UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

PLAN DE INVESTIGACIÓN DE FIN DE CARRERA

TITULADO:

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.

REALIZADO POR:

Ing. Galo Cárdenas

DIRECTOR DEL PROYECTO:

Ing. Edison Estrella

COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE: MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD Y REDES

DECLARACIÓN JURAMENTADA

Yo, GALO DAVID CÁRDENAS CALDERÓN, con cédula de identidad # 1716129547, 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.

Galo David Cárdenas Calderón
C.C.: 1716129547

DECLARATORIA

El presente trabajo de investigación titulado:

“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.”

Realizado por:

GALO DAVID CÁRDENAS CALDERÓN

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:

ING. VERÓNICA RODRÍGUEZ, MBA

MSC. FABIÁN HURTADO

Después de revisar el trabajo presentado,

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

Ing.Verónica Rodríguez. MBA

Msc. Fabián Hurtado

Quito, 23 de abril de 2018

DEDICATORIA

Dedico el presente trabajo de investigación a mi hermosa familia, mi esposa que es mi apoyo y compañera de vida, con quien emprendimos un objetivo y cada día lo cumplimos a base de sacrificios y dedicación, para mis hijos quienes con sus ocurrencias me dan el valor para luchar y la fuerza para conseguir los objetivos, mis padres quienes supieron inculcarme valores y principios que han guiado mi vida y a mi hermano, compañero de toda la vida.

AGRADECIMIENTO

Al profesor Edison Estrella por su acertada dirección de la tesis. Su profesionalismo y entrega fueron determinantes a la hora de conformar este documento.

A la profesora, Verónica Rodríguez quien con su conocimiento me guio para abrir horizontes en el mundo de la gestión de tecnologías de la información.

Al profesor, Fabián Hurtado por su tiempo y dedicación en la revisión del trabajo.

A la Universidad Internacional SEK, por su esfuerzo de formar profesionales íntegros

Índice de Contenido

Índice de Figuras

Índice de Tablas

Resumen

Para el desarrollo de este trabajo se utiliza 4 fases tales como identificación, planeación, diseño y socialización, para lograr el objetivo de tener una política de seguridad que permita garantizar que la información cumpla con 3 factores importantes, la confidencialidad, integridad y disponibilidad.

Por medio de un análisis documental se determinan posibles fallos de seguridad en el uso de aplicaciones médicas, con auditorías internas y notificaciones de entidades de control como el Arcotel, advierten de daños potenciales a la infraestructura e información del Hospital. Por lo tanto, se requiere mediante el análisis de riesgos a la infraestructura y aplicaciones del Hospital Axxis determinar las causas de estos vacíos de seguridad.

Para realizar un análisis de riesgos completo se realizan entrevistas y encuestas al personal del Hospital para determinar las brechas de seguridad existentes, con este análisis exhaustivo se seleccionan un conjunto de controles según la norma ISO 27799, que se especializa en el sector sanitario y tiene controles específicos para el uso de aplicaciones médicas que permitan crear una política de seguridad con el objetivo de mitigar el riesgo en el acceso a las mismas en el Hospital Axxis, una vez definida la política de seguridad es imprescindible su difusión, comunicación y aplicación para permitir el correcto uso de las aplicaciones médicas.

Palabras clave: Política de seguridad, Aplicaciones médicas, riegos de seguridad

Summary

For the development of this work we use the methodology of 4 phases that are identification, planning, design and socialization, to achieve the objective of having a security policy that ensures that the information complies with 3 important factors, confidentiality, integrity and availability.

By means of a documentary analysis, possible security failures in the use of medical applications are determined, with internal audits and notifications from control entities such as Arcotel, warn of potential damage to infrastructure and hospital information. Therefore, the analysis of risks to the infrastructure and applications of Axxis Hospital is necessary to determine the causes of these security gaps.

To carry out a complete risk analysis, interviews and surveys are carried out with Hospital staff to determine the existing safety gaps, with this exhaustive analysis a set of controls according to ISO 27799 is selected, which specializes in the health sector and has controls specific for the use of medical applications that allow the creation of a security policy with the objective of mitigating the risk of access to the medical applications of the Axxis Hospital, once the security policy is defined, its dissemination, communication and application to enable the correct use of medical applications.

Keywords: Security policy, Medical applications, security risks, norms

CAPÍTULO I

1. INTRODUCCIÓN

Las organizaciones que prestan servicios de salud, están en una etapa de transición hacia el uso de aplicaciones médicas, la información es un componente indispensable en la conducción y consecución de los objetivos planeados, razón por la cual es necesario que la empresa establezca políticas de seguridad que asegure que la información es protegida de una manera adecuada, independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

El uso creciente y no planificado de la tecnología para el manejo de información crítica y sensible de las organizaciones han dejado de lado la seguridad y prevención de la información, lo que ha permitido elevar los delitos informáticos a través de las vulnerabilidades presentes en las diversas aplicaciones de las organizaciones, "Enrique García, fiscal provincial, informó que desde el 2016 hasta la presente han detectado cuatro clases de delitos informáticos, pero el principal es la apropiación fraudulenta por medios electrónicos, tipificada en el artículo 190 del Código Orgánico Integral Penal (COIP). En base a estos datos se puede apreciar que los delitos informáticos crecerán exponencialmente conforme a las empresas adquieren aplicaciones o servicios informáticos, por ende, aumentará la vulnerabilidad de la información.

El problema al administrar los recursos tecnológicos se debe principalmente a que el planteamiento y la planeación estratégica, prácticamente no existen. Las tendencias de crecimiento actuales de TI en el mundo, se han caracterizado por el crecimiento desordenado y sin un objetivo claro. Muy poco esfuerzo es puesto en especificar la estrategia de negocios y en construir un modelo de la organización, como precursores en la determinación de requerimientos de TI.

Las aplicaciones son diseñadas para cumplir objetivos a corto plazo o problemas inmediatos, aislando al departamento de TI en segmentos de cada área que componen la organización. La necesidad de un plan de TI es clara, pero el proceso para implementarlo no es fácil.

Entender los riesgos específicos que aquejan a cada organización que incluso puede suponer el riesgo en la continuidad del negocio, llevan a proponer una política de seguridad que deben ser aplicadas a las organizaciones con el fin de precautelar la información como un bien que afecta directamente al giro del negocio.

La aplicación de una política de seguridad en el Hospital Axis evitará la fuga de información sensible que pueda poner en riesgo la institucionalidad de la organización.

El trabajo se basa en la premisa de Seguridad de la información en la infraestructura tecnológica de Hospital Axxis.

1.1. EL PROBLEMA DE INVESTIGACIÓN

1.1.1. Planteamiento del Problema

La fuga de información médica, venta de base de datos a farmacéuticas, robo de información susceptible de pacientes requieren ser mitigadas mediante mecanismos de seguridad. La implementación de software de historias clínicas electrónicas se las ha realizado de manera acelerada sin tomar en cuenta posibles vulnerabilidades que afecten a la información del paciente.

La Ley de Derechos y Amparo al Paciente, en el artículo 4, dispone: "Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial".

Los hospitales, centros médicos y toda entidad encargada de brindar servicios médicos en el Ecuador, se encuentran en proceso de adaptación tecnológica, según el Ministerio de Salud Pública Ecuatoriana todas las entidades de salud deben ocupar el formato de historia médica electrónica única.

Según el Código Orgánico Integral Penal, en el artículo 179, dispone: "Revelación de secreto. - La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.";

La modernización tecnológica en el campo médico es muy importante para hospitales y centros de salud ya que les permite manejar el historial del paciente no solo de una especialidad sino de todo su expediente médico, por otro lado, existen riesgos ligados a la tecnología como fuga de información sensible, robo de base de datos de pacientes, que afectan directamente a la institucionalidad de la empresa de salud.

Por lo tanto, el Hospital Axxis como una organización que brinda servicios de salud debe tomar acciones para proteger la información de las diferentes aplicaciones que funcionan dentro del Hospital Axxis, detectando las vulnerabilidades de las aplicaciones, corrigiéndolas e implementando medidas de seguridad para mitigar los riesgos y mantener los tres factores importantes para el Hospital Axxis en temas de información:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- **S**u disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran. La seguridad de la

información se consigue implantando un conjunto adecuado de controles, tales como una adecuada política de seguridad, buenas prácticas, procedimientos claros, estructuras organizativas. Estos controles deben ser establecidos para asegurar que se cumplen los objetivos específicos de seguridad de la empresa.

1.1.1.1. Diagnóstico del Problema.

Del análisis documental encontrado en el Hospital Axxis, se detecta una mala gestión del departamento de TI en el manejo de la seguridad de la información, se requiere reducir los diferentes vacíos de seguridad que existen tanto a nivel lógico como físico que se han detectado dentro del Hospital Axxis.

De la auditoría interna (Anexo 1 Hallazgos Auditoría Interna) realizada en el Hospital Axxis de los hallazgos se obtiene que el uso de la aplicación de gestión médica en el Hospital está expuesta al robo de información, del análisis de vulnerabilidades al software de agendamiento médico EXMED del Hospital Axxis, se determina que existe acceso a la base de datos de pacientes con usuario root sin password como indica en la Figura 1 de igual manera el acceso al calendario de pacientes de la Figura 2.

Figura 1 *Información de pacientes desde el navegador*
Fuente: *Elaboración propia*

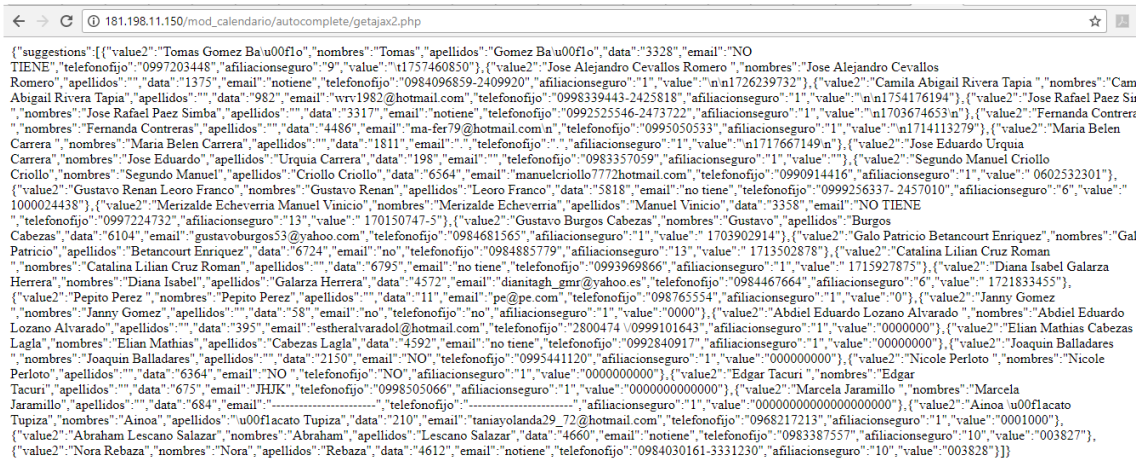


Figura 2 *Información del calendario desde el navegador*
Fuente: *Elaboración propia*

Otro hallazgo de la auditoría es la falta de control de periféricos, que permite el ingreso de dispositivos USB que infectan con virus malware a máquinas de la red, los que generan san mediante spamboots consecuencia de esto se cae en listas negras como indica en la Figura 3.

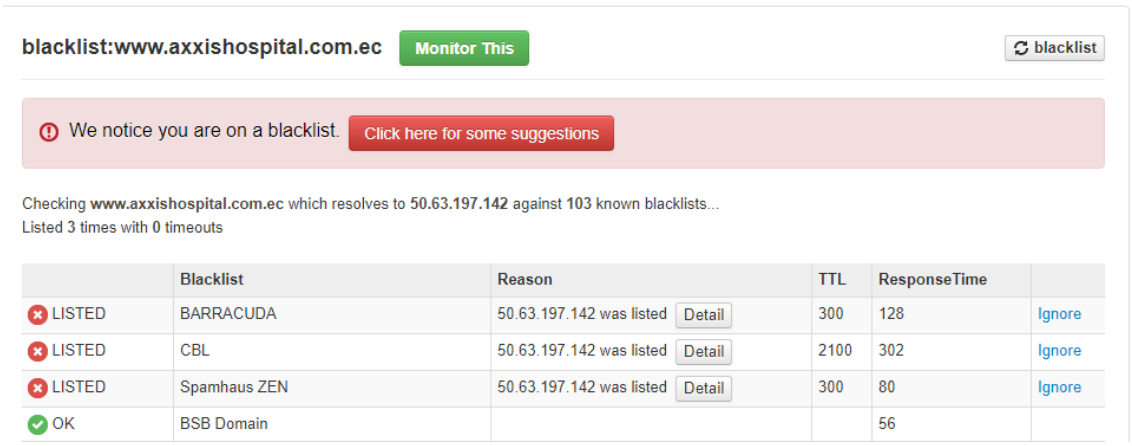
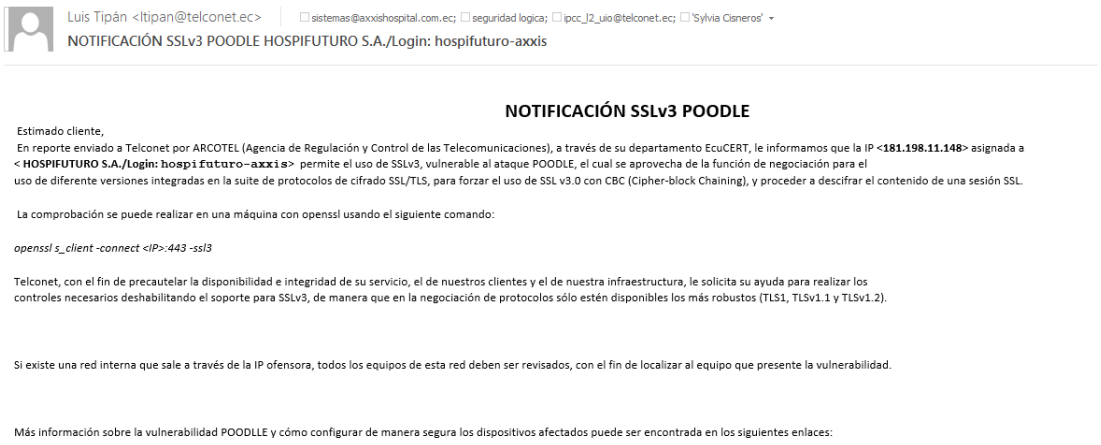


Figura 3 *IP registrada en listas negras*
Fuente: *Tomado de MXTOOLBOX*

Según el análisis documental la incidencia reportada por el Arcotel al departamento de sistemas existe vulnerabilidades por el uso de protocolos fuera de uso como SSL v3, según el informe emitido por el departamento de sistemas existe un servidor proxy en Linux que está conectado directo a la IP pública y no detrás del Firewall indica la Figura 4.



Luis Tipán <ltipan@telconet.ec> | sistemas@axxishospital.com.ec; seguridad logica; ipcc_l2_uio@telconet.ec; 'Sylvia Cisneros'

NOTIFICACIÓN SSLv3 POODLE HOSPIFUTURO S.A./Login: hospifuturo-axxis

NOTIFICACIÓN SSLv3 POODLE

Estimado cliente,

En reporte enviado a Telconet por ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones), a través de su departamento EcuCERT, le informamos que la IP **<181.198.11.148>** asignada a **< HOSPIFUTURO S.A./Login: `hospifuturo-axxis`>** permite el uso de SSLv3, vulnerable al ataque POODLE, el cual se aprovecha de la función de negociación para el uso de diferente versiones integradas en la suite de protocolos de cifrado SSL/TLS, para forzar el uso de SSL v3.0 con CBC (Cipher-block Chaining), y proceder a descifrar el contenido de una sesión SSL.

La comprobación se puede realizar en una máquina con openssl usando el siguiente comando:

openssl s_client -connect <IP>:443 -ssl3

Telconet, con el fin de precautelar la disponibilidad e integridad de su servicio, el de nuestros clientes y el de nuestra infraestructura, le solicita su ayuda para realizar los controles necesarios deshabilitando el soporte para SSLv3, de manera que en la negociación de protocolos sólo estén disponibles los más robustos (TLS1, TLSv1.1 y TLSv1.2).

Si existe una red interna que sale a través de la IP ofensora, todos los equipos de esta red deben ser revisados, con el fin de localizar al equipo que presente la vulnerabilidad.

Más información sobre la vulnerabilidad POODLLE y cómo configurar de manera segura los dispositivos afectados puede ser encontrada en los siguientes enlaces:

Figura 4 *Notificación del Arcotel por SSLV3 POODLE*
Fuente: *Arcotel*

Del análisis documental en Hospital Axxis en una auditoría interna para la renovación de la ISO9001 se registran ACPM que evidencian que no presentan un sistema de control de acceso hacia la infraestructura tecnológica del hospital, la Figura 5 indica la ACPM levantada.

Solicitante de la ACPM	Responsable de atender la solicitud de ACPM
Administración General	Jefe de TIC

Descripción del problema real o potencial
En el recorrido realizado por las instalaciones de la organización se indago sobre el control de accesos a los diferentes cuartos de sistemas a Juan Carlos Cumbicus analista 1, Ricardo Arias analista 1 dichas personas manifestaron que se entra con la llave y no existe la forma de trabajo en control de accesos

Análisis de Causa
El crecimiento del Hospital a dejado de lado un control de acceso a los cuarto de sistemas

Plan de Acción		
Actividad	**Responsable**	**Fecha**
Solicitar al área de Sistemas el listado de usuarios que deben ingresar a los cuartos de sistemas.	Jefe de TIC	9/9/2016

Figura 5 *Incidencia ACPM de una auditoría interna*

Fuente: *ACPM ISO 9001*

De acuerdo a las entrevistas realizadas a personal del Hospital Axxis, se ha podido notar que no existen medidas de seguridad de información aplicadas para el acceso a la red, las personas del departamento de TI requieren capacitación sobre temas de seguridad informática, esta deficiencia en seguridad ocasiona que la institución esté expuesta a vulnerabilidades como:

- Información sin acceso restringido.
- No existe un control de implementación de aplicaciones
- Se puede realizar copias no autorizadas de historias clínicas
- No se controlan los periféricos de las computadoras.

1.1.1.2. Pronóstico

Con una población creciente y un incremento en el número de pacientes, la automatización de los sistemas médicos es cada vez más necesaria, por ende, existe más riegos para la información almacenada electrónicamente. Con la implementación de más

aplicaciones médicas se debe tener en cuenta las vulnerabilidades y el riesgo potencial de las empresas ante ataque informático.

Enrique García, fiscal provincial, informó que desde el 2016 hasta la presente han detectado cuatro clases de delitos informáticos, pero el principal es la apropiación fraudulenta por medios electrónicos, tipificada en el artículo 190 del Código Orgánico Integral Penal (COIP).

En base a estos datos se puede apreciar que los delitos informáticos crecerán exponencialmente conforme a las empresas adquieren aplicaciones o servicios informáticos, por ende, aumentaran los delitos informáticos y se pondrá en riesgo la divulgación, fuga o robo de información.

1.1.1.3. Control del Pronóstico

Se debe tratar de mitigar los riegos de seguridad informática en las aplicaciones del Hospital Axxis para garantizar la confidencialidad, integridad y disponibilidad de la información. Debido a la identificación de vulnerabilidades en las aplicaciones médicas es necesario proteger la información del Hospital Axxis, caso contrario existe el riesgo de pérdida o fuga de información, lo que puede ocasionar problemas legales a las entidades de salud.

1.1.2. Formulación del Problema

La inadecuada gestión de la seguridad de la información en las aplicaciones médicas del Hospital Axxis, pone en riesgo la confidencialidad integridad y disponibilidad de la misma.

1.1.3. Sistematización del Problema.

Los aspectos antes indicados generan interrogantes que necesitan soluciones como:

- ¿Qué procedimiento permitirá al investigador conocer las vulnerabilidades en las aplicaciones médicas del Hospital Axxis?
- ¿Qué marco regulatorio se debe tomar en cuenta para que las aplicaciones médicas en Hospitales sean implementadas correctamente?
- ¿Con las vulnerabilidades encontradas cómo se puede minimizar el riesgo?
- ¿Cuál es la referencia técnica ante posibles eventos de seguridad en el Hospital Axxis?

1.1.4. Objetivo General.

Diseñar una política de seguridad de la información basada en la norma ISO 27799 para el control de accesos a las aplicaciones médicas en la red del Hospital Axxis.

1.1.5. Objetivos Específicos.

- Diagnosticar el estado actual de las aplicaciones médicas mediante un análisis de riesgos para detectar las vulnerabilidades existentes en el Hospital Axxis.
- Analizar las leyes y normativas que regulan a las entidades Hospitalarias, mediante el estudio de la Pirámide de Kelsen, para ser aplicados en la elaboración de la política de seguridad.
- Establecer los controles de la norma ISO 27799 para el diseño de la política de seguridad del Hospital Axxis, que garanticen la confiabilidad, disponibilidad e integridad de la información.
- Elaborar el documento de política de seguridad para el Hospital Axxis mediante los controles de la ISO 27799 para que sirva como referencia al departamento de TI en la seguridad la información contenida en las aplicaciones médicas.

1.1.6. Justificación

Ante el esquema de globalización de la tecnología de la información se ha originado el uso masivo de aplicaciones y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear y robar se convierten en retos para delincuentes informáticos conocidos como Hackers, Crackers, etc., es decir, en transgresores. El continuo riesgo al que están expuestos, obliga a las entidades a crear políticas de seguridad para precautelar la confidencialidad, integridad y disponibilidad de la información. En nuestro país existen muchas instituciones que han sido víctimas de ataques en sus instalaciones, tanto desde el interior como del exterior, por lo que es necesario mitigar los riesgos y amenazas que aquejan a las instituciones. Ante este panorama se requiere implementar una política de seguridad que ayude a gestionar la seguridad informática de mejor manera.

La Ley de Derechos y Amparo al Paciente, en el artículo 4, dispone: "Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial".

Según el Código Orgánico Integral Penal, en el artículo 179, dispone: "Revelación de secreto. - La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año."

Metodológica

Alineándose a los criterios de Cruz, Parra, & Ariza (2016) La metodología a utilizar se describe en 4 fases: Identificación, planeación, diseño y socialización que cumpla con el objetivo general del proyecto y teniendo en cuenta el marco de referencia

la norma ISO/ 27799. Esta metodología pretende dar cumplimiento a los objetivos específicos propuestos, donde se definen los entregables como productos para el desarrollo del proyecto. Para el desarrollo de la metodología se describen las actividades a realizar en cada una de las fases con su entregable:

- Identificación: En esta fase se realizará la identificación y se realizará el análisis de las vulnerabilidades, amenazas, que afectan la información de las áreas médicas
- Planeación: En Esta fase se realizará de acuerdo al resultado del análisis un bosquejo de la política de seguridad a las amenazas de alto nivel identificadas que nos permitan asegurar la información en las áreas médicas, especificando el alcance, contexto, cumplimiento y responsables.
- Diseño: En esta fase se diseñará la política de seguridad de acuerdo a la ISO /IEC 27799.
- Socialización: Entrega de documento de la política de seguridad.

Relevancia Social

Se requiere asegurar la información clínica de los pacientes en el Hospital Axxis para garantizar la confidencialidad de los datos entregados en cada visita médica de los pacientes para que exista un ambiente de confianza, y cumplir los objetivos de la institución. Para diseñar las políticas de seguridad se cuenta con el compromiso del Hospital Axxis para mejorar la seguridad en su paquete de aplicaciones médicas.

1.2. MARCO TEÓRICO

ISO 27799:2016

La norma ISO27799 (2016, pp13.14) internacional proporciona orientación a las organizaciones sanitarias y a otros custodios de información personal sanitaria sobre la mejor forma de proteger la confidencialidad, integridad y disponibilidad de dicha

información a través de la implementación de la Norma ISO/IEC 27002/1). Específicamente, esta norma internacional trata sobre las necesidades especiales de gestión de seguridad de la información del sector sanitario y sus entornos operativos únicos. Mientras que la protección y seguridad de la información personal es importante para todos los individuos, corporaciones, instituciones y gobiernos, en el sector sanitario existen requisitos especiales que es necesario cumplir para asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de los datos personales sanitarios. La mayoría considera este tipo de información entre las más confidenciales de todos los tipos de datos personales. Para mantener la privacidad de los sujetos de la asistencia médica es esencial proteger esta confidencialidad. La integridad de la información sanitaria se debe proteger para dar la seguridad al paciente, y un componente importante de tal protección es asegurar que el ciclo de vida completo de la información es totalmente auditable. La disponibilidad de la información sanitaria también es crítica para la prestación sanitaria efectiva. Los sistemas de informática sanitaria deben cumplir demandas únicas para mantenerse operativos ante desastres naturales, fallos de sistema y ataques de denegación de servicio. Por lo tanto, proteger la confidencialidad, integridad y disponibilidad de la información sanitaria requiere habilidades específicas del sector sanitario.

Ley de Protección de datos Personales

Según el Código Orgánico Integral Penal, en el artículo 179, dispone:

> "Revelación de secreto. - La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año."

Lineamientos de políticas de Seguridad de la Información del Ministerio de Salud

Ministerio de Salud Pública del Ecuador, Se expide el reglamento para el manejo de información confidencial en el sistema nacional de salud Acuerdo No. 00005216-A

La Ley de Derechos y Amparo al Paciente, en el artículo 4, dispone: "Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial".

Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información.

Art. 3.- Integridad de la información. - Es la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por tanto, mantiene sus características y valores asignados o recogidos en la fuente. Esta cualidad debe mantenerse en cualquier formato de soporte en el que se registre la información, independientemente de los procesos de migración entre ellos.

Art. 4.- Disponibilidad de la información. - Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional.

Art. 5.- Seguridad en el manejo de la información. - Es el conjunto sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su condición de confidencial, así como su integridad y disponibilidad. Inicia

desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona.

El deber de confidencialidad respecto a la información de los documentos que contienen información de salud perdurará, incluso, después de finalizada la actividad del establecimiento de salud, la vinculación profesional o el fallecimiento del titular de la información.

Art. 6.- Secreto Médico. - Es la categoría que se asigna a toda información que es revelada por un/a usuario/a al profesional de la salud que le brinda la atención de salud. Se configura como un compromiso que adquiere el médico ante el/la usuario/a y la sociedad, de guardar silencio sobre toda información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional.

Los profesionales de salud de los establecimientos de salud cumplirán con el deber del secreto médico, para generar condiciones de confianza en la relación con los/as usuarios/as y así garantizar el derecho a la intimidad. El secreto médico es extensible a toda la cadena sanitaria asistencial.

Vulnerabilidad informática

"Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software". (Whitten, 2011)

Amenaza

"Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo". (Whitten, 2011)

Riesgo

"El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al sistema. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza." (Whitten, 2011)

El riesgo se utiliza sobre todo el análisis de riesgos de un sistema informático. Esté riesgo permite tomar decisiones para proteger mejor al sistema. Se puede comparar con el riesgo límite que acepte para su equipo, de tal forma que, si el riesgo calculado es inferior al de referencia, éste se convierte en un riesgo residual que podemos considerar cómo riesgo aceptable.

1.2.1. Estado del Arte

Según Orel y Bernik (2013) Utiliza enfoques comunes ampliamente extendidos para la seguridad de sistemas en entornos controlados dedicados a la salud, se evalúa un nivel de conciencia, confianza y aceptación de la estandarización relevante.(p.195)

El nivel de conciencia de seguridad con los usuarios, los pacientes y los profesionales de la atención no es lo suficientemente alto para que las amenazas y los riesgos potenciales no se tomen en cuenta, los estándares como la familia ISO / IEC 27000, las pautas de seguridad de la información ISO / IEC 27799 en salud a menudo no son bien conocidas, y pueden ayudar a mitigar los riesgos informáticos en organizaciones de salud

Para Ouhbi, Fernández, Carrillo, Toval, y Idri (2017), menciona sobre la seguridad actual y futura de la información mediante el uso estándares que permitan que la información este protegida:

"Los programas de salud en línea actuales y futuros deberían tener en cuenta los aspectos de internacionalización. Este documento presenta una especificación de

requisitos de internacionalización en la forma de un catálogo de requisitos reutilizables, obtenido de los principales estándares relacionados, y describe los elementos metodológicos clave necesarios para realizar una auditoría de software de salud electrónica mediante el uso del conocimiento de internacionalización previamente reunido." (p. 47)

Según Box y Pottas, (2010) la seguridad de un sistema informático de la salud es un factor principal en el desarrollo de la atención al paciente.

"La confianza es un componente importante en la seguridad de un sistema de información. El advenimiento del registro electrónico de salud (EHR) y el sistema de información de salud (HIS) lo han elevado a una mayor prominencia. Estos sistemas y sus beneficios previstos se vuelven menos eficaces a través de un bajo nivel de confianza entre los interesados. Se investiga la posible relación recíproca entre responsabilidad y confianza. Un estudio de literatura examina ambos conceptos y su interrelación. Los controles de responsabilidad y auditoría proporcionados por la guía de seguridad NIST SP 800-53 y la norma de seguridad ISO 27799 se extraen, compilan y expanden para fortalecer los mecanismos de responsabilidad dentro de un programa de seguridad HIS. Se produce un conjunto dedicado de controles de responsabilidad (NIM) que es específico del entorno de atención médica. Se propone que a través del fortalecimiento de la función de rendición de cuentas del SIS, se puede mejorar su nivel de confiabilidad."(p.51)

Según Ledezma (2015) "Dentro de las instituciones se producen grandes cantidades de información y comunicación, las cuales son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional" (p.1), por lo tanto, éstas, deben cumplir con estándares de seguridad, que permitan la eficiencia, e integridad

de la información y que ésta no sea modificada, dañada o eliminada por parte de terceras personas que acceden a la misma. La seguridad debe ser preservada dando cumplimiento a las políticas de seguridad de la información, las cuales fueron establecidas para resguardar la misma.

Para Ganthan, Rabiah, y Zuraini, (2010) "Se intenta investigar los diversos tipos de amenazas que existen en los sistemas de información de salud (HIS). El estudio identificó 22 tipos de amenazas según las principales categorías de amenazas basadas en ISO / IEC 27002 (ISO 27799: 2008)." (p.21). Los resultados muestran que la amenaza más importante es la falla de energía seguida de actos de error o error humano y otros factores tecnológicos

Según Ramirez y Camargo (2017). "La seguridad se puede determinar cómo un proceso continuo, que debe ser vigilado, tratado y controlado. La norma ISO 27001, pretende establecer una metodología cuyo objetivo es preservar la confidencialidad, integridad y disponibilidad de la información" (p.21).

> Según Dussan (2006) "La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. La creación de políticas de seguridad es una labor fundamental que involucra las personas, los procesos y los recursos de la compañía. Este articulo presenta los puntos clave a tener en cuenta para diseñar una política de seguridad basándose en la norma ISO 27799" (p.25)

Orejuela (2015) afirma que en términos generales estas "políticas y normas de seguridad informática, propende por englobar los procedimientos más adecuados,

tomando como lineamientos principales los siguientes criterios: Seguridad Organizacional, Seguridad Lógica, Seguridad Física y Seguridad Legal" (p.14)

Para implementar una política de seguridad del Hospital Axxis, se toma como referencia la ISO/IEC 27799 que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La norma ISO 27799 determina un conjunto de controles específicos para la gestión de seguridad de la información aplicada a la industria sanitaria proporcionando directrices sobre las mejores prácticas.

1.2.2. Adopción de una perspectiva teórica

Los requerimientos de seguridad informática que necesita el Hospital Axxis, se alinean a los criterios de Kotsonis y Eliakis. Los desarrollos actuales en el campo del tratamiento integrado muestran la necesidad de enfoques de seguridad IS en el ámbito de la asistencia sanitaria. Los sistemas de información de salud están llamados a cumplir con demandas únicas para permanecer operativos frente a desastres naturales, fallas del sistema y ataques de denegación de servicio. Al mismo tiempo, los datos contenidos en los sistemas de información de salud son estrictamente confidenciales y, debido a las implicaciones éticas, judiciales y sociales en caso de pérdida de datos, los datos relacionados con la salud requieren un manejo extremadamente delicado. El objetivo es

proporcionar una visión general de los estándares de gestión de la seguridad de la información en el contexto de los sistemas de información de atención médica y centrarse en la familia de normas ISO / IEC 27000 más ampliamente aceptada para la gestión de la seguridad de la información. Al final, se proporcionará una guía para desarrollar un sistema de gestión de la seguridad de la información completo y sólido para una organización de atención médica, mencionando las implicaciones especiales que se cumplen en una organización de atención médica, así como consideraciones especiales relacionadas con la salud aplicaciones web.

Los cuales identifican al sector de la salud como un sistema vulnerable y poco atendido en medidas de seguridad y acogen la norma ISO27799 para mitigar las vulnerabilidades existentes dentro de hospitales, centros médicos o en cualquier dependencia médica.

1.2.3. Marco Conceptual

Política de Seguridad

"La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad." (García, 2009)

Seguridad de la información

"La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma." (García, 2009)

ISO 27799

La norma ISO 27799:2008 define las directrices que pueden apoyar la interpretación y la aplicación al sector sanitario de las ya conocidas ISO 27001 y 27002, puesto que especifica un conjunto detallado de controles para la gestión de la seguridad de la información específicas para el ámbito sanitario y nos proporciona una serie de claras directrices de seguridad sobre las mejores prácticas a seguir en los temas relacionados con la salud.

1.2.4. Hipótesis.

Mediante el diseño de una política de seguridad de la información basada en la norma ISO 27799, se podrá mejorar la confidencialidad integridad y disponibilidad de la información del Hospital Axxis.

CAPÍTULO II

2. MÉTODO

2.1. TIPO DE ESTUDIO

Exploratorios.

La presente investigación utiliza el tipo de estudio exploratorio con el objetivo de investigar adecuadamente los tipos de vulnerabilidades en el acceso a la red del Hospital Axxis para ello hemos realizado un análisis documental de la auditoría interna, el levantamiento de ACPM de la auditoría para la calificación ISO 9001 y las incidencias generadas por el Arcotel en cuanto a las vulnerabilidades de acceso a la red del Hospital. Adicional la entrevista a los integrantes del departamento de TI sobre la vulnerabilidad en las aplicaciones médicas del Hospital Axxis, seguido por una encuesta al personal administrativo del Hospital Axxis para determinar su percepción en base a la seguridad en el uso de aplicaciones médicas.

Descriptivos.

Mediante el diagrama de bloques se describe el proceso frente a un ingreso no permitido a las aplicaciones de médicas en la red del Hospital Axxis.

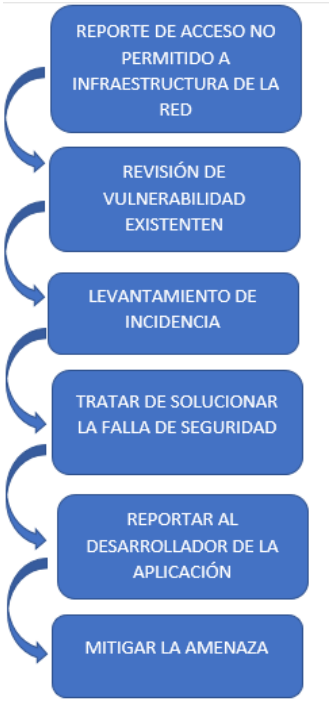


Figura 6 *Diagrama de bloque sobre el procedimiento en una incidencia de seguridad*
Fuente: *Elaboración propia*

Explicativos.

Para entender con más claridad los problemas de seguridad en las aplicaciones médicas del Hospital Axxis, en la entrevista realizada a la Gerente del departamento de TI se solicita que dé un alcance de sus respuestas indicando el porqué de estos problemas.

Según la Ing. María Palma los problemas de seguridad en las aplicaciones médicas son porque no se cuenta con procedimientos claros en la implementación de las aplicaciones, seguido de la falta de infraestructura para mitigar las posibles vulnerabilidades, estos factores hacen que los problemas de seguridad sean grandes.

2.2. MODALIDAD DE INVESTIGACIÓN

De campo.

Describe todos los hechos observados y se realiza en el sitio mismo donde se encuentra presente el problema, en nuestro caso el análisis de vulnerabilidades físicas se

lo realiza en las dependencias del Hospital Axxis, para constatar los vacíos de seguridad existentes.

Documental

Describe todas las incidencias reportadas en las auditorías internas de la ISO 9001, incidencias generadas por el ARCOTEL y documentos de incidencias reportadas por personal del Departamento de TI que permitan tener mayor información sobre los problemas de seguridad en el Hospital Axxis.

2.3. MÉTODO

Método Inductivo-Deductivo

Mediante este método buscamos la solución al problema por falta de confidencialidad, integridad y disponibilidad de la información, La política de seguridad es necesaria para prevenir posibles brechas de seguridad en consecuencia el Hospital Axxis requiere implementar una política de seguridad.

2.4. POBLACIÓN Y MUESTRA

Todo el personal humano que conforma el Hospital Axxis entre administrativos, médicos, pacientes se describe en la tabla 1.

Tabla 1 *Personal que conforma la muestra*

POBLACIÓN	PERSONAS	%
ADMINISTRATIVOS	75	19,74
MÉDICOS	305	80,26
TOTAL	**380**	**100**

Fuente: *Elaboración propia*

Se procede a calcular el tamaño de la muestra de una población de 380 elementos con un nivel de confianza del 95%

Datos:

Se tiene una población N=380, para el 95% de confianza Zα=1.64, se usará σ =0.5, y e=0.05.

Reemplazando valores en la fórmula se obtiene:

$$n = N\sigma^2 z_\sigma^2 \,/\, e^2(N-1) + \sigma^2 Z_\sigma^2$$

n= 380*0.5^2*1.64^2/0.05^2(380-1)+0.5^2*1.64^2

n= 157,73

Con la muestra de 158 personas escogemos entre el personal que trabaja en el Hospital Axxis, las incidencias de seguridad reportadas mediante la intranet del Hospital Axxis permite escoger la muestra como indica en la tabla 2.

Tabla 2 *Incidencias de seguridad reportadas en el Hospital Axxis*.

MUESTRA	PERSONAS	%
ADMINISTRATIVOS	31	19,62
MÉDICOS	127	80,38
TOTAL	**158**	**100,00**

Fuente: *Elaboración propia*

2.5. SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN.

- Mediante un banco de preguntas se realiza una entrevista al responsable del departamento de TI, Ing. María Fernanda Palma y a 2 analistas nivel 1, Ing. Juan Cumbicus y al Ing. Ricardo Arias del Hospital Axxis, los cuales son consultados acerca de las falencias de seguridad en la red del Hospital Axxis

- Se realiza una encuesta mediante un cuestionario de preguntas a 158 personas entre personal administrativo, médico del Hospital Axxis, para saber qué tan segura es la información que ellos proporcionan al Hospital Axxis.
- Mediante el análisis de incidencias documentadas en el departamento de TI, auditorías internas e ISO 9001 con las ACPMs, se puede obtener un análisis previo del estado actual del Hospital Axxis.

2.6. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS.

En la técnica de la entrevista realizada a los especialistas del departamento de TI del Hospital Axxis, se aplica el instrumento banco de preguntas. En primer lugar, se realiza un piloto con el personal de soporte técnico de TI para validar que las preguntas sean claras y concisas, luego estas preguntas son avaladas por un experto de la rama la Ing. Mónica Romero, se validan las preguntas y se las aplica la entrevista a los integrantes de TI.

En la técnica de encuesta realizada al personal administrativo y médico del Hospital Axxis, se aplica el instrumento cuestionario. En primer lugar, se realiza un piloto con el personal administrativo del Hospital para validar que el cuestionario sea claro y conciso, luego éste es avalado por un experto de la rama la Ing. Mónica Romero, se valida el cuestionario y se las aplica el cuestionario al personal administrativo, médico y pacientes.

En la técnica del análisis documental la auditoría interna al departamento de TI se valida mediante la calificación para ISO 9001 de gestión de calidad la cual levanta varias ACPMs para el departamento de TI, las incidencias reportadas por el Arcotel que es la Agencia de regulación y control de telecomunicaciones en Ecuador.

2.7. OPERACIONALIZACIÓN DE VARIABLES

Amenazas

Definición conceptual: Conjunto de vulnerabilidades que ponen en riesgo la información hasta la fecha de aplicación del estudio.

Dimensión: El número de incidencias registradas.

Indicador: Cálculo a partir del registro de eventos.

Instrumento: Encuesta.

Aplicaciones médicas

Definición conceptual: Total de aplicaciones médicas utilizadas en el Hospital.

Dimensión: Nivel de seguridad de las aplicaciones.

Indicador: Cálculo a partir del nivel de riesgos en la aplicación

Instrumento: Encuesta

Seguridad

Definición conceptual: Políticas de seguridad implementadas en hospital para precautelar la información.

Dimensión: El número de incidencias solucionadas.

Indicador: Cálculo a partir de las soluciones de vacíos de seguridad.

Instrumento: Encuesta.

Nivel de compromiso

Definición conceptual: Es el nivel de apoyo que se brinda a los sistemas de seguridad de la información.

Dimensión: Cumplimiento de procedimientos y controles de seguridad.

Indicador: Adquisición de herramientas para la seguridad de la información.

Instrumento: Encuesta.

2.8. PROCESAMIENTO DE DATOS.

2.8.1. Entrevista

Se realizan entrevistas al Gerente de TI Ing. María Palma y a los analistas de nivel 1 Juan Carlos Cumbicus y Ricardo Arias del Hospital Axxis, sobre el estado de la seguridad tanto física como lógica. (Anexo 2 entrevistas)

Análisis:

De acuerdo a las entrevistas realizadas a personal del Hospital Axxis, se ha podido notar que no existen medidas de seguridad de información aplicadas para el acceso a la red, las personas del departamento de TI requieren capacitación sobre temas de seguridad informática, esta deficiencia en seguridad ocasiona que la institución está expuesta a vulnerabilidades como:

- Información sin acceso restringido.
- No existen un control de implementación de aplicaciones
- Se puede realizar copias no autorizadas de historias clínicas
- No se controlan los periféricos de las computadoras

2.8.2. Encuesta

La encuesta se la realiza a 158 personas entre administrativos y médicos, nos dan un claro ejemplo que la mitad de los encuestados están inseguros sobre la seguridad de los documentos en las instalaciones del Hospital, la percepción de seguridad que da el departamento de TI es regular, no confían en la gestión de seguridad, la mitad de los encuestados sostuvo que tienen una contraseña débil y se siente expuestos a virus o malware.

CAPÍTULO III

3. RESULTADOS

3.1. SITUACIÓN ACTUAL

El Hospital Axxis incorpora a sus servicios de prestador de salud varias aplicaciones médicas que permiten brindar servicios de calidad a sus pacientes, mediante tecnología de punta tanto en Historias Clínicas, Área de imagen, laboratorio, y un sistema ERP de gestión administrativa. La topología de red con la que cuenta el Hospital Axxis actualmente es la siguiente:

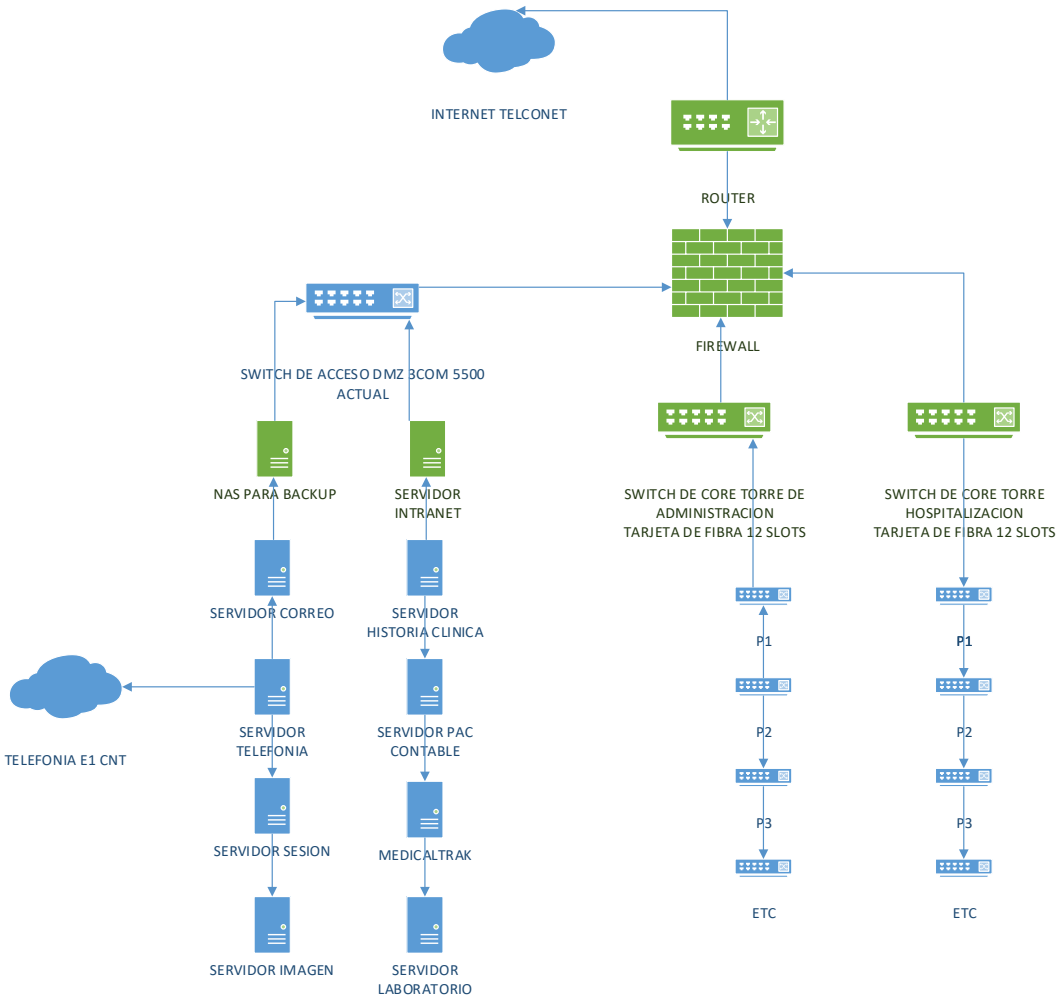


Figura 7 *Diagrama de la red actual del Hospital Axxis*

Fuente: *Elaboración propia*

- Granja de Servidores: Se alojan las aplicaciones médicas como el programa de historias clínicas EXMED, procesamiento de imágenes RISPAC, procesamiento laboratorio ENTERPRICE, gestión administrativa PAC, correo electrónico, Directorio Activo, intranet entre otros servicios.
- La entidad cuenta con Internet de 20 Mbps contratado con proveedor de servicios TELCONET, este se encuentra distribuido para todo el Hospital.
- En cuanto a la solución de seguridad perimetral está implementada con equipos Netgear el cual se tiene implementado en el Datacenter.
- En Hospital Axxis tiene control para los virus mediante la aplicación Kaspersky que provee el servicio la empresa de seguridad GMS, cuyo fin es la de proteger los equipos de usuarios finales de los posibles ataques a la seguridad de la información.
- Esta aplicación es administrada mediante la consola de gestión de Kaspersky la cual es administrada por el departamento de TI
- Las máquinas de los empleados, tiene direccionamiento IP estático y por DHCP las conexiones inalámbricas mientras que la telefonía está en otro segmento de red.
- Actualmente se realiza backups a la información en discos duros externos cada viernes de manera manual.
- No existe una documentación actualizada de la configuración de los equipos, tampoco una estandarización de configuración de estos.
- Aunque en la entidad se cuenta con personal calificado no hay políticas de seguridad establecidas, esto no se encuentra documentado.

3.1.1. Descripción técnica de equipos.

El Hospital Axxis está contemplada la instalación de estaciones diagnósticas de 2MP.

Figura 8 *Estación diagnóstica 2MP GenRad*

Fuente: *Elaboración propia*

Compuesta cada una por:

(1) CPU: Se puede ubicar sobre la mesa o en un soporte debajo de los monitores. Las dimensiones por CPU son

- Alto: 44,8 cm
- Ancho: 17,2 cm
- Profundo: 47,1 cm
- Peso: 20 Kg

(2) Monitores Diagnósticos Barco: Las dimensiones por Monitor son

- Alto: 70 cm
- Ancho: 37 cm
- Profundidad 30 cm
- Peso: 15 kg

(1) Monitor a Color: Las dimensiones por Monitor son

- Alto: 35 cm
- Ancho: 44 cm
- Profundidad 21 cm
- Peso: 8 kg

Conexión de red: Se requiere un punto de red (Giga-Ethernet).

Conexión eléctrica: Cada estación debe conectarse a una toma regulada (UPS Online) a 120 VAC, cada estación consume 700 W incluyendo monitor.

Condiciones Ambientales: Temperatura ambiente entre 10° C y 35 °C.

3.1.2. Descripción de servidores

Tabla 3 *Descripción de equipos del Hospital*

Nombre de la Aplicación	Modelo CPU	CPU [Ghz]	Ram [Gb]	Disco Duro	Sistema Operativo	Plataforma (hardware)	Plataforma a Reemplazar [si/no]
EXMED	Rack hp Intel Xeon	3,1 GHz	12Gb	2t	Linux 64 bits	HP x86_64	no
CORREOS	hp proliant ml 150g6	2 GHz	20Gb	1t	Centos Linux 10	HP x86_64	no
TELEFONÍA	Rack hp	2,1 GHz	4 Gb	1t	Asterisk Linux	HP x86_64	no
PAC	Rack hp	3,1 GHz	32Gb	4t	Centos Linux 6	HP x86_64	no
GESTOR DE PACIENTES	Intel Xeon Rack hp	1,6 GHz	32Gb	2t	W. server 2012	HP x86_64	no
RISPAC	Dell 815 4*8 Core	5 Ghz	32Gb	16 t	W. server 2012	Dell	no
RISPAC	Dell 815 4*8 Core	5 Ghz	32 Gb	16 t	W. server 2012	Dell	no
Almacenamiento Ris	VMAX EMC	EMC	EMC	50 t	EMC	EMC	no

Fuente: *Elaboración propia*

3.1.3. Descripción de aplicaciones médicas

3.1.3.1. Historia Clínica Electrónica

La historia clínica es el conjunto de documentos que contienen los datos, valoraciones e información de cualquier índole, sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial. Permite tener registrado los datos de

filiación del paciente, así como también la información médica durante la estadía del paciente en el Hospital.

3.1.3.2. Software de imagen

Almacenamiento de imágenes radiológicas en un servidor PACS usando el estándar DICOM (tanto a nivel de comunicaciones como de formato de las imágenes alojadas en los servidores PACS). Es un software que funciona sobre una computadora potente o servidor, y que almacena las imágenes médicas, para que desde estaciones de trabajo los médicos puedan dictar los informes con visores (web o móviles).

3.1.3.3. Software de laboratorio

El sistema de información de un laboratorio clínico permite tener agilidad en los procesos y centralización de la información en una sola localización bajo un ambiente cliente servidor o web.

- Órdenes de laboratorio.
- Resultados
- Informes y consultas.
- Estadística.
- Control de calidad.
- Tarifas y Facturación.
- Utilidades.
- Configuración.
- Consulta web
- Interfase HIS

3.1.3.4. Sistema de gestión de pacientes

Permite administrar la gestión de los pacientes, su rol principal es el ingreso del paciente, la asignación de una cama, y por último la liquidación del paciente durante su estadía en el Hospital.

3.1.4. Acceso a la información

El personal administrativo al interior de las instalaciones del Hospital Axis tiene acceso a la información que cada unidad autoriza, sin ningún mecanismo automatizado para controlar los niveles de acceso al personal ya sea médico o administrativo a las aplicaciones médicas, y está regulado por los procedimientos definidos por la dirección de planeación y de cada área. Se requiere implementar seguridades cuando personal renuncia o deja de trabajar en el Hospital, para impedir el acceso a información posterior a dejar sus funciones. Los proveedores o terceras personas solamente tienen privilegios durante el desarrollo o modificación de la aplicación, estos accesos deben ser aprobadas por el área respectiva departamento de sistemas y no por las unidades médicas.

3.1.5. Administración de cambios en hardware y software de la Red

Los cambios como son: creación, modificación de aplicativos, reportes, configuraciones, instalaciones, entre otros, los cuales puedan llegar afectar los recursos informáticos de la entidad, deben ser solicitados por los usuarios de la información y aprobado por el encargado de la administración de este, a nivel de jefe inmediato o quien haga sus veces, este tiene la responsabilidad de aceptar o rechazar la solicitud. Estas aprobaciones siempre se deben dar por el encargado de cada unidad médica.

Actualmente no se tienen creados ni implementados procesos en conjunto entre la oficina de planeación y el departamento de TI, los cuales en el momento de efectuar algún cambio se debe tener en cuenta los procedimientos establecidos en dichas áreas.

Todos los cambios realizados en las plataformas tecnológicas del Hospital Axxis, deben ser solicitados por la mesa de servicios y justificación de estos. Esto con el fin de realizar seguimiento desde la solicitud hasta la implementación y garantizar el cumplimiento del procedimiento establecido.

3.1.6. Seguridad de la Información

Tanto personal administrativo y médico del Hospital son responsables de la información que manejen y deben protegerla, para evitar pérdidas, accesos no autorizados, exposición y uso indebido de ésta.

Toda la información del Hospital, no puede ser vendida, transferida o intercambiada con terceras personas bajo ningún pretexto o propósito.

Los datos o la información son considerados como uno de los activos más importantes y sensibles de la entidad, por esto se debe garantizar la protección de esta, y su uso será solamente de acuerdo a las necesidades y propósitos de la entidad.

3.1.7. Seguridad física

El Hospital Axxis cuenta con un DataCenter con acceso restringido, el cual requiere implementar un control de acceso por medio de autenticación biométrica y uso de tarjetas inteligentes. El centro de cómputo cuenta con elementos de control de incendios, y aire acondicionado para mantener los equipos bajo los requerimientos de temperatura del fabricante. Las personas ajenas que no tengan relación con la entidad, no pueden acceder a los recursos informáticos de esta.

3.1.8. Identificación de las amenazas y riesgos

Para identificar los riesgos que pueden afectar al acceso a las aplicaciones médicas, se consideran los eventos que afecten directamente a la integridad,

disponibilidad y confidencialidad de la información en base a las recomendaciones de la ISO 27799 como los son:

- **Suplantación interna:** La suplantación interna consiste en el uso del sistema por aquellos que utilizan cuentas que no son suyas.
- **Suplantación mediante proveedores de servicio:** La suplantación mediante proveedores de servicio consiste en que el personal contratado utiliza sus accesos privilegiados a los sistemas para obtener acceso no autorizado a los datos.
- **Suplantación por externos:** La suplantación por externos tiene lugar cuando terceros no autorizados obtienen acceso a los recursos o datos del sistema, bien haciéndose pasar por un usuario autorizado o convirtiéndose de forma fraudulenta en un usuario autorizado.
- **Uso no autorizado de una aplicación de informática sanitaria:** Puede ser sorprendentemente fácil conseguir acceder a una aplicación de informática sanitaria. Los usuarios autorizados también pueden realizar acciones no autorizadas tales como alteraciones malintencionadas de los datos.
- **Introducción de software dañino o perjudicial:** Los virus informáticos están implicados en la mayoría de incidentes de seguridad en TI. La introducción de software dañino o perjudicial constituye un fallo en la protección anti-virus o en el control de cambios de software.
- **Uso indebido de los recursos del sistema:** Esta amenaza incluye a los usuarios que utilizan los sistemas y servicios de información sanitaria para su trabajo personal, a los usuarios que bajan información no relacionada con su trabajo desde Internet hacia ordenadores dedicados exclusivamente a dar soporte a los sistemas de información sanitaria, a los usuarios que crean bases de datos u otras aplicaciones para materias no

relacionadas con su trabajo, o a los usuarios que degradan la disponibilidad del sistema de información sanitaria.

- **Infiltración en las comunicaciones:** La infiltración en las comunicaciones electrónicas tienen lugar cuando un individuo manipula indebidamente el flujo normal de los datos a lo largo de la red.
- **Intercepción de las comunicaciones:** Si no se encuentra encriptada durante la transmisión, la confiabilidad de la información contenida en un mensaje puede anularse mediante la intercepción de la comunicación.
- **Repudio:** Esta amenaza incluye a los usuarios que niegan que han enviado un mensaje y a los usuarios que niegan que han recibido un mensaje.
- **Fallo en la conexión:** Todas las redes están sujetas a apagones periódicos del servicio. La calidad del servicio es un factor importante en la provisión de servicios de red en sanidad**.** El fallo en la conexión también puede deberse a una dirección indebida de los servicios de red. Los fallos en las conexiones pueden facilitar la revelación de información confidencial al forzar a los usuarios a enviar mensajes por mecanismos menos seguros.
- **Código malicioso empotrado:** Esta amenaza incluye virus de correo electrónico y descargas hostiles. Aunque de ninguna manera sean exclusivos de los sistemas de información sanitaria. El código malicioso empotrado constituye un fallo en la aplicación de controles de software antivirus o en la prevención efectiva de las intrusiones
- **Asignación de ruta indebida accidental:** Esta amenaza incluye la posibilidad de que la información pudiera entregarse a un destino incorrecto cuando se envía en una red. La asignación de ruta indebida accidental podría constituir un fallo en la formación del

usuario o un fallo en el mantenimiento de la integridad de los directorios de los proveedores sanitarios.

- **Fallo técnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red:** Estas amenazas incluyen los fallos de hardware, los fallos de red o fallos en los equipos de almacenamiento de datos. Estos fallos constituyen típicamente un fallo de uno o más de los controles de gestión de operaciones.
- **Fallos de entorno de soporte:** Los sistemas de información sanitaria pueden ser críticos durante los desastres naturales y otros eventos que pueden constituir amenazas para la vida de un gran número de personas.
- **Fallo en el software de sistemas o en el software de red:** Los ataques de denegación del servicio se facilitan enormemente por las debilidades en él, o la mala configuración del software de sistema operativo o del software del sistema operativo de red. El fallo del software de sistemas o de red constituye un fallo en la comprobación de la integridad del software, en la prueba del sistema o en los controles de mantenimiento del software.
- **Fallo en las aplicaciones de software:** Los fallos en las aplicaciones de software pueden ser explotados en un ataque de denegación del servicio y también pueden utilizarse para comprometer la confidencialidad de los datos protegidos. Los fallos en las aplicaciones de software constituyen un fallo en la prueba del software, en el control de cambios o en la comprobación de la integridad del software.
- **Error del operador:** Los errores del operador suman un pequeño pero significativo porcentaje de revelaciones no intencionadas y una gran proporción de disposiciones de datos no intencionados. El error del operador constituye un fallo de control de operaciones, seguridad del personal, recuperación de desastres.

- **Errores de mantenimiento:** Los errores de mantenimiento se pueden cometer por personal, así como empleados de terceros contratados para realizar tareas de mantenimiento.
- **Error de usuario:** Los errores de los usuarios pueden darse con la divulgación de información confidencial accidentalmente
- **Escasez de personal:** La amenaza de la escasez de personal incluye la posibilidad de la ausencia de personal clave y la dificultad de su reemplazo.
- **Robo por internos:** Los internos típicamente tienen acceso mayor a la información confidencial que los externos.
- **Robo por externos:** El robo por externos de dato y equipamiento es un problema grave en algunos hospitales. El robo puede tener como resultado brechas de confidencialidad.
- **Daño premeditado por internos:** El daño premeditado por internos incluye los actos de vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta.
- **Daño premeditado por externos:** La amenaza de daño premeditado por externos incluye los actos de vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno.
- **Terrorismo:** La amenaza de terrorismo incluye actos extremistas que buscan el daño o la alteración del trabajo de las organizaciones sanitarias.
- **Desastres naturales:** Eventos catastróficos que pueden comprometer la infraestructura física del medio donde funciona las aplicaciones médicas.
- **Alteraciones del entorno:** Los cambios bruscos de temperatura o las condiciones de humedad por ende puede causar problemas a las aplicaciones médicas.

- **Accesos físicos:** Son aquellas incidencias cuando personal no autorizado accede físicamente a las aplicaciones médicas.
- **Fallas en Hardware:** Incidencia suscitada por diferentes razones el hardware falla (falla en disco por agotamiento, memoria, BIOS, etc.)
- **Virus:** Perdida, captura o daños de las aplicaciones médicas por gusanos maliciosos o malware que no son detectados por los antivirus.
- **Corrupción lógica:** Actualizaciones de sistemas operativos que generan daños en el hardware o software de los equipos donde funciona las aplicaciones médicas.

3.1.8.1. Análisis de los riesgos

Para el análisis de los riesgos se toma como referencia los puntos expuestos anteriormente en el numeral 3.1.8, la probabilidad de ocurrencia y el impacto del riesgo son ponderados por la Gerente Administrativa, la Gerente de Sistemas del Hospital Axxis y el jefe del área médica se realiza un cuadro integral del análisis y valoración de los riesgos, como se muestra a continuación en la tabla 4:

Tabla 4 *Riesgos que afectan al Hospital Axxis.*

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)
RMS1	Suplantación interna	HOSPITAL	Alto	3,7	5,0	VOTO IMPACTO	5,0	5,0	5,0
						VOTO VULNERABILIDAD	2,0	4,0	5,0
RMS2	Suplantación mediante proveedores de servicio	HOSPITAL	Medio	2,3	2,5	VOTO IMPACTO	3,0	3,5	1,0
						VOTO VULNERABILIDAD	3,0	3,0	1,0
RMS3	Suplantación por externos	HOSPITAL	Alto	4,0	4,3	VOTO IMPACTO	5,0	4,0	4,0
						VOTO VULNERABILIDAD	4,0	4,0	4,0
RMS4	Uso no autorizado de una aplicación de informática sanitaria	HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	5,0	4,0	4,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0

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)
RMS5	Introducción de software dañino o perjudicial	HOSPITAL	Medio	4,3	3,3	VOTO IMPACTO	3,0	4,0	3,0
						VOTO VULNERABILIDAD	5,0	5,0	3,0
RMS6	Uso indebido de los recursos del sistema	HOSPITAL	Bajo	2,0	1,7	VOTO IMPACTO	2,0	1,0	2,0
						VOTO VULNERABILIDAD	3,0	1,0	2,0
RMS7	Infiltración en las comunicaciones	HOSPITAL	Medio	3,3	3,3	VOTO IMPACTO	3,0	4,0	3,0
						VOTO VULNERABILIDAD	2,0	4,0	4,0
RMS8	Intercepción de las comunicaciones	HOSPITAL	Medio	3,0	3,0	VOTO IMPACTO	4,0	3,0	2,0
						VOTO VULNERABILIDAD	4,0	4,0	1,0
RMS9	Repudio	HOSPITAL	Bajo	1,7	1,3	VOTO IMPACTO	1,0	1,0	2,0
						VOTO VULNERABILIDAD	2,0	1,0	2,0
RMS10	Fallo en la conexión	HOSPITAL	Medio	2,0	3,3	VOTO IMPACTO	4,0	3,0	3,0
						VOTO VULNERABILIDAD	1,0	3,0	2,0
RMS11	Código malicioso empotrado	HOSPITAL	Medio	3,3	4,3	VOTO IMPACTO	4,0	4,0	5,0
						VOTO VULNERABILIDAD	3,0	5,0	2,0
RMS12	Asignación de ruta indebida accidental	HOSPITAL	Bajo	1,3	2,3	VOTO IMPACTO	2,0	3,0	2,0
						VOTO VULNERABILIDAD	2,0	1,0	1,0

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)
RMS13	Fallo técnico del equipo, de los dispositivos de almacenamiento o de red	HOSPITAL	Medio	2,3	2,7	VOTO IMPACTO	3,0	2,0	3,0
						VOTO VULNERABILIDAD	3,0	2,0	2,0
RMS14	Fallos de entorno de soporte	HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	5,0	4,0	4,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0
RMS15	Fallo en el software de sistemas o en el software de red	HOSPITAL	Medio	3,3	3,7	VOTO IMPACTO	4,0	4,0	3,0
						VOTO VULNERABILIDAD	3,0	4,0	3,0
RMS16	Fallo en las aplicaciones de software	HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	5,0	4,0	4,0
						VOTO VULNERABILIDAD	4,0	3,0	4,0
RMS17	Error del operador	HOSPITAL	Bajo	2,0	1,7	VOTO IMPACTO	2,0	2,0	1,0
						VOTO VULNERABILIDAD	3,0	1,0	2,0
RMS18	Errores de mantenimiento	HOSPITAL	Alto	3,7	4,7	VOTO IMPACTO	5,0	5,0	4,0
						VOTO VULNERABILIDAD	4,0	4,0	3,0
RMS19	Error de usuario	HOSPITAL	Bajo	1,7	2,0	VOTO IMPACTO	2,0	3,0	1,0
						VOTO VULNERABILIDAD	1,0	2,0	2,0

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)
RMS20	Escasez de personal	HOSPITAL	Bajo	1,3	1,7	VOTO IMPACTO	2,0	1,0	2,0
						VOTO VULNERABILIDAD	1,0	1,0	2,0
RMS21	Robo por internos	HOSPITAL	Medio	2,3	3,3	VOTO IMPACTO	3,0	3,0	4,0
						VOTO VULNERABILIDAD	1,0	3,0	3,0
RMS22	Robo por externos	HOSPITAL	Medio	3,0	2,3	VOTO IMPACTO	2,0	3,0	2,0
						VOTO VULNERABILIDAD	3,0	4,0	2,0
RMS23	Daño premeditado por internos	HOSPITAL	Bajo	1,7	1,7	VOTO IMPACTO	2,0	1,0	2,0
						VOTO VULNERABILIDAD	1,0	1,0	3,0
RMS24	Daño premeditado por externos	HOSPITAL	Bajo	2,0	2,0	VOTO IMPACTO	2,0	1,0	3,0
						VOTO VULNERABILIDAD	2,0	3,0	1,0
RMS25	Terrorismo	HOSPITAL	Medio	2,3	2,7	VOTO IMPACTO	3,0	2,0	3,0
						VOTO VULNERABILIDAD	3,0	3,0	1,0
RMS26	Alteraciones del entorno	HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	4,0	5,0	4,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0
RMS27	Accesos físicos no autorizados a las aplicaciones médicas	HOSPITAL	Alto	4,0	4,0	VOTO IMPACTO	4,0	4,0	4,0
						VOTO VULNERABILIDAD	5,0	3,0	4,0

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)
RMS28	Fallas en Hardware	HOSPITAL	Medio	3,0	3,0	VOTO IMPACTO	3,0	3,0	3,0
						VOTO VULNERABILIDAD	3,0	4,0	2,0
RMS29	Virus	HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	4,0	4,0	5,0
						VOTO VULNERABILIDAD	4,0	3,0	4,0
RMS30	Corrupción lógica	HOSPITAL	Medio	2,0	2,3	VOTO IMPACTO	4,0	1,0	2,0
						VOTO VULNERABILIDAD	3,0	2,0	1,0
RMS31	Vulnerabilidades en los sistemas de seguridad:	HOSPITAL	Alto	4,3	4,0	VOTO IMPACTO	4,0	4,0	4,0
						VOTO VULNERABILIDAD	4,0	4,0	5,0
RMS32	Fugas de información	HOSPITAL	Alto	3,7	4,3	VOTO IMPACTO	4,0	4,0	5,0
						VOTO VULNERABILIDAD	3,0	4,0	4,0

Fuente: *Elaboración propia*

3.1.8.2. Matriz de riesgos

Se obtiene la matriz de riesgos en la cual se observa que los riegos ligados al acceso de aplicaciones médicas están en zona roja por suplantación interna, suplantación externa, uso de aplicaciones sin autorización, software malicioso, mediante la política de seguridad se podrá tratar estos riesgos para mantenerlos controlados y que no sean una amenaza para la institución.

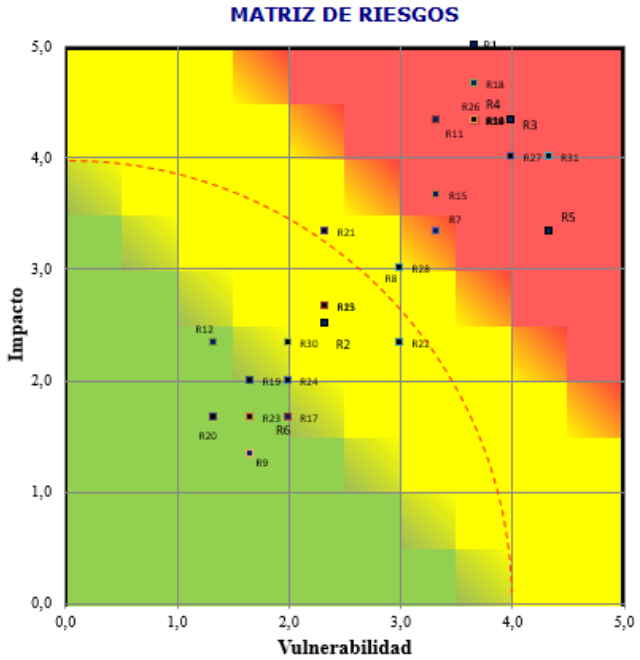


Figura 9 *Matriz de Riesgos Hospital Axxis*

Fuente: *Elaboración propia*

Tabla 5 *Riesgos detectados según la Norma ISO 27799*

Identificación del riesgo		Tratamiento del riesgo					
Amenaza	**Riesgo**	**Concepto de seguridad**	**Análisis**		**Nivel del riesgo**	**Acciones a tomar**	**Recomendaciones**
		Informática afectada	**Probabilidad de ocurrencia**	**Impacto del riesgo**			
Suplantación interna	Acceso a las aplicaciones médicas utilizando cuentas validas existentes de otros usuarios	Integridad	Probable	Mayor	(A) Riesgo Alto	Diseñar un control de acceso efectivo	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Suplantación mediante proveedores de servicio	Personal contratado utiliza sus accesos privilegiados a los sistemas para obtener acceso no autorizado a los datos	Integridad Confidencialidad	Probable	Menor	(M) Riesgo Medio	Restringir el uso de usuarios con privilegios	Implementar políticas de seguridad
Suplantación por externos	Terceros no autorizados obtienen acceso a los recursos o datos del sistema	Integridad Confidencialidad	Probable	Mayor	(A) Riesgo Alto	Implementar equipos perimetrales de seguridad	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Uso no autorizado de una aplicación de informática sanitaria	Los usuarios autorizados pueden realizar acciones no autorizadas tales como alteraciones malintencionadas de los datos	Integridad Confidencialidad	Probable	Mayor	(A) Riesgo Alto	Implementar políticas de cambios	Implementar políticas de seguridad
Introducción de software dañino o perjudicial	La introducción de software dañino o perjudicial constituye un fallo en la protección anti-virus o en el control de cambios de software	Integridad	Probable	Moderado	(M) Riesgo Medio	Actualizar software y realizar campañas de concientización	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Uso indebido de los recursos del sistema	Los usuarios que utilizan los sistemas y servicios de información sanitaria para su trabajo personal y degradan los servicios de la red	Disponibilidad	Improbable	Menor	(B) Riesgo Bajo	Realizar una correcta segregación de tareas	Implementar políticas de seguridad
Infiltración en las comunicaciones	Datos se pueden manipular indebidamente el flujo normal de los datos a lo largo de la red	Integridad	Improbable	Moderado	(M) Riesgo Medio	Implementar equipos perimetrales de seguridad	Implementar políticas de seguridad
Intercepción de las comunicaciones	Paquetes de datos pueden anularse mediante la intercepción de la comunicación	Confidencialidad	Improbable	Moderado	(M) Riesgo Medio	Implementar equipos perimetrales de seguridad	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Repudio	Usuarios niegan que han enviado un mensaje o los usuarios que niegan que han recibido un mensaje	Confidencialidad	Improbable	Menor	(B) Riesgo Bajo	Supervisión de tareas	Implementar políticas de seguridad
Fallo en la conexión	Perdida de conectividad	Disponibilidad	Probable	Moderado	(M) Riesgo Medio	Plan de contingencia	Implementar políticas de seguridad
Código malicioso empotrado	Perdida de información y funcionalidad de las aplicaciones médicas	Confidencialidad Integridad	Probable	Moderado	(M) Riesgo Medio	Capacitación constante sobre riesgos de código malicioso	Implementar políticas de seguridad
Asignación de ruta indebida accidental	La información pudiera entregarse a un destino incorrecto cuando se envía en una red	Confidencialidad	Improbable	Menor	(B) Riesgo Bajo	Documentación de cambios de software	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Fallo técnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red	Fallos de hardware, los fallos de red o fallos en los equipos de almacenamiento de datos.	Disponibilidad	Improbable	Moderado	(M) Riesgo Medio	Plan de contingencia	Implementar políticas de seguridad
Fallos de entorno de soporte	Daños en los sistemas que soportan las aplicaciones médicas	Disponibilidad	Probable	Mayor	(A) Riesgo Alto	Plan de contingencia	Implementar políticas de seguridad
Fallo en el software de sistemas o en el software de red	Perdida de información y funcionalidad de las aplicaciones médicas	Disponibilidad	Probable	Moderado	(M) Riesgo Medio	Plan de contingencia	Implementar políticas de seguridad
Fallo en las aplicaciones de software	Comprometer la confidencialidad de los datos clínicos protegidos	Confidencialidad	Probable	Mayor	(A) Riesgo Alto	Plan de contingencia	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Error del operador	Revelación de información médica no intencionadas por parte de TI	Confidencialidad	Probable	Menor	(B) Riesgo Bajo	Documentación de cambios de software	Implementar políticas de seguridad
Errores de mantenimiento	Perdida de información y funcionalidad de las aplicaciones médicas	Integridad	Probable	Mayor	(A) Riesgo Alto	Implementar plan de procedimientos técnicos	Implementar políticas de seguridad
		Confidencialidad					Implementar políticas de seguridad
Error de usuario	Divulgación de información confidencial accidentalmente	Confidencialidad	Probable	Menor	(B) Riesgo Bajo	Implementar plan de procedimientos técnicos	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Escasez de personal	Ausencia de personal clave y la dificultad de su reemplazo	Integridad	Improbable	Menor	(B) Riesgo Bajo	Manual de funciones	Implementar políticas de seguridad
Robo por internos	Divulgación de información confidencial	Confidencialidad	Probable	Moderado	(M) Riesgo Medio	Política de seguridad	Implementar políticas de seguridad
Robo por externos:	Divulgación de información confidencial	Confidencialidad	Probable	Moderado	(M) Riesgo Medio	Política de seguridad	Implementar políticas de seguridad
Daño premeditado por internos	Vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta	Integridad	Improbable	Menor	(B) Riesgo Bajo	Política de seguridad	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Daño premeditado por externos	Vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta	Integridad	Improbable	Menor	(B) Riesgo Bajo	Política de seguridad	Implementar políticas de seguridad
Terrorismo	Alteración del trabajo del Hospital	Disponibilidad	Improbable	Moderado	(M) Riesgo Medio	Plan de contingencia	Implementar políticas de seguridad
Alteraciones del entorno	Daños en los sistemas que soportan las aplicaciones médicas	Disponibilidad	Posible	Mayor	(A) Riesgo Alto	El Departamento de TI debe tener un plan de contingencia para tomar acciones y poder eliminar, mitigar, reducir o trasferir el riesgo.	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Accesos físicos no autorizados a las aplicaciones médicas	Modificación o daños en las aplicaciones médicas	Disponibilidad	Posible	Mayor	(A) Riesgo Alto	El Departamento de TI debe implementar mecanismos de autenticación	Implementar políticas de seguridad
Fallas en Hardware	Perdida de disponibilidad de la información y posible pérdida de información	Disponibilidad	Posible	Moderado	(M) Riesgo Medio	El Hospital debe invertir recursos para tener equipamiento redundante	Implementar políticas de seguridad
Virus	Perdida de información y funcionalidad de las aplicaciones médicas	Disponibilidad Integridad	Probable	Moderado	(A) Riesgo Alto	Departamento de TI debe integrar un procedimiento para la revisión de amenazas	Implementar políticas de seguridad

Identificación del riesgo		Tratamiento del riesgo					
Corrupción lógica	Daños en la información y los registros almacenados	Integridad	Improbable	Moderado	(M) Riesgo Medio	Departamento de TI debe exigir a los proveedores externos la estabilidad de las actualizaciones	Implementar políticas de seguridad
Vulnerabilidades en los sistemas de seguridad:	Accesos no autorizados de persona mal intencionado para modificar o robar información	Integridad Confidencialidad	Posible	Moderado	(A) Riesgo Alto	Departamento de TI debe realizar Hacking Ético a sus instalaciones	Implementar políticas de seguridad
Fugas de información	Información confidencial utilizada para usos mal intencionados	Confidencialidad	Improbable	Moderado	(A) Riesgo Alto	Departamento de TI debe implementar seguridades en periféricos para evitar robo de Historias Clínicas	Implementar políticas de seguridad

Fuente: *Elaboración propia*

3.2. MARCO REGULATORIO

3.2.1. Análisis mediante la Pirámide de Kelsen del sector sanitario en Ecuador

Figura 10 *Descripción de la pirámide de Kelsen sobre la legislatura sanitaria en Ecuador*

Fuente: *Elaboración propia*

3.2.2. Constitución de la República del Ecuador

Es la ley fundamental de un Estado, con rango superior al resto de las leyes, que define el régimen de los derechos y libertades de los ciudadanos y delimita los poderes e instituciones de la organización política

Que, la Constitución de la República del Ecuador, en el artículo 3, numeral 1, atribuye como deber primordial del Estado garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en ella y en los instrumentos internacionales, en particular la salud;

Que, la citada Constitución de la República del Ecuador, en el artículo 32, dispone que: "La salud es un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos, entre ellos el derecho al agua, la alimentación, la educación, la cultura física, el trabajo, la seguridad social, los ambientes sanos y otros que sustentan el buen vivir. El Estado garantizará este derecho mediante políticas económicas, sociales, culturales, educativas y ambientales; y el acceso permanente, oportuno y sin exclusión a programas, acciones y servicios de promoción y atención integral de salud, salud sexual y salud reproductiva. La prestación de los servicios de salud se regirá por los principios de equidad, universalidad, solidaridad, interculturalidad, calidad, eficiencia, eficacia, precaución y bioética, con enfoque de género y generacional."

3.2.3. Norma Suprema del Ecuador

Establece el origen de la soberanía en la nación o el pueblo (soberanía nacional, soberanía popular), reconoce los derechos fundamentales (o derechos constitucionales) y los mecanismos de participación y representación política, establece la forma de Estado.

Que, la Norma Suprema, en el artículo 361, ordena al Estado ejercer la rectoría del Sistema Nacional de Salud a través de la Autoridad Sanitaria Nacional, instancia a quien corresponde la responsabilidad de formular la política nacional de salud y de normar, regular y controlar todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector.

3.2.4. Carta Magna

Carta Magna es el título que se le da al documento que representa todos los derechos y deberes que una sociedad constituida como nación debe gozar y cumplir respectivamente. La etimología del término nos lleva a la época de la monarquía cuando el Rey Juan I de Inglaterra se vio obligado a realizar un ordenamiento jurídico

prácticamente a solicitud del pueblo, en vista de todas las problemáticas que se suscitaban en la sociedad.

Que, la Carta Magna, en el artículo 362, manda: "La atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las medicinas ancestrales alternativas y complementarias. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes (…)";

3.2.5. Ley Orgánica de Salud

Que, la Ley Orgánica de Salud, en el artículo 4, prescribe que la Autoridad Sanitaria Nacional es el Ministerio de Salud Pública, entidad a la que corresponde el ejercicio de las funciones de rectoría en salud; así como la responsabilidad de la aplicación, control y vigilancia del cumplimiento de dicha Ley; siendo las normas que dicte para su plena vigencia obligatorias;

Que, la citada Ley Orgánica de Salud, en el artículo 6, determina entre las responsabilidades del Ministerio de Salud Pública: "(…) 5. Regular y vigilar la aplicación de las normas técnicas para la detección, prevención, atención integral y rehabilitación, de enfermedades transmisibles, no transmisibles, crónico-degenerativas, discapacidades y problemas de salud pública declarados prioritarios, y determinar las enfermedades transmisibles de notificación obligatoria, garantizando la confidencialidad de la información; (…) 34. Cumplir y hacer cumplir esta Ley, los reglamentos y otras disposiciones legales y técnicas relacionadas con la salud; (…).";

3.2.6. Código Orgánico Integral Penal

Que, el Código Orgánico Integral Penal, en el artículo 179, dispone: "Revelación de secreto. - La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.";

3.2.7. Ley Ibidem

Que, la Ley Ibidem, en el artículo 7, establece como derecho de todas las personas en relación a la salud, sin discriminación por motivo alguno: "Tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida (…)";

3.2.8. Ley de Derechos y Amparo al Paciente

Que, Ley de Derechos y Amparo al Paciente, en el artículo 4, dispone: "Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial";

3.2.9. Acuerdo Ministerial

Que, mediante Acuerdo Ministerial No. 00005213 expedido el 24 de diciembre de 2014 se subrogaron las funciones del Despacho Ministerial a favor del doctor David Acurio Páez, Viceministro de Gobernanza y Vigilancia de la Salud desde el 29 de diciembre de 2014 hasta el 4 de enero de 2015; y,

Que, mediante memorando No. MSP-DNN-2014-1391-M de 12 de noviembre de 2014, la Directora Nacional de Normalización solicita emitir el presente Acuerdo Ministerial.

En ejercicio de las atribuciones conferidas por los artículos 151 y 154 de la Constitución de la República del Ecuador, y 17 del Estatuto de Régimen Jurídico Administrativo de la Función Ejecutiva.

3.3. ELECCIÓN DE LOS CONTROLES DE LA NORMA ISO 27799

Según el acuerdo Ministerial No. 00005213. Las organizaciones que procesan información sanitaria que incluya datos personales sanitarios, deberán tener una política de seguridad de la información escrita, aprobada por la dirección, publicada, y a continuación comunicada a todos los empleados y partes externas relevantes.

Para ello los controles de la norma ISO27799 elegidos para brindar seguridad hacia el acceso a las aplicaciones médicas se seleccionan desde el punto de vista de (Sánchez et al., 2014) en la cual recomiendan buenas prácticas para el uso de aplicaciones médicas.

Tabla 6 *Controles seleccionados de la Norma ISO 27799*

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.3.2	**ORGANIZACIÓN INTERNA**	
7.3.2.3	Acuerdos de confidencialidad	Las organizaciones que traten datos personales sanitarios deberán tener un acuerdo de confidencialidad en vigor que especifique la naturaleza confidencial de esta información. El acuerdo deberá ser aplicable a todo el personal que accede a la información.
7.3.3	**TERCEROS**	

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.3.3.1	Identificación de los riesgos relativos a las partes externas	Las organizaciones que traten información sanitaria deberán evaluar los riesgos asociados con el acceso por partes externas a estos sistemas o a los datos que contienen, y a continuación implementar los controles de seguridad que sean apropiados para el nivel de riesgo identificado y las tecnologías empleadas
7.3.3.2	Tratamiento de la seguridad en la relación con los clientes	
7.3.3.3	Tratamiento de la seguridad en contratos con terceros	La naturaleza y valor confidencial de los datos personales sanitarios
		Las medidas de seguridad a implementar y/o cumplir
		Los límites de los terceros para acceder a esos servicios
		Los niveles de servicio a alcanzar en los servicios proporcionados
		El formato y la frecuencia de la notificación al ISMF de la organización de salud
		La disposición para la representación de la tercera parte en las reuniones y grupos de trabajos de la organización de salud
		Las disposiciones para las auditorías de conformidad de los terceros
		Las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.4	**GESTIÓN DE ACTIVOS**	
7.4.1	Responsabilidad para los activos de información sanitaria	Controlar los activos de información sanitaria (es decir mantener un inventario de tales activos)
		Tener designado un custodio de esos activos de información
		Tener reglas para el uso aceptable de estos activos que estén identificadas, documentadas e implementadas
7.4.2	**CLASIFICACIÓN DE INFORMACIÓN SANITARIA**	
7.4.2.1	Directrices de Clasificación	Las organizaciones que traten datos personales sanitarios deberían clasificar uniformemente tales datos como confidenciales.
7.4.2.2	Etiquetado y manejo de la información	Todos los sistemas de información sanitarios que traten datos personales sanitarios deberían informar a los usuarios de la confidencialidad de los datos personales sanitarios accesibles desde el sistema (por ejemplo, en el arranque o inicio de sesión) y deberían etiquetar las salidas impresas como confidenciales cuando contengan datos personales sanitarios
7.5	**SEGURIDAD EN RECURSOS HUMANOS**	
7.5.1	**PREVIO AL EMPLEO**	
7.5.1.1	Roles y responsabilidades	Es necesario prestar una atención especial a los roles y responsabilidades del personal temporal

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.5.1.2	Selección	Todas las organizaciones cuyo personal, contratistas o voluntarios traten (o se espera que traten) datos personales sanitarios deberían, como mínima, verificar la identidad, domicilio actual y empleos anteriores de dicho personal, contratistas y voluntarios en el momento de las solicitudes de trabajo.
7.5.1.3	Términos y condiciones de empleo	Todas las organizaciones que traten datos personales sanitarios deberían incluir en los términos y condiciones de contratación de los empleados que procesan, o procesarán, datos personales sanitarios una declaración sobre las responsabilidades del empleado en seguridad de la información.
7.5.2	**DURANTE EL EMPLEO**	
7.5.2.1	Responsabilidades de gestión	Es importante destacar el énfasis especial que es necesario poner sobre las preocupaciones de los sujetos de la asistencia que no desean que accedan a sus datos personales sanitarios aquellos trabajadores sanitarios que sean vecinos, compañeros o familiares. Tales inquietudes a menudo esconden un alto porcentaje de reclamaciones de aquellos con temor sobre la confidencialidad de sus datos personales sanitarios.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.5.2.2	Concienciación, formación y capacitación en seguridad de la información	Todas las organizaciones que traten datos personales sanitarios deberán asegurar que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios que tratan datos personales sanitarios.
7.5.2.3	Proceso disciplinario	Los procesos disciplinarios en las organizaciones sanitarias con respecto a las brechas de seguridad de la información deberían seguir procedimientos que están reflejados en las políticas y sean por tanto conocidos por log sujetos objeto del proceso disciplinario. Además de cumplir con las leyes aplicables, tales procesos deberían cumplir con los acuerdos alcanzados entre los profesionales sanitarios y los organismos de los profesionales sanitarios.
7.5.3	**FINALIZACIÓN O CAMBIO DE EMPLEO**	

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.5.3.1	Finalización de responsabilidades y devolución de activos	Es importante resaltar que, en sanidad, muchos tipos de personal, por ejemplo, los médicos y las enfermeras, habitualmente progresan a través de programas de formación y otras "rotaciones" en los que sus derechos de acceso pueden cambiar sustancialmente. Para asegurar la finalización de los derechos anteriores que ya no son necesarios para su rol, tales cambios de empleo deberían ser inicialmente tratados de la misma forma que en aquellos individuos que abandonan el empleo en la organización.
7.5.3.2	Eliminación de derechos de acceso	Todas las organizaciones que tratan datos personales sanitarios deberán, tan pronto como sea posible, rescindir los privilegios de acceso de los usuarios con respecto a tal información de cualquier empleado que se vaya de forma temporal o permanece, contratista tercero o voluntario hasta la finalización del empleo, el contrato o las actividades de voluntariado.
7.6	**SEGURIDAD FÍSICA Y DEL ENTORNO**	
7.6.1	**ÁREAS SEGURAS**	

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.6.1.1	Perímetro de seguridad física	Las organizaciones que realizan tratamiento de datos personales sanitarios deberían utilizar perímetros de seguridad para proteger las áreas que contienen recursos para el tratamiento de la información para esas aplicaciones sanitarias. Esas áreas seguras se deberían proteger mediante controles de entrada adecuados para asegurar que solo se permite el acceso de personal autorizado.
7.6.1.2	Controles físicos de entrada; seguridad de oficinas, despachos e instalaciones; protección contra las amenazas externas y de origen ambiental; trabajo en áreas seguras	Las organizaciones que tratan datos personales sanitarios deberían adoptar las medidas precisas para asegurar que el público esta solo tan cerca del equipamiento TI (servidores, dispositivos de almacenamiento, terminales y monitores) como requieran las restricciones físicas y demanden los procesos clínicos.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.6.1.3	Áreas de acceso público de carga y descarga	Es importante destacar que la provisión de asistencia sanitaria incluye distintas circunstancias en las que el público (los sujetos de la asistencia y sus acompañantes) es físicamente ingresado en áreas con grandes cantidades de información sensible (por ejemplo, laboratorios de análisis en los que el flujo de trabajo obliga a recoger información de los sujetos de la asistencia en el mismo área en el que se están procesando datos de los sujetos anteriores; zonas de tratamiento en áreas de urgencias en las que los acompañantes o los parientes podrían exponerse potencialmente a grandes cantidades de información verbal y visualmente sensible sobre otros sujetos de la asistencia; estaciones de trabajo de enfermería a pie de cama ubicadas cerca de las habitaciones de los pacientes). Aquellas áreas físicas en la asistencia sanitaria que recogen información sanitaria mediante entrevistas y que contienen sistemas en los que se ven datos en una pantalla deberían, por tanto, estar sujetos a un escrutinio adicional.
7.6.2	**SEGURIDAD DE EQUIPOS**	

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.6.2.1	Emplazamiento y protección de equipos	Los dispositivos médicos que registran o informan de datos también pueden requerir consideraciones especiales de seguridad en relación al entorno en el que operan y a las emisiones electromagnéticas que se producen durante su funcionamiento. Las organizaciones sanitarias, especialmente los hospitales, deberían asegurar que las directrices de emplazamiento y protección de TI minimizan la exposición a esas emisiones.
		Las organizaciones que traten datos personales sanitarios deberían situar todas las estaciones de trabajo que permita el acceso a datos personales sanitarios de forma que prevenga la visión no atendida o el acceso por los sujetos de la asistencia y el público.
7.6.2.2	Instalaciones de suministro, seguridad del cableado y mantenimiento de los equipos	Las organizaciones sanitarias deberían prestar la consideración debida al apantallado de la red y demás cables en áreas con altas emisiones por parte de dispositivos médicos.
7.6.2.3	Seguridad de los equipos fuera de las instalaciones	Las organizaciones que traten datos personales sanitarios deberían asegurar que ha sido autorizado todo uso, fuera de las instalaciones, de dispositivos médicos que registrar o informan datos. Esto debería incluir los equipos utilizados por los teletrabajadores, incluso cuando esa utilización sea permanente

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.6.2.4	Reutilización o retirada segura de equipos	Las organizaciones que traten aplicaciones de informática sanitaria deberán sobrescribir de forma segura o incluso destruir todos los medios que contengan software de sistemas informáticos sanitarios o datos personales sanitarios cuando ya no sean necesarios.
7.6.2.5	Retirada de materiales propiedad de la empresa	Las organizaciones que proporcionen o utilicen equipos, datos o software para dar soporte a una aplicación sanitaria que contenga datos personales sanitarios no deberá permitir quo esos equipos, datos o software salgan de las instalaciones o sean reubicados dentro de ellas sin autorización de la organización.
7.7	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**	
7.7.1	**RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIONES**	
7.7.1.1	**DOCUMENTACIÓN DE LOS PROCEDIMIENTOS OPERACIONALES**	
7.7.1.2	Gestión de cambios	Las organizaciones que traten datos personales sanitarios deberán, mediante un proceso formal y estructurado de control de cambios, controlar los cambios en las instalaciones y sistemas para el tratamiento de datos personales sanitarios, que garanticen el control adecuado de las aplicaciones y sistemas alojados y la continuidad de la atención al paciente.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.7.1.3	Segregación de tareas	Las organizaciones que traten datos personales sanitarios deberían, cuando sea viable, segregar las tareas y áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de use indebido de los datos personales sanitarios.
		Las organizaciones que traten datos personales sanitarios deberían asegurar que los sistemas de TI empleados contienen funcionalidades que cumplan los procesos clínicos aprobados para los diferentes titulares de roles, cuando esto sea obligatorio.
7.7.1.4	Separación de los recursos de desarrollo, prueba y operación	Las organizaciones que traten datos personales sanitarios deberán separar (física o virtualmente) los entornos de desarrollo y prueba de los sistemas de información sanitarios que tratan tal información de los entornos operativos que albergan esos sistemas de información sanitarios. Las normas para la migración de software desde el estado de desarrollo al operacional deberán definirse y documentarse por la organización que albergue las aplicaciones afectadas.
7.7.2	Gestión de la provisión de servicios por terceros	La gestión de la provisión de servicios por terceros se simplifica mucho cuando se adopta un acuerdo formal que especifica el mínimo conjunto de controles a implementar-.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.7.3	**PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA**	
7.7.3.1	Gestión de capacidades	
7.7.3.2	Aceptación del sistema	Las organizaciones que traten datos personales sanitarios deberán establecer criterios de aceptación de los nuevos sistemas de información planificados, de las actualizaciones y de las nuevas versiones. Deberán realizar pruebas adecuadas del sistema antes de la aceptación.
7.7.4	**PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y DESCARGABLE**	
7.7.4.1	Controles contra el código malicioso	Las organizaciones que traten datos personales sanitarios deberán implantar controles adecuados de prevención, detección y respuesta para proteger contra el software malicioso y deberán implantar la formación adecuada para la concienciación del usuario.
7.7.4.2	Controles contra el código descargable	
7.7.5	Copias de seguridad de información sanitaria	Las organizaciones que traten datos personales sanitarios deberán realizar copias de seguridad de todos los datos personales sanitarios y almacenarlas en un entorno físicamente seguro que garantice su futura disponibilidad.
		Para proteger su confidencialidad, las copias de seguridad de los datos personales sanitarios deberían almacenarse en un formato encriptado.
7.8	**CONTROL DE ACCESOS**	

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.1	**REQUISITOS PARA EL CONTROL DE ACCESOS EN SANIDAD**	
7.8.1.1	Generalidades	Las organizaciones que traten datos personales sanitarios deberán controlar los accesos a esa información. En general, los usuarios de sistemas de informaci6n sanitarios solo deberían acceder a datos personales sanitarios
		a) Cuando exista una relación de asistencia sanitaria entre el usuario y el sujeto de los datos (el sujeto de La asistencia cuyos datos sanitarios están siendo accedidos
		b) cuando el usuario este realizando una actividad en nombre del sujeto de los datos
		c) cuando existe la necesidad de datos específicos para dar soporte a esta actividad.
7.8.1.2	Política de control de accesos	Las organizaciones que traten datos personales sanitarios deberán tener una política de control de accesos que regale el acceso a los datos.
		La política de la organización sobre el control de accesos debería establecerse sobré la base de roles predefinidos con autoridades asociadas que sean adecuadas, pero limitadas a, las necesidades de ese rol.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.1.2	Política de control de accesos	La política de control de accesos, como un componente del marco general de la política de seguridad de la información descrito en 7.2.1, deberá reflejar los requisitos profesionales, éticos, legales y relativos al sujeto de la asistencia y debería tener en cuenta las tareas realizadas para los profesionales sanitarios' y el flujo de trabajo de las tareas.
		Es importante destacar que, para que la prestación de la asistencia sanitaria no se impida o no se retrase, hay requisitos más fuertes que los habituales para que una política y proceso claros, con la autorización adecuada, puedan invalidar las reglas de control de accesos "normales" en situaciones de emergencia.
		Se recomienda a las organizaciones de salud considerar la implementación de una solución de identidad federada y gestión de accesos reconociendo el potencial del soporte adicional y la reducción de costos de administración que esto proporcionaría a la política de control de accesos. Adicionalmente, esto dará soporte a los procesos de acceso de mayor nivel de seguridad, tales como los basados en tarjetas inteligentes y en las capacidades de "inicio registro de sesión".

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.2	**GESTIÓN DE ACCESOS DE LOS USUARIOS**	
7.8.2.1	Registro de usuarios	El acceso a los sistemas de información sanitaria que traten datos personales sanitarios deberá estar sujeto a un proceso de registro formal de usuarios. Los procedimientos de registro de usuarios deberán asegurar que el nivel de autenticación requerido por la identidad reclamada por el usuario es consistente con los niveles de acceso que estarán disponibles para el usuario.
		Los detalles del registro de usuarios deberán revisarse periódicamente para asegurar que están completos, son exactos y que el acceso todavía es necesario.
		Es importante comprender que la tarea de identificar y registrar a los usuarios de los sistemas de información sanitaria incluye todo lo siguiente:
		a) la captura exacta de la identidad del usuario (por ejemplo, Joan Smith, nacida el actualmente reside en una dirección determinada);
		b) la captura exacta, después de su verificación, de las credenciales profesionales del usuario
		c) la asignación de un identificador de usuario no ambiguo.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.2.1	Registro de usuarios	Destacar que los sujetos de la asistencia no son usuarios típicos del sistema, aunque aquellos que tengan acceso en línea a todo a parte de sus datos personales (por ejemplo, mediante un portal) serian por tanto usuarios del sistema (aunque se les ha proporcionado un acceso limitado). Nótese también que hay aplicaciones sanitarias en las que un usuario puede buscar indicaciones e información general sobre salud. Mientras que esta solicitud de información puede ser registrada, el usuario que está accediendo permanece anónimo. Muchos sitios web que ofrecen información sobre maternidad, SIDA u otros temas de salud funcionan de esta forma. Los usuarios de estos sitios de información general habitualmente no necesitan registrarse y por lo tanto están excluidos del análisis que sigue.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.2.2	Gestión de privilegios	En el análisis que sigue, se especifican varias estrategias de control de accesos que pueden ayudar significativamente a garantizar la confidencialidad y la integridad de los datos personales sanitarios. Estas son:
		a) control de accesos basado en rol, que depende de las credenciales del profesional y del nombre del trabajo de los usuarios establecidos durante el registro para restringir los privilegios de acceso de los usuarios a solo aquellos necesarios o que satisfacen uno o más roles definidos;
		b) control de accesos basado en grupos de trabajo, que depende de la asignación de usuarios a grupos de trabajo (tales como equipos clínicos) para determinar a qué registros pueden acceder;
		c) control de acceso discrecional, que permite a los usuarios de los sistemas de información sanitaria que tienen una relación legitima con los datos personales sanitarios de un sujeto de la asistencia (por ejemplo, un médico de familia) permitir el acceso a otros usuarios que no han establecido previamente una relación con los datos personales sanitarios de ese sujeto de la asistencia (por ejemplo, un especialista).

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.2.2	Gestión de privilegios	Además de seguir las orientaciones dadas en la Norma ISO/1EC 27002, los sistemas de información sanitaria que contengan datos personales sanitarios deberían dar soporte al control de accesos basado en rol capaz de establecer una correspondencia para cada usuario a uno o más roles, y para cada rol a una o más funciones del sistema.
		Un usuario de un sistema de información sanitaria que contenga datos personales sanitarios deberá acceder a sus servicios como un único rol (es decir los usuarios que se han registrado con más de un rol deberán designar un único rol durante cada sesión de acceso al sistema de información sanitaria).
		Los sistemas de información sanitaria deberían asociar los usuarios (incluyendo a los profesionales sanitarios, el personal de apoyo y otros) con las historian de los sujetos de la asistencia y permitir el acceso futuro basado en esta asociación.
		Se pueden encontrar orientaciones adicionales sobre la gestión de privilegios en sanidad en las Especificaciones Técnicas ISO/TS 22600-1 e ISO/TS 22600-2.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.2.3	Gestión de contraseñas de usuario	No es necesaria ninguna orientación adicional para la gestión de la seguridad de la información en sanidad, aunque se debería destacar que las presiones de tiempo halladas a veces en la prestación sanitaria pueden hacer que sea difícil hacer use de forma efectiva de las contraseñas. Muchas organizaciones sanitarias han considerado la adopción de tecnologías de autenticación alternativas para tratar este problema.
7.8.2.4	Revisión de los derechos de acceso del usuario	Además de seguir las orientaciones dadas en la Norma ISO/IEC 27002, es necesario tener una consideración especial con los usuarios que sé que proporcionen atención urgente; ya que pueden necesitar acceder a datos personales sanitarios en situaciones urgentes en las que el sujeto de in asistencia podría ser incapaz de dar sus consentimientos.
7.8.3	Responsabilidades del usuario	Además de seguir las orientaciones dadas en la Norma ISO/1EC 27002, las organizaciones que traten información sanitaria deberían, cuando se determinen las responsabilidades de los usuarios, respetar los derechos y responsabilidades éticas de los profesionales sanitarios, según las leyes y tal como está aceptado por los miembros de las organizaciones profesionales de salud.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.4	Control de acceso a la red y al sistema operativo	No hay orientaciones adicionales para la gestión de seguridad de la información en salud.
7.8.5	**CONTROL DE ACCESO A LAS APLICACIONES Y A IA INFORMACIÓN**	
7.8.5.1	Restricción del acceso a la información	Los sistemas de información sanitaria que tratan datos personales sanitarios deberán autenticar a los usuarios y deberían hacerlo mediante una autenticación que implique al menos dos factores.
		Además de seguir las orientaciones dadas en la Norma ISO/IEC 27002, debería darse una consideración especial a las medidas técnicas mediante las cuales se autentifica a un sujeto de la asistencia de forma segura cuando accede a todo o a parte de su propia información (en aquellos sistemas de información sanitaria que permitan tales accesos). También debería darse un énfasis similar a la facilidad de uso de tales medidas, especialmente para sujetos de la asistencia con minusvalías, y para las disposiciones de acceso de los tutores.
7.8.5.2	Aislamiento de sistemas sensibles	No hay orientaciones adicionales para la gestión de seguridad de la información en salud.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.6	**ORDENADORES PORTÁTILES Y TELETRABAJO**	
7.8.6.1	Ordenadores portátiles y comunicaciones móviles	Además de seguir las orientaciones dadas en la Norma ISO/IEC 27002, las organizaciones que traten datos personales sanitarios deberían: a) valorar específicamente los riesgos que supone la informática móvil en sanidad; b) preparar políticas sobre las precauciones a adoptar cuando se utilizan dispositivos móviles, incluyendo los dispositivos inalámbricos; c) obligar a Los usuarios de los dispositivos móviles a seguir esta política. Tal como se destaca en la Norma ISO/IEC 27002, las conexiones de red inalámbricas móviles, aunque similares a las redes de cable, tienen algunas diferencias importantes desde punto de vista de la seguridad de la información. Algunos protocolos de encriptación inalámbricos tales como la Privacidad Equivalente a Cableado (Wired Equivalent Privacy (WEP)) todavía están en uso a pesar de sus conocidas debilidades que los han convertido en muy ineficientes. Mas no siempre puede hacerse copia de seguridad de la información almacenada en dispositivos móviles.

NÚMERO	POLÍTICA DE SEGURIDAD	DESCRIPCIÓN
7.8.6.2	Teletrabajo	Además de seguir las orientaciones dadas en la Norma ISO/IEC 27002, las organizaciones que traten datos personales sanitarios deberían:
		a) Preparar políticas sobre las precauciones a adoptar en el teletrabajo;
		b) Asegurar que los usuarios del teletrabajo en sistemas de información sanitarios acatan esta política.
		Es importante considerar que, en sanidad, el teletrabajo puede traspasar Las fronteras jurisdiccionales e incluso puede realizarse a bordo de aviones y barcos situados más allá de cualquier jurisdicción nacional. Los médicos envían de forma rutinaria imágenes medidas por correo electrónico, etc. cruzando fronteras para interconsultas. Los equipos internacionales implicados en rescates pueden, en el futuro, depender de los sistemas de información sanitaria en jurisdicciones diferentes a su jurisdicción de origen. Es necesario tener en cuenta las consideraciones legales de esto en el diseño y despliegue de los sistemas de información sanitarios (especialmente los sistemas nacionales) que puedan utilizarse de esta forma. Véase también los apartados 7.7.7.1

Fuente: *ISO 27799*

3.4. DOCUMENTO DE LA POLÍTICA DE SEGURIDAD

3.4.1. Introducción

Con la definición de los riegos y la selección de los controles de seguridad informática se busca establecer mecanismos de control en las aplicaciones médicas en el interior del Hospital Axxis. Las políticas de seguridad, son diseñadas en base a la Norma ISO27799 estándar que cubre las necesidades del Hospital Axxis en materia de seguridad, las normas y políticas realizadas son de referencia, las mismas pueden estar sujetas a cualquier cambio, siempre y cuando se tengan presentes los objetivos de seguridad de la información y los servicios que presta el Hospital Axxis.

La política de seguridad, pretende, ser el medio que norme y controle el uso de aplicaciones y recursos informáticos a través de la comunicación de las unidades médicas. Todo usuario que utilice los servicios informáticos del Hospital Axxis, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

El manual de política de seguridad informática, engloba los procedimientos más adecuados, tomando como lineamientos principales nueve criterios seleccionados de la norma ISO27799, que se detallan a continuación:

- Organización Interna
- Gestión de Activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos

3.4.2. Objetivo

Dotar de la información necesaria a los usuarios, empleados y médicos, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software del Hospital Axxis.

3.4.3. Evaluación de la Política

Artículo 1.- Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

3.4.4. Organización Interna

Artículo 2.- El Hospital Axxis a través de su junta directiva debe adquirir el compromiso de gestión para la seguridad de la información y la asignación de responsabilidades en seguridad de la información a través de su Gerente de sistemas.

Artículo 3.- Las aplicaciones médicas y recursos de la red del Hospital Axxis son de exclusivo uso para gestiones administrativas y médicas, estas serán utilizadas para cumplir funciones únicamente del Hospital Axxis, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

Artículo 4.- El Hospital Axxis a través de su junta directiva debe adquirir el compromiso de gestión para la seguridad de la información y la asignación de responsabilidades en seguridad de la información a través de su Gerente de sistemas.

Artículo 5.- Todo empleado que ingrese al Hospital Axxis debe tener firmado un acuerdo de confidencialidad en vigor que especifique la naturaleza confidencial de la

información médica. El acuerdo deberá ser aplicable a todo el personal que accede a la información sanitaria.

Artículo 6.- Todo proveedor externo que ingrese al Hospital Axxis debe tener un acuerdo de confidencialidad en vigor que especifique la naturaleza confidencial de la información médica. El acuerdo deberá ser aplicable a todo el personal que accede a la información sanitaria.

Artículo 7.- El Hospital Axxis a través del área de sistemas debe evaluar los riesgos asociados con el acceso por partes externas a los sistemas o a los datos que contienen, y a continuación implementar los controles de seguridad que sean apropiados para el nivel de riesgo identificado y las tecnologías empleadas

3.4.5. Gestión de Activos

3.4.5.1. Responsabilidad para los Activos de la información sanitaria

Artículo 8.- El administrador de sistemas a través de su equipo técnico delegará un responsable para realizar un control de activos tanto en software como en hardware de las aplicaciones médicas que estén en uso en el Hospital Axxis, se lo actualizará cada semestre.

Artículo 9.- El administrador de sistemas seleccionará un responsable de la integridad física de los equipos que almacenan las aplicaciones médicas, se debe llevar una bitácora sobre el estado semanal de los equipos y sus respectivas aplicaciones.

Artículo 10.- Antes del uso de cualquier activo del Hospital Axxis, un representante del área de sistemas deberá socializar las reglas de uso de los equipos y aplicaciones médicas.

3.4.5.2. Clasificación de información sanitaria

Artículo 11.- De forma individual, las unidades médicas, son responsables, de clasificar de acuerdo al nivel de importancia, la información que en ella se procese.

Artículo 12.- Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:

a) PÚBLICA

b) INTERNA

c) CONFIDENCIAL.

Artículo 13.- Los activos de información de mayor importancia para el Hospital Axxis deberán clasificarse por su nivel de exposición o vulnerabilidad dentro de las aplicaciones médicas

Artículo 14.- El administrador de sistemas con su equipo debe solicitar a los proveedores externos de las aplicaciones, que la información dentro de estas se ingrese con etiquetas de pública, interna o confidencial.

3.4.6. Seguridad de los Recursos Humanos

3.4.6.1. Previo al Empleo

Artículo 15.- La unidad médica que requiera contratar personal para utilizar las aplicaciones médicas debe solicitar el perfil a recursos humanos, mientras que los directores de la unidad médica junto con el administrador de sistemas definirán los roles y responsabilidades del personal temporal o de corta duración tales como los sustitutos, estudiantes, residentes, etc.

Artículo 16.- El Hospital Axxis a través de recursos humanos deberá verificar la identidad, domicilio actual y anteriores empleos del personal nuevo que tendrá acceso a las aplicaciones médicas y por ende información sanitaria.

Artículo 17.- Recursos Humanos deberá especificar en los contratos del personal nuevo las normas de seguridad establecidas en el Hospital Axxis en seguridad de la información.

Artículo 18.- La información procesada, manipulada o almacenada por el empleado es propiedad exclusiva del Hospital Axxis.

3.4.6.2. Durante el Empleo

Artículo 19.- EL Hospital Axxis a través del departamento de sistemas deberá organizar charlas de capacitación semestrales sobre las políticas de seguridad informática y procedimientos de seguridad de la organización.

Artículo 20.- Todo servidor o funcionario nuevo del Hospital Axxis deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

Artículo 21.- El Hospital Axxis no se hace responsable por daños causados provenientes de sus empleados a la información o activos de procesamiento, daños efectuados desde sus instalaciones de red a equipos informáticos externos

Artículo 22.- Es responsabilidad de los empleados de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Empleados del presente Manual.

3.4.6.3. Finalización o Cambio de Empleo

Artículo 23.- Las unidades médicas del Hospital Axxis, deben notificar inmediatamente la finalización de las actividades del personal a su cargo al departamento de sistemas, el cual debe dar de baja los usuarios y contraseñas del empleado que deja sus funciones en el instante de su notificación, de igual manera con proveedores externos.

3.4.7. Seguridad Física y del Entorno.

3.4.7.1. Áreas Seguras

Artículo 24.- El cuarto de control y todos los racks del Hospital Axxis deben contar con un sistema de control de acceso centralizado para el ingreso únicamente del personal autorizado.

3.4.7.2. Seguridad de Equipos

Artículo 25.- El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

Artículo 26.- Queda prohibido el uso de las aplicaciones médicas fuera de las instalaciones del Hospital Axxis.

Artículo 27.- Toda la información sanitaria debe ser respaldada y protegida, si existe un medio extraíble con información sanitaria se deberá sobrescribir de forma segura o incluso destruirlo si la información ya no es necesaria.

Artículo 28.- Los servidores, sin importar al dominio o grupo de trabajo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento, para que puedan salir de las instalaciones del Hospital Axxis.

3.4.8. Gestión de Comunicaciones y Operaciones

3.4.8.1. Responsabilidades y Procedimientos de Operaciones

Artículo 29.- El departamento de sistemas deberá manejar una bitácora sobre el control de cambios en las instalaciones y sistemas de tratamiento de datos personales sanitarios, que garanticen el control adecuado de las aplicaciones médicas.

Artículo 30.- Antes de implementar una aplicación el departamento debe realizar pruebas adecuadas de forma y fondo antes de su aceptación.

Artículo 31.- El personal administrador de algún servicio, es el responsable absoluto por mantener en óptimo funcionamiento ese servicio, coordinar esfuerzos con el coordinador de sistemas, para fomentar una cultura de administración segura y servicios óptimos.

Artículo 32.- Las configuraciones y puesta en marcha de servicios, son normadas por el departamento de informática.

Artículo 33.- El personal responsable de los servicios, llevará archivos de registro de fallas de seguridad del sistema, revisará estos archivos de forma frecuente y en especial después de ocurrida una falla.

Artículo 34.- Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.

Artículo 35.- La aceptación y uso de los sistemas no exonera, de responsabilidad alguna sobre el gestor de seguridad, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

Artículo 36.- El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el gestor de seguridad, antes de su implementación

3.4.8.2. Protección contra código malicioso y descargable

Artículo 37.- El Antivirus del Hospital Axxis es Kaspersky, este debe estar instalado y actualizado en todas las máquinas y servidores de la institución.

Artículo 38.- El departamento de sistemas se encarga de la supervisión de las actualizaciones periódicas del antivirus mediante la consola del Antivirus y activada la protección en tiempo real.

Artículo 39.- La máquina que no cumpla con las condiciones establecidas no podrá acceder a las aplicaciones médicas.

3.4.9. Control de Accesos

3.4.9.1. Requisitos para el control de accesos en sanidad

Artículo 40.- Antes de usar cualquier aplicación médica del Hospital Axxis, el área de sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a manuales y capacitación de las aplicaciones médicas.

Artículo 41.- Cualquier petición de información, servicio o acción proveniente de un determinado usuario, se realizará siguiendo los canales de gestión formalmente establecidos.

3.4.9.2. Gestión de Accesos de los Usuarios

3.4.9.2.1. Usuarios Internos

Artículo 42.- Son usuarios de las aplicaciones médicas del Hospital Axxis los empleados, administrativos, médicos, contratistas, y toda aquella persona, que tenga contacto directo y utilice la infraestructura del Hospital.

Artículo 43.- El acceso a los sistemas de información sanitaria que traten datos personales sanitarios deberá estar sujetos a un proceso de registro formal de usuarios.

Artículo 44.- El registro de usuarios se lo debe realizar a través del directorio activo del dominio del Hospital Axxis, en el cual se debe llenar todos los datos de

identidad del usuario y sus respectivos privilegios, por ningún motivo se podrá crear un usuario que no exista en el directorio activo

Artículo 45.- El área de sistemas nombrará un delegado para validar y revisar periódicamente los usuarios, para asegurar que estén completos, sean exactos y que el acceso todavía sea necesario.

Artículo 46.- Los datos mínimos obligatorios que se debe realizar son, la captura exacta de la identidad del usuario, sus credenciales profesionales, el cargo que ocupa y su identificador nombre de usuario.

Artículo 46.- Se creará una cuenta temporal del usuario, en caso de olvido o perdida de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando se muestre un documento de identidad personal.

Artículo 47.- La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.

Artículo 48.- La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación alfanumérica.

3.4.9.2.2. Usuarios Externos

Artículo 49.- Los usuarios externos, son usuarios limitados, estos tendrán acceso únicamente a los servicios del portal cautivo e Internet por el tiempo de 20 minutos.

Artículo 50.- Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con el Hospital Axxis fuera del ámbito de empleado/contratista y siempre que tenga una vinculación con los servicios que brinda el Hospital Axxis

Artículo 51.- El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad con el Hospital Axxis y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

Artículo 52.- No se proporcionará el servicio solicitado por un usuario, o área de trabajo, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución según la política de seguridad

Artículo 53.- La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.

Artículo 54.- La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación alfanumérica.

Artículo 55.- El acceso de externos será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.

Artículo 56.- Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.

3.4.9.3. Responsabilidad del Usuario

Artículo 57.- El usuario es responsable exclusivo de mantener a salvo su contraseña.

Artículo 58.- El usuario será responsable de la información que sea enviada con su cuenta.

Artículo 59.- El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios, con la posibilidad de incurrir en una denuncia penal por mal uso de los servicios informáticos del Hospital.

Artículo 60.- Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guardada en un lugar seguro.

Artículo 61.- El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Administrador de la red, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Artículo 62.- El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

Artículo 63.- El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

Artículo 64.- Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos del Hospital Axxis, está obligado a reportarlo a los administradores del sistema.

Artículo 65.- El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

3.4.9.4. Responsabilidad del Departamento de Sistemas

Artículo 66.- El área de sistemas, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

Artículo 67.- La creación de cuentas y usuarios para acceder a este servicio debe ser supervisada y aprobada por el área de sistemas para sus fines pertinentes.

Artículo 68.- La creación de cuentas y usuarios con todos los campos dentro del dominio activo del Hospital Axxis.

Artículo 69.- Supervisión y monitoreo del acceso de usuarios internos y externos hacia las aplicaciones médicas

Artículo 70.- Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

Artículo 71.- Los archivos de Log, almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

3.4.9.5. Control de acceso a las aplicaciones y a la información.

Artículo 72.- Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación, y los diferentes accesos a los módulos permitidos.

Artículo 73.- Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos,

y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

Artículo 74.- Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

Artículo 75.- Las salidas de información, de las aplicaciones, en un entorno de red, deberán ser documentadas, y especificar la terminal por la que deberá ejecutarse exclusivamente la salida de información.

Artículo 76.- Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

3.4.9.5.1. Correo Electrónico

Artículo 77.- El servicio de correo electrónico, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

Artículo 78.- El correo electrónico es de uso exclusivo, para los empleados y contratistas del Hospital Axxis.

Artículo 79.- Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

3.4.9.5.2. Internet

Artículo 80.- El acceso a Internet provisto a los usuarios y funcionarios del Hospital Axxis es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

Artículo 81.- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el Hospital Axxis, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el área de Sistemas.

Artículo 82.- Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización del Área de Sistemas.
- La utilización de Internet es para el desempeño de sus funciones y cargo en el Hospital Axxis y no para propósitos personales.

Artículo 83.- El acceso a Internet puede ser Gestionado, limitado y Personalizado por el Área de Sistemas siempre y cuando la situación lo amerite y casos especiales de trabajo para los usuarios y funcionarios del Hospital Axxis. Es decir, se pueden bloquear y denegar algunos accesos a paginas para Optimizar el ancho de banda de Internet para su total aprovechamiento.

3.4.9.5.3. Historias Clínicas Electrónica

Artículo 84.- El acceso al sistema de Historias Clínicas del Hospital Axxis es de uso exclusivo para médicos y enfermeras.

Artículo 85.- Cualquier usuario que encuentre accidentalmente una sesión abierta deberá automáticamente cerrarla y notificar al área de sistemas

3.4.9.5.4. Sistema de Gestión de Pacientes

Artículo 86.- El acceso al sistema de Gestión de Pacientes del Hospital Axxis es de uso exclusivo para administrativo.

Artículo 87.- Cualquier usuario que encuentre accidentalmente una sesión abierta deberá automáticamente cerrarla y notificar al área de sistemas

3.4.9.5.5. Sistema de Imagen

Artículo 88.- El acceso al sistema de Imagen del Hospital Axxis es de uso exclusivo radiólogos y técnicos de imagen.

Artículo 89.- Cualquier usuario que encuentre accidentalmente una sesión abierta deberá automáticamente cerrarla y notificar al área de sistemas

3.4.9.5.6. Sistema de Laboratorio

Artículo 90.- El acceso al sistema de Laboratorio del Hospital Axxis es de uso exclusivo de analistas del área.

Artículo 91.- Cualquier usuario que encuentre accidentalmente una sesión abierta deberá automáticamente cerrarla y notificar al área de sistemas

CAPÍTULO IV

4. DISCUSIÓN

4.1. CONCLUSIONES

Las organizaciones en Ecuador no toman en cuenta los riesgos y vulnerabilidades que están presentes en el uso de aplicaciones médicas, es necesario implementar y socializar políticas de seguridad dentro de la plataforma tecnológica de las organizaciones médicas.

Es de vital importancia identificar las amenazas y riesgos que existen en sector sanitario en la implementación de software y aplicaciones médicas, para evitar problemas legales que afecten al giro del negocio de las entidades de salud.

Se requiere establecer una política de seguridad que sean aprobadas por los coordinadores de todas las unidades médicas, que se comprometan y se garanticen la implementación, actualización y cumplimiento de estas.

Es necesario aplicar una política de seguridad para mantener la confidencialidad, integridad y disponibilidad de la información se recomienda trabajar con normas como las ISO 27799, que son especializadas en el sector sanitario que ayuden a mitigar los riegos y vulnerabilidades informáticas.

Para asegurar que la información sanitaria mantenga estándares de buenas prácticas como son la integridad, confidencialidad y disponibilidad es necesario la creación de las Políticas de Seguridad de la Información.

Debido a requerimientos operacionales y regulaciones técnicas en el área sanitaria, existe la necesidad de crear la política de seguridad de la información,

La participación de todos los empleados del Hospital Axxis es necesaria para la ejecución y cumplimiento de la política de seguridad.

4.2. RECOMENDACIONES

Implementar un Sistema de Gestión de la Seguridad de la Información, para establecer políticas y procedimientos en relación a los objetivos del Hospital Axxis.

Realizar una valoración semestral de la política de seguridad para que se encuentre actualizada y acorde a los requerimientos del Hospital.

Se requiere crear en el departamento de sistemas un área dedica a la seguridad de la información, para implementar los mecanismos de control de acceso a la información y mantener la información confidencial integra y disponible en el Hospital Axxis.

Previo a la instalación de cualquier aplicación se debe realizar procedimientos para la implementación y que las aplicaciones no presenten fallos o vacíos de seguridad.

Debido a que la información es muy importante para el Hospital Axxis, se recomienda la capacitación de su personal técnico de las normas de Seguridad de la Información.

Se debe comunicar a los empleados sobre los beneficios y ventajas que se obtendrán luego de la implementación de estas políticas. De igual manera las sanciones descritas en las políticas.

BIBLIOGRAFÍA

Box, D., & Pottas, D. (2010). Trust - Can it be controlled? *Studies in Health Technology and Informatics*, *160*(PART 1), 651–655. https://doi.org/10.3233/978-1-60750-588-4-651

Cruz, G., Parra, L., & Ariza, M. (2016). Diseño de las políticas de seguridad para la empresa social del estado hospital integrado San Antonio de Puente Nacional.

Dussan, A. (2006). Políticas de seguridad informática. *Red de Revistas Científicas de América Latina, El Caribe, España Y Portugal*.

Ganthan, N., Rabiah, A., & Zuraini, I. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. https://doi.org/10.1177/1460458210377468

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

Kotsonis, E., & Eliakis, S. (2017). Information Security Standards for Health Information Systems. *User-Driven Healthcare*, (iso 27799), 225–257. https://doi.org/10.4018/978-1-4666-2770-3.ch013

Ledezma, D. (2015). Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC Departamento de Investigación y Postgrados.

Norma, I. I. 27799: (2016). Tecnología de la información. Informática en salud. Gestión de seguridad de la información en salud utilizando la ISO/IEC, 27002.

Orejuela, C. (2015). Elaboración e implementación del manual de políticas y normas de seguridad informática para la empresa Eléctrica Regional Norte S.A. – EMELNORTE.

Orel, A., & Bernik, I. (2013). Implementing healthcare information security: standards can help. *Studies in Health Technology and Informatics*, *186*(iso 27799), 195–9. https://doi.org/10.3233/978-1-61499-240-0-195

Ouhbi, S., Fernández, J., Carrillo, J., Toval, A., & Idri, A. (2017). E-health internationalization requirements for audit purposes. *Computer Methods and Programs in Biomedicine*, *144*, 49–60. https://doi.org/10.1016/j.cmpb.2017.03.014

Ramirez, D., & Camargo, J. (2017). Diseño de un sistema de Gestión de la Seguridad de la Información (SGSI) en el área tecnológica de la Comisión Nacional del Servicio Civil-CNSC basado en la norma ISO27000 e iso27001.

Sánchez, A., Fernández, J., Toval, A., Hernández, I., Sánchez, A., & Carrillo, J. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atencion Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

Whitten, J, B. L. . y K. C. D. (2011). Sistem análisis & design methods. Mc Graw Hill. México.

ANEXO 1

AUDITORÍA INTERNA

AXXIS HOSPITAL	**SOLICITUD DE ACPM**

Fecha de Solicitud	**Proceso o Subproceso**
OCTUBRE 30, 2015	

Fuente de solicitud de las ACPM

Evaluación de Servicio	
Análisis de indicadores	
Auditoría de calidad (interna)	X
Auditoría de calidad (externa)	
Quejas de clientes	
Revisión por la Dirección	
Producto no Conforme	
Otros	

Tipo de ACPM

Correctiva	X
Preventiva	
De Mejora	

Solicitante de la ACPM	**Responsable de atender la solicitud de ACPM**
ELIZABETH FLORES	MARÍA FERNANDA PALMA

Descripción del problema real o potencial

No existe un documento de procesos para el área de sistemas

Análisis de Causa

PARA CUMPLIR DE MEJOR MANERA EL NUMERAL 6.3

Plan de Acción

Actividad	Responsable	Fecha	Recursos	Evaluación de la Eficacia
Socializar y realizar un proceso de funcionamiento y seguridad de sistemas y su infraestructura	Juan Cumbicus	9/11/2016		
Respaldo de la información	Ricardo Arias	9/11/2016		
Implementación de seguridades	Departamento TI	9/11/2016		

ANEXO 2

Ponderación de la entrevista

RIESGO EVALUADO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
Suplantación interna	VOTO IMPACTO	5,0	5,0	5,0
	VOTO VULNERABILIDAD	2,0	4,0	5,0
Suplantación mediante proveedores de servicio	VOTO IMPACTO	3,0	3,5	1,0
	VOTO VULNERABILIDAD	3,0	3,0	1,0
Suplantación por externos	VOTO IMPACTO	5,0	4,0	4,0
	VOTO VULNERABILIDAD	4,0	4,0	4,0
Uso no autorizado de una aplicación de informática sanitaria	VOTO IMPACTO	5,0	4,0	4,0
	VOTO VULNERABILIDAD	3,0	4,0	4,0
Introducción de software dañino o perjudicial	VOTO IMPACTO	3,0	4,0	3,0
	VOTO VULNERABILIDAD	5,0	5,0	3,0
Uso indebido de los recursos del sistema	VOTO IMPACTO	2,0	1,0	2,0
	VOTO VULNERABILIDAD	3,0	1,0	2,0
Infiltración en las comunicaciones	VOTO IMPACTO	3,0	4,0	3,0
	VOTO VULNERABILIDAD	2,0	4,0	4,0
Intercepción de las comunicaciones	VOTO IMPACTO	4,0	3,0	2,0
	VOTO VULNERABILIDAD	4,0	4,0	1,0
Repudio	VOTO IMPACTO	1,0	1,0	2,0
	VOTO VULNERABILIDAD	2,0	1,0	2,0
Fallo en la conexión	VOTO IMPACTO	4,0	3,0	3,0
	VOTO VULNERABILIDAD	1,0	3,0	2,0
Código malicioso empotrado	VOTO IMPACTO	4,0	4,0	5,0
	VOTO VULNERABILIDAD	3,0	5,0	2,0
Asignación de ruta indebida accidental	VOTO IMPACTO	2,0	3,0	2,0
	VOTO VULNERABILIDAD	2,0	1,0	1,0

RIESGO EVALUADO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
Fallo técnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red	VOTO IMPACTO	3,0	2,0	3,0
	VOTO VULNERABILIDAD	3,0	2,0	2,0
Fallos de entorno de soporte	VOTO IMPACTO	5,0	4,0	4,0
	VOTO VULNERABILIDAD	3,0	4,0	4,0
Fallo en el software de sistemas o en el software de red	VOTO IMPACTO	4,0	4,0	3,0
	VOTO VULNERABILIDAD	3,0	4,0	3,0
Fallo en las aplicaciones de software	VOTO IMPACTO	5,0	4,0	4,0
	VOTO VULNERABILIDAD	4,0	3,0	4,0
Error del operador	VOTO IMPACTO	2,0	2,0	1,0
	VOTO VULNERABILIDAD	3,0	1,0	2,0
Errores de mantenimiento	VOTO IMPACTO	5,0	5,0	4,0
	VOTO VULNERABILIDAD	4,0	4,0	3,0
Error de usuario	VOTO IMPACTO	2,0	3,0	1,0
	VOTO VULNERABILIDAD	1,0	2,0	2,0
Escasez de personal	VOTO IMPACTO	2,0	1,0	2,0
	VOTO VULNERABILIDAD	1,0	1,0	2,0
Robo por internos	VOTO IMPACTO	3,0	3,0	4,0
	VOTO VULNERABILIDAD	1,0	3,0	3,0
Robo por externos:	VOTO IMPACTO	2,0	3,0	2,0
	VOTO VULNERABILIDAD	3,0	4,0	2,0
Daño premeditado por internos	VOTO IMPACTO	2,0	1,0	2,0
	VOTO VULNERABILIDAD	1,0	1,0	3,0
Daño premeditado por externos	VOTO IMPACTO	2,0	1,0	3,0
	VOTO VULNERABILIDAD	2,0	3,0	1,0
Terrorismo	VOTO IMPACTO	3,0	2,0	3,0
	VOTO VULNERABILIDAD	3,0	3,0	1,0
Alteraciones del entorno	VOTO IMPACTO	4,0	5,0	4,0
	VOTO VULNERABILIDAD	3,0	4,0	4,0

RIESGO EVALUADO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Gerente de sistemas)	Calificación Funcionario Nro. 3 (Jefe de área médica)
Accesos físicos no autorizados a las aplicaciones medicas	VOTO IMPACTO	4,0	4,0	4,0
	VOTO VULNERABILIDAD	5,0	3,0	4,0
Fallas en Hardware	VOTO IMPACTO	3,0	3,0	3,0
	VOTO VULNERABILIDAD	3,0	4,0	2,0
Virus	VOTO IMPACTO	4,0	4,0	5,0
	VOTO VULNERABILIDAD	4,0	3,0	4,0
Corrupción lógica	VOTO IMPACTO	4,0	1,0	2,0
	VOTO VULNERABILIDAD	3,0	2,0	1,0
Vulnerabilidades en los sistemas de seguridad:	VOTO IMPACTO	4,0	4,0	4,0
	VOTO VULNERABILIDAD	4,0	4,0	5,0
Fugas de información	VOTO IMPACTO	4,0	4,0	5,0
	VOTO VULNERABILIDAD	3,0	4,0	4,0

Preguntas de la Entrevista

1.- ¿Cree usted que pueden robar información del Datacenter?

Si

¿Por qué considera usted que se puede perder información?

No existe control de accesos al Datacenter y el área está destinada para sistemas y monitoreo.

2.- ¿Qué tan probable es que exista fuga de información?

Si

¿Por qué?

Las aplicaciones médicas requieren control de periféricos y las máquinas que utilizan los médicos son de ellos no las podemos intervenir

3.- ¿Como califica el nivel de seguridad de la organización?

Regular

¿Por qué?

Se requiere la implementación de infraestructura acorde a las aplicaciones implementadas

4.- ¿Existe actualizaciones periódicas de las aplicaciones?

Si

¿Por qué?

Las empresas nos notifican para realizar la actualización

5.- ¿Cómo se integran los smartphones de tus empleados en la red de tu empresa?

Red plana

¿Por qué?

El Hospital se lo construyo por etapas en algunos pisos existen switchs administrables en otros no por lo tanto no podemos administrar la infraestructura.

6.- ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura IT de tu empresa?

Algunos

¿Por qué?

Las aplicaciones contables requieren permisos de administrador

7.- ¿Saben tus empleados reconocer un e-mail sospechoso?

Algunos

¿Por qué?

Existe rotación de personal en cuanto a secretarias

8.- ¿Encriptas de alguna forma tus bases de datos y la información sobre tus clientes?

Si

¿Por qué?

Es un requerimiento para los proveedores de software

9.- ¿Están tus sitios web protegidos?

No

¿Por qué?

No existe un firewall que proteja los servicios

10.- ¿Pides a tus empleados que cambien de contraseña con regularidad?

Si

¿Por qué?

Para mantener los niveles de seguridad óptimos

11.- ¿Cuáles son las vulnerabilidades entonces?

La falta de infraestructura como un buen firewall y procedimientos para la implementación de aplicaciones en Hospital permite vacíos de seguridad.

Preguntas de la Encuesta

1.- ¿Cree usted que su información es segura en las instalaciones del Hospital?

Respuesta

No	120
Tal vez	26
Si	12

2.- ¿Como califica el nivel de seguridad de la organización?

Respuesta

Buena	92
Regular	58
Mala	8

3.- ¿A sufrido algún tipo de para de servicio informático con el cual trabaja?

Respuesta

Si	99
No	59