de los activos.

Artículo 18. El personal de AXXIS Hospital, deberá firmar y conservar el acta de custodia de equipos a su cargo, mantener actualizada la documentación en caso de que existiera un cambio. (ANEXO 9)

Artículo 19. El usuario deberá proteger y salva guardar el equipo informático que fue entregado como custodio, evitar que personas que no estén bajo su cargo accedan a la información almacenada en el mismo, mediante el uso de una herramienta de bloqueo temporal, protegida con contraseña, el cual debe activarse cuando el usuario deba ausentarse de su puesto de trabajo. (COMBINACIÓN WINDOWS + L). La longitud mínima en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluido caracteres especiales, la longitud máxima en una contraseña se establece en 18 caracteres, los cuales tendrán una combinación alfanumérica, incluido caracteres especiales. La contraseña deberá cambiarse cada seis meses.

Artículo 20. Los recursos informáticos son de uso exclusivo para gestiones directamente relacionadas al giro de negocio de AXXIS Hospital, serán utilizados para cumplir únicamente funciones de la organización, cualquier cambio en la normativa, deberá ser modificada dentro de la política de seguridad en una versión nueva del documento.

Artículo 21. Cualquier usuario que encuentre un equipo desprotegido está en la obligación de notificar mediante correo electrónico la falla de seguridad al departamento de TICs de AXXIS HOSPITAL a sistemas@AXXIShospital.com.ec.

4.1.7. SEGURIDAD FÍSICA Y AMBIENTAL.

Áreas seguras.

Artículo 22. El lugar designado para la ubicación de los sistemas de información, equipos de comunicaciones y de usuario final, deben tener protecciones como barreras y controles físicos, evitando intrusiones físicas, inundaciones y cualquier tipo de amenazas que afecten su normal operación.

Artículo 23. Se debe definir el perímetro de seguridad de manera clara y precisa, con un estricto control de acceso a las áreas.

Artículo 24. El lugar en donde se ubiquen equipos de red o equipos informáticos deben tener estructuras sólidas, protegiéndolos contra factores naturales o incidentes de seguridad ambiental mediante alarmas o barreras de protección.

Artículo 25. El personal de monitoreo y seguridad responsable de los ingresos a AXXIS Hospital, deberán controlar el acceso de personas ajenas a la institución, mediante actas de ingreso de personal autorizado, bitácora de fecha y hora de ingreso y salida del personal y con las observaciones del propósito del ingreso.

Artículo 26. Se debe asignar un área de recepción encargada del ingreso del personal autorizado.

Artículo 27. Las salidas de emergencia ubicadas dentro del perímetro de seguridad deben tener alarmas y deberán cerrarse automáticamente.

Artículo 28. Proveedores externos que deseen ingresar a AXXIS Hospital, deben presentar de manera obligatoria un documento de identificación ya sea este una credencial o cédula de identidad.

Artículo 29. Los usuarios o personal que ingrese a áreas donde se ubiquen sistemas de información deberán portar obligatoriamente sus credenciales de manera visible.

Artículo 30. Las contraseñas o credenciales en áreas donde se encuentren equipos o sistemas de información, deben ser revisados, modificados o actualizados frecuentemente, se recomienda cada tres meses.

Artículo 31. En áreas restringidas se debe entregar una credencial de identificación al personal ya sea "Proveedor" o "Visitante", en donde se detalle el piso o área a donde tiene autorización de ingreso.

Artículo 32. La persona que ingrese con equipos como computadores, deberá registrar los datos como marca, modelo y número de serie.

Artículo 33. El acceso al Data Center de AXXIS Hospital deberá ser únicamente a personal autorizado o bajo la custodia del personal autorizado. (ANEXO 10)

Artículo 34. La Gerencia del Área de TICs, solicitará al Departamento Técnico de Seguridad, Salud y Ambiente de AXXIS Hospital, impartir diferentes capacitaciones sobre cómo evitar daños generados por riesgos naturales como inundaciones, terremotos, explosiones, incendios y otras amenazas que pueden ser ocasionadas por la acción misma del hombre.

Artículo 35. La Gerencia de TICs, debe delegar al personal que integre la Brigada de Gestión de Riesgos de AXXIS Hospital, quienes se capacitarán y manejarán procesos y protocolos ante las amenazas descritas anteriormente.

Artículo 36. Está completamente prohibido el consumo de alimentos o líquidos dentro del Data Center, Cuartos de telecomunicaciones o áreas donde reposen equipos de sistemas de información.

Artículo 37. El aseo y limpieza de áreas donde se encuentren equipos de sistemas de información, debe realizarse siempre y cuando se encuentre personal autorizado como custodio.

Artículo 38. Se deberá capacitar al personal de limpieza para el manejo y precauciones mínimas durante el proceso de aseo y limpieza de áreas en donde se encuentren equipos de sistemas d seguridad y cables de conexión.

Artículo 39. Se prohibirá el acceso del personal de limpieza y mantenimiento con maletas o elementos que no sean de uso para su labor de aseo y limpieza en áreas de equipos de sistemas de información.

Artículo 40. La estructura de áreas asignadas para equipos de sistemas de información será de material no combustible.

Artículo 41. Cada área donde se ubiquen equipos de sistemas de información, debe contar con extintores de incendios, con la finalidad de detener el fuego que pueda generarse por fallas eléctricas o papel, estos extintores deben ser revisados periódicamente.

Artículo 42. Deberán almacenarse los suministros de oficina como papel a distancias considerables de equipos de sistemas de información, con la finalidad de evitar daños ante desastres en que se vean afectados.

Artículo 43. Todos los trabajadores de AXXIS Hospital deben estar vigilantes ante la presencia de personas extrañas y reportar inmediatamente al área de monitoreo.

Artículo 44. Todos los visitantes extraños, deberán ser monitoreados durante su estadía, principalmente si ingresan a áreas restringidas, con el fin de proteger ante posibles daños a equipos de sistemas de información o hurto.

Artículo 45. Se prohíbe el uso de equipos como cámaras, videograbadoras, grabadoras, analizadores de datos, (hardware especial), dentro de las instalaciones de AXXIS Hospital, a no ser que se cuente con una autorización oficial por parte de la administración y custodia del personal de monitoreo.

Artículo 46. Todo elemento que ingrese a AXXIS Hospital, deberá pasar por una inspección rigurosa con la finalidad de identificar riesgos, materiales peligrosos y validar que los materiales que ingresen coincidan con las guías de remisión para emitir una autorización de ingreso.

Artículo 47. El ingreso de terceros con elementos, productos o materiales, se debe realizar a través de las áreas asignadas para descargue las cuales estarán debidamente identificadas y así evitar accesos innecesarios a las instalaciones del hospital.

Artículo 48. Los materiales, productos o elementos que deban ingresar a AXXIS Hospital, serán inspeccionados en el área de descargue, así evitar el ingreso de elementos que se consideren peligrosos.

Artículo 49. Se deberá manejar un inventario del material, equipos o elementos que entren o salgan de la institución y se deberá actualizarlo continuamente.

Seguridad de los equipos.

Artículo 50. Todos los equipos de sistemas de información, deberán contar con fuentes de energía eléctrica ininterrumpidas.

Artículo 51. Deberá disponerse de un estricto monitoreo y control de temperatura y humedad en áreas donde se encuentren equipos de sistemas de información, donde si ocurriera una falla afectarían la operación del negocio.

Artículo 52. Se dispondrá de controles para minimizar robos o hurtos, haciendo que el personal porte sus credenciales de forma visible y permanente durante su estadía dentro de la institución, estos controles deben ser adoptados y día a día actualizados por el área de monitoreo.

Artículo 53. Todas las áreas de la institución deberán contar con sensores de detección de humo y calor, instalados y monitoreados 24 horas los 7 días de la semana y deberán realizarse mantenimientos preventivos y correctivos para su óptimo funcionamiento, con la finalidad de prevenir incidentes con incendios, conatos de incendio y fuego.

Artículo 54. Se debe tener extintores de incendios con la capacidad de detener incendios, conato de incendio y fuego, deberán ser probados y verificados periódicamente.

Artículo 55. Todas las personas que ingresen a un área de equipos de sistemas de información deberán portar una identificación que autorice su ingreso a determinada área dentro de AXXIS Hospital, por ninguna razón deberá portar material explosivo dentro o cerca de áreas establecidas como seguras dentro del hospital.

Artículo 56. Se deberá ubicar los equipos de sistemas de información en pisos a una altura superior del nivel de la calle, con la finalidad de evitar inundaciones.

Artículo 57. Las cañerías de desagüe, deberán tener válvulas de retención de líquidos en flujo inverso, con la finalidad de evitar inundaciones ante sobre flujos.

Artículo 58. El Sistema de Cableado Estructurado deberá contar con canaletas o chaquetas y las distancias mínimas de instalación con respecto al cableado eléctrico para disponer de protección ante interferencias electromagnéticas.

Artículo 59. Los cables eléctricos deben estar instalados con distancias mínimas según las normas técnicas con respecto al cableado de comunicaciones.

Artículo 60. Se deberá proteger el cableado de comunicaciones ante daños ambientales cumpliendo normas.

Artículo 61. Los cables de comunicaciones deberán estar correctamente codificados e identificados para un manejo correcto de las conexiones y evitar errores.

Artículo 62. El cableado de comunicaciones deberá ser instalado y mantenido por ingenieros certificados y calificados para garantizar la calidad del enlace.

Artículo 63. Los puntos de pared que no estén utilizados deben ser notificados para deshabilitar los puertos de equipos de conexión de red al que correspondan y sellados para mantener su estado.

Artículo 64. Se debe precautelar la integridad de la red ante un daño malicioso que afecte gravemente a los equipos de sistemas de la información.

Artículo 65. Se revisará periódicamente los puntos desconectados de la red para evitar conexiones ilegales que pueden comprometer la seguridad de los datos, usuarios y contraseñas.

Artículo 66. Se deberá considerar enlaces redundantes y con fibra óptica a conexiones del Core de la red.

Artículo 67. El jefe del área de TICs, es responsable de coordinar y comunicar los planes de mantenimientos preventivos de los equipos, realizar el cronograma de

actividades en horarios que no se interrumpa el funcionamiento de equipos correspondientes al área administrativa, médicos y demás unidades dentro del hospital.

Artículo 68. Es responsabilidad del área de TICs, realizar oportunamente los mantenimientos preventivos/correctivos de los equipos de las áreas administrativas, médicos y demás unidades del hospital.

Artículo 69. El área de TICs, debe tener los informes de los mantenimientos realizados en los equipos de cómputo, con la firma del usuario custodio del equipo avalando el trabajo realizado.

Artículo 70. El área de TICs deberá comunicar con anticipación el cronograma de mantenimientos de los equipos de los usuarios del hospital.

Artículo 71. Los mantenimientos se realizarán bajo los parámetros y especificaciones emitidas por los fabricantes.

Artículo 72. Si el mantenimiento de uno de los equipos debe realizarse fuera de AXXIS Hospital, se debe tomar en cuenta los requerimientos de pólizas de seguro y la información confidencial del mismo.

Artículo 73. El jefe o gerente de área es el responsable de autorizar la salida, uso de equipos de sistemas de información o software fuera de AXXIS Hospital.

Artículo 74. Es responsabilidad del usuario custodio de un equipo bloquear el acceso de su computador cuando requiera ausentarse de su puesto de trabajo, deberá utilizar bloqueo de pantalla con contraseña, cerrar la sesión o apagar el equipo.

Artículo 75. Está estrictamente prohibido que los usuarios muevan, reinstalen, retiren sellos o reubiquen equipos sin autorización del jefe del área de TICs.

Artículo 76. Se deberá notificar al área de TICs, cualquier solicitud de cambio o reubicación de computadores con mínimo 48 horas de anticipación.

Artículo 77. Es obligatorio que todas las computadoras estén configuradas con usuario y contraseña para protección de la información.

Artículo 78. Los equipos que se utilizaron como almacenamiento de información deben ser destruidos físicamente o utilizar herramientas especiales para verificar que no exista información remanente.

Artículo 79. Al finalizar la jornada laboral los equipos deberán ser apagados.

4.1.8. SEGURIDAD EN LA TELECOMUNICACIONES.

Artículo 80. Los computadores y equipos de comunicaciones de AXXIS Hospital, deberán estar conectados únicamente a la red de datos provisto por el área de TICs.

Artículo 81. Los computadores y equipos de comunicación asociados a la red de AXXIS Hospital, estarán dentro de las políticas y normas establecidas por el área de TICs en donde se contempla:

- Control de contenidos.
- Bloqueo de páginas no autorizadas.
- Filtrado de correo electrónico.
- Filtrado web.
- Protección y detección de intrusos.
- Filtrado de puertos de comunicación.

Artículo 82. Si una institución requiere retirar un equipo de sistemas de información, deberán remitir un oficio formal dirigido a la Dirección Administrativa, donde se indique el equipo requerido y el propósito del requerimiento.

Artículo 83. La Dirección Administrativa de AXXIS Hospital o su delegado, serán los únicos funcionarios en autorizar la entrega de equipos.

Artículo 84. Si por autorización de la Dirección administrativa, un activo informático sale de las instalaciones de AXXIS Hospital, el encargado será el custodio del equipo y es totalmente responsable de regresarlo en iguales condiciones. Si por alguna circunstancia el equipo informático se pierde o está deteriorado por mal uso, el custodio deberá reponerlo con las mismas especificaciones técnicas o superiores de acuerdo a la vigencia del mercado.

Artículo 85. El documento, paquete o equipo a enviarse estará sometido a las políticas de mensajería de AXXIS Hospital a través de actas de envío, entrega y recepción.

Artículo 86. Las fallas en el manejo de los equipos estarán sometidos a las normativas vigentes institucionales y a las obligaciones y responsabilidades en caso de pérdida del equipo.

Artículo 87. El acuerdo de confidencialidad de la información deberá incluir entre sus cláusulas los siguientes ítems:

- Comparecientes.
- Antecedentes.
- Definiciones.
- Objeto.
- Obligaciones.
- Sanciones.
- Indemnizaciones.
- Vigencia.

Artículo 88. Los acuerdos de confidencialidad deberán suscribirse en las siguientes circunstancias:

- Entrega de equipos de sistemas de información.
- Entrega de credenciales con privilegios.
- Suscripción de contratos con proveedores que requieran acceso a la infraestructura de red.

Artículo 89. El departamento Jurídico de AXXIS Hospital deberá elaborar y validar acuerdos de confidencialidad anexos a los contratos con los proveedores.

4.1.9. RELACIONES CON SUMINISTRADORES.

Artículo 90. Los proveedores deberán estar calificados en la selección de proveedores de AXXIS Hospital, teniendo la documentación de contratos

especificaciones técnicas, actas de entrega recepción, acuerdos de confidencialidad con la finalidad de garantizar una correcta administración.

Artículo 91. Los acuerdos de confidencialidad suscritos se deben enfocar para garantizar la integridad, confidencialidad y disponibilidad de la información, en caso de ocurrir un incidente se establecerán las sanciones o multas de acuerdo a la falla detectada o faltas al acuerdo suscrito por las partes.

Artículo 92. AXXIS Hospital delegará un administrador de contrato, quién será el responsable de velar el cumplimiento de os términos, contratos acuerdos especificaciones técnicas de los equipos y documentos suscritos con proveedores de servicios tecnológicos, además se asignará un fiscalizador para los ismos fines.

Artículo 93. El personal delegado deberá monitorear los servicios tecnológicos prestados por proveedores para validar el cumplimiento de cronogramas y plazos establecidos en las contrataciones.

Artículo 94. El personal designado deberá validar los informes técnicos remitidos por los proveedores, en caso de incumplimiento, deberán informar al jefe del área de TICs, para considerar plazos, multas o sanciones descritas en los contratos suscritos.

4.1.10. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Artículo 95. El personal de AXXIS Hospital está en la obligación de reportar incidentes de seguridad de la infraestructura de red.

Artículo 96. Al presentarse incidentes de seguridad en la infraestructura de red, el personal deberá notificar a través de un correo electrónico a la dirección sistemas@AXXIShospital.com.ec.

Artículo 97. Se considera como incidentes de seguridad a la infraestructura de red a lo siguiente:

- Error humano.

- Acceso no autorizado.
- Violación de confidencialidad, integridad o disponibilidad de la información.
- Incumplimiento de normas establecidas en la seguridad de la infraestructura de red.
- Deficientes controles de seguridad.

Artículo 98. Es obligación recopilar la información para evidenciar un incidente y su origen.

Artículo 99. Se deben registrar de forma correcta las acciones ejecutadas como respuesta al incidente presentado.

Artículo 100. El área de TICs deberá mantener una bitácora o registros de incidentes de seguridad de la infraestructura de red notificados, para mantener una retroalimentación de acciones preventivas y correctivas.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Con base en el estudio realizado se analizó las fortalezas y falencias en el control de acceso a la infraestructura de red, obteniendo así el diseñó de una política de seguridad de la información basada en la Norma ISO/IEC 27002:2013, la cual tiene como objetivo principal el subsanar las amenazas y sobre todo de manera proactiva minimizar su ocurrencia, elevando el nivel de servicio y la continuidad del negocio logrando precautelar la integridad, confidencialidad y disponibilidad de la información.

A través del análisis de la situación actual de la infraestructura de red de AXXIS Hospital con la aplicación de la metodología de Magerit, se pudo determinar los riesgos y categorizarlos según su prioridad, siendo esta valoración la base que permitió elaborar una política de seguridad para mitigar los riesgos, amenazas y vulnerabilidades, que apoye al correcto manejo de la administración y gestión de la infraestructura de red.

Las estrategias que se plantean para mitigar los riesgos en el hospital toman en consideración el alto tráfico de personas, entre los que están: pacientes, proveedores, empleados, entre otros; y establece parámetros para identificar áreas de acceso restringido y el uso de buenas prácticas para el manejo de equipos y activos de red.

La política de seguridad diseñada para AXXIS Hospital debe llevarse a cabo de manera efectiva y eficiente, sabiendo que la eficiencia significa hacer algo al menor costo posible y la efectividad significa hacer lo correcto para crear el mayor valor para la empresa minimizando los riesgos de seguridad en conjunto con los requisitos legales. Por medio de la implementación de la política de seguridad se pretende manejar la seguridad de la infraestructura de red de manera que la correcta administración de los recursos permita controlar y garantizar la integridad, confidencialidad y disponibilidad de la información para así mejorar su ventaja competitiva en comparación con los hospitales de la ciudad y del país, concibiendo y manejando procesos eficientes. Se necesita la asignación del presupuesto para el área de TICs para la implementación de los cambios y reubicación especialmente del Data Center en la institución.

Una vez finalizado el proyecto de titulación, se entregará la política de seguridad de la infraestructura de red al departamento de Gestión de Calidad, para dar paso a la aprobación de la Gerencia General y así socializarla en la institución mediante la Junta Directiva, dentro del marco de procesos institucionales del Hospital.

5.2. RECOMENDACIONES

Se recomienda la aprobación de la política de seguridad de la infraestructura de red por la Gerencia General de AXXIS Hospital y la socialización de la misma al personal administrativo y médico, para el correcto manejo de los activos pertenecientes al hospital.

La política de seguridad de la infraestructura de red debe ser revisada periódicamente por el departamento de TICs, de existir cambios o actualizaciones, deben ser documentados y registrados en una nueva versión de la misma.

Se recomienda la implementación de la política de seguridad a través del departamento de TICs, para tomar medidas enfocadas a la prevención y corrección de incidentes con la finalidad de minimizar los riesgos presentes evitando daños y pérdidas de activos en el hospital y se vea afectada la continuidad del negocio.

La socialización de la política de seguridad de control de acceso a la infraestructura de red es de gran importancia para AXXIS Hospital, permitirá al personal estar alerta e identificar amenazas y vulnerabilidades presentes, otorgando el conocimiento para mantener niveles de seguridad enfocados a los activos de comunicación informáticos, dictando charlas semestrales en coordinación con el departamento de RRHH.

El departamento de TICs en conjunto con el departamento de Recursos Humanos deberá encabezar y promocionar capacitaciones acerca de la importancia de la seguridad de la infraestructura de red en AXXIS Hospital, de esta manera direccionar a la Dirección Administrativa sobre el desarrollo de sistemas de seguridad, planes y administración de la información con un carácter de estricto ya que como hospital se maneja información confidencial de pacientes e información de gestión del negocio mismo.

Una vez que la política esté aprobada, implementada y probada, se sugiere realizar como trabajo futuro a la política de seguridad de infraestructura de red basada en la norma ISO/IEC 27002:2013, el diseño e implementación de un Sistema de Gestión de la Información, que pueda ser implementado por el departamento de TICs para orientar y fortalecer la gestión de la información y crear un lineamiento conjunto de los subsistemas y políticas que serían parte del sistema.

BIBLIOGRAFÍA

Aguilera, P. (2010). *Seguridad informática*. *Madrid: Editex*

Álvarez, A., & Fernández, L. (2012). *Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para pymes*. *Asociación Española de Normalización y Certificación.*

Cárdenas, G. D. (2018). *Diseño de una política de seguridad de la información basada en la norma ISO 27799 para el control de accesos a las aplicaciones médicas de la red en el Hospital AXXIS. Ecuador*.

Chiu, S. H. (2006). *Segur idad en Redes Inalámbr icas 802.11*. *Caracas: Recuperado de http://www. ciens. ucv. ve, 8080.*

Dirección General de Modernización Administrativa, & Electrónica, P. e I. de la A. (2012a). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos*. 1–75. Madrid

Dirección General de Modernización Administrativa, & Electrónica, P. e I. de la A. (2012b). *Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas*. *2006*. Retrieved from http://administracionelectronica.gob.es/

Disterer, G. (2013). *ISO / IEC 27000 , 27001 and 27002 for Information Security Management*. *2013*(April), 92–100. Madrid

Patiño, C. (2019). *Hospitales y clínicas del Ecuador | El Comercio. S.I. [24 de junio de 2019] [Suplemento]*.

Franco, D. C., & Guerrero, C. D. (2013). *Sistema de Administración de Controles de Seguridad Informática basado en ISO / IEC 27002*. *Villavicencio: In 11th Latin American and Caribbean Conference for Engineering and Technology.* 1–10.

García, G. (2009). *Propuesta de políticas de seguridad de la información para la CORPAIRE*.

Gehrmann, M. (2012). *Combining ITIL , COBIT and ISO / IEC 27002 for structuring comprehensive information technology for management in organizations*. *Santa Catarina: Navus-Revista de Gestão e Tecnologia*

Guerrero, H. A., Lasso, L. A., & Legarda, P. A. (2015). *Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa ingelec SAS.Colombia.*

Montaño Orrego, V. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, *4*(6), 21–23. Retrieved from http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view/57

Mosquera Quintero, G. C., Saravia Alvernia, J. A., & Pacheco Pérez, J. J. (2016). *Tecnología de la información. Informática en salud. Gestión de seguridad de la información en salud utilizando la ISO/IEC, 27002.*

Năstase, P., Năstase, F., & Ionescu, C. (2009). CHALLENGES GENERATED BY THE IMPLEMENTATION OF THE IT STANDARDS COBIT 4 . 1 , ITIL V3 AND ISO / IEC 27002 IN 1 . Premises. *Candidate The Bucharest Academy of Economic Studies*.

Montaño Orrego, V. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, *4*(6), 21–23. Retrieved from http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view/57

Paredes, G. G. (2006). *INTRODUCCIÓN A LA CRIPTOGRAFÍA. México D.F.: Revista digital universitaria, 7(7), 1-17.*

Ramos, Y., Urrutia, O., & Bravo, A. (2017). *Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO / IEC 27002 : 2013 para la Cooperativa Codelcauca Adopt an information security policy based on an NTC ISO / IEC 27002 : 2013 standard for the Codelcauca Cooper*. 88–95.

Registro Oficial N°180. *Código Orgánico Integral Penal (COIP), de la República del Ecuador, Quito, Ecuador. [10 de febrero de 2014]*.

Sahibudin, S., & Ayat, M. (2018). *Combining ITIL , COBIT and ISO / IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations Combining ITIL , COBIT and ISO / IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations Mohammad Sharifi Centre for Advanced So*. (June).

Sarubbi, J. P. (2008). *Seguridad Informática Técnicas de defensa comunes bajo variantes del sistema operativo Unix*.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO / IEC 27001 [Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC*. *28*(Diciembre), 492–507.

ANEXO 1

ENCUESTA

Encuesta dirigida a trabajadores de AXXIS HOSPITAL, con la finalidad de determinar el estado actual de la infraestructura de red.

1. **¿Conoce usted cual es la infraestructura de la red de datos?**

   SI _____

   NO _____

2. **¿Ha recibido un inventario de los equipos de cómputo a su cargo?**

   SI _____

   NO _____

3. **¿Porta su carnet de identificación como trabajador del hospital en todo su horario laboral?**

   SI _____

   NO _____

4. **¿Su área de trabajo brinda seguridad ante el acceso no autorizado de terceros?**

   SI _____

   NO _____

5. **¿Está usted satisfecho con los mantenimientos realizados a los equipos de cómputo que tiene a su cargo?**

   SI _____

   NO _____

6. **¿Considera que la información que usted almacena en su computador cuenta con seguridades adecuadas ante un ataque?**

   SI _____

   NO _____

7. **¿Conoce la ubicación del rack de datos de su piso?**

SI _____

NO _____

8. **¿Ha recibido indicaciones de no comer, no beber cerca de los equipos de cómputo dentro del hospital?**

SI _____

NO _____

9. **¿Si su equipo de trabajo, se queda sin actividad en un tiempo prolongado, lo apaga?**

SI _____

NO _____

10. **¿Si usted debe ausentarse de su área de trabajo, cierra la sesión del computador?**

SI _____

NO _____

11. **¿Ha recibido alguna directriz acerca de qué hacer en caso de que personal no identificado se acerque o ingrese a los racks de comunicación de su piso?**

SI _____

NO _____

12. **¿Al ausentarse de su área de trabajo, se queda gente no autorizada en la misma?**

SI _____

NO _____

13. **¿Se le ha informado de los mantenimientos que se realizan a los equipos a su cargo?**

SI _____

NO _____

14. **¿Ha constatado que el departamento de TICs tenga un Back-up de la información de sus equipos?**

SI _____

NO _____

15. **¿Considera usted que los equipos informáticos tienen protección ante incidentes?**

SI _____

NO _____

16. **¿Ha recibido capacitación sobre el uso de los dispositivos de detección de incendios?**

SI _____

NO _____

17. **¿Su trabajo se ha visto interrumpido por fallas eléctricas?**

SI _____

NO _____

18. **¿Su trabajo se ha visto interrumpido por caídas en telecomunicaciones?**

SI _____

NO _____

19. **¿Conoce políticas internas que regulen la salida de equipos de cómputo del hospital?**

SI _____

NO _____

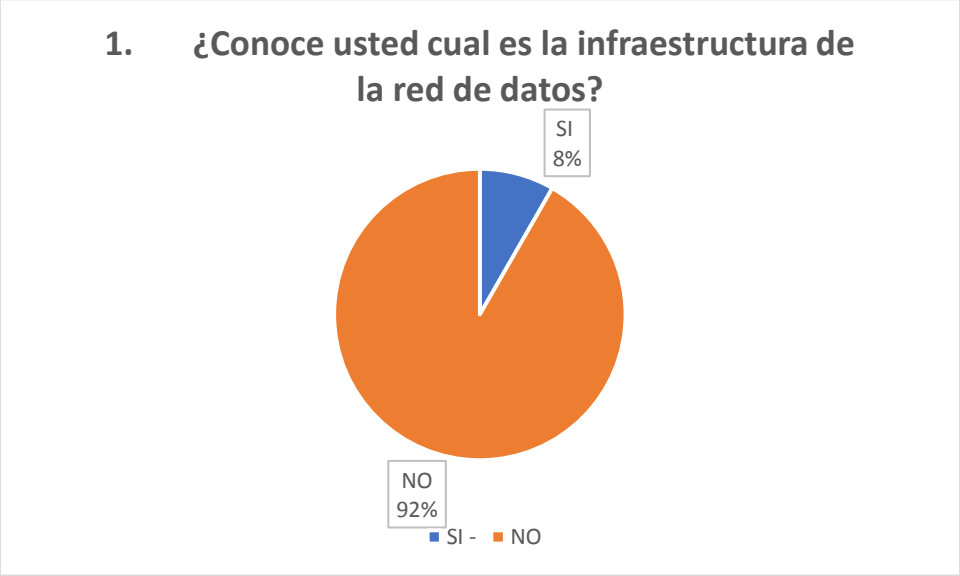
20. **¿Considera necesario implementar políticas de seguridad de la información en el hospital?**

SI _____

NO _____

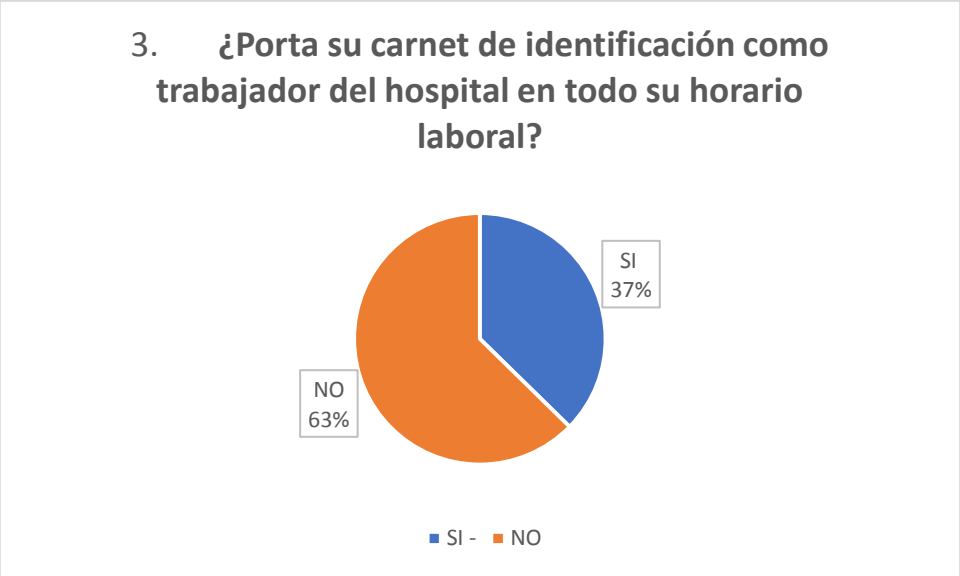
ANEXO 2
TABULACIÓN DE ENCUESTA

1. ¿Conoce usted cual es la infraestructura de la red de datos?	
SI	46
NO	495

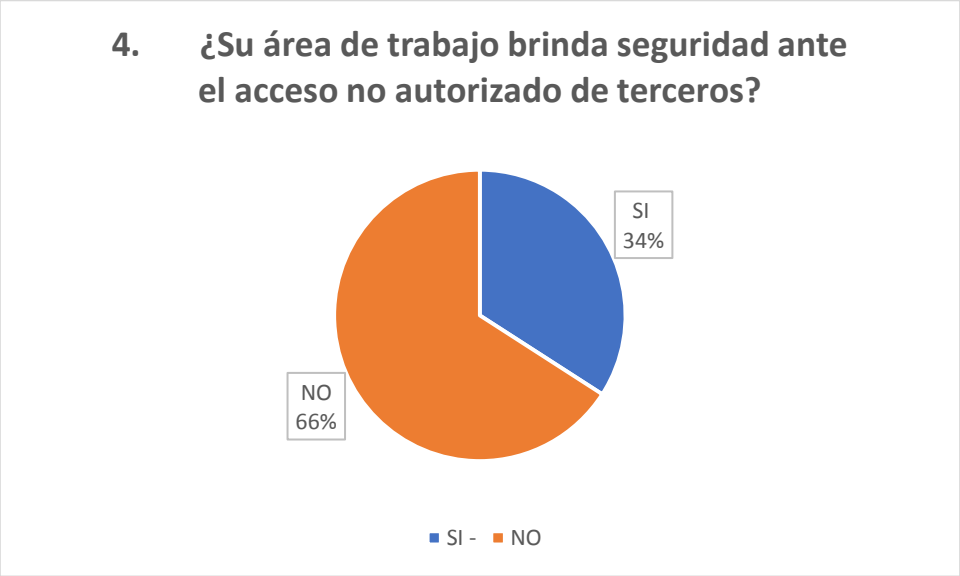


2. ¿Ha recibido un inventario de los equipos de cómputo a su cargo?	
SI	257
NO	284

3. ¿Porta su carnet de identificación como trabajador del hospital en todo su horario laboral?	
SI	202
NO	339

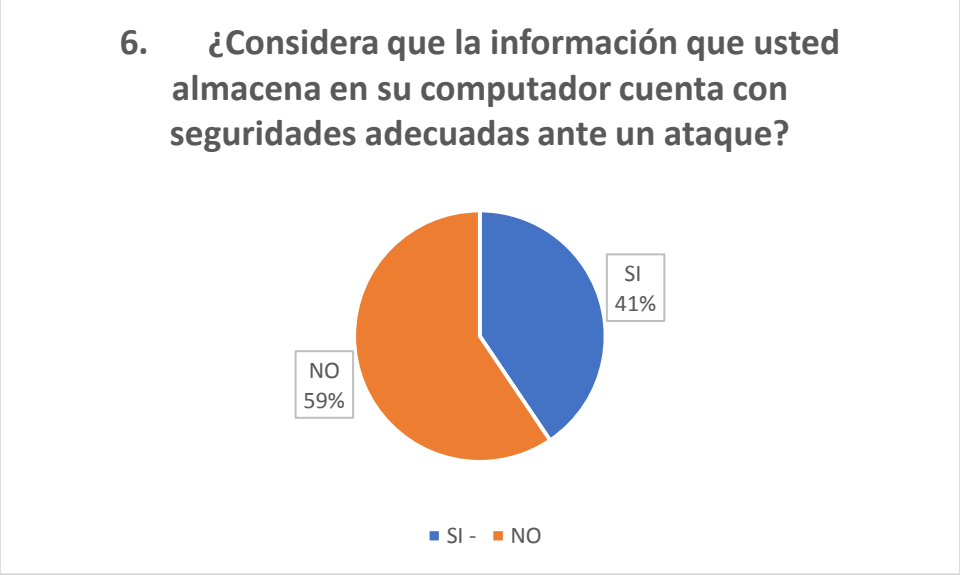


4. ¿Su área de trabajo brinda seguridad ante el acceso no autorizado de terceros?	
SI	183
NO	358

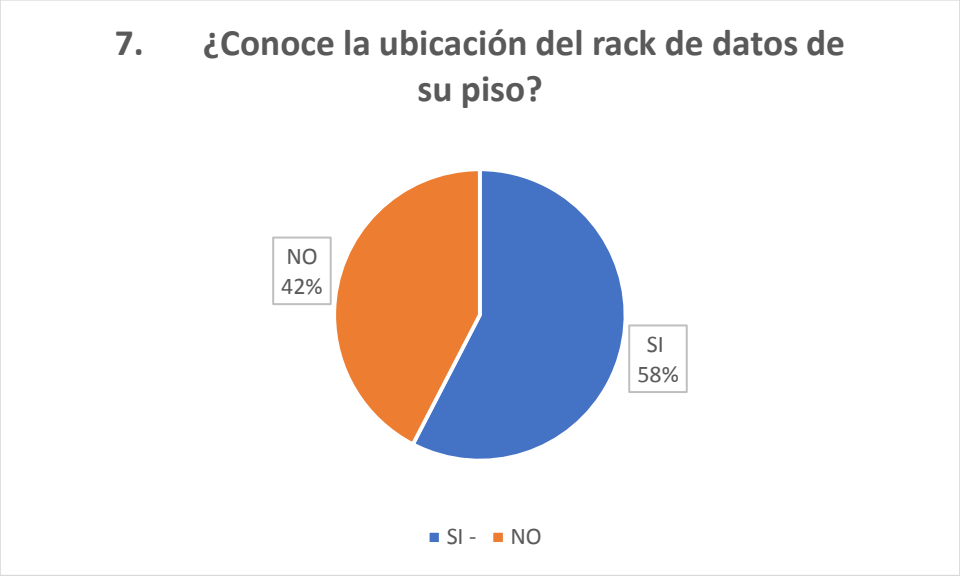


5. ¿Está usted satisfecho con los mantenimientos realizados a los equipos de cómputo que tiene a su cargo?	
SI	330
NO	211

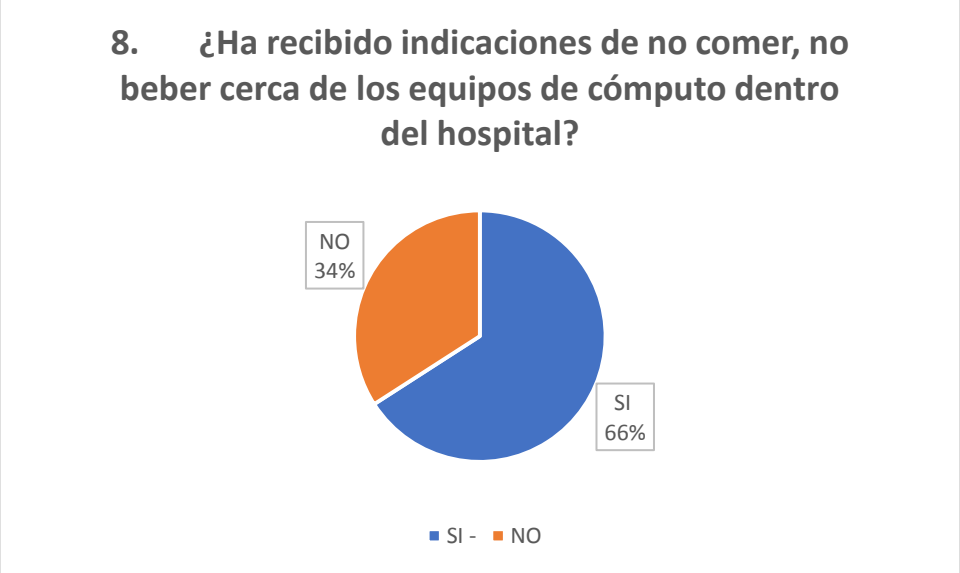
6. ¿Considera que la información que usted almacena en su computador cuenta con seguridades adecuadas ante un ataque?	
SI	220
NO	321



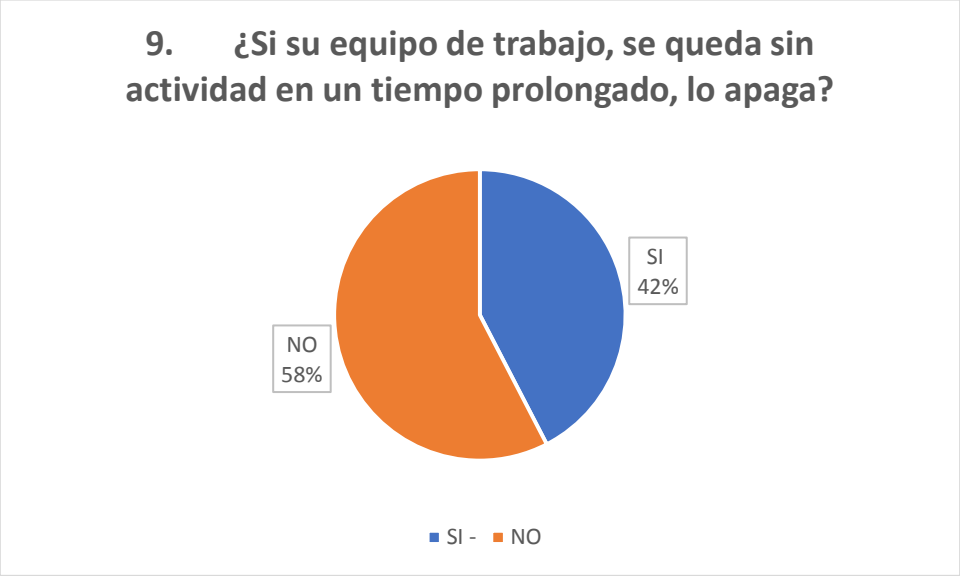
7. ¿Conoce la ubicación del rack de datos de su piso?	
SI	312
NO	229



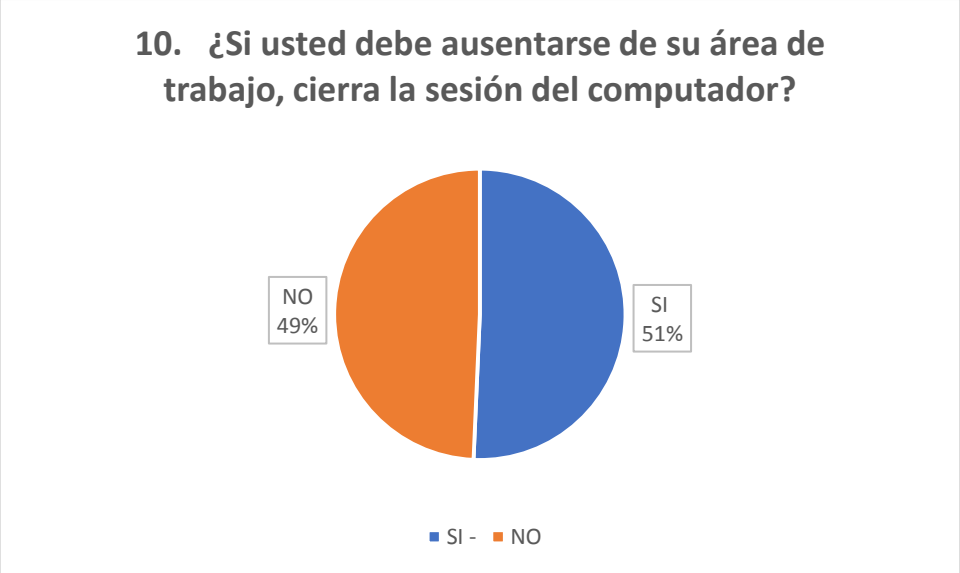
8. ¿Ha recibido indicaciones de no comer, no beber cerca de los equipos de cómputo dentro del hospital?	
SI	358
NO	183



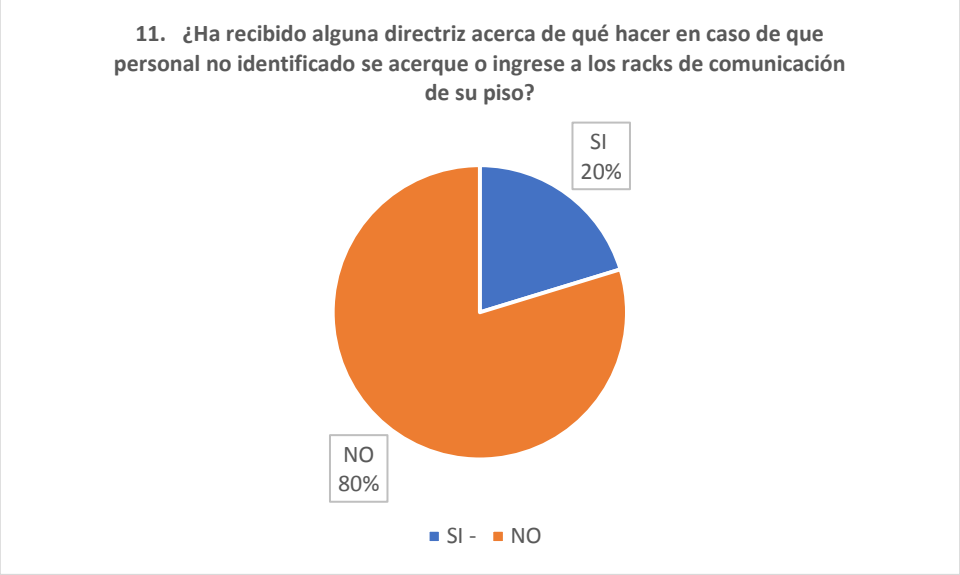
9. ¿Si su equipo de trabajo, se queda sin actividad en un tiempo prolongado, lo apaga?	
SI	229
NO	312



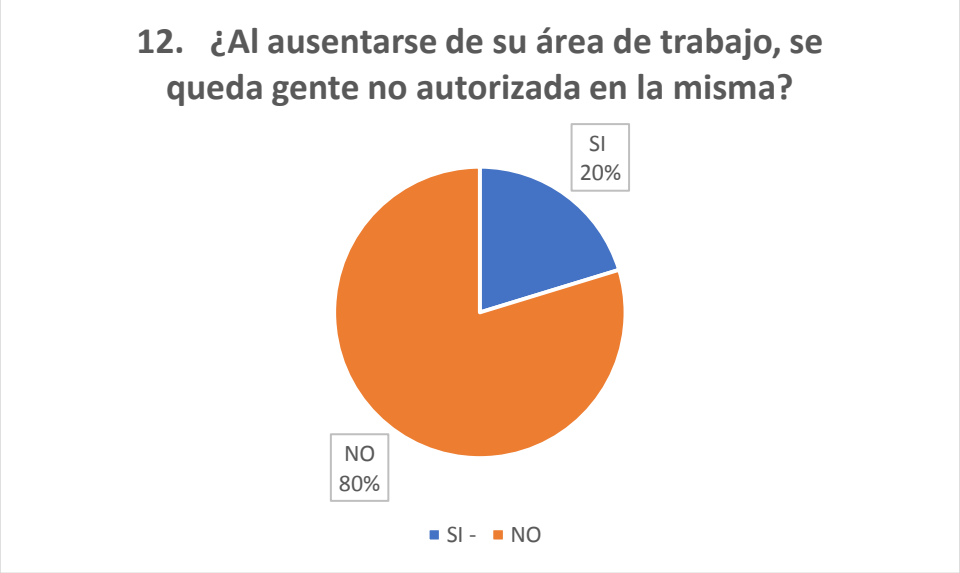
10. ¿Si usted debe ausentarse de su área de trabajo, cierra la sesión del computador?	
SI	275
NO	266



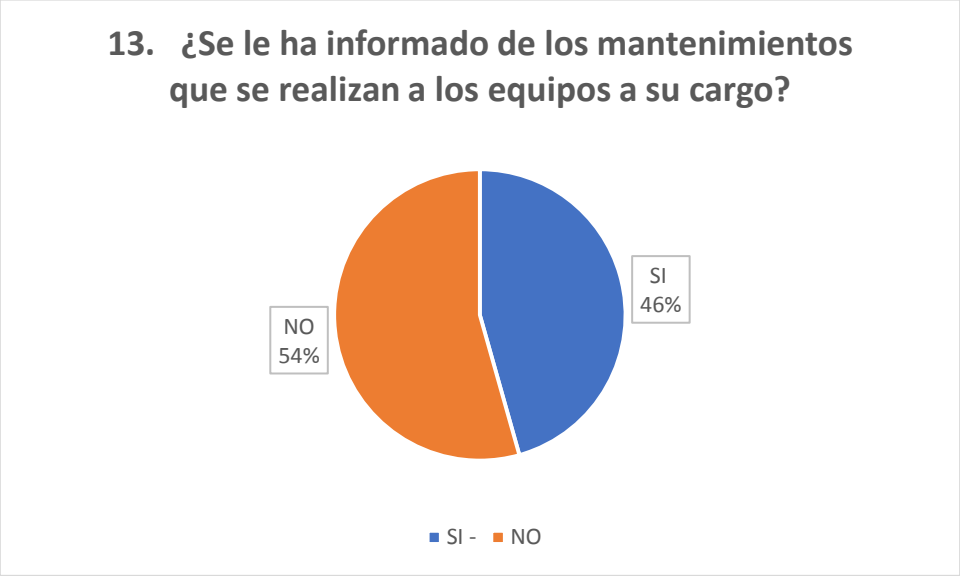
11. ¿Ha recibido alguna directriz acerca de qué hacer en caso de que personal no identificado se acerque o ingrese a los racks de comunicación de su piso?	
SI	110
NO	431



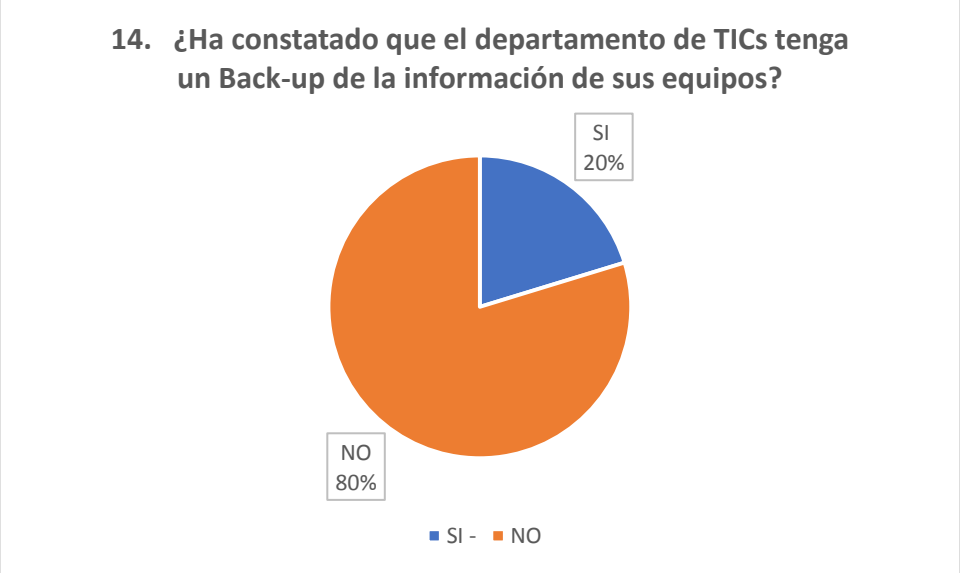
12. ¿Al ausentarse de su área de trabajo, se queda gente no autorizada en la misma?	
SI	110
NO	431



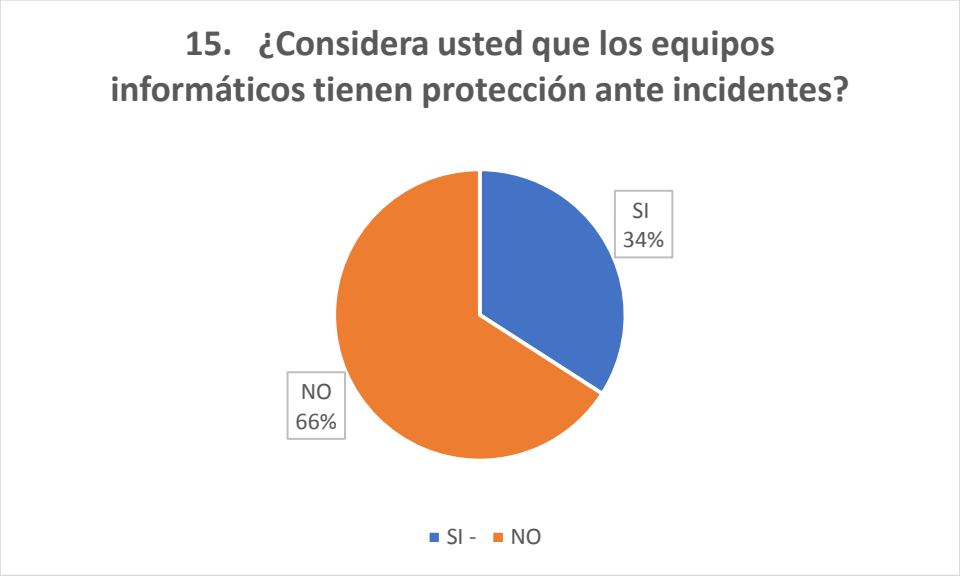
13. ¿Se le ha informado de los mantenimientos que se realizan a los equipos a su cargo?	
SI	248
NO	293



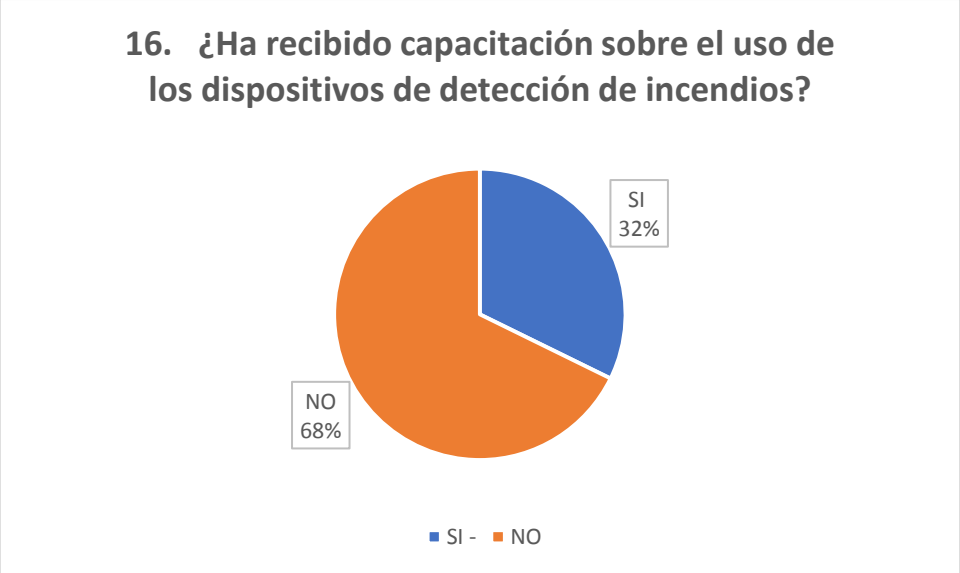
14. ¿Ha constatado que el departamento de TICs tenga un Back-up de la información de sus equipos?	
SI	110
NO	431



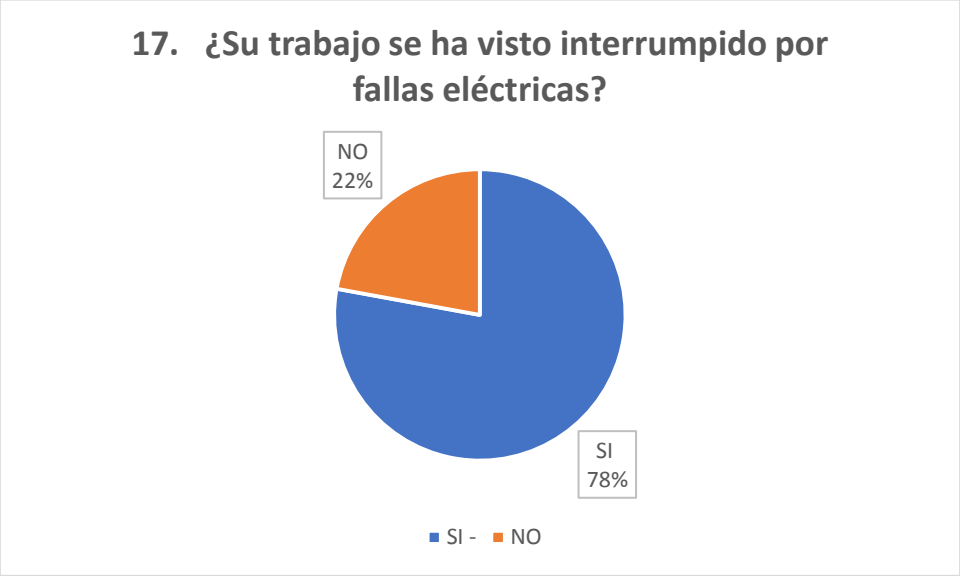
15. ¿Considera usted que los equipos informáticos tienen protección ante incidentes?	
SI	183
NO	358



16. ¿Ha recibido capacitación sobre el uso de los dispositivos de detección de incendios?	
SI	174
NO	367

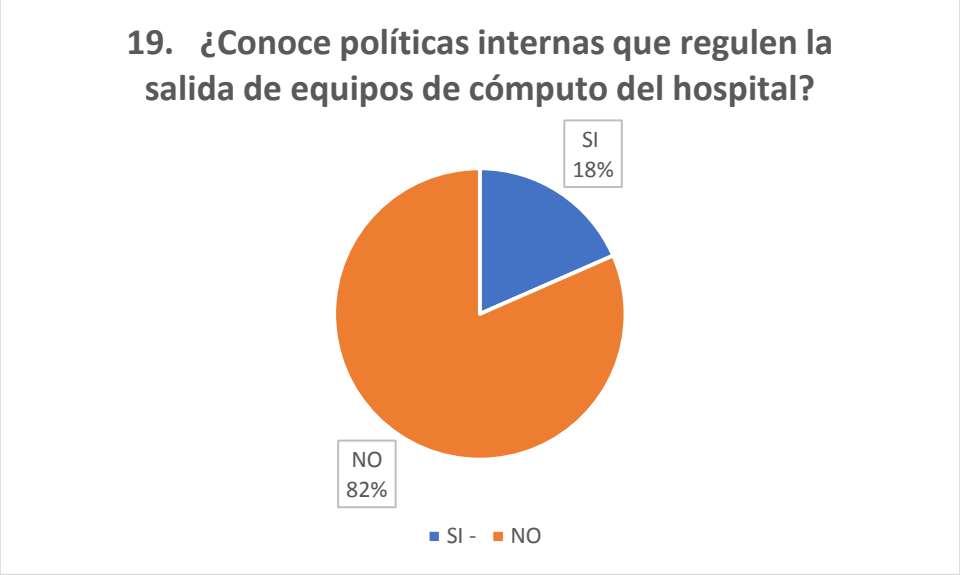


17. ¿Su trabajo se ha visto interrumpido por fallas eléctricas?	
SI	422
NO	119

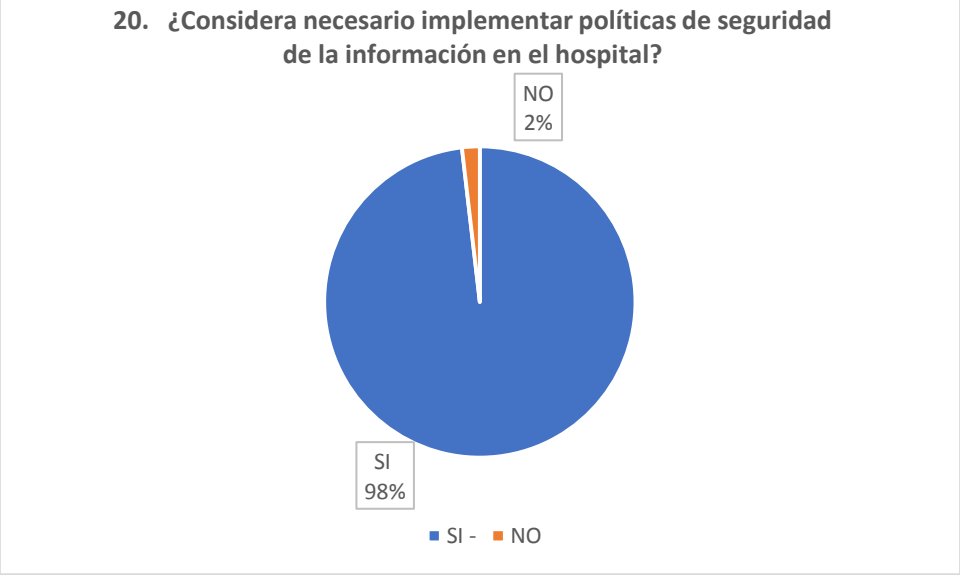


18. ¿Su trabajo se ha visto interrumpido por caídas en telecomunicaciones?	
SI	431
NO	110

19. ¿Conoce políticas internas que regulen la salida de equipos de cómputo del hospital?	
SI	101
NO	440



20. ¿Considera necesario implementar políticas de seguridad de la información en el hospital?	
SI	532
NO	9



ANEXO 3

FORMATO DE SOLICITUD DE CAMBIO

AXXIS HOSPITAL	FORMATO SOLICITUD DE CAMBIO
FECHA:	
UBICACIÓN:	
DEPARTAMENTO:	
ENTREGA:	
RECIBE:	
Por medio de la presente, se hace la entrega formal de la Solicitud de Cambio en la Política de Seguridad	
Observaciones	
Firman:	
Entrega	Recibe
C.I._____	C.I._____

ANEXO 4

FORMATO ACEPTACIÓN DE POLÍTICA DE SEGURIDAD

AXXIS HOSPITAL	FORMATO ACEPTACIÓN DE POLÍTICA DE SEGURIDAD
FECHA:	
UBICACIÓN:	
DEPARTAMENTO:	
ENTREGA:	
RECIBE:	

Por medio de la presente, se hace la entrega formal de la socialización y aceptación de la Política de Seguridad.

Observaciones

Firman:

Entrega	Recibe
C.I._____	C.I._____

ANEXO 5

FORMATO ACTA DE SEGURIDAD PERIMETRAL DE ACTIVOS FIJOS

AXXIS HOSPITAL	FORMATO ACTA DE SEGURIDAD PERIMETRAL DE ACTIVOS FIJOS				
FECHA:					
UBICACIÓN:					
DEPARTAMENTO:					
ENTREGA:					
RECIBE:					
Por medio de la presente, se hace la entrega formal de los siguientes Activos Fijos					
Descripcion del Activo	**Marca**	**Serie**	**Color**	**Estado**	**Observaciones**
Soy responsable de los equipos detallados anteriormente. Cualquier tipo de novedad que suceda con dichos activos, como daño, necesidad de mantenimiento preventivo, movimiento a otra oficina o traslado a otra persona, debo informar inmediatamente a la Administración de Hospifuturo S.A.					
Firman:					
Entrega				Recibe	
C.I._____				C.I._____	

ANEXO 6

CONTRATO DE CONFIDENCIALIDAD

AXXIS HOSPITAL

Edif. Axxis Hospital,
Av. 10 de Agosto N 39 - 155
y Diguja

+ (593 - 2) 3 060 100
www.axxishospital.com.ec

Quito, DD/MM/AAAA

CONTRATO DE CONFIDENCIALIDAD

Al objeto de garantizar la confidencialidad del proyecto de implementación de firma electrónica, se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado el acuerdo por ambas partes.

El contenido del acuerdo es el que figura a continuación. Contenido

DE UNA PARTE: Hospital Axxis y en su nombre y representación **[nombre completo]**, en calidad de **[cargo, administrador, apoderado,...]**

DE OTRA PARTE: **[nombre de la organización].** y en su nombre y representación **(con poder suficiente para ello)** D/Dña. [nombre completo], en calidad de **[cargo, administrador, apoderado,...]**

Reunidos en **Quito** a **dd** de **mm** de **aaaa**

EXPONEN

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes.

CLÁUSULAS

PRIMERA – Definiciones

A los efectos del presente Acuerdo, los siguientes términos serán interpretados de acuerdo con las definiciones anexas a los mismos. Entendiéndose por:

- **«Información propia»:** tendrá tal consideración y a título meramente enunciativo y no limitativo, lo siguiente: descubrimientos, conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos de cualquier tipo, aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes, esté o no incluida en la solicitud de oferta

AXXIS HOSPITAL
Edif. Axxis Hospital,
Av. 10 de Agosto N 39 - 105
y Diguja
+ (593 - 2) 3 960 100
www.axxishospital.com.ec

presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

- **«Fuente»**: tendrá la consideración de tal, cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ella la que suministre la Información Propia y/o cualquiera de los implicados (accionistas, directores, empleados, ...) de la empresa o la organización.

- **«Destinatarios»**: tendrán la consideración de tales cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ellos quienes reciban la Información Propia de la otra parte.

SEGUNDA.- Información Propia.

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, o en su caso, de los acuerdos a los que se lleguen (con independencia de que tal transmisión sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea) tendrá consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento. Esa información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» los efectos del presente acuerdo.

TERCERA.- Exclusión del Presente Acuerdo.

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que:

I – Sea de conocimiento público en el momento de su notificación al «Destinatario» o después de producida la notificación alcance tal condición de pública, sin que para ello el «Destinatario» violentara lo establecido en el presente acuerdo, es decir, no fuera el «Destinatario» la causa o «Fuente» última de la divulgación de dicha información.

II – Pueda ser probado por el «Destinatario», de acuerdo con sus archivos, debidamente comprobados por la «Fuente», que estaba en posesión de la misma por medios legítimos sin que estuviese vigente en ese momento algún y anterior acuerdo de confidencialidad al suministro de dicha información por su legítimo creador.

III – Fuese divulgada masivamente sin limitación alguna por su legítimo creador.

IV – Fuese creada completa e independientemente por el «Destinatario», pudiendo este demostrar este extremo, de acuerdo con sus archivos, debidamente comprobados por la «Fuente».

CUARTA.- Custodia y no divulgación.

Las partes consideran confidencial la «Información propia» de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» de la «Fuente» por parte del «Destinatario» venga impuesta por Ley en vigor o Sentencia Judicial Firme.

Edif. Axxis Hospital,
Av. 10 de Agosto N 39 - 1068
y Rábida

+(593 - 2) 3 980 100
www.axxishospital.com.ec

Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la «Fuente» por parte del «Destinatario» será recibida por éste con el previo consentimiento de la misma.

QUINTA.- Soporte de la «Información propia».

Toda o parte de la «Información propia», firma electrónica, papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología en el que el suministro fuese hecho bajo la condición de «Información propia», con independencia del soporte que la contuviera, tendrá la clasificación de secreta, confidencial o restringida

SEXTA.- Responsabilidad en la Custodia de la «Información propia».

La «Información propia» podrá ser dada a conocer por el «Destinatario» o sus directivos y/o sus empleados, sin perjuicio de que el «Destinatario» tome cuantas medidas sean necesarias para el exacto y fiel cumplimento del presente Acuerdo, debiendo necesariamente informar a unos y otros del carácter secreto, confidencial, o restringido de la información que da a conocer, así como da existencia del presente Acuerdo.

Así mismo, el «Destinatario» deberá dar a sus directivos y/o sus empleados, las directrices e instrucciones que considere oportunas y convenientes a los efectos de mantener el secreto, confidencial, o restringido de la información propia de la «Fuente». El «Destinatario» deberá advertir a todos sus directivos, empleados, etc., que de acuerdo con lo dispuesto en este acuerdo tengan acceso a la «Información propia», de las consecuencias y responsabilidades en las que el «Destinatario» puede incurrir por la infracción por parte de dichas personas, de lo dispuesto en este Acuerdo.

Sin perjuicio de lo anterior, la «Fuente» podrá pedir y recabar del «Destinatario», como condición previa al suministro de la «Información propia», una lista de los directivos y empleados que tendrán acceso a dicha información, lista que podrá ser restringida o reducido por la «Fuente».

Esta lista será firmada por cada uno de los directivos y empleados que figuren en ella, manifestando expresamente que conocen la existencia del presente Acuerdo y que actuarán de conformidad con lo previsto en él. Cualquier modificación de la lista de directivos y/o empleados a la que se hizo referencia anteriormente será comunicada de forma inmediata a la «Fuente», por escrito conteniendo los extremos indicados con anterioridad en este párrafo.

Sin perjuicio de lo previsto en los párrafos anteriores, cada parte será responsable tanto de la conducta dos sus directivos y/o empleados como de las consecuencias que de ella se pudieran derivarse de conformidad con lo previsto en el presente Acuerdo.

SÉPTIMA.- Responsabilidad en la custodia de la «Información propia».

El «Destinatario» será responsable de la custodia de la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», en orden a su tratamiento, como secreta, confidencial o restringida, en el momento presente y futuro, salvo indicación explícita de la «Fuente».

Al objeto de garantizar esta custodia, se deberá devolver la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», a la terminación de las relaciones comerciales, o antes, si fuera requerido por la «Fuente» y respondiendo a los daños y perjuicios correspondientes, en el caso de incumplimiento de lo aquí dispuesto

OCTAVA.- Incumplimiento.

El incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante.

NOVENA.- Duración del Acuerdo de Confidencialidad.

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones comerciales.

DECIMA.- Legislación Aplicable

El presente Acuerdo de Confidencialidad se regirá por la Legislación Ecuatoriana, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo será sometido a la jurisdicción de los Tribunales de (Quito), con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

Y en prueba de esta conformidad, las partes firman o presente acuerdo, por duplicado y a un solo efecto, en el lugar y fecha ut supra.

Entidad	Entidad
_____	_____
Firma representante _____	Firma representante_____
DNI representante_____	DNI representante_____

ANEXO 7

FORMATO CAMBIO DE FUNCIONES

AXXIS HOSPITAL	**FORMATO CAMBIO DE FUNCIONES**				
FECHA:					
UBICACIÓN:					
DEPARTAMENTO:					
ENTREGA:					
RECIBE:					
Por medio de la presente, se hace la entrega formal de los siguientes Activos Fijos					
Descripcion del Activo	**Marca**	**Serie**	**Color**	**Estado**	**Observaciones**
Soy responsable de los equipos detallados anteriormente. Cualquier tipo de novedad que suceda con dichos activos, como daño, necesidad de mantenimiento preventivo, movimiento a otra oficina o traslado a otra persona, debo informar inmediatamente a la Administración de Hospifuturo S.A.					
Firman:					
Entrega				Recibe	
C.I._____				C.I._____	

ANEXO 8

INVENTARIO DE EQUIPOS Y MATERIALES EN CUSTODIA

AXXIS HOSPITAL

INVENTARIO EQUIPOS Y MATERIALES EN CUSTODIA

No. ID	NOMBRE DEL EQUIPO/MATERIAL	DESCRIPCIÓN GENERAL	No. SERIE / DATOS DE PLACA (SI EXISTE)	USO ORIGINAL	PESO UNITARIO (KG)	VOLUMEN UNITARIO (M3)	NÚMERO UNIDADES	CANTIDAD TOTAL		ESTADO	OBSERVACIONES SOBRE EL ESTADO DEL RESIDUO	REFERENCIA ANEXO FOTOGRÁFICO
								PESO (KG)	VOLUMEN (m3)			

REGISTRO FOTOGRÁFICO	
Foto1:	**Foto2:**

ANEXO 9
FORMATO ACTA CUSTODIA DE EQUIPOS

AXXIS HOSPITAL	FORMATO ACTA CUSTODIA DE EQUIPOS
FECHA:	
UBICACIÓN:	
DEPARTAMENTO:	
ENTREGA:	
RECIBE:	

Por medio de la presente, se hace la entrega formal de los siguientes Activos Fijos

Descripcion del Activo	Marca	Serie	Color	Estado	Observaciones

Soy responsable de los equipos detallados anteriormente. Cualquier tipo de novedad que suceda con dichos activos, como daño, necesidad de mantenimiento preventivo, movimiento a otra oficina o traslado a otra persona, debo informar inmediatamente a la Administración de Hospifuturo S.A.

Firman:

Entrega	Recibe
C.I._____	C.I._____

ANEXO 10

CONTROL DE SOPORTE SISTEMAS

SOPORTE SISTEMAS

FECHA: Quito, 08 de Mayo del 2019

MEDIO	SOLICITANTE	PROBLEMA	TÉCNICO	SOLUCIÓN	INFORME
TELEFONÍA	Urologia	No pueden imprimir	RICARDO ARIAS	SI	Reinstalación de controladores
MEDIO	**SOLICITANTE**	**PROBLEMA**	**TÉCNICO**	**SOLUCIÓN**	**INFORME**
TELEFONÍA	Secretaria piso 6	No puede enviar correo	RICARDO ARIAS	SI	Correo de 8 megas
MEDIO	**SOLICITANTE**	**PROBLEMA**	**TÉCNICO**	**SOLUCIÓN**	**INFORME**
TELEFONÍA	Docencia	No tiene internet	RICARDO ARIAS	SI	Cable de red desconectado
MEDIO	**SOLICITANTE**	**PROBLEMA**	**TÉCNICO**	**SOLUCIÓN**	**INFORME**
TELEFONÍA	Docencia	No vale wifi	RICARDO ARIAS	SI	Se reinició router
MEDIO	**SOLICITANTE**	**PROBLEMA**	**TÉCNICO**	**SOLUCIÓN**	**INFORME**
TELEFONÍA	Lic. Rocio Reyes	No pueden enviar correo	RICARDO ARIAS	SI	reparación de la cuenta
MEDIO	**SOLICITANTE**	**PROBLEMA**	**TÉCNICO**	**SOLUCIÓN**	**INFORME**
TELEFONÍA	Secretaria Emer4gencia	No puede scanear	RICARDO ARIAS	SI	Se cambió predeterminado otro scanner
MEDIO	**SOLICITANTE**	**PROBLEMA**	**TÉCNICO**	**SOLUCIÓN**	**INFORME**
TELEFONÍA	LabLink	No se abre google chrome	RICARDO ARIAS	SI	Reinstalación de google

ANEXO 11
OFICIO DE ACEPTACIÓN DE POLÍTICA DE SEGURIDAD

AXXIS HOSPITAL

Quito, 28 de septiembre de 2019

Estimado

Ing. Leonardo Torres

Gerente de Calidad de Axxis Hospital

Presente.

Por medio de la presente, me permito hacerle llegar el documento de la Política de Seguridad de la Infraestructura de Red para Axxis Hospital, para la posterior aprobación de Gerencia General y así realizar la socialización del mismo para toda la comunidad Axxis.

La presente política de seguridad tiene por objeto el precautelar la infraestructura física de red de Axxis entregando lineamientos claros y de estricto cumplimiento para todos quienes somos usuarios de los activos de red que dispone el hospital.

Contando con su apertura para la aceptación del mismo, anticipo mis más sinceros agradecimientos.

Atentamente,

HOSPIFUTURO S.A.
FIRMA AUTORIZADA

Ing. María Fernanda Palma

Gerente de TICs.

Hospifuturo S.A.

PBX: (02) 398 0100 ext. 1283

Dir.: 10 de Agosto N39 -155 y Diguja

HOSPIFUTURO S.A.
14 OCT 2019
RECIBIDO

1