Polo del Conocimiento

Pol. Con. (Edición núm. 41) Vol. 5, No 01
Enero 2019, pp. 362-379
ISSN: 2550 - 682X
DOI: 10.23857/pc.v5i01.1228

Riesgos de seguridad de la información, del Departamento de Tecnologías de la Información y Comunicación, Hospital Isidro Ayora-Loja

Information security risks, from the Department of Information and Communication Technologies, Isidro Ayora-Loja Hospital

Riscos de segurança da informação, do Departamento de Tecnologias da Informação e Comunicação do Hospital Isidro Ayora-Loja

Ximena del Cisne Quevedo-Rojas [I]
ximeqr3b@gmail.com
https://orcid.org/0000-0003-0878-7429

Silvia Eulalia Vintimilla-Jara [II]
svintimillaj@ucacue.edu.ec
https://orcid.org/0000-0003-2758-0466

Correspondencia: ximeqr3b@gmail.com

Ciencias de las ingenierías
Artículo de investigación

*Recibido: 10 de noviembre de 2019 *Aceptado: 22 diciembre de 2019 * Publicado: 17 de enero 2020

I. Ingeniera en Sistema, Jefatura de Posgrados. Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniera de Sistemas, Docente de la Unidad Académica de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca, Jefatura de Posgrados, Cuenca, Ecuador.

Resumen

El presente trabajo de investigación tiene como objetivo realizar un análisis y tratamiento de riesgos de seguridad de la información, basado en la norma ISO 27005, en este artículo se define el contexto, donde se hace una selección de los activos principales, para realizar el análisis de riesgos, tomando en cuenta los criterios de evaluación de los activos, posteriormente se selecciona las amenazas y vulnerabilidades, considerando el nivel de ocurrencia, para finalmente realizar el tratamientos de los riesgos, estableciendo el valor de los riesgos para cada uno de los activos. Este plan se lo realiza a nivel de infraestructura, quedando como un referente para la elaboración de un plan de gestión de riesgos de seguridad de la información que abarque todas las áreas de la institución.

Palabras clave: Seguridad de la información; análisis de riesgos; tratamiento de riesgos; ISO 27005.

Abstract

This research work aims to perform an analysis and treatment of information security risks, based on ISO 27005, in this article the context is defined, where a selection of the main assets is made, to perform the analysis of risks, taking into account the criteria of evaluation of the assets, subsequently the threats and vulnerabilities are selected, considering the level of occurrence, to finally carry out the treatment of the risks, establishing the value of the risks for each of the assets. This plan is carried out at the infrastructure level, remaining as a reference for the elaboration of an information security risk management plan that covers all areas of the institution.

Keywords: Security of the information; Risk analysis; Risk treatment; ISO 27005

Resumo

Este trabalho de pesquisa tem como objetivo realizar uma análise e tratamento de riscos à segurança da informação, com base na ISO 27005, neste artigo é definido o contexto, onde é feita uma seleção dos principais ativos, para realizar a análise dos riscos, levando-se em consideração os critérios de avaliação dos ativos, as ameaças e vulnerabilidades são selecionadas, considerando o nível de ocorrência, para finalmente realizar o tratamento dos riscos, estabelecendo o valor dos riscos para cada um dos ativos. Esse plano é realizado no nível de infraestrutura, permanecendo como

referência para a elaboração de um plano de gerenciamento de riscos à segurança da informação que abranja todas as áreas da instituição.

Palavras chaves: segurança da informação; analise de riscos; tratamento de risco; ISO 27005

Introducción

El uso de las tecnologías de la información (TI) se ha hecho indispensable dentro de las organizaciones, sin importar la actividad económica a la que se dediquen, las TI se encuentran en constante evolución adaptándose de las organizaciones y sus necesidades.

Con los avances tecnológicos, la seguridad de la información se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado. La seguridad puede verse afectada por diversos factores, entre ellos, podemos mencionar: el uso indebido de la tecnología, la falta de procesos de planificación de seguridad o el desconocimiento de las personas acerca de las distintas medidas de seguridad informática(Alemán & Rodríguez, 2015)

(Ramirez & Ortiz, 2011) establecen una metodología en base a los estándares ISO 31000 e ISO 27005, la metodología propuesta es una guía para entender los conceptos definidos en los estándares utilizados para la gestión de riesgos, con un enfoque en los riesgos tecnológicos. Esta brinda una pauta para la aplicación del proceso de gestión de riesgos utilizando la norma 27005 evitando los vacíos y ambigüedades que tienen los estándares ISO, con indicaciones sobre cómo llevar a cabo las acciones descritas en la documentación.

En el sector salud, la implementación de las TICs, da como resultado mejores tiempos de respuesta en: Diagnósticos, resultados de exámenes, seguimientos de historias clínicas, entre otros servicios, es por esta razón que la confidencialidad, disponibilidad e integridad de la información se convierte en un factor de vital importancia, por lo que surge la necesidad de contar con un plan de tratamiento de riesgos de seguridad de la información ayudando a prevenir posibles eventos negativos que se puedan suscitar en la ejecución de los procesos diarios, para elaborar dicho plan se debe especificar una metodología capaz de analizar, y gestionar el riesgo de la información que se ajuste a las necesidades de la empresa (Chávez, Carrera, & Pazmay, 2017)

El uso de las TICs (Tecnologías de información y comunicación) constituye una herramienta que aporta beneficios a los médicos y pacientes; sin embargo, a medida que los hospitales recopilan información, el riesgo de fuga de información o incumplimiento de privacidad es alto, por lo que

se debería prestar atención a los problemas de seguridad de acuerdo a normas, leyes o regulaciones. Hay muchas preocupaciones legales en cuanto al uso y funcionamiento de las tecnologías, especialmente, si la red de Internet es su principal recurso, como por ejemplo en farmacias en línea, telemedicina, sistemas de información de salud, entre otras (Mazorra & Pacheco, 2018)

En Ecuador, con el fin de dar seguridad a la creciente implementación de las TI en las instituciones públicas y su penetración, la Secretaria Nacional de Administración Pública solicitó la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) como parte del Programa Nacional de Gobierno por Resultados (GPR), basada en la norma NTE INEN ISO/IEC 27000:2011, publicada por el Instituto Ecuatoriano de Normalización. Este esquema está siendo aplicado en las instituciones públicas dependientes de la administración central de forma obligatoria, con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de la información administrada y procesada, fundamentado en este contexto (Pazmiño Vallejo, 2015) realiza una investigación ejecutando una metodología planteada por el autor, utilizando herramientas tales como la entrevista y observación directa en tres instituciones del sector público, el objetivo es validar la metodología planteada y conocer el nivel de calidad de gestión de la seguridad de la información, con la finalidad encontrar las fortalezas y oportunidades de mejora de cada institución evaluada.

En la presente investigación se realiza un análisis de riesgos y se plantea el plan de tratamiento de riesgos de seguridad de la información, orientado a cubrir las necesidades de seguridad del departamento de Tecnologías de Información y Comunicación (DTICs) del Hospital General Isidro Ayora, aplicando el Estándar NTC ISO 27005, esta metodología es utilizada para gestionar los riesgos de forma documentada, basada en los objetivos de seguridad de la información, mantiene una estructura con directrices que siguen una guía de procesos para identificar las amenazas, evaluar las vulnerabilidades y probabilidades de ocurrencia y analizar los impactos, con la finalidad de presentar un plan de tratamiento adecuado(Kowask Bezerra, Alcántara Lima, Motta, & Piccolini, 2014).

La norma “ICONTEC NTC-ISO/IEC 27005. “Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información” fue publicada en julio de 2008 y presenta las directrices para la gerencia del riesgo de seguridad de información. Emplea los

conceptos de la norma ICONTEC NTC-ISO 27001:2005, que especifica los requisitos de sistemas de gestión de la seguridad de la información (Kowask Bezerra et al., 2014).

Esta norma describe todo el proceso necesario para la gestión del riesgo de seguridad de la información y las actividades necesarias para la perfecta ejecución de la gestión. Presenta prácticas para gestión del riesgo de la seguridad de la información. Las técnicas en ella descritas siguen el concepto, los modelos y los procesos globales especificados en la norma ICONTEC NTC-ISO/IEC 27001, además de presentar la metodología de evaluación y tratamiento de los riesgos requeridos por la misma norma (Kowask Bezerra et al., 2014).

Desarrollo

Para el plan de tratamiento de riesgos, se toma como referencia el proceso de gestión del riesgo de seguridad de la información, basado en la norma INEC NTC-ISO/ IEC 27005, donde se aborda el establecimiento del contexto, la evaluación del riesgo y por último el plan de tratamiento del riesgo, que se resumen en el siguiente gráfico.

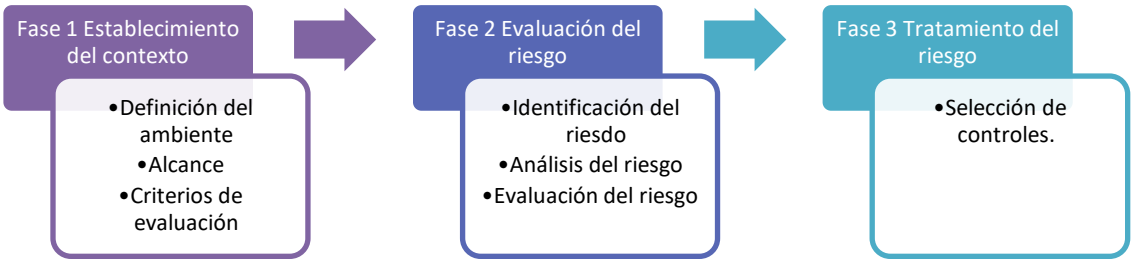

Ilustración 1. Estructura de análisis y tratamiento de riesgos, realizado en base la norma ISO/IEC 27005 (Cortes & Adolfo, 2017)

Fase 1. Establecimiento del contexto: Dentro del proceso, la definición de contexto es responsable de definir el ambiente, alcance y los criterios de evaluación. Esta etapa es esencial para el equipo que lleva a cabo la gestión del riesgo para conocer toda la información sobre la organización (Alemán Novoa & Rodríguez Barrera, 2015)

Criterios a ser definidos:

Probabilidad: representa las posibilidades de que ocurra un evento negativo.

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp. 362-379, ISSN: 2550 - 682X

Relevancia del activo: importancia del activo para los negocios/servicios de la organización.

Gravedad de las consecuencias: grado de las consecuencias sufridas por un activo al ser atacado o dejar de funcionar.

Impacto: índice para medir la cantidad de daños o costos a la organización causados por la ocurrencia de un evento de seguridad de la información.

Criterio del riesgo: define el nivel la escala de aceptación de los riesgos y depende de las políticas, objetivos y metas de la organización.

Fase 2. Evaluación del riesgo: Esta fase se subdivide en las siguientes etapas:

Identificación del riesgo: (identificación de activos, identificación de amenazas)

Análisis del Riesgo: (Identificación de vulnerabilidades, identificación de consecuencias)

Evaluación del riesgo: En esta fase se analiza los resultados obtenidos de la fase anterior, para tomar decisiones sobre el tratamiento que se les dará a los riesgos mediante una comparación de los niveles de riesgos identificados en la fase anterior con los criterios de evaluación y aceptación del riesgo.

Fase 3. Tratamiento de Riesgos: En esta fase se define el tratamiento que se va a dar a los riesgos como se muestra en el siguiente gráfico.

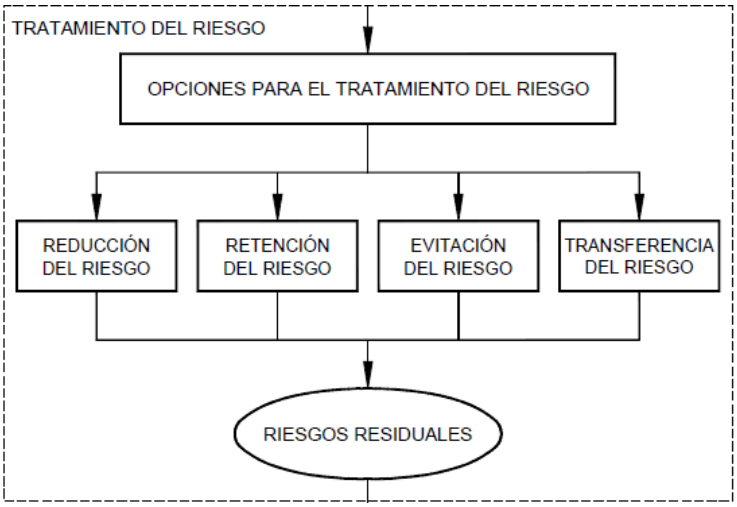

Ilustración 2.Tratamiento de Riesgos según la norma INEC ISO 27005

La ilustración 2, indica las diferentes opciones de tratamiento del riesgo, por las que se puede optar según el nivel de impacto del mismo.

Metodología

De acuerdo a los objetivos planteados, el estudio que se realizará es una investigación de tipo bibliográfica descriptiva, con un enfoque cualitativo y cuantitativo.

Los métodos utilizados en el desarrollo del trabajo de investigación son: La observación científica, utilizada para obtener información sobre la infraestructura tecnológica del hospital Isidro Ayora, logrando identificar las posibles amenazas y vulnerabilidades a las que están expuestos los activos informáticos que están a responsabilidad directa del departamento de TICs. **El método Analítico** – Sintético, que sirve para realizar un análisis de la información teórica sobre las metodologías existentes en el ámbito de seguridad de la información con la finalidad de realizar el plan de tratamiento de riesgos.

Método Inductivo – Deductivo, se utiliza para la generalización de la información y luego contrastarla con el problema de la falta de seguridad y la gestión de la información, para realizar el plan de tratamiento de riesgos atreves de la norma ISO 27005.

El "Plan de tratamiento de riesgos de seguridad de la información para el departamento de Tecnologías de Información y Comunicación del Hospital Regional Isidro Ayora-Loja" consta de las etapas:

- Análisis bibliográfico del estándar ISO 27005 de la gestión del riesgo, en lo relacionado a actividades correspondientes a las fases de: definición del contexto, evaluación del riesgo y tratamiento del riesgo que se aplicaran en el proyecto
- Levantamiento de información mediante la utilización de encuestas, análisis documental y entrevistas con la finalidad de determinar la situación actual de la infraestructura de TI en relación a la seguridad informática para realizar la definición del contexto
- Levantamiento de información para desarrollar la evaluación del riesgo.
- Desarrollar el plan de tratamiento de riesgo.

Las técnicas de investigación que se utilizaron fueron: La encuesta, para realizar la recopilación de la información sobre los servicios prestados por el departamento de TICs y verificar las falencias en los mismos, esta encuesta se la realizó al personal que labora en el departamento, como instrumento de investigación se utilizó el cuestionario para conocer los problemas que se presentan, que conocimientos tienen sobre la importancia de la seguridad de información y si

existen medidas de seguridad implementadas para resguardar la información en caso de que ocurra algún evento negativo.

La población utilizada fue todo el personal que labora en el departamento de TICs, debido a que son un total de 3 personas, se tomará como muestra todo el universo.

Resultados

Fase 1. Establecimiento del contexto

El hospital Provincial General Isidro Ayora de Loja (HIAL), es un hospital de segundo nivel de atención, según la tipología ministerial, El HIAL constituye un centro de referencia para pacientes provenientes de toda la provincia de Loja, la provincia de Zamora Chinchipe, parte alta de la provincia de El Oro, e incluso regiones fronterizas del norte del vecino país del Perú.

El hospital Isidro Ayora Loja, tiene la siguiente estructura organizacional:

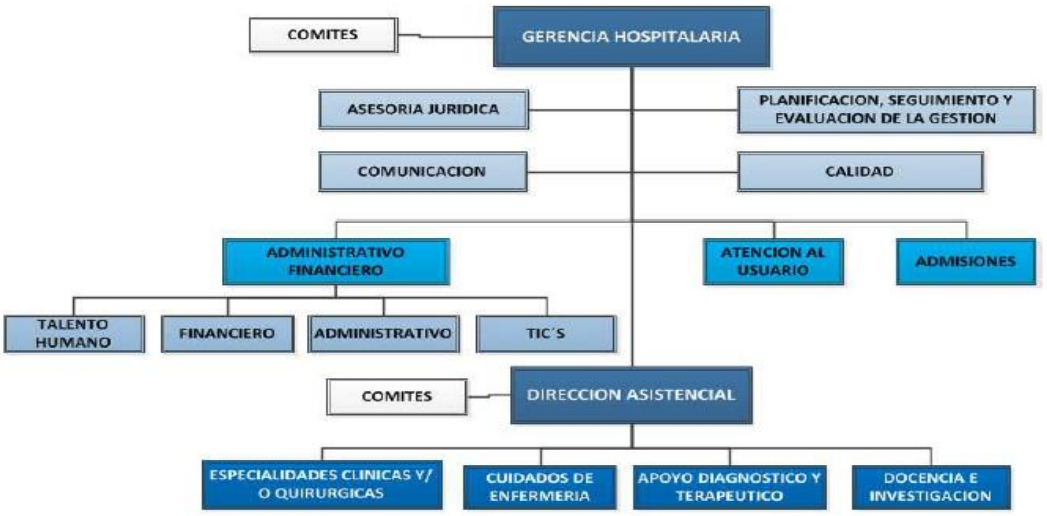

Ilustración 3 Estructura Organizacional Hospital Isidro Ayora Loja

El plan de tratamiento de riesgos, se realizó en el departamento de Tecnologías de la Información y Comunicación del Hospital Isidro Ayora, teniendo en cuenta los criterios de evaluación que nos proporciona la norma ISO 27005, el propósito es la preparación de un plan de respuesta a incidentes para realizar la valoración del riesgo y establecer un plan de tratamiento para al mismo a nivel de infraestructura.

Criterios de evaluación.

Para realizar el análisis de los riesgos se ha definido los siguientes criterios de evaluación:

Criterios de Probabilidad de ocurrencia de incidentes		
Nivel	**Definición**	**Peso**
Frecuente	Ha ocurrido por lo menos una vez al mes	4
Probable	Puede ocurrir cada 6 meses o menos. En los últimos seis meses ya se ha producido	3
Ocasional	En el último año se han producido al menos una vez	2
Remoto	En los últimos cinco años se ha producido al menos tres veces	1
Improbable	Nunca ocurrió	0

Tabla 1 Criterios de probabilidad de ocurrencia de incidentes

Relevancia de activos		
Nivel	**Definición**	**Peso**
Insignificante	Los daños en estos activos deja fuera de servicio a los sistemas por menos de 5 minutos	1
Baja	Los sistemas se quedaran fuera de servicio durante un máximo de 10 minutos.	2
Media	El daño en los activos deja los sistemas fuera de funcionamiento durante más de 15 minutos.	3
Alta	Los sistemas se quedaran fuera de funcionamiento por más de 30 minutos	4
Elevada	Daños irreparables a los equipos o instalaciones, perjuicios a nivel de reputación los sistemas quedan fuera de funcionamiento por las de 30 minutos	5

Tabla 2 Relevancia de activos

Severidad de las consecuencias		
Nivel	**Definición**	**Peso**
Insignificante	Los acontecimientos no afectan al negocio o no causan interrupción durante más de cinco minutos	1
Baja	Los acontecimientos afectan levemente al negocio, no causan interrupción durante más de 10 minutos	2
Media	Los acontecimientos afectan al negocio causan interrupción durante más 15 minutos	3
Alta	Los acontecimientos afectan al negocio causan interrupción durante más 20 minutos, causa reclamos severos en los usuarios	4
Elevada	Los acontecimientos afectan al negocio causan interrupción durante más 30 minutos, generan molestias en los usuarios, probabilidad de demandas, perdida de reputación	5

Tabla 3 severidad de consecuencias

Fase 2. Evaluación del riesgo.

En esta fase se realizan las siguientes actividades:

Identificación del riesgo: identificación de activos, identificación de amenazas.

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp. 362-379, ISSN: 2550 - 682X

Los activos del HIAL, que están bajo la responsabilidad del departamento se clasifican según la siguiente tabla:

CLASIFICACION	ACTIVO	RESPONSABLE
HARDWARE	Servidores	Departamento de TICs
	Computadores de escritorio	Departamento de TICs
	Portátiles	Departamento de TICs
	Equipos de videoconferencia.	Departamento de TICs
	Ups	Departamento de TICs
	Cámaras de seguridad	Departamento de TICs
SOFTWARE	Sistemas de seguridad	Departamento de TICs
	Sistemas Operativos	Departamento de TICs
	Sistemas de Gestión Hospitalaria	Departamento de TICs
	Sistemas de Antivirus	Departamento de TICs
REDES	Routers	Departamento de TICs
	Access point	Departamento de TICs
	Switch	Departamento de TICs
	Cableado Estructurado	Departamento de TICs
	Fibra óptica	Departamento de TICs

Tabla 4 Identificación de activos

Realizamos la identificación de amenazas y vulnerabilidades en los activos, dando la valoración correspondiente en base a los criterios del análisis realizado.

Activos	**Relevancia**	**Amenazas**	**Vulnerabilidades**	**Probabilidad de ocurrencia**	**Severidad de las consecuencias**
Servidores	**5**	-Errores de uso -Almacenamiento sin protección Copia no controlada -Destrucción del equipo o los Medios. Polvo, corrosión, congelamiento	-Falta de control de cambio con configuración Eficiente -Hurto de medios o documentos -Falta de esquemas de reemplazo periódico. -Susceptibilidad a la humedad, el polvo y la suciedad	**3**	**5**
Computadores de escritorio	**3**	-Errores de uso	-Falta de control de cambio con configuración Eficiente	**2**	**2**

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp. 362-379, ISSN: 2550 - 682X

Portátiles	**2**	-Errores de uso	-Falta de control de cambio con configuración Eficiente	**2**	**2**
Equipos de videoconferencia.	**3**	-Destrucción del equipo o los Medios. Polvo, corrosión congelamiento	-Susceptibilidad a la humedad, el polvo y la suciedad	**2**	**2**
Ups	**5**	-Destrucción del equipo o los Medios. Polvo, corrosión congelamiento	-Susceptibilidad a la humedad, el polvo y la suciedad	**4**	**5**
Cámaras de seguridad	**3**	-Destrucción del equipo o los Medios. Polvo, corrosión congelamiento	-Susceptibilidad a la humedad, el polvo y la suciedad	**3**	**2**
Sistemas de seguridad	**3**	-Abuso de los derechos	-Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	**2**	**2**
Sistemas Operativos	**4**	-Falsificación de derechos	-Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	**3**	**4**
Sistemas de Gestión Hospitalaria	**5**	-Procesamiento ilegal de datos -Error de uso -Manipulación con software	-Falta de copias de respaldo -Habilitación de servicios innecesarios -Configuración incorrecta de parámetros	**3**	**5**
Sistemas de Antivirus	**2**	-Manipulación con software	-Descarga y uso no controlados de software	**2**	**2**
Routers	**2**	-Espionaje remoto	-Arquitectura insegura de la red	**3**	**4**
Access point	**3**	-Saturación del sistema de información	-Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	**4**	**5**
Switch	**1**	-Espionaje remoto	-Arquitectura insegura de la red	**2**	**2**

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp. 362-379, ISSN: 2550 - 682X

Cableado Estructurado	**2**	-Falla del equipo de telecomunicaciones	-Conexión deficiente de los cables.	**3**	**4**
Fibra óptica	**3**	-Falla del equipo de telecomunicaciones	-Conexión deficiente de los cables.	**1**	**3**

Tabla 5 Amenazas y vulnerabilidades tomados de la norma ISO 27005(Chávez et al., 2017)

Fase 3. Tratamiento de Riesgos

Después de la identificación de amenazas y vulnerabilidades, se realiza la tabla de tratamiento del riesgo

Valores	**Nivel del riesgo**	**Acciones necesarias**
13-15	Alto	Aplicación de políticas de seguridad con atención prioritaria y controlada por los directivos principales.
10-12	Medio Alto	Se necesita medidas de seguridad controladas por el jefe de departamento de TICS
7-9	Medio	Se necesita implementar políticas de seguridad en un tiempo prudente
4-6	Medio Bajo	Se acepta el riesgo, dejando a responsabilidad de los técnicos el seguimiento
0-3	Bajo	Se hace el control de manera correcta.

Tabla 6 Escala para medir el riesgo
Elaborado por el autor

Se realiza la tabla de la aplicación del cálculo de los riesgos sobre los activos.

Activos	**Amenazas**	**Vulnerabilidades**	**Probabilidad de ocurrencia**	**Severidad de las consecuencias**	**Relevancia**	**Valor del riesgo**
Servidores	-Errores de uso -Almacenamiento sin protección -Copia no controlada -Destrucción del equipo o los Medios. Polvo, corrosión, congelamiento	-Falta de control de cambio con configuración Eficiente -Hurto de medios o documentos -Falta de esquemas de reemplazo periódico. -Susceptibilidad a la humedad, el polvo y la suciedad	**3**	**5**	**5**	**13**

Computadores de escritorio	-Errores de uso	-Falta de control de cambio con configuración Eficiente	**2**	**2**	**3**	**7**
Portátiles	-Errores de uso	-Falta de control de cambio con configuración Eficiente	**1**	**1**	**1**	**3**
Equipos de videoconferencia.	-Destrucción del equipo o los Medios. Polvo, corrosión congelamiento	-Susceptibilidad a la humedad, el polvo y la suciedad	**2**	**2**	**3**	**7**
Ups	-Destrucción del equipo o los Medios. Polvo, corrosión congelamiento	-Susceptibilidad a la humedad, el polvo y la suciedad	**4**	**5**	**5**	**14**
Cámaras de seguridad	-Destrucción del equipo o los Medios. Polvo, corrosión congelamiento	-Susceptibilidad a la humedad, el polvo y la suciedad	**3**	**2**	**3**	**8**
Sistemas de seguridad	-Abuso de los derechos	-Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	**2**	**2**	**3**	**7**
Sistemas Operativos	-Falsificación de derechos	-Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	**3**	**4**	**4**	**11**
Sistemas de Gestión Hospitalaria	-Procesamiento ilegal de datos -Error de uso -Manipulación con software	-Falta de copias de respaldo -Habilitación de servicios innecesarios -Configuración incorrecta de parámetros	**3**	**5**	**5**	**13**
Sistemas de Antivirus	-Manipulación con software	-Descarga y uso no controlados de software	**2**	**2**	**2**	**6**
Routers	-Espionaje remoto	-Arquitectura insegura de la red	**3**	**4**	**2**	**9**
Access point	-Saturación del sistema de información	-Gestión inadecuada de la red (capacidad de	**4**	**5**	**3**	**12**

		recuperación del enrutamiento)				
Switch	- Espionaje remoto	-Arquitectura insegura de la red	**2**	**2**	**1**	**5**
Cableado Estructurado	-Falla del equipo de telecomunicaciones	-Conexión deficiente de los cables.	**3**	**4**	**2**	**9**
Fibra óptica	-Falla del equipo de telecomunicaciones	-Conexión deficiente de los cables.	**2**	**3**	**3**	**8**

Tabla 7 Calculo de los riesgos con respecto a los activos
Elaborado por el autor

Una vez realizada el análisis de riesgo se debe dar el tratamiento a los riesgos con mayor relevancia por parte del departamento de TICs del Hospital Isidro Ayora, estableciendo que los niveles de riesgo alto y medio alto deben ser tratados inmediatamente a través de la aplicación de un plan de seguridad que contenga políticas necesarias para la mitigación de estos riesgos, además de aceptar los otros niveles por no presentar peligro a la continuidad del negocio, esto no significa que no se de tratamiento, si no que se hará de forma paulatina hasta lograr que el riesgo sea mínimo.

Conclusiones

- El análisis y tratamiento de riesgos permitió ver las amenazas existentes a nivel de infraestructura en el Departamento de TICs del Hospital Isidro Ayora Loja, y la exposición que tienen los activos a las distintas vulnerabilidades que afecta directamente a la disponibilidad, confidencialidad e integridad de la información.
- Actualmente no existen políticas tratamiento de riesgos que ayuden a recuperarse en caso de un evento negativo.
- En el departamento de TICs hace falta personal de seguridad de la información, que se encargue de la gestión de riesgos y de que las políticas de seguridad que se implementen se cumplan en todas las áreas de la institución.
- La infraestructura de la institución, posee debilidades en cuanto a políticas y controles de seguridad, muy importantes para la protección de la información, lo que significa que se encuentra vulnerable ante cualquier ataque informático, siendo de gran importancia la implementación de un SGSI.

Referencias

1. Alemán, H., & Rodríguez, C. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones e Investigación, 9, 73. https://doi.org/10.22490/25394088.1435

2. Alemán Novoa, H., & Rodríguez Barrera, C. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones e Investigación, 9, 73. https://doi.org/10.22490/25394088.1435

3. Alexandra Aracely Enríquez Collaguazo, M. S. K. N. P. (2018). MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE SALUD, BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013 APLICADA A LA CLÍNICA MÉDICA (Vol. 10).

4. Andrei, H., Tapiero, T., & Ramirez, H. S. (2017). Hawin andrei tapiero tapiero heiner suarez ramirez. 0–100.

5. Chávez, S., Carrera, F., & Pazmay, G. (2017). PLAN DE SEGURIDAD INFORMÁTICO BASADO EN EL ESTÁNDAR RFC-2196 Y LA GESTIÓN ADMINISTRATIVA DE LOS SERVICIOS DE SALUD DEL DISTRITO 12D05 VINCES.

6. Esteban Crespo Martínez, P., & Rodrigo Salgado Arteaga, F. (n.d.). Gestión Del Riesgo Informático Aplicable a Mpymes. Retrieved from http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/26105/1/Tesis.pdf

7. Fernanydez, P. I. (2017). Universidad Nacional Tecnológica De Lima Sur. Universidad Nacional Tecnològica de Lima Sur, 1, 1–81. Retrieved from http://repositorio.untels.edu.pe/handle/UNTELS/166

8. Kowask Bezerra, E., Alcántara Lima, F., Motta, A. C., & Piccolini, J. D. B. (2014). Gestión del riesgo de las TI NTC 27005. 217.

9. Mazorra, E., & Pacheco, R. (2018). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información ISO/IEC 27001: Para soporte de áreas de admisión y atención de un hospital público. 20.

10. Pazmiño Vallejo, L. M. (2015). Calidad de la gestión en la seguridad de la información basada en la norma ISO/IEC 27001, en instituciones públicas, en la ciudad de Quito D.M.

Pontificia Universidad Católica Del Ecuador. Retrieved from http://repositorio.puce.edu.ec/handle/22000/10177

11. Ramirez, A., & Ortiz, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56–66. https://doi.org/10.14483/23448393.3833

References

1. Alemán, H., & Rodríguez, C. (2015). Methodologies for risk analysis in the sgsi. Publications and Research, 9, 73. https://doi.org/10.22490/25394088.1435
2. Alemán Novoa, H., & Rodríguez Barrera, C. (2015). Methodologies for risk analysis in the sgsi. Publications and Research, 9, 73. https://doi.org/10.22490/25394088.1435
3. Alexandra Aracely Enriquez Collaguazo, M. S. K. N. P. (2018). INFORMATION SECURITY MANAGEMENT MODEL FOR HEALTH INSTITUTIONS, BASED ON ISO 27799: 2008, ISO / IEC 27005: 2008 AND ISO / IEC 27002: 2013 APPLIED TO THE MEDICAL CLINIC (Vol. 10).
4. Andrei, H., Tapiero, T., & Ramirez, H. S. (2017). Hawin Andrei Tapiero Tapiero Heiner Suarez Ramirez. 0–100.
5. Chavez, S., Carrera, F., & Pazmay, G. (2017). COMPUTER SECURITY PLAN BASED ON THE RFC-2196 STANDARD AND THE ADMINISTRATIVE MANAGEMENT OF DISTRICT HEALTH SERVICES 12D05 VINCES.
6. Esteban Crespo Martínez, P., & Rodrigo Salgado Arteaga, F. (n.d.). Computer Risk Management Applicable to Mpymes. Retrieved from http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/26105/1/Tesis.pdf
7. Fernanydez, P. I. (2017). National Technological University of South Lima. National Technological University of South Lima, 1, 1–81. Retrieved from http://repositorio.untels.edu.pe/handle/UNTELS/166
8. Kowask Bezerra, E., Alcántara Lima, F., Motta, A. C., & Piccolini, J. D. B. (2014). IT risk management NTC 27005. 217.
9. Mazorra, E., & Pacheco, R. (2018). Methodology for the implementation of an Information Security Management System ISO / IEC 27001: For support of admission and care areas of a public hospital. twenty.

10. Pazmiño Vallejo, L. M. (2015). Quality of information security management based on ISO / IEC 27001, in public institutions, in the city of Quito D.M. Pontifical Catholic University of Ecuador. Retrieved from http://repositorio.puce.edu.ec/handle/22000/10177
11. Ramirez, A., & Ortiz, Z. (2011). Technological Risk Management based on ISO 31000 and ISO 27005 and their contribution to business continuity. Engineering, 16 (2), 56–66. https://doi.org/10.14483/23448393.3833

Referências

1. Alemán, H. e Rodríguez, C. (2015). Metodologias para análise de risco no sgsi. Publicações e Pesquisa, 9, 73. https://doi.org/10.22490/25394088.1435
2. Alemán Novoa, H. e Rodríguez Barrera, C. (2015). Metodologias para análise de risco no sgsi. Publicações e Pesquisa, 9, 73. https://doi.org/10.22490/25394088.1435
3. Alexandra Aracely Enriquez Collaguazo, M.S.N.P. (2018). MODELO DE GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO PARA INSTITUIÇÕES DE SAÚDE, COM BASE NA ISO 27799: 2008, ISO / IEC 27005: 2008 E ISO / IEC 27002: 2013 APLICADO À CLÍNICA MÉDICA (Vol. 10).
4. Andrei, H., Tapiero, T., & Ramirez, H. S. (2017). Andrei, Hawier Andrei, Tapiero e Heiner Suarez Ramirez. 0-100.
5. Chavez, S., Carrera, F., & Pazmay, G. (2017). PLANO DE SEGURANÇA DO COMPUTADOR BASEADO NO PADRÃO RFC-2196 E NO GERENCIAMENTO ADMINISTRATIVO DOS SERVIÇOS DE SAÚDE DISTRITOS 12D05 VINCES.
6. Esteban Crespo Martínez, P. e Rodrigo Salgado Arteaga, F. (n.d.). Gerenciamento de risco de computador aplicável a Mpymes. Disponível em http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/26105/1/Tesis.pdf
7. Fernanydez, P. I. (2017). Universidade Tecnológica Nacional do Sul de Lima. Universidade Tecnológica Nacional do Sul de Lima, 1, 1-81. Recuperado em http://repositorio.untels.edu.pe/handle/UNTELS/166
8. Kowask Bezerra, E., Alcântara Lima, F., Motta, A. C., & Piccolini, J. D. B. (2014). Gerenciamento de riscos de TI NTC 27005. 217.
9. Mazorra, E., & Pacheco, R. (2018). Metodologia para a implementação de um Sistema de Gerenciamento de Segurança da Informação ISO / IEC 27001: Para apoio às áreas de admissão e assistência de um hospital público. 20

10. Pazmiño Vallejo, L.M. (2015). Qualidade do gerenciamento da segurança da informação com base na ISO / IEC 27001, em instituições públicas, na cidade de Quito D.M. Pontifícia Universidade Católica do Equador. Disponível em http://repositorio.puce.edu.ec/handle/22000/10177

11. Ramirez, A. e Ortiz, Z. (2011). Gerenciamento de risco tecnológico baseado nas normas ISO 31000 e ISO 27005 e sua contribuição para a continuidade dos negócios. Engineering, 16 (2), 56–66. https://doi.org/10.14483/23448393.3833