FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN HOSPITAL NACIONAL, 2017

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

AUTOR:

MIGUEL ANGEL AYALA MEDRANO

ASESOR:

Dr. ERNESTO FLORES CISNEROS

LÍNEA DE INVESTIGACIÓN:

AUDITORÍA DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

LIMA - PERÚ

2017

Presidente

Secretario

Vocal

DEDICATORIA

Dedico el presente trabajo:

A Dios, a mi familia en especial a mis padres por su ayuda en todo momento, esposa e hijo por su amor.

Los cuales me han enseñado a seguir adelante con logros y tropiezos, con honradez y trabajo.

AGRADECIMIENTO

A la Universidad César Vallejo por guiarme en todo momento de mi carrera, especialmente a mi asesor por brindarme su conocimiento y su apoyo en todo momento para el desarrollo de la presente investigación. A mis amigos y personas que me alentaron para la culminación de la presente investigación.

DECLARACIÓN DE AUTENTICIDAD

Yo, Miguel Angel Ayala Medrano con DNI N° 10053719, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Asimismo, declaro también bajo juramento que todos los datos e información que se presenta en la presente tesis son auténticos y veraces.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a los dispuesto en las normas académicas de la Universidad César Vallejo.

Lima, 16 de Setiembre del 2017.

Miguel Angel Ayala Medrano

PRESENTACIÓN

Señores miembros del jurado:

En cumplimiento de las normas establecidas en el Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada “SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN HOSPITAL NACIONAL, 2017” la misma que someto a vuestra consideración y espero que cumpla con todos los requisitos de aprobación para obtener el título profesional de ingeniero de sistemas.

Esta investigación tiene como objetivo determinar el efecto de la implementación de la metodología del Sistema de Gestión de Seguridad de la Información (SGSI) para el proceso de gestión del riesgo en el Hospital Nacional de Policía “Luis N. Sáenz”, Jesús María, la cual consta de siete capítulos; el capítulo I plantea una introducción describiendo la realidad problemática, trabajos previos, teorías relacionadas al tema, formulación del problema, justificación del estudio, hipótesis y objetivos que lo guían, el capítulo II describe y explica el diseño de investigación, las variables de estudio y su operacionalización. Adicionalmente se explica la población, la muestra y se detalla las técnicas e instrumentos para la recogida y procesamiento de la información, la validación y confiabilidad del instrumento, los métodos de análisis de datos y aspectos éticos de la investigación, el capítulo III se refiere a los resultados de la investigación así como a la comprobación de la hipótesis, en el capítulo IV se presenta y se discuten los resultados de la investigación, en el capítulo V se presentan las conclusiones, en el capítulo VI se presentan las recomendaciones, en el capítulo VII se detallan las referencias bibliográficas utilizadas y finalmente se completa con los anexos.

Esperamos señores miembros del jurado que la presente investigación se ajuste a los requerimientos establecidos y que este trabajo de origen a posteriores estudios.

El autor

ÍNDICE GENERAL

INDICE DE TABLAS

INDICE DE GRÁFICOS

INDICE DE ANEXOS

RESUMEN

La presente investigación lleva por título “Sistema de Gestión de Seguridad de Información para mejorar el proceso de gestión del riesgo en un Hospital Nacional, 2017”, tuvo como objetivo general evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo de un Hospital Nacional. Para la variable independiente, según Areitio, J (2008)[1] el sistema de gestión de seguridad de la información es un sistema que se basa en el enfoque de los riesgos del negocio y que evalúa, monitorea y optimiza la seguridad de la información; para la variable dependiente, Peltier, T (2014)[2] define el proceso de gestión de riesgos, en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable.

La investigación fue de tipo aplicada, el diseño de investigación fue pre experimental, como población y muestra fueron tomados todos los activos críticos de información que intervienen en el proceso de gestión del riesgo en el Hospital Nacional. Para la recolección de datos fue mediante la aplicación del instrumento Ficha de Observación. En cuanto a los métodos de análisis de datos, para la determinar la normalidad de la data, se realizó con el estadístico Shapiro Wilks, el análisis y diferenciación de los resultados en fase pre test y post test, se realizó mediante el uso de la estadística descriptiva, asimismo, el método estadístico utilizado para la validación de las hipótesis fue la prueba estadística de Wilcoxon para los indicadores Nivel de Riesgo y el Número de Controles Aplicados.

Finalmente se concluye que la implementación del sistema de gestión de seguridad de la información mejora el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”.

PALABRAS CLAVE: Sistema de gestión de seguridad de la información, proceso de gestión del riesgo, magerit

[1] AREITIO, Javier. Seguridad de la información: redes, informática y sistemas de información. España: Ediciones Paraninfo, 2008. p. 24

[2] PELTIER, Thomas. Information Security Fundamentals. 2da. Edición. Florida: CRC Press, 2014. p. 67

ABSTRACT

The present investigation is entitled "Information Security Management System to improve the process of risk management in a National Hospital, 2017", had as general objective to evaluate the way in which the implementation of the Information Security Management System Influences the risk management process of a National Hospital. For the independent variable, according to Areitio (2008), the information security management system is a system that is based on the business risk approach and which evaluates, monitors and optimizes information security; For the dependent variable, Peltier (2014) defines the process of risk management, identifying risks, assessing the likelihood of them occurring, and then taking steps to reduce all risks to an acceptable level.

The research was of applied type, the research design was pre-experimental, as population and sample were taken all critical information assets involved in the process of risk management at the National Hospital. For the collection of data was through the application of the instrument Observation Sheet. As for the data analysis methods, to determine the normality of the data, we performed with the statistic Shapiro Wilks, the analysis and differentiation of the results in pre and post test phase, was performed using the statistic The statistical method used for the validation of the hypotheses was the Wilcoxon statistical test for the Risk Level indicators and the Number of Applied Controls.

Finally, it is concluded that the implementation of the information security management system improves the risk management process in the National Hospital PNP "Luis N. Sáenz"

KEYWORDS: Information security management system, Risk management process, magerit

CAPÍTULO I
INTRODUCCIÓN

I. INTRODUCCIÓN

1.1. Realidad problemática

Fueron en Europa los intentos iniciales para controlar las nuevas formas de delito informático que afectaron la seguridad de la información en las empresas, tales esfuerzos fueron la creación de marcos legales y jurídicos de protección en el uso de tecnologías, como la Ley Orgánica 15/99 de Protección de Datos de carácter Personal (LOPD), Ley 34/2002 de Servicios de la Sociedad de la Información y Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Por tanto, la seguridad de la información ha sido la principal preocupación que se fue extendiendo por todo el globo, y se iniciaron la conceptualización y su entorno para lograr tratarla. Muchos autores lo hicieron, entre algunos: Phillips, G (2013)[3] La seguridad absoluta no existe, la seguridad es un concepto asociado a la certeza, al conocimiento claro y seguro que tengamos de algo, esto no implica necesariamente que tenga veracidad o exactitud. Bradanovic, T (s.f.)[4], Al estar dentro de una extensión de la certeza, el elemento de riesgo siempre está presente así tomemos medidas para reducirlas o anularlas, por lo que debemos expresarnos en niveles de seguridad.

Fonseca, G (2012)[5] Otra concepción que debemos tener siempre presente, es que el activo más significativo para una organización es la información, por lo que se debe tener especial consideración y conciencia de la importancia que tiene la información para una empresa; igual importancia tendrá conocer qué información es útil. El cuidado de la información no es fácil, se requiere muchos esfuerzos para mantener su integridad, confidencialidad y disponibilidad.

Desde los inicios de la computación, luego con el trabajo compartido en red y ahora más aún, con la computación móvil y servicios en la nube, se incrementan los inconvenientes provenientes de la seguridad de la información, han cambiado y

[3] PHILLIPS, Glenn. *Mission Impossible: 4 Reasons Compliance Is Impossible* [en línea]. 2013. Párr. 4

[4] BRADANOVIC, Tomás. *Conceptos básicos de Seguridad Informática* [en línea]. s.f. Párr. 1.

[5] FONSECA, Guillermo. *La información, el activo mas importante de cualquier organización* [en línea]. 2012 [fecha de consulta: 12 Enero 2016]. Disponible en: < https://guillermofonseca.wordpress.com/2012/04/18/la-informacion-el-activo-mas-importante-de-cualquier-organizacion/>. Párr. 3

evolucionan. Las organizaciones tienen que ir adaptándose a nuevos requerimientos técnicos de protección contra ataques cada vez más complejos, en igual proporción deberán aumentar sus esfuerzos en brindar soluciones, sin olvidar que el factor humano es el principal riesgo, es decir a nivel interno.

El interés de actuar en la seguridad de la información es especialmente necesaria y atractiva en instituciones de salud, ya que la protección de la información que éstas manejan es crítica. Se debe tener cuidado cuando se administran los datos e información relacionada a pacientes, para garantizar un adecuado servicio de atención de salud y proteger su intimidad y privacidad personal. El documento sanitario en el que convergen todos los elementos citados, como datos personales, demográficos, de salud, derechos, y prestación asistencial es la historia clínica. Por ello, la importancia de la implementación de la metodología del Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar el proceso de gestión del riesgo, por consiguiente, generar un cambio en una institución médica que se traducirá en mejoras en los servicios de atención de salud hacia los pacientes.

La Dirección de Salud de la Policía Nacional está encargada de promover estilos de vida saludable en bienestar del personal policial y familiares. Uno de sus órganos de ejecución de más alta especialización es el Hospital Nacional de la Policía Nacional “Luis N. Sáenz” que brinda atención de servicios de salud a los efectivos policiales y sus familiares con derecho, orientándose a la atención del más alto nivel de complejidad de los problemas de salud, trabajando coordinadamente con los Establecimiento de Salud (EE.SS) de menor nivel, como hospitales regionales, policlínicos y postas médicas; esto permite incrementar la eficiencia en sus procesos, produciendo mejores resultados en menor tiempo, con mayor calidad y alto ahorro económico, asimismo, realiza actividades de recuperación y rehabilitación, así como también actividades preventivo promocionales, de la misma forma actividades de enseñanza a nivel de pre y post grado.

Por otro lado, el Hospital Nacional, cuenta con un Sistema Informático de Gestión de Salud que administra la información de sus pacientes, durante el proceso de atención de salud. Para ello, la Unidad de Telemática, cuenta con un Centro de Datos que opera los servidores, soporte que contiene las bases de datos en un ambiente de producción que aún no ostenta mecanismos de seguridad.

Actualmente la Unidad de Telemática del Hospital Nacional PNP “Luis N. Sáenz”, no cuenta con una buena política de seguridad de información para sus procesos de gestión del riesgo, por lo que existe un gran peligro de seguridad, en mantener la confidencialidad del historial médico de los pacientes y de la información médica de los profesionales de la salud. La información altamente sensible es hallada en la historia clínica de pacientes, administrando información y conocimiento médico, que debe estar debidamente protegido para poder darle una explotación correcta sin poner en riesgo la calidad y fiabilidad de la información.

Los procesos de gestión del riesgo de un hospital, implican los riesgos propiamente dichos de la seguridad de la información, que abarcan desde el uso indebido de la data de pacientes, ataque de terceros a los sistemas de información de salud que podría provocar un impacto potencial, peligro a la integridad y confidencialidad de la información, además de su disponibilidad para la atención de salud, pérdida de información por robo o sustracción en el sistema de almacenamiento o a consecuencia de un desastre natural. La carencia o nula implementación de disposiciones, controles y procedimientos pertinentes, conlleva a un escenario que perjudique a la información, dejando al hospital en un contexto de pérdida o distorsión de información, afectación de la credibilidad o conllevar a un proceso civil o penal por vulnerabilidad de la protección de datos personales. Por tales afirmaciones, en la presente investigación se determinaron la evaluación el riesgo y el tratamiento del riesgo, mediante la implementación de la metodología SGSI en el proceso de gestión del riesgo del hospital, elevando el grado de seguridad y justificando su implementación.

Una mención especial, se hace sobre la Ley de Protección de Datos Personales (Ley N° 29733), que establece que toda información relativa a una persona debe tratarse como un dato personal, por lo que el objeto de la mencionada ley es el de garantizar y proteger el derecho fundamental a la privacidad de los datos personales, por tanto, debe dársele un tratamiento adecuado. Asimismo, la ley ha determinado una protección muy especial para los datos sensibles, incluyendo a la información relacionada a la salud de las personas. La norma también precisa las obligaciones que debe tener el titular de los bancos de datos personales, entre los que mencionan los siguientes: solicitar al titular un consentimiento expreso previo para realizar el tratamiento de información (salvo las

excepciones); acopiar datos personales necesarios y pertinentes que lo exprese la ley, de acuerdo a la finalidad de la institución, el titular debe tener la posibilidad de ejercer sus derechos según la información que brinda la institución por tanto ésta debe facilitarlo, gestionar la inscripción en el Registro Nacional de Protección de Datos Personales y por último, lo más importante preservar la confidencialidad de los datos personales.

1.2. Trabajos previos

1.2.1. Antecedentes nacionales

INCA Salas Rocío Milagros. Implementación del Sistema de Gestión de Seguridad de la Información en el Proceso de Administración de Base de Datos del Hospital Municipal Los Olivos. Tesis (Título profesional de ingeniero de sistemas). Lima, Perú: Universidad César Vallejo. Facultad de Ingeniería. (2012. p.28).

Dicha tesis señaló como objetivos reducir los riesgos implementando la metodología del Sistema de Gestión de Seguridad de la Información, mediante la aplicación del estándar ISO 27001 conjuntamente con la metodología Magerit II; la investigación fue de tipo aplicada con un diseño de pre experimental, teniendo como población y muestra los activos de información determinados por la investigadora como críticos, utilizándose la observación directa mediante la aplicación de una ficha de observación.

Tuvo como conclusiones que al implementar la metodología propuesta se redujo el nivel de riesgo en un 23.329%, los controles aplicados se incrementaron un 44.88% y se mejoró las opciones de tratamiento de en un 57.45%.

Los procedimientos desarrollados mediante la metodología SGSI fueron de valioso aporte, cuyos resultados sirvieron como contrastación con la presente investigación.

ALIAGA Flores Luis Carlos. Diseño de un Sistema de Gestión de Seguridad de la Información para un instituto educativo. Tesis (Título profesional de ingeniero informático) Lima, Perú: Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. (2013 p.3).

Dicha tesis precisó como objetivo el diseño de un SGSI basado en ISO/IEC 27001:2005 e ISO/IEC 27005:2005, con la adopción del framework de negocios Cobit, la investigación fue de tipo aplicada, tuvo como población los activos de información al que se realizaron el análisis de riesgos y su tratamiento respectivo.

Concluyó en que no hay un compromiso en las entidades educativas respecto a la seguridad de la información y presentó un modelo de Declaración de Aplicabilidad en la que estableció la utilidad de los controles para mitigar o reducir el riesgo.

La metodología de aplicabilidad de controles constituyó un valioso aporte y referencia para la presente investigación.

BARRANTES Porras Carlos Eduardo y HUGO Herrera Javier Roberto. Diseño e implementación de un sistema de gestión de seguridad de la información en procesos tecnológicos. Tesis (Título profesional de ingeniero de computación y sistemas). Lima, Perú: Universidad de San Martín de Porres. Facultad de Ingeniería y Arquitectura. (2012. p.3).

Dicha tesis indica como objetivo principal reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la Gerencia de Tecnología que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos, la investigación fue de tipo aplicada, la metodología para la gestión del proyecto fue PMBOK y para la gestión de riesgos Magerit.

Concluyó entre otras, que aún después de implementar el SGSI, en el futuro se presentarán más activos de información, amenazas y vulnerabilidades, por tanto, mayores riesgos, a los que se tiene que estar preparado para actuar en estos nuevos escenarios.

El plan de tratamiento de riesgos propuesto por los investigadores, fue de valioso aporte a la presente investigación debido a su rigurosidad y detalle empleado.

AMPUERO Chang Carlos Enrique. Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Tesis (Título profesional

de ingeniero informático). Lima, Perú: Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. (2011. p.4).

Precisó como objetivos cumplir la circular G-140 dictada por la Superintendencia de Banca, Seguros y AFP, para uso de todas las instituciones peruanas fiscalizadas por ese organismo y que deben contar con una planificación en cuanto a la seguridad de la información; la investigación fue de tipo aplicada, la metodología fue la aplicación de la norma ISO 27001.

El investigador concluyó que para brindar un nivel aceptable de seguridad se debe utilizar estándares y buenas prácticas reconocidos mundialmente como son Cobit versión 4.1, la norma ISO/IEC 27001 y el ISO/IEC 27002, estas 2 últimas en sus versiones del 2005.

Esta investigación contribuyó en el presente proyecto por la aplicación de la metodología Cobit dentro del marco del ISO 27001, para ampliar la perspectiva del investigador sobre otra metodología para la gestión seguridad de la información.

CÁCERES Serrano Joan Manuel. Sistema de gestión de seguridad de la información en el proceso de gestión de incidencias de seguridad de la información en una entidad bancaria. Tesis (Título profesional de ingeniero de Sistemas). Lima, Perú: Universidad César Vallejo. Facultad de Ingeniería. (2015. p.12).

Señala como objetivos determinar el nivel de eficacia del reporte de los incidentes de seguridad de la información y el porcentaje promedio de incidentes de seguridad atendidos dentro del tiempo establecidos en el SLA, ambos para el proceso de control de incidencias de seguridad de la información en la entidad bancaria, la investigación fue de tipo aplicada con un diseño de pre experimental, teniendo como población y muestra los activos de información, utilizando el instrumento de recolección de datos la Ficha de Registro.

Concluyó que el nivel de eficacia en el reporte de incidentes de seguridad de la información mejoró de 26,73% (pre test) a 66.86% (post test), asimismo, el porcentaje de incidentes atendidos dentro del tiempo establecido en el SLA, mejoró de 25.40% (pre test) a 82.13% (post test), determinando en su conclusión general,

que la implementación del sistema de gestión de seguridad de la información mejora el proceso de control de incidencias de seguridad de la información en la entidad bancaria.

Esta investigación aportó ampliamente a la presente, por su carácter riguroso en cuanto a la determinación del análisis estadístico descriptivo e inferencial.

1.2.2. Antecedentes internacionales

BASTIDAS Paruma Henry Eduardo, LÓPEZ Ortiz Iván Arturo y PEÑA Hidalgo Hernando José. Análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del Hospital Susana López de Valencia de la Ciudad de Popayán. Trabajo de especialización en Seguridad Informática. Bogotá, Colombia: Universidad Nacional Abierta y a Distancia. (2014. p.21).

Consignó como objetivo principal, el diseño de mejoras a los niveles de seguridad informática con la aplicación del proceso de evaluación y análisis de riesgos de seguridad de la información en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E de la ciudad de Popayán, fue una investigación de tipo aplicada.

Concluyó, entre otras, que la aplicación de la norma ISO 27001, en procesos sensibles que se manejan en el Hospital se establecen las bases para acreditar la seguridad y disponibilidad de los servicios que ofrece la Institución.

La metodología utilizada enmarcado en la norma ISO 27001 para una institución de salud, aportó una substancial contribución con la presente investigación por darle un enfoque orientado a optimizar la protección de información en el campo de la salud.

MOLINA Miranda María Fernanda. Propuesta de un Plan de Gestión del Riesgo en Tecnología aplicado en la Escuela Superior Politécnica del Litoral. Tesis (Título de máster). Madrid, España: Universidad Politécnica de Madrid. (2015. p.3).

Tuvo como objetivos determinar el alcance del plan de riesgos, definir los activos y amenazas, proponer salvaguardas para minimizar el riesgos y contrastar el riesgo e impacto actual y el residual, la investigación fue de tipo aplicada; una entre varias de las conclusiones se refiere a que la gestión de riesgos en una empresa debería considerarse como un proceso intrínseco, ya que si no se conoce el riesgo de los activos de información, no se podrá evitar las amenazas y sus consecuencias.

El investigador determinó la metodología Magerit para el análisis de riesgo en tecnologías de información, procedimientos que sirvieron para la presente investigación, ya que justamente será el método a utilizar.

TIBAQUIRA Cortes Yesid Alberto. Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en el estándar ISO/IEC 27035 y norma ISO/IEC 27005. Trabajo de Investigación (Título de especialista en Seguridad Informática). Bogotá, Colombia: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. (2015 p.14).

Tuvo como objetivo específico, entre otros, definir la metodología, política y procesos de gestión riesgos teniendo como base la ISO/IEC 27035 para los incidentes de seguridad identificados en la plataforma SIEM (Gestión de incidentes en seguridad de la información) 2014, el tipo de investigación fue aplicada.

El investigador concluyó que teniendo como base las normas ISO 27035:2011 e ISO 27005:2008 se logra construir un modelo íntegro que abarca la gestión de incidentes y la gestión de riesgos asociada a estos incidentes.

Ésta adopción de un estándar ISO 27005 constituyó un aporte substancial para la presente investigación, en el aspecto de la gestión del riesgo.

AGUIRRE Cardona Juan David y ARISTIZABAL Betancourt Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda. Proyecto de grado. Pereira, Colombia: Universidad Tecnológica de Pereira. Facultad de Ingenierías. (2013 p.11).

Explicó como uno de sus objetivos, la aplicación de controles del estándar ISO 27001 que permita la administración del funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información, la investigación fue de tipo aplicada.

Concluyó que toda implementación SGSI se debe establecer en referencia a estándares y mejores prácticas encauzadas a seguridad de la información, basándose en el marco de Cobit y la norma ISO/IEC 27001 y el ISO/IEC 27002 en sus versiones 2015 para determinar el marco de control e implantar los controles pertinentes.

Esta investigación contribuyó en la parte de aplicación de controles, ya que el investigador realizó un especial tratamiento del mismo.

GARCÍA Guevara Camilo Augusto. Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001: 2005. Informe de Postgrado. Bogotá, Colombia: Universidad EAN. Facultad de Postgrados. (2012 p.12).

Sustentó como uno de sus objetivos la evaluación del riesgo a través de la metodología de 6 pasos expresada en la cláusula 4.2.1 del estándar, fue una investigación de tipo aplicada.

Entre otras, concluyó que la metodología de análisis de riesgos y priorización sugirió que el mayor segmento de los riesgos están relacionados con la formación técnica de los trabajadores.

Esta investigación contribuyó en los procedimientos para el análisis de riesgos orientados a los recursos humanos.

1.3. Teorías relacionadas al tema

1.3.1. Sistema de Gestión de Seguridad de la Información (SGSI)

Para la adecuada administración de una empresa o institución, en la actualidad tiene que dirigir sus esfuerzos para ostentar de una adecuada seguridad de la información, por lo que es necesario instaurar un modelo que aborde esta función de una forma metódica, argumentada y justificada en unos objetivos exactos de

seguridad y evaluación de los riesgos inherentes al manejo de la información de la institución u organización.

Para ISO/IEC 27001 (2013)[6], la adopción del SGSI es una decisión estratégica para la organización, su implementación debe estar relacionada a los objetivos, requisitos de seguridad, los procesos organizacionales, la dimensión y complejidad de la organización. Por ello, el SGSI mantiene la confidencialidad, integridad y disponibilidad en el manejo y tratamiento de la información al utilizar un proceso de gestión de riesgo, el cual debe ser administrado de manera adecuada.

Otra concepción importante lo expresa la NTP-ISO/IEC 27001 (2014)[7], precisando que el Sistema de Gestión de Seguridad de la Información preserva la confidencialidad, integridad y disponibilidad de la información, que aplica un proceso de gestión de riesgos y ofrece confianza a los interesados, ya que se manejan los riesgos adecuadamente.

A su vez, Sigler K y Rainey J(2016)[8], define al Sistema de Gestión de Seguridad de la Información, como un conjunto de elementos relacionados que las organizaciones usan para administrar y controlar los riesgos de seguridad de la información y para proteger y preservar la confidencialidad, integridad y disponibilidad de la información. Estos elementos incluyen todas las políticas, procedimientos, procesos, planes, prácticas, funciones, responsabilidades, recursos y estructuras que se utilizan para gestionar los riesgos de seguridad y para proteger la información.

Metodología ISO/IEC 27001

Es un estándar de la Organización Internacional de Normalización que proporciona un modelo para implantar, utilizar, monitorear, revisar, sostener y optimizar un Sistema de Gestión de Seguridad de la Información (SGSI), que debe contener la siguiente información:

Alcance del SGSI

[6] INSTITUTO Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Perú), NTP-ISO/IEC 27001:2013 Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de la Información. Lima: INDECOPI, 2013. p. v.

[7] INSTITUTO Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Perú), NTP-ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de la Información. Lima: INDECOPI, 2014. p. vii.

[8] SIGLER, Ken y RAINEY, James. *Securing an IT Organization through Governance, Risk Management and Audit*. Boca Raton – Florida: CRC Press, 2016. p. 42.

Es el ámbito de influencia de la organización sometida a la intervención, que incluye las dependencias, interacción y límites.

Identificación de activos

Se identificarán todos los activos de información, posteriormente se determinará su criticidad para ser el objeto del tratamiento respectivo.

Política de seguridad de la información

Es el documento de contenido general que determina el compromiso de la Alta Dirección de cada organización y el enfoque de ésta en la gestión de seguridad de la información acorde a sus objetivos estratégicos institucionales.

Procedimientos y mecanismos de control

Son aquellos que sistematizan el propio funcionamiento del SGSI, son documentos necesarios para asegurar la planificación, evolución y control del proceso de seguridad de la información.

Enfoque de evaluación de riesgos

En esta sección se describe la metodología a usar, criterios de aceptación del riesgo y niveles de riesgo aceptable.

Plan de tratamiento de riesgos

En este apartado se detallan las acciones, recursos, responsabilidades y prioridad en la gestión del riesgo.

Declaración de aplicabilidad

Se especifican los elementos de control determinados en el SGSI y su estado de intervención, justificando inclusiones y exclusiones.

Otras metodologías de sistemas de gestión de seguridad de información y manejo de riesgos

Existen diversas metodologías que se pueden mencionar: Octave, Magerit, ISM3, entre otras; las mismas que se desarrollarán a continuación.

Metodología Octave

Esta metodología de gestión de riesgos de seguridad de información, engloba tanto las perspectivas organizacionales como los propiamente técnicos. Hace especial interés en una evaluación inicial para realizar un diagnóstico del riesgo de seguridad de la información dentro de la organización, sirviendo de base para optimizar los

aspectos más importantes: riesgos operativos, experiencias y acciones de seguridad y tecnología.

Existen diversas variantes: Octave-S específico para organizaciones pequeñas, utilizando un proceso simplificado; el Octave Allegro, otra variante simplificada basada en los activos de la información.

Modelo Magerit

Es la metodología más usada en el análisis y gestión de riesgos para los sistemas de información formulada por el Consejo Superior de Administración Electrónica - Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, órgano dependiente del Ministerio de Hacienda y Administraciones Públicas del Gobierno de España; se basa en darle prioridad al uso de las tecnologías de la información, trayendo como consecuencia mejores beneficios y ventajas a los interesados; implementa el proceso de gestión de riesgos con una determinada metodología para que las entidades tomen conciencia de los riesgos generados y vinculados al uso de las tecnología de la información y comunicaciones.

El modelo Magerit en su versión 3.0 basa sus procedimientos en la norma ISO/IEC 31000 y se implementa bajo el “Marco de Gestión de Riesgos”, precisando las fases:

Fase 1: Principios de gestión del riesgo.

Fase 2: Marco de trabajo para la gestión del riesgo.

Fase 3: Proceso de gestión del riesgo.

Metodología ISM3

Del inglés, information security management maturity model. El concepto manejado en esta metodología es el riesgo aceptable, teniendo como prioridad el cumplimiento de los objetivos críticos y sensibles del negocio basado en mejoras de seguridad.

Esta metodología pretende generar un estándar sencillo y aplicable, pero con calidad dirigidos en la implementación para sistemas de gestión de seguridad de la información y puede aplicarse a entidades pequeñas hasta grandes organizaciones.

1.3.2. Proceso de gestión del riesgo

El quehacer humano siempre ha generado datos. Cualquier elemento informativo que tenga importancia para el sistema, es denominado dato. Su organización y ordenamiento ha permitido a las empresas generar información, y en época del uso de internet su crecimiento ha sido exponencial. Una empresa o institución al administrar información está expuesta al riesgo, en su obtención, manejo intercambio o resguardo.

Peltier T (2014)[9], precisa el concepto como:

> […]El proceso de gestión de riesgos consiste en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable. Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo). A continuación, identifique los controles que llevarían el efecto a un nivel aceptable.

Este concepto identifica claramente, que el proceso implica identificar y evaluar el riesgo para lo cual es necesario identificar al activo, sus amenazas y vulnerabilidad, probabilidad de ocurrencia, y otro, identificar el tratamiento del riesgo a través de controles para conducir al riesgo a un nivel aceptable.

Para ISO/IEC 27005 (2011)[10], "La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable".

---

[9] PELTIER, Thomas. Information Security Fundamentals. 2da. Edición. Florida: CRC Press, 2014. p. xxi.

[10] ORGANIZACIÓN Internacional de Normalización, Norma ISO 27005. Tecnología de la Información – Gestión de riesgos de la Seguridad de la Información. ISO, 2005, 2011. p. 6.

Esta acepción se toma de la metodología estándar ISO, en la que se colige al proceso de gestión del riesgo como un conjunto de acciones progresivas, tales como evaluar el riesgo y tratarlos.

Pritchard C (2015)[11], describe el concepto de proceso de gestión del riesgo indicando:

> […]El desarrollo de la respuesta al riesgo, es un elemento crítico en el proceso de gestión del riesgo, que determina que acción se llevará a cabo para evaluar el riesgo en los aspectos de su identificación, calificación y esfuerzos de cuantificación (p. 48).

Este autor incide en que es crítico afrontar el riesgo, previamente con su evaluación e identificación.

Sigler (2016), explica:

> […]La evaluación del riesgo apoya la estrategia que se utiliza para organizar el proceso de gestión del riesgo y brinda a los gestores la información necesaria para desplegar controles específicos que respondan a esos riesgos. Las evaluaciones también miden la eficacia de los controles, una vez que han sido aplicados.

En este concepto el autor hace referencia a que en este proceso, la evaluación del riesgo brinda información de que controles aplicar, además que éstos pueden dimensionarse en su eficacia.

Passenheim O (2010)[12], describe este proceso, "…un paso en el proceso de gestión de riesgos es el control de riesgos, incluyendo la ejecución de la estrategia de respuesta al riesgo, monitoreo y desencadenamiento de eventos, inicio de planes de contingencia y vigilancia de nuevos riesgos", el autor hace incidencia a que frente a la gestión del riesgo debe exigirse una respuesta al riesgo, éstos se deben observar y destaca que siempre se está expuesto a nuevos riesgos.

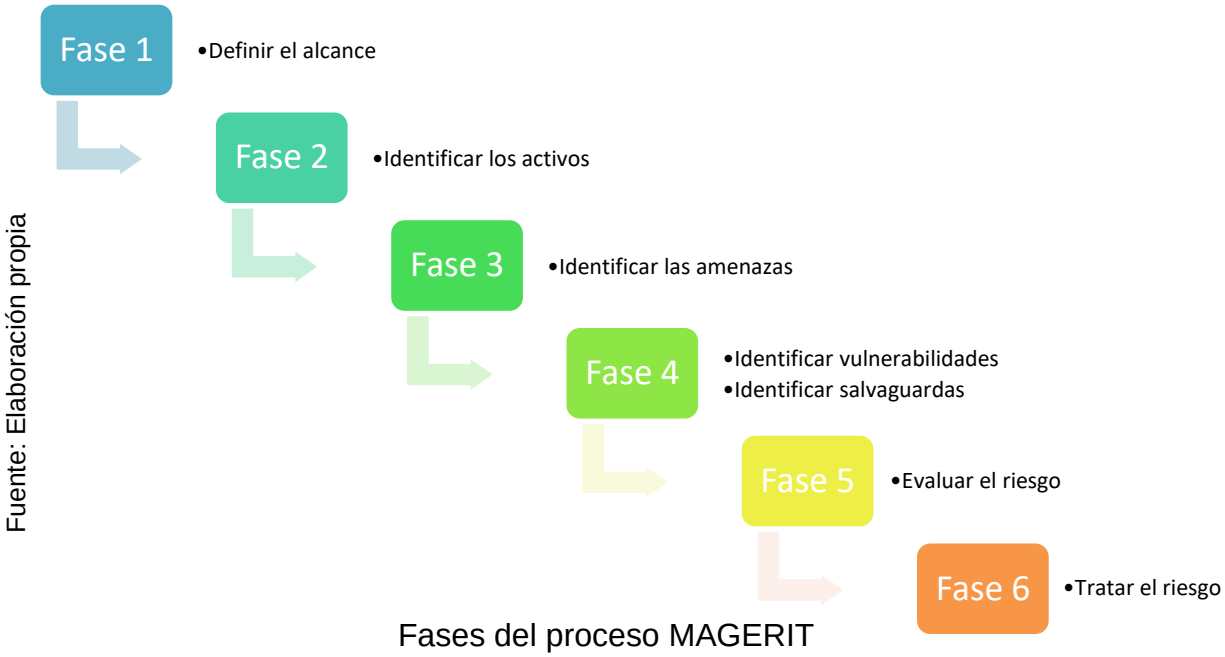
Gorrod M (2004)[13], sobre el proceso de gestión del riesgo, explica "La clave para el proceso de gestión de riesgo es la identificación y análisis de los riesgos dentro de la organización, junto con su visualización e información". A juicio del autor, dentro del proceso de gestión del riesgo predomina la identificación y análisis del riesgo, constituyendo un asunto clave para determinar en una institución.

---

[11] PRITCHARD, Carl. *Risk Management Concepts and Guidance*. 5ª edición. Boca Raton – Florida: CRC Press, 2015. p. 84.
[12] PASSENHEIM, Olaf. Enterprise Risk Management. Ventus Publishing, 2010. p. 32.
[13] GORROD, Martin. Risk Management Systems. Process, Technology and Trens. Editorial Palgrave MacMillan, 2004. p. 61.

La metodología para el proceso de gestión del riesgo es desarrollada para identificar la falta de aplicación de controles y la instauración de un plan de salvaguardas o medidas. La metodología que la presente investigación adopta es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), las fases que contempla esta metodología se pueden apreciar en el Gráfico N° 1.

Gráfico N° 1



Fuente: Elaboración propia

Fases del proceso MAGERIT

La fase de la definición del alcance, es parte del establecimiento del contexto de la información relevante de la institución. Se determina hasta que punto se intervendrá, se especificará que áreas y personal estarán comprometidos.

La fase de la identificación de los activos, determina todos los activos en base a una encuesta al personal comprometido o en base a la recolección de información, tales pueden ser: Procesos del negocio, actividades e información, que incluyen hardware (equipos de procesamiento de datos, periféricos y medios de comunicación), software (sistema operativo, servicio, software de aplicación), red, personal (directores, usuarios, personal de operación y desarrolladores), lugar y infraestructura de la organización (centro de datos, servidores).

La fase de identificación de amenazas implica identificar las causas potenciales de un incidente contra un activo, pueden ser de origen natural (inundación, lluvias, terremotos), de entorno (incendio, sobrecarga eléctrica), defecto de aplicaciones o software desarrollado, causadas por personas de forma accidental o deliberada.

La fase de identificación de vulnerabilidades y salvaguardas, implica clasificar las amenazas midiendo la degradación que le supone a un activo, a su vez, se determina que salvaguarda se empleará para disminuir el riesgo a un nivel aceptable.

La fase principal de evaluación del riesgo, identifica de forma cuantitativa o cualitativa los riesgos y les da prioridad a los criterios de evaluación que están inmersamente comprometidos dentro de los objetivos estratégicos de la organización.

Como última fase, se encuentra el tratamiento del riesgo, tiene como objetivo identificar las medidas de seguridad para reducir los riesgos y establecer un plan de tratamiento del riesgo. El proceso recibe como entrada la salida del proceso de evaluación de riesgos y produce como salida el plan de tratamiento de riesgos.

Dimensiones de la variable

Para la presente investigación se tomarán como dimensiones de la variable "proceso de gestión del riesgo", la evaluación del riesgo y el tratamiento del riesgo.

Para Peltier T (2014)[14], "El riesgo es la posibilidad de que algo adverso suceda" (p. xxi), además explica que:

> […] el proceso de evaluación de riesgos ayuda a la gestión en el cumplimiento de sus obligaciones de proteger los activos de la organización. Al ser un activo en el proceso de evaluación de riesgos, la gestión, cuando actúa en su condición de propietario, tiene la oportunidad de ver lo que las amenazas están al acecho en todo el proceso de negocio.

[14] PELTIER, Thomas. Information Security Fundamentals. 2da. Edición. Florida: CRC Press, 2014. p. 50.

Al especificar en que momento procede a analizar y gestionar riesgos, el Ministerio de Hacienda y Administraciones Públicas (2012)[15], detalla:

> Un análisis de riesgos TIC es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se practique la tramitación electrónica de bienes y servicios, sea en contexto público o privado. El análisis de riesgos permite tomar decisiones de gestión y asignar recursos con perspectiva, sean tecnológicos, humanos o financieros.

Además, al definir el nivel de riesgo como algo que tiene que ser aceptado por la alta dirección de una organización, el Ministerio de Hacienda y Administraciones Pública (2012)[16], indica:

> El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección.

Asimismo, en la certificación del sistema de gestión de seguridad de la información implementado en cualquier organización, se requiere previamente la aplicación de controles, por lo que el Ministerio de Hacienda y Administraciones Pública (2012), detalla al respecto:

> Antes de proceder a la certificación, debe haberse realizado un análisis de riesgos a fin de conocer los riesgos y de controlarlos mediante la adopción de los controles adecuados, además, será un punto de control de la gestión del producto o sistema. (p. 16).

Seguridad de la información

Según la Organización Internacional de Normalización, ISO/IEC 27001 (2005)[17] sostiene que la seguridad de la información consiste en la salvaguarda de su (a) confidencialidad: la información no puede proveerse ni revelarse a individuos, entidades o procesos sin la debida autorización, (b) integridad: la información debe mantenerse exacta y completa, y (c) disponibilidad: la información y sus sistemas

[15] MINISTERIO de Hacienda y Administraciones Públicas. Magerit, Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método. Madrid: 2012. p. 16.
[16] Ibíd 15, p. 10.
[17] ORGANIZACIÓN Internacional de Normalización, *Norma ISO 27001. Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos*. ISO, 2005, 2013. p. 15.

de tratamiento debe estar accesibles y puedan ser utilizados cuando lo requieran o necesiten.

Existen distintas acepciones del término Seguridad Informática. De ellas, entre las más completas, es la definición procurada por el estándar ISO/IEC 27001 (2005)[18], que en el 2005 fue aprobado y publicado, por la Organización Internacional de Normalización (ISO) y por la Comisión International Electrotécnica (IEC):

> La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

1.4. Formulación del problema

Problema General

PG: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional?

Problemas específicos

PE1: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional?

PE2: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional?

1.5. Justificación del estudio

1.5.1. Justificación tecnológica

Carrasco, S (2005)[19], refiere como justificación tecnológica a los resultados de la investigación que posibilita la elaboración de técnicas e instrumentos, para la producción de bienes económicos, científicos, etc. que dinamicen el desarrollo de procesos productivos.

La metodología SGSI proporciona un modelo generalmente aplicados y aceptados para las buenas prácticas de control en TI, orientados a administrar las

[18] Ibíd. p. 10.
[19] CARRASCO, Sergio. *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005. p. 120.

tecnologías, respaldado por una comunidad de expertos en constante evolución; orientado a procesos, sobre la base de dominios de responsabilidad dentro del ámbito de la empresa o institución.

Una de las primordiales cualidades que debe poseer una institución que busque establecer un modelo de SGSI es un enfoque por procesos, por lo que la presente investigación presentó una solución metodológica asociada a la tecnología que permitirá salvaguardar la información en el proceso de gestión del riesgo del Hospital Nacional PNP “Luis N. Sáenz”.

1.5.2. Justificación teórica

Carrasco, S (2005)[20] reseña como justificación teórica - científica en que el resultado de la investigación podrá generalizarse e incorporarse al conocimiento científico, asimismo, complementar espacios cognoscitivos existentes.

La presente investigación aplica el estándar ISO 27001 promovido por una organización internacional para mejorar el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”, además Peltier, T (2014)[21], sostiene el proceso de gestión de riesgos en una serie de acciones, como identificar el riesgo, efectos de producirse y aplicar medidas para reducirlos a un nivel aceptable, por lo que se colige que los resultados de la investigación incorporaron conocimientos a la institución en seguridad de la información, lo cual permitirá su aprovechamiento en la gestión integral del servicio de atención de salud.

1.5.3. Justificación práctica

Carrasco, S (2005)[22] sostiene que la justificación práctica de una investigación servirá para resolver problemas prácticos.

El producto de la presente investigación influyó en el cumplimiento de la Ley 29733, Ley de Protección de Datos Personales, cuyo cumplimiento en la inscripción en el Banco de Datos Personales del Ministerio de Justicia y Derechos Humanos venció el 08 de mayo del 2015, más si se sabe que la Dirección General de

[20] Ibíd. p. 119.
[21] PELTIER, Thomas. *Information Security Fundamentals*. 2da. Edición. Florida: CRC Press, 2014. p. xxi.
[22] CARRASCO, Sergio. *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005. p. 119.

Protección de Datos Personales, es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales, quien tiene facultad sancionadora y realiza constantemente inspecciones en toda entidad pública y privada.

Asimismo, al establecer los principales procesos que involucra la gestión de información crítica para el Hospital Nacional PNP "Luis N. Sáenz", se cumplió con la normatividad del Ministerio de Salud en el proceso de implementación de la historia clínica electrónica, al adoptar las identificaciones estándar de datos en salud.

Internamente, debido a la actual carencia de una metodología que permita la seguridad de la información en la institución de estudio, además de la falta de modelamiento de los procesos, fue necesario que se realice el inventario de activos de información, el análisis de riesgos y la implantación de controles que sirvieron como protección ante posibles amenazas internas y externas.

1.5.4. Justificación metodológica

Carrasco, S (2005)[23] sostiene que la investigación tiene justificación metodológica cuando los métodos, procedimientos, técnicas e instrumentos tienen validez y confiabilidad para ser utilizados en investigaciones similares y resultan eficaces.

En la presente investigación se ha diseñado el instrumento de recolección de datos como la Ficha de Observación, asimismo, se ha establecido la validez por opinión de expertos y una confiabilidad aceptable mediante la prueba de coeficiente de estabilidad test-retest, obteniendo el valor de 0.747 de correlación; por tanto, el instrumento podrá ser utilizado en investigaciones similares.

1.5.5. Justificación económica

Carrasco, S (2005)[24] precisa que una investigación se justifica socioeconómicamente al resultar en beneficio y utilidad hacia una población.

La información es un activo primordial para el éxito y el mantenimiento de la competitividad de cualquier organización en general. El aseguramiento de dicha información y de sus procesos de tratamiento, por tanto, un objetivo de esencial relevancia para la institución.

---

[23] Ibíd.

[24] CARRASCO, Sergio. *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005. p. 120.

El desarrollo de la presente investigación permitió a los encargados de la gestión de TI, adquirir un mejor nivel de servicio en calidad, funcionalidad y facilidad en el uso de la seguridad, de manera tal que se minimizó costos a la institución. Una pérdida o adulteración de información del paciente, podría conllevar a sanciones económicas por parte de los entes reguladores, como el Ministerio de Salud o la Superintendencia Nacional de Salud, por otra parte, el impacto que acarrearía un evento que posibilite la falta de disponibilidad del sistema de gestión de salud traería como consecuencia efectuar la contingencia de procesos manuales que estarían fuera de comprobación y traería por consiguiente pérdidas en horas/hombre de trabajo.

Asimismo, al cumplir la Ley de Protección de Datos Personales se evitó estar sometido a un procedimiento sancionador por parte de la Dirección General de Protección de Datos Personales – MINJUS, quien puede determinar una sanción administrativa de multa, cuyo monto máximo en caso de infracciones graves es de 10UIT.

1.1.1. Justificación técnica

Para la aplicación de la metodología SGSI se definió el ámbito de la organización, incluyendo una identificación estructurada de las dependencias y áreas; que en el caso de la institución de estudio, fue principalmente la Unidad de Telemática del HN PNP “LNS”, esto implicó mejoras y beneficios en la seguridad de acceso al Sistema de Gestión de Salud del Hospital Nacional PNP “Luis N. Sáenz”, así como, se aseguró la disponibilidad de los sistemas del área crítica del hospital, como son: Sistema de Emergencia, Farmacia de Emergencia y Centro Quirúrgico, ya que se formularon los controles respectivos, que estableció las mejoras en la seguridad lógica y física y de entorno (infraestructura de servidores de producción, desarrollo y backup, conectividad y comunicaciones), control de acceso, sistemas de contingencia, el sistema de energía eléctrica y copias de seguridad.

Además, propició en la Gerencia del Hospital y sirvió para que se inicien las gestiones para el cumplimiento del uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, ya

que el Hospital Nacional, es una entidad integrante del Sistema Nacional de Informática (RM N° 004-2016-PCM del 08/10/2016).

1.2. Hipótesis

Hipótesis general

HG: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva en el proceso de gestión del riesgo de un Hospital Nacional.

Hipótesis específicas

HE1: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva reduciendo el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

HE2: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

1.3. Objetivos

Objetivo General

OG: Evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional.

Objetivos específicos

OE1: Evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

OE2: Evaluar la manera en que la implementación del sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

CAPÍTULO II
MÉTODO

II. MÉTODO

2.1. Diseño de investigación

Behar, D (2008)[25], conceptualiza a una investigación de tipo aplicada, porque explora la aplicación de los conocimientos que se alcanzan. Precisa que la investigación aplicada se encuentra estrechamente emparentada con la investigación básica, ya que pende de los resultados y progresos de esta última; esto se establece al colegir de que toda investigación aplicada para su validación y justificación necesita de un marco teórico; concluyendo que busca cotejar la teoría con la realidad.

El tipo de estudio del presente proyecto es una investigación aplicada que implica la implementación de la metodología de sistema de gestión de seguridad de la información por parte del investigador, sobre el proceso de gestión del riesgo en el Hospital PNP "Luis N. Sáenz", orientado a mejorar la seguridad de la información como uno de los activos más importantes, para lo cual se aplicará la norma ISO 27001 y la metodología Magerit v3.0 para el análisis y gestión de riesgos.

Carrasco, S (2005)[26], explica el diseño de investigación pre experimental como la aplicación a un grupo de una prueba previa al estímulo o tratamiento experimental, para luego administrar el tratamiento, para luego aplicar la prueba o medición posterior. Mediante este diseño de investigación se tiene un punto de referencia inicial (pre test), que nos permite evaluar posterior al estímulo mediante una segunda medición (post test).

Con respecto al diseño de la investigación, la presente investigación fue de diseño pre experimental, ya que se aplicó la metodología del sistema de gestión de seguridad de la información (variable independiente) para determinar el efecto en el proceso de gestión del riesgo (variable dependiente), es decir, se esperará en los resultados un efecto positivo o negativo.

[25] BEJAR, Daniel. *Metodología de la Investigación*. Cabo Verde, Cuba: Editorial Shalom, 2008. p. 20.
[26] CARRASCO, Sergio. *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005. p. 64.

El tipo de investigación será cuantitativa, ya que al determinar el efecto sobre el proceso de gestión del riesgo (variable dependiente), se utilizarán indicadores para medir las dimensiones de las variables.

Por el número de variables el estudio es analítico porque tenemos dos variables y lo que se trata es determinar si tiene algún efecto o no en la aplicación de la metodología de sistema de gestión de información en el proceso de gestión del riesgo de un hospital.

2.2. Variables, operacionalización

2.2.1. Definición conceptual

Variable independiente: Sistema de gestión de seguridad de la información.

Según Areitio, J (2008)[27], el sistema de gestión de seguridad de la información es un sistema que se basa en el enfoque de los riesgos del negocio y que establece, implementa, opera, monitoriza, sostiene y optimiza la seguridad de la información. Esto implica generar una estructura organizacional dentro de la institución, establecer políticas de seguridad de la información, responsabilidades, procesos procedimientos y recursos.

Variable dependiente: Proceso de Gestión del riesgo.

Para definir la variable dependiente de esta investigación, se toma el concepto de Peltier, T (2014)[28], quien sostiene:

> "El proceso de gestión de riesgos consiste en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable. Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo). A continuación, identifique los controles que llevarían el efecto a un nivel aceptable".

[27] AREITIO, Javier. *Seguridad de la información: redes, informática y sistemas de información.* España: Ediciones Paraninfo, 2008. p. 200.
[28] PELTIER, Thomas. *Information Security Fundamentals*. 2da. Edición. Florida: CRC Press, 2014. p. xxi.

Definición operacional

Variable independiente: Sistema de gestión de seguridad de la información. Según Pacheco, F (2010)[29], "Un SGSI es un elemento para la administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño, implementación y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información". Al implementar la metodología del estándar ISO 27001, en la administración de base de datos del Hospital Nacional PNP "Luis N. Sáenz" se estará realizando una serie de actividades con la finalidad de mejorar la seguridad de la información y por consiguiente asegurar su confiabilidad, integridad y disponibilidad. Para cumplir con la implementación del SGSI en el hospital, según la ISO 27001, deberá elaborarse toda la documentación necesaria especificada en el numeral 1.3.1.

Variable dependiente: Proceso de Gestión del riesgo.

El proceso de gestión del riesgo es un conjunto de fases sucesivas, que implican evaluar el riesgo y tratar el riesgo en el contexto de la organización, estas acciones involucran llevar el nivel de riesgo a un grado aceptable y determinar el número de controles aplicados para su reducir el riesgo, respectivamente, para ello, es necesario la aplicación de un instrumento de recopilación directa de datos, como es la Ficha de Observación.

Operacionalización de variables

La Matriz de Operacionalización de las variables está enunciada en el Anexo N° 2. A continuación se definirá operacionalmente la variable independiente y dependiente:

Variable independiente: Sistema de gestión de seguridad de la información. Según la metodología del ISO 27001, requiere la elaboración de la documentación básica que será establecida como las dimensiones, a saber:

[29] PACHECO, Federico. *La importancia de un SGSI* [en línea]. 2010 [fecha de consulta: 25 de Febrero 2016]. Disponible en: < http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/>. párr. 2.

- Alcance del SGSI.
- Políticas de seguridad de información.
- Identificación de activos.
- Mecanismos de control SGSI.
- Análisis y evaluación del riesgo
- Plan de tratamiento del riesgo.
- Documentación de procedimientos.
- Declaración de aplicabilidad.

Los indicadores para estas dimensiones, serán medidas como el resultado positivo de cumplimiento en la elaboración de los documentos (check list) con los valores o escala: si / no (si entregado o no entregado, respectivamente).

Variable dependiente: Proceso de Gestión del riesgo.

Según las dimensiones ya definidas para la variable dependiente, serán medibles, según los siguientes criterios:

- Dimensión: Evaluación del Riesgo

  Como indicador tendremos el nivel de riesgo, cuya medida será cuantitativa y estará dada por la siguiente fórmula:

  $$NR = \frac{I + P}{2}$$

  En donde:

  NR = Nivel de riesgo.

  I = Nivel de impacto sobre el activo.

  P = Probabilidad de ocurrencia

  La técnica utilizada para obtener el nivel de riesgo será el de observación directa, cuyo instrumento de recolección será la Ficha de Observación.

- Dimensión: Tratamiento del riesgo

  Como indicador tendremos el número de controles aplicados, cuya medida será cuantitativa y estará dada por la siguiente fórmula:

  $$CA = Ciso – (CNE + CNA)$$

En donde:

CA = N° de controles aplicados.

Ciso = N° de controles ISO 27001

CNE = N° de controles no existentes.

CNA = N° de controles no aplicables.

La técnica utilizada para obtener el número de controles aplicados será el de observación directa, cuyo instrumento de recolección será la Ficha de Observación.

2.3. Población y muestra

Ñaupas, H (2014)[30], explica a la población como el conjunto de individuos, personas o instituciones que son motivo de la investigación.

Según el estándar ISO 27001, se identificarán los activos dentro de los procesos e información más sensibles del hospital, por lo que los activos se identificarán y evaluarán en base a un proceso de levantamiento de información que será recogida en la documentación del hospital y en base a consultas al personal profesional y técnico comprendido dentro de las funciones operativas de desarrollo de sistemas, control y seguridad de la información que labora en la Unidad de Telemática del Hospital Nacional PNP “Luis N. Sáenz”.

Valderrama, S (2013)[31], define a la muestra como un subconjunto representativo de un universo o población, es representativo porque refleja las características de la población al aplicársele adecuadamente la técnica del muestreo.

Castro, F (2003)[32], expresa que "si la población es menor a cincuenta (50) individuos, la población es igual a la muestra". Por tanto, si la población, por la cantidad de unidades que la conforman, alcanza su accesibilidad en su totalidad, no será necesario extraer una muestra.

---

[30] ÑAUPAS, Humberto *et al*. *Metodología de la investigación cuantitativa – cualitativa y redacción de la tesis*. 4ª edición. Bogotá: Ediciones de la U, 2014. p. 246.

[31] VALDERRAMA, Santiago. *Pasos para elaborar proyectos de investigación científica: Cuantitativa, cualitativa y mixta*. 2ª. edición. Lima: Editorial San Marcos, 2013. p. 184.

[32] CASTRO, Fernando. *El proyecto de investigación y su esquema de elaboración.* Caracas: Editorial Uyapar, 2003. p. 69.

Para el desarrollo de la presente investigación, la muestra será el total de activos críticos, que fueron 23 los identificados (ver Anexo N° 3), por tanto, conforma el mismo número que la población.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

2.4.1. Técnicas e instrumentos de recolección de datos

Gavagnin, O (2009)[33], define a la observación como el registro visual de lo que acontece en un contexto real, clasificando y registrando los datos, teniendo como referente un esquema previamente elaborado y el problema que se investiga.

La técnica e instrumentos de recolección de datos, fue la observación de campo mediante la aplicación de una Ficha de Observación, en la cual el investigador consignó datos para cada uno de los dos indicadores de la presente investigación, esto permitió determinar la realidad problemática en el proceso de gestión del riesgo en el Hospital Nacional PNP "Luis N. Sáenz", tomando como base el antes de la aplicación de la metodología de la ISO 27001 (ver Anexo N° 4 y 5) y posteriormente realizando la evaluación del después de la implantación de la metodología (ver Anexo N° 6 y 7). Las tablas resumen pueden verse en el Anexo N° 8 y 9, para las dimensiones mencionadas, respectivamente.

2.4.2. Validez de los instrumentos

Ñaupas, H (2014)[34] se refiere a la validez como la pertinencia de un instrumento de medición, para medir lo que se requiere medir, valorando la eficacia del instrumento para representar o describir el atributo que le interesa al investigador. Para tal fin, en la presente investigación se diseñó el instrumento, específicamente para estimar a cada uno de los indicadores.

Valderrama, S (2013)[35] explica a la validez de expertos, como el conjunto de opiniones que proponen los profesionales de experiencia, quienes deben valorar la

[33] GAVAGNIN, Osvaldo. *La creación del conocimiento*. Lima: Editorial Universidad Peruana Unión, 2009. p. 35.
[34] ÑAUPAS, Humberto *et al*. *Metodología de la investigación cuantitativa – cualitativa y redacción de la tesis*. 4ª edición. Bogotá: Ediciones de la U, 2014. p. 215.
[35] VALDERRAMA, Santiago. *Pasos para elaborar proyectos de investigación científica: Cuantitativa, cualitativa y mixta*. 2ª. edición. Lima: Editorial San Marcos, 2013. p. 198.

pertinencia de los indicadores respecto a las dimensiones del análisis y emitir opinión sobre cada pregunta del instrumento. Por tanto, para establecer la validez de contenido, se usó la aplicación del juicio de expertos, mediante la opinión informada de 3 profesionales de la Escuela de Ingeniería de Sistema de la Universidad César Vallejo (Ver Anexo N° 12), con amplia trayectoria en el tema, para evaluar la aplicación de una ficha de observación, obteniendo el resultado de opinión Aplicable, según se muestra en la Tabla N° 1.

Tabla N° 1. Resultados de la validación del instrumento Ficha de Observación

EXPERTO VALIDADOR	GRADO ACADÉMICO	OPINIÓN DE APLICABILIDAD
Even Deyser Pérez Rojas	Magister	Aplicable
Erika Patricia Cortés Alvarez	Magister	Aplicable
Arthur Huamaní Cuba	Magister	Aplicable

Fuente: Elaboración propia

2.4.3. Confiabilidad de los instrumentos

Para establecer la confiabilidad de los instrumentos, se realizó la prueba de coeficiente de estabilidad test-retest, para medir el grado en que el instrumento produce resultados consistentes y coherentes, es decir, en que el instrumento repetido al mismo grupo produzca resultados similares. Para tal fin se tomó el instrumento del indicador Nivel de Riesgo, posterior a 2 semanas de tomada la primera (17 al 21 de abril de 2017).

Para obtener el coeficiente de fiabilidad test-retest se procedió a correlacionar los datos de los resultados test-retest, obteniendo el valor de 0.747, representando una confiabilidad aceptable. Los resultados se muestran en la Tabla N° 2.

Tabla N° 2. Resultados de la confiabilidad del instrumento

	Valor
Correlación de Spearman	.747
N° de casos válidos	23

Fuente: Elaboración propia

Para el instrumento del indicador Número de Controles Aplicados, se toma como confiabilidad aceptable, ya que la data se recoge en base a si el control se usa, no se usa o se usa parcialmente, directamente con la documentación o evidencia existente sobre el uso de tal control.

2.5. Métodos de análisis de datos

Un análisis estadístico es el recurrido para comparar dos grupos relacionados de observaciones con relación a una variable numérica, por lo que es necesario hallar la diferenciación numérica que requiere la normalidad de las observaciones para cada uno de los grupos. La prueba de normalidad de la data, se efectuó a través del método Shapiro Wilks y el tipo de metodología exige que la varianza en ambos grupos de observaciones sea semejante.

El análisis y diferenciación de los resultados en fase pre test y post test, se realizó mediante el uso de la estadística descriptiva. El método estadístico utilizado para la validación de las hipótesis fue la prueba estadística de Wilcoxon para los indicadores Nivel de Riesgo y el Número de Controles Aplicados.

2.5.1. Hipótesis Específicas

Hipótesis H_{E1}: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva reduciendo el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

I_{1a} = Nivel de riesgo en el proceso de gestión del riesgo, antes de implementar la metodología SGSI.

I_{1d} = Nivel de riesgo en el proceso de gestión del riesgo, después de implementar la metodología SGSI.

H_0 La implementación del sistema de gestión de la seguridad de la información incrementa el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

$$H_0 = I_{1a} >= I_{1d}$$

H_a La implementación del sistema de gestión de la seguridad de la información disminuye el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

$$H_a = I_{1a} < I_{1d}$$

Hipótesis H_{E2}: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

I_{2a} = Número de controles aplicados en el proceso de gestión del riesgo, antes de implementar la metodología SGSI.

I_{2d} = Número de controles aplicados en el proceso de gestión del riesgo, después de implementar la metodología SGSI.

H_0 La implementación del sistema de gestión de la seguridad de la información disminuye el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

$$H_0 = I_{2a} >= I_{2d}$$

H_a La implementación del sistema de gestión de la seguridad de la información aumenta el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

$$H_a = I_{2a} < I_{2d}$$

2.5.2. Nivel de significancia

Nivel de significancia (x) : 0.05

Nivel de confiabilidad (1-x) : 0.95

2.5.3. Estadístico de la prueba

Distribución de T Student. Se denota de la siguiente manera por {X1, X2,...,Xn} e {Y1,Y2,...,Ym} al nivel de riesgo observado en cada uno de los activos de

información en la observación pre test y a la observación post test, respectivamente.

El t test para dos muestras independientes se basa en el estadístico:

$$t = \frac{\overline{X} - \overline{Y}}{\sqrt{\frac{(n-1)\hat{S}_1^2 + (m-1)\hat{S}_2^2}{n+m-2}}\sqrt{\frac{1}{n}+\frac{1}{m}}}$$

Donde $\overline{X}$ e $\overline{Y}$ denotan la media, en cada uno de los grupos:

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

$$\overline{Y} = \frac{1}{m}\sum_{i=1}^{m} Y_i$$

Y $\hat{S}_1^2$, $\hat{S}_2^2$ las cuasivarianzas muestrales correspondientes:

$$\hat{S}_1^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \overline{X})^2$$

$$\hat{S}_2^2 = \frac{1}{m-1}\sum_{i=1}^{m}(Y_i - \overline{Y})^2$$

2.5.4. Desviación estándar

$$s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2}$$

Donde:

$\bar{x}$ = Media muestral

x_i = Valores de la variable

n = Tamaño de la muestra

2.5.5. Región de rechazo

La región de rechazo es $z = z_x$

Donde zx = es tal que:

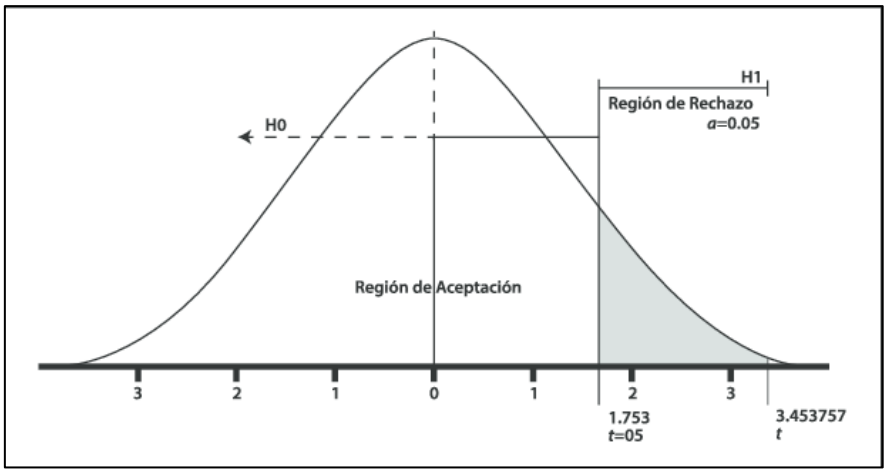
P [Z > Z] = 0.05

Donde z_x = Valor tabular empleando los rangos de Wilcoxon

Luego RR: z > zx

Los resultados obtenidos se evalúan y comparan con el p – valor o nivel de contraste “sig” (bilateral) para determinar la normalidad de la muestra.

Gráfico N° 2



Fuente: Spiegel (2007)

Prueba de Wilcoxon para verificar la región de rechazo

2.6. Aspectos éticos

El presente proyecto de investigación respetará las normas de la Universidad César Vallejo: Este estudio se encuentra amparado en el Reglamento de grados y títulos de la Universidad Cesar Vallejo, capítulo V, artículos, 33, 34, 39.

Y por el artículo 38 que dice: “Presentada la tesis y, contando con la aprobación del asesor y del jurado o la comisión permanente de grados y títulos de la facultad, programa la fecha de sustentación. No se podrá fijarse mientras no se haya cumplido con todos y cada de los requisitos establecidos”.

La documentación necesaria, de manera específica, los requisitos establecidos en la norma ISO 27001 para la implementación de un SGSI estarán definidos conforme a lo estipulado en la mencionada norma y serán validados por la Jefatura de la Unidad de Telemática del Hospital Nacional PNP “Luis N. Sáenz”, y se establecerán en la respectiva Acta de reunión.

Se cumplirá estrictamente con los términos de confidencialidad establecidos por la Jefatura de la Unidad de Telemática del Hospital Nacional PNP “Luis N. Sáenz”, manteniendo la reserva respectiva de toda información que contuviera la base de datos del hospital.

CAPÍTULO III
RESULTADOS

III. RESULTADOS

3.1. Análisis descriptivo

En la presente investigación se implementó el Sistema de Gestión de Seguridad de la Información para evaluar el nivel de riesgo y en número de controles aplicados en el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”; por tanto, se aplicó una evaluación pre test que reconoce las situaciones iniciales del indicador, posteriormente se implementó la metodología propuesta para estimar nuevamente cada indicador. Los resultados del análisis descriptivo se detallan a continuación.

Indicador: Nivel de riesgo (Pre test y Post test)

Los resultados descriptivos del nivel de riesgo, se aprecian en la Tabla N° 3

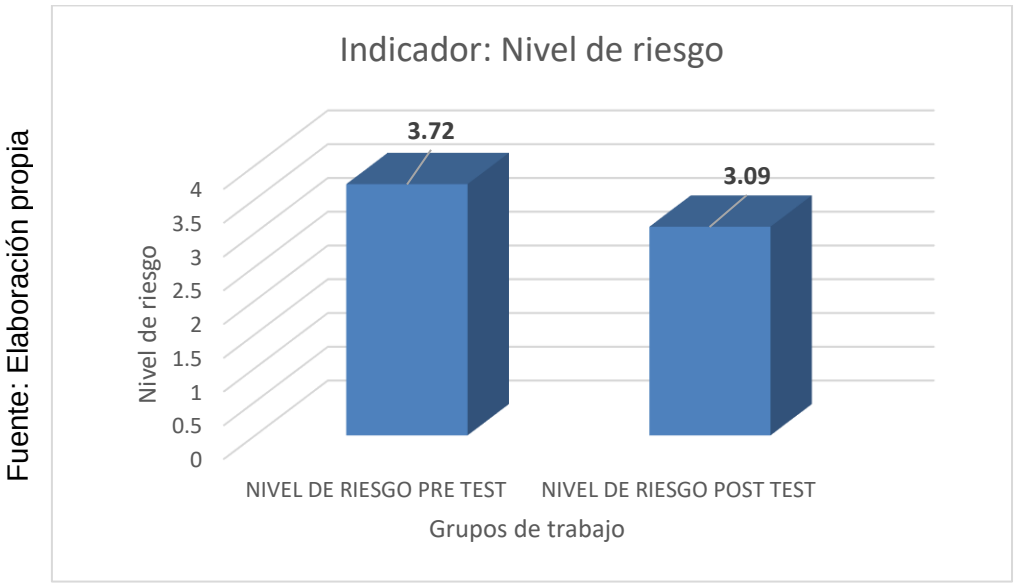
Tabla N° 3: Resultados descriptivos del nivel de riesgo en fase pre y post test

Test	N	Rango	Mínimo	Máximo	Media	Desviación estándar
En fase pre test	23	1.77	2.75	4.52	3.72	0.49243
En fase post test	23	2.23	1.75	3.98	3.09	0.54855

Fuente: Elaboración propia

Interpretación: Según muestra la Tabla N° 3 y el Gráfico N° 3, se determina que hay una disminución del nivel de riesgo de 0.63, lo que representa una reducción del 16.96%, al realizar la implementación de la metodología del Sistema de Gestión de Seguridad de la Información en el proceso de gestión del riesgo en un Hospital Nacional; estos resultados destacan una diferencia antes y después de la implementación de la metodología, asimismo, el mínimo nivel de riesgo para un activo de información fue de 2.75 (pre test) y se redujo a 1.75 (post test).

Gráfico N° 3



Fuente: Elaboración propia

Variación del nivel de riesgo

Indicador: Número de controles aplicados (Pre y Post test)

Los resultados descriptivos del número de controles aplicados, se aprecian en la Tabla N° 4

Tabla N° 4: Resultados descriptivos del número de controles aplicados en fase pre y post test

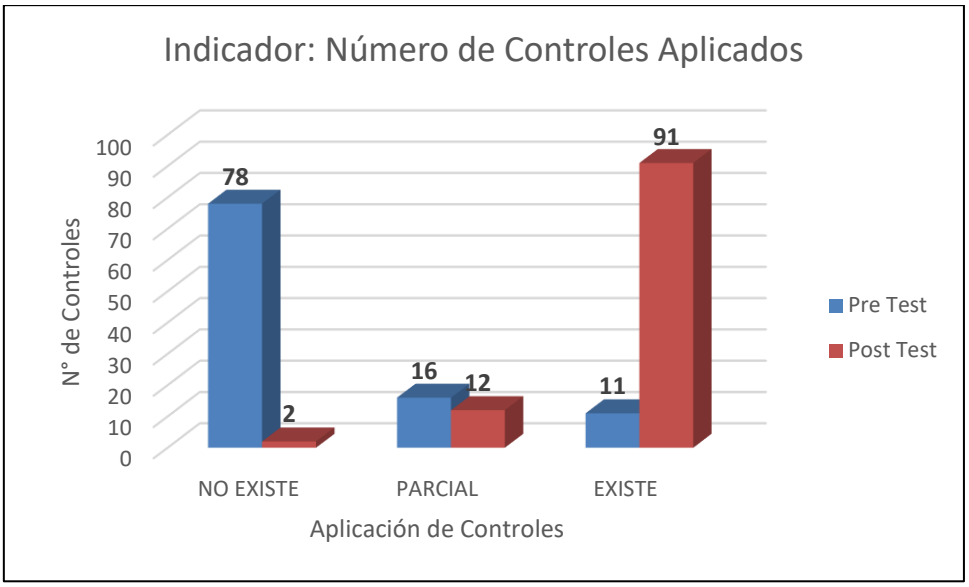
Test	N	Aplicación	Total	%
En fase pre test	105	No existente	78	74.28
		Parcialmente existente	16	15.24
		Si existente	11	10.48
En fase post test	105	No existente	2	1.90
		Parcialmente existente	12	11.43
		Si existente	91	86.67
Variación	105	No existente		-72.38
		Parcialmente existente		-3.81
		Si existente		76.19

Fuente: Elaboración propia

Interpretación: Según la Tabla N° 4 y el Gráfico N° 4, se puede apreciar que con la implementación de la metodología del Sistema de Gestión de Seguridad de la Información para el proceso de gestión del riesgo en un Hospital Nacional, se

logra disminuir los controles no existentes en 72.38% y por consecuencia aumentar los controles existentes en 76.19%.

Gráfico N° 4



Fuente: Elaboración propia

Variación del N° de Controles Aplicados en fase pre y post test

3.2. Pruebas de normalidad

Al ser una investigación con muestra menor a 50 elementos, se realizó la prueba de normalidad en cada uno de los indicadores mediante el método Shapiro Wilks. Para determinar este método se utilizó el software estadístico SPSS en su versión 24 con un nivel de confiabilidad del 95%, con los cumplimientos:

Si:

sig < 0.05 adopta una distribución no normal.
Sig => 0.05 adopta una distribución normal.

Donde: sig: p – valor o nivel crítico del contraste.

Los resultados fueron los siguientes:

Indicador: Nivel de riesgo (Pre test y Post test)

Tabla N° 5: Prueba de normalidad de Shapiro Wilks en fase pre y post test
Indicador: Nivel de riesgo

	Shapiro Wilks		
	Estadístico	gl	Sig.
Pre Test	.958	23	.429
Post Test	.912	23	.045

Fuente: Elaboración propia

Interpretación: Como se puede apreciar en la tabla N° 5, el valor de sig de Shapiro Wilks en fase pre test es de 0.429 mayor que 0.05, por lo que representa un distribución normal. Sin embargo, el valor de sig de Shapiro Wilks en fase post test es de 0.045 menor que 0.05, por lo que representa una distribución no normal. En consecuencia, se aplicará el estadístico no paramétrica de Wilcoxon para comparar el rango medio de las dos muestras relacionadas a fin de precisar si existen diferencias entre ellas.

Indicador: Número de controles aplicados (Pre y Post test)

Tabla N° 6: Prueba de normalidad de Shapiro Wilks en fase pre y post test
Indicador: Número de controles aplicados

	Shapiro Wilks		
	Estadístico	gl	Sig.
Pre Test	.593	105	.000
Post Test	.465	105	.000

Fuente: Elaboración propia

Interpretación: Como se puede apreciar en la tabla N° 6, el valor de sig de Shapiro Wilks en fase pre test y post test es de 0.000 menor que 0.05, por lo que representa una distribución no normal.

3.3. Pruebas de hipótesis

Prueba de Hipótesis H_{E1}:

La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva reduciendo el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

Hipótesis H_0: La implementación del sistema de gestión de la seguridad de la información incrementa el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

$$I_{NRS} <= I_{NRC}$$

Hipótesis H_a: La implementación del sistema de gestión de la seguridad de la información disminuye el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.

$$I_{NRS} > I_{NRC}$$

Donde:

I_{NRS} = Nivel de riesgo en el proceso de gestión del riesgo, sin la implementación de la metodología SGSI.

I_{NRC} = Nivel de riesgo en el proceso de gestión del riesgo, con la implementación de la metodología SGSI.

El presente trabajo de investigación ha demostrado en el ítem 3.1, que para el indicador Nivel de Riesgo, los datos representan un valor no normal, concluyéndose que para la validación de la hipótesis se usará los rangos de Wilcoxon.

Tabla N° 7: Determinación del contrate Post y Pre Test
Estadístico de contraste (b)
Indicador: Nivel de riesgo

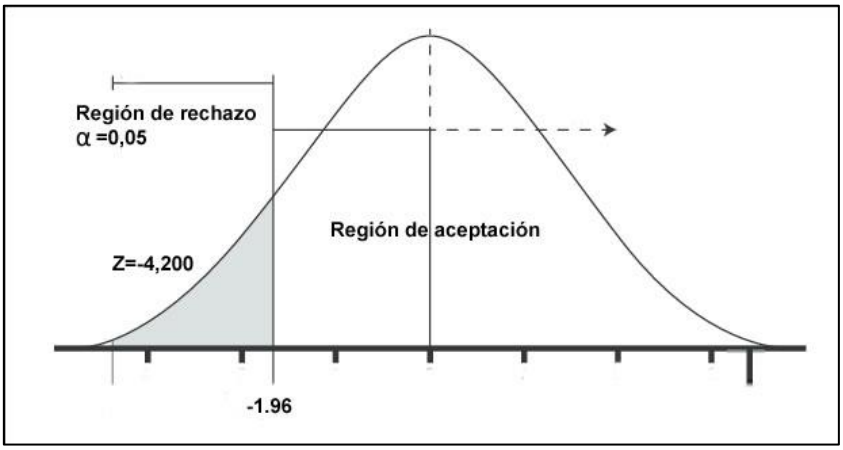
	Post Test - Pre Test
Z	-4.200 (a)
Sig. Asintót. (bilateral)	.000

(a) Datos en los rangos positivos

(b) Rangos bajo la prueba Wilcoxon

Fuente: Elaboración propia

Gráfico N° 5



Fuente: Elaboración propia

Prueba Z de Wilcoxon para el Nivel de Riesgo

Interpretación: Como se puede apreciar en la Tabla N° 7 y en el Gráfico N° 5, el nivel crítico de contraste (sig) es 0.00, debido a que es menor que 0.05, cae en la región de rechazo, por tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna, que dice:

“La implementación del sistema de gestión de la seguridad de la información disminuye el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.”

Prueba de la Hipótesis H_{E2}

La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

Hipótesis H_0 La implementación del sistema de gestión de la seguridad de la información disminuye el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

$$I_{NCAS} >= I_{NCAC}$$

Hipótesis H_a La implementación del sistema de gestión de la seguridad de la información aumenta el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.

$$I_{NCAS} < I_{NCAC}$$

Donde:

I_{NCAS} = Número de controles aplicados en el proceso de gestión del riesgo, sin la implementación de la metodología SGSI.

I_{NCAC} = Número de controles aplicados en el proceso de gestión del riesgo, con la implementación de la metodología SGSI.

El presente trabajo de investigación ha demostrado en el ítem 3.1, que para el indicador Número de controles aplicados, los datos representan un valor no normal, concluyéndose que para la validación de la hipótesis se usará los rangos de Wilcoxon.

Tabla N° 8: Determinación del contrate Post y Pre Test
Estadístico de contraste (b)
Indicador: Número de controles aplicados

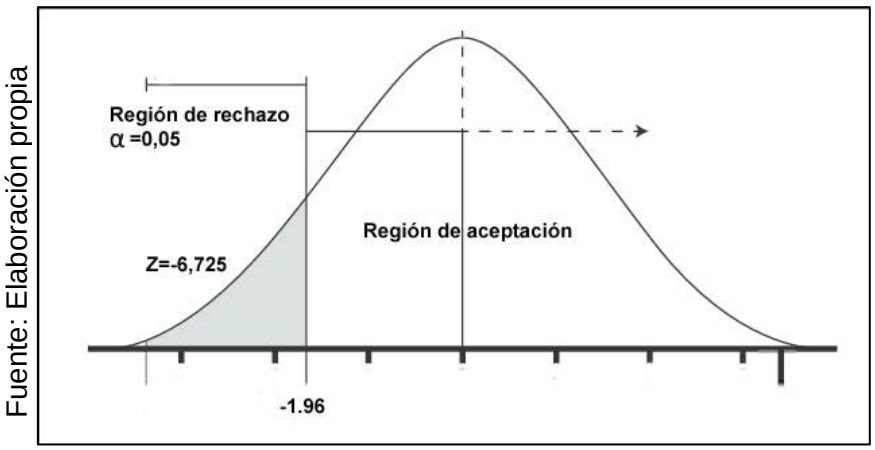
	Post Test - Pre Test
Z	-6.725 (a)
Sig. Asintót. (bilateral)	.000

(a) Datos en los rangos positivos

(b) Rangos bajo la prueba Wilcoxon

Fuente: Elaboración propia

Gráfico N° 6



Fuente: Elaboración propia

Prueba Z de Wilcoxon para el Número de controles aplicados

Interpretación: Como se puede apreciar en la Tabla N° 6 y en el Gráfico N° 4, el nivel crítico de contraste (sig) es 0.00, debido a que es menor que 0.05, cae en la región de rechazo, por tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna, que dice:

“La implementación del sistema de gestión de la seguridad de la información aumenta el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.”

CAPÍTULO IV
DISCUSIÓN

IV. DISCUSIÓN

Según la investigación efectuada por Inca (2012), comprobó que la implementación del sistema de gestión de seguridad de la información en una similar institución de salud, para el proceso de administración de base de datos, se redujo en 23.33% en relación al nivel de riesgo. Asimismo, comprobó que la implementación del sistema de gestión de seguridad de la información para el valor de los controles aplicados existentes, se aumentó en 44.84%.

En la presente investigación, los resultados para el indicador nivel de riesgo, en la medición pre test se determinó un valor de 3.72 y luego de la implementación de la metodología del Sistema de Gestión de Seguridad de la Información, en fase post test se redujo a 3.09. Los resultados precisan que existe una reducción de 0.63, por tanto, se puede afirmar que con la implementación de la mencionada metodología, se ha alcanzado una disminución del 16.96%; asimismo, para el indicador número de controles aplicados, en la medición pre test se determinó un valor de 11 para los controles existentes, luego de aplicada la metodología SGSI, en post test, se determinó un valor de 91 controles, por tanto, se puede afirmar que con la implementación de la mencionada metodología, se alcanza un aumento de los controles aplicados existentes en un 76.19% en el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”.

Los resultados conseguidos en la presente investigación comprueban que al implementar una metodología estándar de seguridad de la información, mejora el nivel de riesgo en los activos de información, tal como lo sostiene Peltier (2014) que define el proceso de gestión de riesgos, en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable.

CAPÍTULO V
CONCLUSIÓN

V. CONCLUSIONES

Con los resultados de la presente investigación, se precisan las siguientes conclusiones:

Mediante la implementación de la metodología del sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”, el nivel del riesgo se consigue disminuir de 3.72 a 3.09, representando un 16.96%. Por tanto, se determina que el nivel de riesgo de los activos críticos identificados en la presente investigación ha disminuido (Anexo N° 8).

De otro lado, con la implementación de la metodología mencionada, se logra la reducción de los controles no existentes en 72.38% y consecuentemente, aumentar los controles existentes en 76.19%; en cuanto a los controles parcialmente aplicados se reduce en 3.81%. Por tanto, se determina que el número de controles aplicados empleando la metodología SGSI, ha aumentado (Anexo N° 9).

Finalmente, luego de haber alcanzado resultados satisfactorios de los indicadores de la presente investigación, se concluye que la implementación de la metodología del sistema de gestión de seguridad de la información logró mejorar el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”.

CAPÍTULO VI
RECOMENDACIONES

VI. RECOMENDACIONES

Dentro de las instituciones, para el Área de Informática, Gerencia de TI o para el Oficial de Seguridad, se recomienda dentro de una investigación científica, la elección de la Evaluación del Riesgo, tomando como indicador el Nivel de Riesgo, ya que en toda institución se tiene latente e imperiosa necesidad de establecer una debida seguridad en el manejo de la información, para lo cual, puede utilizar una metodología estándar de seguridad de la información, acorde a su entorno, circunstancias y objetivos estratégicos, con el objetivo de llevar su nivel de riesgo en el manejo de la información a un grado aceptable (Ver Tabla N° 3 y Gráfico N° 3).

Asimismo, para la Gerencia de TI o informática de las instituciones, se recomienda realizar en investigaciones similares, la evaluación del Tratamiento del Riesgo, con la finalidad de determinar el Número de Controles Aplicados, por lo que puede servirse de diversas metodologías estándar para asegurar al información, trayendo como consecuencia, gestionar la responsabilidad de reducir el riesgo en los activos de información, por consiguiente, mejorar sus procesos de gestión del riesgo (Ver Tabla N° 4 y Gráfico N° 4).

Como recomendación general a toda institución relacionada a la atención de los servicios de salud, se propone la investigación del proceso de gestión del riesgo, ya que la información médica que se gestiona relacionada al paciente es crítica, por ello, puede optar por implementar la metodología del Sistema de Gestión de Seguridad de la Información para mejorar sus procesos en el manejo de información, contribuyendo de esta manera, a la atención de calidad en los servicios de salud y a la toma de decisiones.

CAPÍTULO VII
REFERENCIAS

IV. REFERENCIAS

LIBROS

AREITIO, Javier. *Seguridad de la información: redes, informática y sistemas de información.* España: Ediciones Paraninfo, 2008. 592 pp. ISBN: 9788497325028.

BEJAR, Daniel. *Metodología de la Investigación*. Cabo Verde, Cuba: Editorial Shalom, 2008. 94 pp. ISBN 9789592127837.

CARRASCO, Sergio. *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005. 474 pp. ISBN 9972342425.

CASTRO, Fernando. *El proyecto de investigación y su esquema de elaboración.* Caracas: Editorial Uyapar, 2003. 144 pp. ISBN: 9806629000.

GAVAGNIN, Osvaldo. *La creación del conocimiento*. Lima: Editorial Universidad Peruana Unión, 2009. 236 pp. ISBN: 978-6120000175.

GORROD, Martin. *Risk Management Systems. Process, Technology and Trens*. Editorial Palgrave MacMillan, 2004. 316 pp. ISBN: 1403916179.

HERNANDEZ, Roberto. *Metodología de la Investigación Científica*. México D.F.: Editorial Mc Graw Hill / Interamericana Editores, 2014. 634 pp. ISBN: 97814562-23960.

HUESO, Luis. *Administración de sistemas gestores de bases de datos*. Madrid: Ra-Ma Editorial, 2011. 306 pp. ISBN: 9788499641003.

MANNINO, Michael. *Administración de bases de datos, diseño y desarrollo de aplicaciones*. 3ª ed. México: McGraw-Hill Interamericana Editores, 2007. 738 pp. ISBN: 9789701061091

ÑAUPAS, Humberto *et al*. *Metodología de la investigación cuantitativa – cualitativa y redacción de la tesis*. 4ª edición. Bogotá: Ediciones de la U, 2014. 537 pp. ISBN: 9789587621884

PASSENHEIM, Olaf. *Enterprise Risk Management. Ventus Publishing*, 2010. 38 pp. ISBN: 9788776816841.

PELTIER, Thomas. *Information Security Fundamentals*. 2da. Edición. Florida: CRC Press, 2014. 375 pp. ISBN 9781439810620.

PRITCHARD, Carl. *Risk Management Concepts and Guidance*. 5ª edición. Boca Raton – Florida: CRC Press, 2015. 465 pp. ISBN: 9781482258462.

RIVERO, Enrique, GUARDIA, Carlos y REIG, José. *Bases de datos relacionales: diseño físico*. Madrid: Universidad Pontificia de Comillas, 2004. 667 pp. ISBN: 8484681386.

SIGLER, Ken y RAINEY, James. *Securing an IT Organization through Governance, Risk Management and Audit*. Boca Raton – Florida: CRC Press, 2016. 364 pp. ISBN: 9781498737326.

VALDERRAMA, Santiago. *Pasos para elaborar proyectos de investigación científica: Cuantitativa, cualitativa y mixta*. 2ª. edición. Lima: Editorial San Marcos, 2013. 495 pp. ISBN: 9786123028787.

TESIS

AGUIRRE, Juan y ARISTIZABAL, Catalina. *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda*. Tesis (Título de Ingeriero de Sistemas y Computación). Risaralda, Universidad Tecnológica de Pereira – Colombia, 2013. 84 pp.

ALIAGA, Luis. *Diseño de un sistema de gestión de seguridad de la información para un instituto educativo*. Tesis (Título de ingeniero informático). Lima, Pontificia Universidad Católica del Perú, 2013. 95 pp.

AMPUERO, Carlos. *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros*. Tesis (Título de Ingeniero Informático). Lima, Pontificia Universidad Católica del Perú, 2011. 106 pp.

BARRANTES, Carlos y HUGO, Javier. *Diseño e implementación de un sistema de seguridad de la información en procesos tecnológicos*. Tesis (Título de ingeniero de computación y sistemas). Lima, Universidad de San Martín de Porres, 2012. 320 pp.

BASTIDAS, Henry, LÓPEZ, Iván y PEÑA, Hernando. *Análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del Hospital Susana López de Valencia de la Ciudad de Popayán*. Tesis (Título de ingeniero de sistemas). Bogotá, Universidad Nacional Abierta y a Distancia de Colombia, 2014. 229 pp.

CÁCERES, Joan. *Sistema de gestión de seguridad de la información en el proceso de gestión de incidencias de seguridad de la información en una entidad bancaria*. Tesis (Título de ingeniero de sistemas). Lima, Universidad César Vallejo, 2015. 121 pp.

FERNÁNDEZ, Dámaris. *Modelo de gestión de riesgos de TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO/IEC 17799,*

Magerit para la Caja de Ahorro y Crédito SIPAN SA. Tesis (Título de ingeniero de Sistemas y Computación). Chiclayo, Universidad Católica Santo Toribio de Mogrovejo, 2015. 224 pp.

GARCÍA, Camilo. *Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001: 2005. Informe final de investigación* (Título de especialista en gerencia de tecnología). Bogotá, Universidad EAN, 2012.59 pp.

INCA, Rocío. *Implementación del sistema de seguridad de la información en el proceso de administración de base de datos (BD) del Hospital Municipal de Los Olivos.* Tesis (Título de ingeniero de sistemas). Lima, Universidad César Vallejo, 2012. 364 pp.

LEPAGE, Diana. *Diseño de un modelo de gobierno de TI con enfoque de seguridad de la información para empresas prestadoras de servicios de salud bajo la óptica de Cobit 5.0*. Tesis (Título de Ingeniero Informático). Lima, Pontificia Universidad Católica del Perú, 2014. 100 pp.

MOLINA, María. *Propuesta de un Plan de Gestión del Riesgos en Tecnología aplicado en la Escuela Superior Politécnica del Litoral*. Tesis (Título de Máster). Madrid, Universidad Politécnica de Madrid, 2015. 89 pp.

TIBAQUIRA, Yesid. *Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la norma ISO/IEC 27035 E ISO/IEC 27005*. Tesis (Título de Especialista en Seguridad Informática). Bogotá, Universidad Nacional Abierta y a Distancia de Colombia, 2015. 91 pp.

VILLENA, Moisés. *Sistema de gestión de seguridad de la información para una institución financiera*. Tesis (Título de Ingeniero Informático). Lima, Pontificia Universidad Católica del Perú, 2006. 76 pp.

DOCUMENTOS ELECTRÓNICOS

AHMED, Zahoor, HUSSAIN, Mahmood y AHMED, Javed. *Information security management needs more holistic approach: A literature review.* Preston, UK. International Journal of Information Management. (36): 215-225, 2015. ISSN: 0268-4012

ÁLVAREZ, Flor y GARCÍA, Pamela. *Implementación de un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud* [en línea]. Proyecto previo a tesis (Título de ingeniero en electrónica y redes de información). Quito: Escuela Politécnica Nacional, 2007. 298 pp. [Fecha de consulta: 24 de enero de 2016]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/565

BRADANOVIC, Tomás. *Conceptos básicos de Seguridad Informática* [en línea]. s.f. [fecha de consulta: 12 Enero 2016]. Disponible en: < http://www.bradanovic.cl/pcasual/ayuda3.html>.

FONSECA, Guillermo. *La información, el activo mas importante de cualquier organización* [en línea]. 2012 [fecha de consulta: 12 Enero 2016]. Disponible en: < https://guillermofonseca.wordpress.com/2012/04/18/la-informacion-el-activo-mas-importante-de-cualquier-organizacion/>.

GUERRERO, Marlene y GÓMEZ, Luis. *Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información*. Cali. Revista Estudios Gerenciales – Universidad ICESI. 27(121). Octubre – Diciembre 2011. ISSN: 0123-5923.

INSTITUTO Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Perú), *NTP-ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de la Información*. Lima: INDECOPI, 2014.

ISACA Information Systems Audit and Control Association. *Cobit 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa*. Madrid. Isaca, 2012. 94 pp.

MINISTERIO de Hacienda y Administraciones Públicas. *Magerit, Metodología de análisis y gestión de riesgos de los sistemas de información*. Libro I – Método. Madrid: 2012. 127 pp.

ORGANIZACIÓN Internacional de Normalización, *Norma ISO 27001. Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos*. ISO, 2005, 2013.

ORGANIZACIÓN Internacional de Normalización, *Norma ISO/IEC 31000. Administración del riesgo*. ISO, 2009.

ORGANIZACIÓN Internacional de Normalización, *Norma ISO 27005. Tecnología de la Información – Gestión de riesgos de la Seguridad de la Información*. ISO, 2005, 2011.

PACHECO, Federico. *La importancia de un SGSI* [en línea]. 2010 [fecha de consulta: 25 de Febrero 2016]. Disponible en: < http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/>.

PHILLIPS, Glenn. *Mission Impossible: 4 Reasons Compliance Is Impossible* [en línea]. 2013 [fecha de consulta: 12 Enero 2016]. Disponible en: <http://www.darkreading.com/risk/mission-impossible-4-reasons-compliance-is-impossible/d/d-id/1139416>.

SOHRABI, Nader, VON, Rossouw y FURNELL, Steven. *Information security policy compliance model in organizations. Computers & Security Journal* [en línea]. (56): 70–82, 2016. ISSN: 0167-4048.

ANEXOS

Anexo N° 1 - Matriz de consistencia

Título: Sistema de Gestión de Seguridad de Información para mejorar el proceso de gestión del riesgo en un Hospital Nacional

Problemas de investigación	Objetivos de investigación	Hipótesis	Variables	Dimensiones	Indicadores	Metodología y Diseño
Problema General	**Objetivo General**	**Hipótesis General**				
¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional?	Evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional.	La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva en el proceso de gestión del riesgo de un Hospital Nacional.	V.I.: Sistema de Gestión de Seguridad de la Información			**Metodología:** SGSI: ISO/IEC 27001:2013 Análisis de riesgos: Magerit v3.0 Aplicación de controles: ISO/IEC 27002:2013 **Tipo de investigación:** Aplicada **Tipo de Diseño:** Pre experimental.
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicas**				
PE1: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional?	OE1: Evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.	HE1: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva reduciendo el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.	V.D. Proceso de Gestión del riesgo	Evaluación del riesgo	Nivel de riesgo	**Instrumento:** - Ficha de Observación
PE2: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional?	OE2: Evaluar la manera en que la implementación del sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.	HE2: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.		Tratamiento del riesgo	Número de controles aplicados	

Anexo N° 2 – Matriz de operacionalización de las variables

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento	Escala de Medición
Proceso de gestión del riesgo	Para Peltier (2014), "El proceso de gestión de riesgos consiste en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable. Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo). A continuación, identifique los controles que llevarían el efecto a un nivel aceptable." (p. xxi).	El proceso de gestión del riesgo es un conjunto de fases sucesivas, que implican evaluar el riesgo y tratar el riesgo en el contexto de la organización, estas acciones involucran llevar el nivel de riesgo a un grado aceptable y determinar el número de controles aplicados para su reducir el riesgo, respectivamente, para ello, es necesario la aplicación de un instrumento de recopilación directa de datos, como es la Ficha de Observación.	Evaluación del riesgo	Nivel de riesgo	Ficha de Observación	Nominal
			Tratamiento del riesgo	Número de controles aplicados	Ficha de Observación	Nominal

ANEXO N° 3 – Relación de activos críticos de información identificados para la presente investigación

N°	CÓDIGO	NOMBRE DEL ACTIVO	TIPO	PROPIETARIO
1	A-01	Base de datos de Titulares	Datos	Jefe Unidad de Telemática
2	A-02	Base de datos de Pacientes	Datos	Jefe Unidad de Telemática
3	A-03	Base de datos de Farmacia	Datos	Jefe Unidad de Telemática
4	E-01	Sistema de Gestión de Salud	Aplicaciones	Jefe Unidad de Telemática
5	E-02	Sistema de Farmacia	Aplicaciones	Jefe Unidad de Telemática
6	E-03	Servicio web Acreditación de Derecho Habientes	Aplicaciones	Jefe Unidad de Telemática
7	E-04	MS Windows Server 2008, MS SQL Server 2008 R2	Software	Jefe Unidad de Telemática
8	E-05	Antivirus Corporativo NOD32	Software	Jefe Unidad de Telemática
9	D-01	Sub Director del Hospital	Software	Director del Hospital
10	D-02	Jefe de la Oficina de administración	Recursos humanos	Director del Hospital
11	D-03	Jefe de la Unidad de Telemática	Recursos humanos	Director del Hospital
12	D-04	Programador	Recursos humanos	Jefe Unidad de Telemática
13	S-01	Servidor de producción	Equipamiento	Jefe Unidad de Telemática
14	S-02	Servidor Backup	Equipamiento	Jefe Unidad de Telemática
15	S-03	Servidor de Antivirus	Equipamiento	Jefe Unidad de Telemática
16	S-04	Servidor de Desarrollo	Equipamiento	Jefe Unidad de Telemática
17	S-05	Switch Capa 3	Infraestructura	Jefe Unidad de Telemática
18	S-06	Web Filter	Infraestructura	Jefe Unidad de Telemática
19	S-07	Firewall	Infraestructura	Jefe Unidad de Telemática
20	H-01	Datacenter	Instalaciones	Jefe Unidad de Telemática
21	H-02	Centro de Energía	Instalaciones	Jefe Unidad de Telemática
22	H-03	Aire Acondicionado de Precisión	Instalaciones	Jefe Unidad de Telemática
23	H-04	Grupo Electrógeno	Instalaciones	Jefe Oficina de Servicios Generales

ANEXO N° 4 – Ficha de observación para el indicador Nivel de Riesgo en fase Pre Test

<table>
<tr><td rowspan="3"></td><td colspan="3">FICHA DE OBSERVACIÓN N° 01:
INDICADOR: NIVEL DEL RIESGO (SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES)
FASE: PRE TEST</td></tr>
<tr><td>CÓDIGO:
FO-001-HN PNP “LNS” OFAD/UT</td><td>VERSIÓN:
2.0</td><td>PÁGINA:
1/9</td></tr>
<tr><td>CLASIFICACIÓN:
CONFIDENCIAL</td><td>FECHA DISEÑO:
03-2017</td><td></td></tr>
<tr><td>Proceso:</td><td colspan="3">Gestión de riesgos</td></tr>
<tr><td>Investigador:</td><td colspan="3">Miguel Angel Ayala Medrano</td></tr>
<tr><td>Fecha de recolección:</td><td colspan="3">3 al 7 de Abril de 2017</td></tr>
<tr><td>Puesto:</td><td colspan="3">Jefe (e) de la Unidad de Telemática</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
</table>

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES
FASE: PRE TEST

ACTIVO CRÍTICO				AMENAZAS POTENCIALES		VULNERABILIDADES IMPORTANTES		EVALUACIÓN DEL RIESGO						
N°	CÓDIGO ACTIVO	ACTIVO	VALOR DEL ACTIVO		AMENAZA		VULNERABILIDAD	DEGRADACIÓN C	DEGRADACIÓN I	DEGRADACIÓN D	DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO
1	A-01	Base de datos de Titulares	4		Alteración de la Información		Falta de capacitación y educación en seguridad de la información	4	5	5	5	4.5	3	3.75
					Introducción de información Incorrecta		Falta de restricción del acceso a la información para usuarios	4	5	5	5	4.5	5	4.75
					Divulgación de La información		Carencia de toma de conciencia en seguridad	5	5	5	5	4.5	4	4.25
					Manipulación de la Configuración		Falta de restricción del acceso a la información para usuarios	4	5	5	5	4.5	3	4.25
					Acceso no autorizado		Falta de restricción del acceso a la información para usuarios	4	5	5	5	4.5	2	3.25
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	4	5	5	5	4.5	1	2.75
					Corrupción de la información		Carencia de backup o respaldo de la información	5	5	5	5	4.5	2	3.25
2	A-02	Base de datos de Pacientes	5		Alteración de la Información		Falta de capacitación y educación en seguridad de la información	4	5	5	5	5.0	3	4.00
					Introducción de información Incorrecta		Falta de restricción del acceso a la información para usuarios	4	5	5	5	5.0	4	4.50
					Divulgación de La información		Carencia de toma de conciencia en seguridad	5	4	5	5	5.0	3	4.00
					Manipulación de la Configuración		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	3	4.00
					Acceso no autorizado		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.5	2	3.25
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	2	3.50
					Corrupción de la información		Carencia de backup o respaldo de la información	5	5	5	5	5.0	2	3.50
3	A-02	Base de datos de Farmacia	4		Alteración de la Información		Falta de capacitación y educación en seguridad de la información	4	4	4	4	4.0	3	3.50

					Introducción de información Incorrecta		Falta de restricción del acceso a la información para usuarios	4	4	5	5	4.5	3	4.25
					Divulgación de La información		Carencia de toma de conciencia en seguridad	5	5	5	5	4.5	4	4.25
					Manipulación de la Configuración		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.0	3	3.50
					Acceso no autorizado		Falta de restricción del acceso a la información para usuarios	4	4	5	5	4.5	3	4.25
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	5	5	5	5	4.5	3	4.25
					Corrupción de la información		Carencia de backup o respaldo de la información	3	4	4	4	4.0	2	3.00
4	E-01	Sistema de Gestión de Salud	5		Errores de Usuario		Falta de capacitación	4	4	5	5	5.0	4	4.50
					Errores de Administrador		Falta de capacitación	4	5	5	5	5.0	4	4.50
					Errores de Configuración		Falta de capacitación	3	4	4	4	4.5	3	3.75
					Escape de Información		Carencia de toma de conciencia en seguridad	4	4	5	5	5.0	4	4.50
					Vulnerabilidad del Sistema		Falta de procedimientos para el monitoreo de sistemas	5	5	5	5	5.0	4	4.50
					Caída del Sistema		Carencia de sistema de contingencia	3	4	4	4	4.5	5	4.75
					Error en Actualización del Sistema		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	5	5	5.0	4	4.5
					Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas de información	5	5	5	5	5.0	3	4.00
					Suplantación de Identidad de Usuario		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	4	4.50
					Abuso de Privilegios de Acceso		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	4	4.50
					Uso no previsto		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.5	3	3.75
					Difusión de Software dañino		Falta de registro de fallas e incidencias	4	4	5	5	5.0	4	4.50
					Acceso no Autorizado		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	3	4.00
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.5	3	3.75
					Manipulación de Programas		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	4	4	4.5	4	4.25
5	E-02	Sistema de Farmacia	4		Errores de Usuario		Falta de capacitación	4	4	5	5	5.0	4	4.50
					Errores de Administrador		Falta de capacitación	4	5	5	5	5.0	4	4.50
					Errores de Configuración		Falta de capacitación	3	4	4	4	4.5	5	4.75

					Escape de Información		Carencia de toma de conciencia en seguridad	4	4	5	5	5.0	4	4.50
					Vulnerabilidad del Sistema		Falta de procedimientos para el monitoreo de sistemas	5	5	5	5	5.0	4	4.50
					Caída del Sistema		Carencia de sistema de contingencia	3	4	4	4	4.5	5	4.75
					Error en Actualización del Sistema		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	5	5	5.0	5	5.00
					Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas de información	5	5	5	5	5.0	3	4.00
					Suplantación de Identidad de Usuario		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	4	4.50
					Abuso de Privilegios de Acceso		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	4	4.50
					Uso no previsto		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.5	4	4.25
					Difusión de Software dañino		Falta de registro de fallas e incidencias	4	4	5	5	5.0	4	4.50
					Acceso no Autorizado		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	4	4.50
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.5	3	3.75
					Manipulación de Programas		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	4	4	4.5	4	4.25
6	E-03	Servicio web Acreditación de Derecho Habientes	5		Errores de Usuario		Falta de capacitación	4	4	5	5	5.0	4	4.50
					Errores de Configuración		Falta de capacitación	4	5	5	5	5.0	4	4.50
					Escape de Información		Carencia de toma de conciencia en seguridad	3	4	4	4	4.5	5	4.75
					Vulnerabilidad del Sistema		Falta de procedimientos para el monitoreo de sistemas	4	4	5	5	5.0	4	4.50
					Caída del Sistema		Carencia de sistema de contingencia	5	5	5	5	5.0	4	4.50
					Error en Actualización del Sistema		Incumplimiento de las políticas para la protección de los sistemas de información	3	4	4	4	4.5	5	4.75
					Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	5	5	5.0	5	5.00
					Suplantación de Identidad de Usuario		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	3	4.00

					Abuso de Privilegios de Acceso		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	4	4.50
					Uso no previsto		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	4	4.50
					Difusión de Software dañino		Falta de registro de fallas e incidencias	3	4	4	4	4.5	4	4.25
					Acceso no Autorizado		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	4	4.50
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	5	5	5	5	5.0	4	4.50
					Manipulación de Programas		Incumplimiento de las políticas para la protección de los sistemas de información	5	5	5	5	5.0	4	4.50
7	E-04	MS Windows Server 2008, MS SQL Server 2008 R2	5		Caída de aplicaciones o del sistema operativo		Falta de registro de fallas e incidencias	5	4	4	5	5.0	4	4.50
					Errores de mantenimiento o actualización de programas		Falta definir responsabilidades de seguridad	5	4	4	5	5.0	4	4.50
8	E-04	Antivirus Corporativo NOD32	3		Caída de aplicaciones o del sistema operativo		Falta de registro de fallas e incidencias	3	4	3	4	3.5	4	3.75
					Difusión de software dañino		Falta o falla de controles contra código malicioso	3	4	4	4	3.5	3	3.25
					Errores de mantenimiento o actualización de programas		Incumplimiento de las políticas para la protección de los sistemas de información	3	4	4	4	3.5	3	3.25
9	D-01	Sub Director del Hospital	5		Deficiencias en la organización		Falta de control y supervisión en la organización	4	4	4	4	4.5	4	4.25
					Indisponibilidad del personal		Falta de personal para desempeñar el rol	4	4	5	5	5.0	4	4.50
					Segregación responsabilidades		Falta de control y supervisión en la organización	3	3	3	3	4.0	2	3.00
10	D-02	Jefe de la Oficina de administración	4		Deficiencias en la organización		Falta de control y supervisión en la organización	4	4	4	4	4.5	4	4.25
					Indisponibilidad del personal		Falta de personal para desempeñar el rol	4	4	5	5	5.0	4	4.50
					Segregación responsabilidades		Falta de control y supervisión en la organización	3	3	3	3	4.0	2	3.00
11	D-03	Jefe de la Unidad de Telemática	5		Deficiencias en la organización		Falta de control y supervisión en la organización	4	4	4	4	4.5	4	4.25
					Indisponibilidad del personal		Falta de personal para desempeñar el rol	4	4	4	4	4.0	4	4.00
					Segregación responsabilidades		Falta de control y supervisión en la organización	3	3	3	3	3.5	2	2.75

12	D-04	Programador	5		Indisponibilidad del personal		Falta de personal para desempeñar el rol	4	4	4	4	4.5	4	4.25
					Introducción de información incorrecta		Falta de capacitación y educación en seguridad de información	4	4	4	4	4.5	4	4.25
					Fraudes		Carencia de toma de conciencia en seguridad	4	5	3	5	4.5	2	3.25
13	S-01	Servidor de producción	5		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	4	4	3	4	4.5	3	3.75
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	4	3	3	4	4.5	4	4.25
					Caída de servidor		Carencia de sistema de contingencia	3	3	4	4	4.5	4	4.25
14	S-02	Servidor Backup	4		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	4	4	3	4	4.5	3	3.75
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	4	3	3	4	4.5	4	4.25
					Caída de servidor		Carencia de sistema de contingencia	3	3	4	4	4.5	4	4.25
15	S-03	Servidor de Antivirus	3		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	3	3	3	3	3.0	3	3.00
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	3	2	2	3	3.0	4	3.50
					Caída de servidor		Carencia de sistema de contingencia	3	3	3	3	3.0	4	3.50
16	S-04	Servidor de Desarrollo	2		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	3	3	3	3	3.0	3	3.00
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	3	2	2	3	3.0	4	3.50
					Caída de servidor		Carencia de sistema de contingencia	3	3	3	3	3.0	4	3.50
17	S-05	Switch Capa 3	4		Manipulación de la Configuración		Falta de políticas y procedimientos operativos específicos	2	2	3	3	3.5	3	3.25
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	3	3	3.5	3	3.25
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	3	3	3.5	3	3.25
18	S-06	Web Filter	2		Manipulación de la Configuración		Falta de políticas y procedimientos operativos específicos	2	2	3	3	3.5	2	2.75

					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	3	3	3.5	2	2.75
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	3	3	3.5	2	2.75
19	S-07	Firewall	3		Manipulación de la Configuración		Falta de políticas y procedimientos operativos específicos	2	2	3	3	3.5	2	2.75
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	3	3	3.5	2	2.75
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	3	3	3.5	2	2.75
20	H-01	Datacenter	5		Acceso no Autorizado		Falta de restricción del acceso a áreas críticas	4	5	3	5	4.5	2	3.25
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	4	4	3	4	4.5	3	3.75
					Pérdida de energía eléctrica		Falta o deficiencia en protección contra amenazas externas y ambientales	4	3	3	4	4.5	4	4.25
21	H-02	Centro de Energía	4		Manipulación de la Configuración			3	3	4	4	4.0	4	4.00
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	3	3	3	3	3.5	4	3.75
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	3	3	3.5	3	3.25
					Pérdida de energía eléctrica		Falta o deficiencia en protección contra amenazas externas y ambientales	2	2	3	3	3.5	3	3.25
22	H-03	Aire Acondicionado de Precisión	4		Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas	3	3	4	4	4.0	3	3.50
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	3	3	3	3	3.5	3	3.25
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	3	3	3.5	3	3.25
23	H-04	Grupo Electrógeno	4		Avería de origen físico		Falla en la seguridad de la eliminación o reutilización del equipo	3	3	4	4	4.0	3	3.50
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	3	3	3	3	3.5	3	3.25
					Interrupción de otros servicios y suministros esenciales		Inadecuadas medidas de control de seguridad para equipos fuera del local	2	2	3	3	3.5	3	3.25
NIVEL DE RIESGO														**3.72**

INDICACIONES

1. Valoración de los activos

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la importancia para la organización:

Escala de valoración	Descripción	Valor
Muy alta	De vital importancia para los objetivos que persigue la organización	5
Alta	Altamente importante para la organización	4
Media	Importante para la organización	3
Baja	Importancia menor para el desarrollo de la organización	2
Muy baja	Irrelevante para efectos prácticos	1

Tabla N° 01 – Escala de puntuaciones de valores de los activos

2. Valoración de la degradación

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la confidencialidad, integridad, disponibilidad de cada uno de los activos.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

Puntuación	Disponibilidad	Integridad	Confidencialidad
5	Siempre	Extrema	Uso confidencial
4	Exenta por horas	Importante	Uso restringido
3	Exenta por 24 horas	Media	Semi restringido
2	Exenta por 48 horas	No importante	Uso interno
1	Exenta por varios días	Insignificante	Acceso público

Tabla N° 02 – Escala de puntuaciones de valores de la degradación

3. Degradación máxima

Al obtener cada uno de los puntajes asignados en la degradación, se determina el máximo valor de la degradación, dato que nos servirá para calcular el nivel de riesgo.

4. Valoración del impacto

El valor del impacto se determina por el promedio entre la degradación máxima y el valor del activo:

Impacto = (Degradación máxima + Valor del activo) / 2

5. Probabilidad

La probabilidad es la posibilidad de que se lleve a cabo una amenaza. Para la presente investigación, se determina en la siguiente escala:

Escala de valoración	Descripción	Valor
Muy alta	Nivel de probabilidad del activo es muy alta	5
Alta	Nivel de probabilidad del activo es alta	4
Media	Nivel de probabilidad del activo es media	3
Baja	Nivel de probabilidad del activo es baja	2
Muy baja	Nivel de probabilidad del activo es muy baja	1

Tabla N° 03 – Escala de puntuaciones de la probabilidad

6. Valoración del riesgo

El valor del riesgo se determina por el promedio entre el impacto y la probabilidad:

Riesgo = (Impacto + Probabilidad) / 2

ANEXO N° 5 – Ficha de observación para el indicador Número de Controles Aplicados en fase Pre Test

<table>
<tr><td rowspan="3"></td><td colspan="3">FICHA DE OBSERVACIÓN N° 02:
INDICADOR: NÚMERO DE CONTROLES APLICADOS
(DECLARACIÓN DE APLICABILIDAD DE CONTROLES)
FASE: PRE TEST</td></tr>
<tr><td>CÓDIGO:
FO-002-HN PNP “LNS” OFAD/UT</td><td>VERSIÓN:
2.0</td><td rowspan="2">PÁGINA:
1/9</td></tr>
<tr><td>CLASIFICACIÓN:
CONFIDENCIAL</td><td>FECHA DISEÑO:
03-2017</td></tr>
<tr><td>Proceso:</td><td colspan="3">Gestión de riesgos</td></tr>
<tr><td>Investigador:</td><td colspan="3">Miguel Angel Ayala Medrano</td></tr>
<tr><td>Fecha de recolección:</td><td colspan="3">3 al 7 de Abril de 2017</td></tr>
<tr><td>Puesto:</td><td colspan="3">Jefe (e) de la Unidad de Telemática</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
</table>

FICHA DE OBSERVACIÓN: INDICADOR NÚMERO DE CONTROLES APLICADOS DECLARACIÓN DE APLICABILIDAD DE CONTROLES FASE: PRE TEST				
OBJETIVOS DE CONTROL		CONTROLES	¿APLICA? SI/NO	¿EXISTE? SI/NO/PARCIAL
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
5.1 Directrices de la Dirección en seguridad de la información.				
	5.1.1 Conjunto de políticas para la seguridad de la información	Control: La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.	S	N
	5.1.2 Revisión de las políticas para la seguridad de la información.	Control: Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas.	S	N
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
6.1 Organización interna				
	6.1.1 Asignación de responsabilidades para la segur. de la información.	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	S	N
	6.1.2 Segregación de tareas.	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	S	N
	6.1.3 Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes	S	S
	6.1.4 Contacto con grupos de interés especial.	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	S	N
	6.1.5 Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto	S	N
6.2 Dispositivos para movilidad y teletrabajo.				
	6.2.1 Política de uso de dispositivos para movilidad.	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	N	N
	6.2.2 Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	N	N
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.				
7.1 Antes de la contratación.				
	7.1.1 Investigación de antecedentes.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	S	N
	7.1.2 Términos y condiciones de contratación.	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	S	N
7.2 Durante la contratación.				
	7.2.1 Responsabilidades de gestión.	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de	S	N

		acuerdo con las políticas y procedimientos establecidos por la organización.		
	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	S	N
	7.2.3 Proceso disciplinario.	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	S	N
7.3 Cese o cambio de puesto de trabajo.				
	7.3.1 Cese o cambio de puesto de trabajo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	S	N
8. GESTIÓN DE ACTIVOS.				
8.1 Responsabilidad sobre los activos.				
	8.1.1 Inventario de activos.	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	S	P
	8.1.2 Propiedad de los activos.	Control: Los activos mantenidos en el inventario deberían tener un propietario.	S	P
	8.1.3 Uso aceptable de los activos.	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	S	N
	8.1.4 Devolución de activos.	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	S	P
8.2 Clasificación de la información.				
	8.2.1 Directrices de clasificación.	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	S	S
	8.2.2 Etiquetado y manipulado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	S	N
	8.2.3 Manipulación de activos.	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	S	S
8.3 Manejo de los soportes de almacenamiento				
	8.3.1 Gestión de soportes extraíbles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	S	N
	8.3.2 Eliminación de soportes.	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	S	N
	8.3.3 Soportes físicos en tránsito.	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte	S	N
9. CONTROL DE ACCESOS.				
9.1 Requisitos de negocio para el control de accesos.				
	9.1.1 Política de control de accesos.	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	S	N

	9.1.2 Control de acceso a las redes y servicios asociados.	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	S	N
9.2 Gestión de acceso de usuario.				
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso	S	P
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	S	P
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	S	N
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	S	N
	9.2.5 Revisión de los derechos de acceso de los usuarios.	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	S	P
	9.2.6 Retirada o adaptación de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	S	N
9.3 Responsabilidades del usuario.				
	9.3.1 Uso de información confidencial para la autenticación.	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta	S	N
9.4 Control de acceso a sistemas y aplicaciones.				
	9.4.1 Restricción del acceso a la información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	S	P
	9.4.2 Procedimientos seguros de inicio de sesión	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	S	P
	9.4.3 Gestión de contraseñas de usuario	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	S	N
	9.4.4 Uso de herramientas de administración de sistemas	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	S	N
	9.4.5 Control de acceso al código fuente de los programas	Control: Se debería restringir el acceso a los códigos fuente de los programas	S	N
10 CIFRADO				
10.1 Controles criptográficos.				
	10.1.1 Política de uso de los controles criptográficos.	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	N	N
	10.1.2 Gestión de claves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	N	N
11. SEGURIDAD FÍSICA Y AMBIENTAL.				
11.1 Áreas seguras.				
	11.1.1 Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información	S	N

	11.1.2 Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado	S	N
	11.1.3 Seguridad de oficinas, despachos y recursos.	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	S	P
	11.1.4 Protección contra las amenazas externas y ambientales.	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	S	P
	11.1.5 El trabajo en áreas seguras.	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	S	N
	11.1.6 Áreas de acceso público, carga y descarga.	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado	S	N
11.2 Seguridad de los equipos.				
	11.2.1 Emplazamiento y protección de equipos.	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado	S	S
	11.2.2 Instalaciones de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	S	S
	11.2.3 Seguridad del cableado.	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño	S	P
	11.2.4 Mantenimiento de los equipos.	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	S	P
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	S	N
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones	N	N
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	S	N
	11.2.8 Equipo informático de usuario desatendido.	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	S	N
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	S	N
12. SEGURIDAD EN LA OPERATIVA.				
12.1 Responsabilidades y procedimientos de operación				
	12.1.1 Documentación de procedimientos de operación.	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	S	S
	12.1.2 Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	S	S
	12.1.3 Gestión de capacidades	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los	S	P

		ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.		
	12.1.4 Separación de entornos de desarrollo, prueba y producción	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	S	P
12.2 Protección contra código malicioso				
	12.2.1 Controles contra el código malicioso	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos	S	N
12.3 Copias de seguridad.				
	12.3.1 Copias de seguridad de la información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	S	S
12.4 Registro de actividad y supervisión				
	12.4.1 Registro y gestión de eventos de actividad.	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	S	P
	12.4.2 Protección de los registros de información.	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	S	N
	12.4.3 Registros de actividad del administrador y operador del sistema.	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	S	N
	12.4.4 Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	S	N
12.5 Control del software en explotación.				
	12.5.1 Instalación del software en sistemas en producción	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	S	N
12.6 Gestión de la vulnerabilidad técnica.				
	12.6.1 Gestión de las vulnerabilidades técnicas.	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	S	N
	12.6.2 Restricciones en la instalación de software.	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	S	N
12.7 Consideraciones de las auditorías de los sistemas de información.				
	12.7.1 Controles de auditoría de los sistemas de información.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	S	S
13. SEGURIDAD EN LAS TELECOMUNICACIONES				
13.1 Gestión de la seguridad en las redes				
	13.1.1 Controles de red.	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	S	S
	13.1.2 Mecanismos de seguridad asociados a servicios en red	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	S	P
	13.1.3 Segregación de redes.	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes	S	N
13.2 Intercambio de información con partes externas.				
	13.2.1 Políticas y procedimientos de intercambio de información.	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia	N	N

		de información mediante el uso de todo tipo de instalaciones de comunicación.		
	13.2.2 Acuerdos de intercambio.	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	N	N
	13.2.3 Mensajería electrónica.	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	S	N
	13.2.4 Acuerdos de confidencialidad y secreto.	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	S	N
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.				
14.1 Requisitos de seguridad de los sistemas de información.				
	14.1.1 Análisis y especificación de los requisitos de seguridad.	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	S	N
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	S	N
	14.1.3 Protección de las transacciones por redes telemáticas.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	S	N
14.2 Seguridad en los procesos de desarrollo y soporte.				
	14.2.1 Política de desarrollo seguro de software.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	S	N
	14.2.2 Procedimientos de control de cambios en los sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	S	N
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización	S	N
	14.2.4 Restricciones a los cambios en los paquetes de software.	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	S	N
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	S	N
	14.2.6 Seguridad en entornos de desarrollo.	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	S	N
	14.2.7 Externalización del desarrollo de software.	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	N	N
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	S	N
	14.2.9 Pruebas de aceptación.	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación	S	N

		relacionados.		
14.3 Datos de prueba.				
	14.3.1 Protección de los datos utilizados en pruebas.	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	S	N
15. RELACIONES CON SUMINISTRADORES.				
15.1 Seguridad de la información en las relaciones con suministradores.				
	15.1.1 Política de seguridad de la información para suministradores.	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	S	N
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	S	N
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	S	N
15.2 Gestión de la prestación del servicio por suministradores.				
	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	S	N
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	S	N
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.				
16.1 Gestión de incidentes de seguridad de la información y mejoras.				
	16.1.1 Responsabilidades y procedimientos.	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	S	N
	16.1.2 Notificación de los eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	S	N
	16.1.3 Notificación de puntos débiles de la seguridad.	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios	S	N
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	S	N
	6.1.5 Respuesta a los incidentes de seguridad.	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	S	N
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	S	N
	16.1.7 Recopilación de evidencias.	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	S	N

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.				
17.1 Continuidad de la seguridad de la información.				
	17.1.1 Planificación de la continuidad de la seguridad de la información.	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	S	N
	17.1.2 Implantación de la continuidad de la seguridad de la información.	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	S	N
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.	S	N
17.2 Redundancias.				
	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	S	S
18. CUMPLIMIENTO				
18.1 Cumplimiento de los requisitos legales y contractuales.				
	18.1.1 Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	S	P
	18.1.2 Derechos de propiedad intelectual (DPI).	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	S	P
	18.1.3 Protección de los registros de la organización.	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	S	N
	18.1.4 Protección de datos y privacidad de la información personal.	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	S	N
	18.1.5 Regulación de los controles criptográficos.	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	N	N
18.2 Revisiones de la seguridad de la información.				
	18.2.1 Revisión independiente de la seguridad de la información.	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	S	S
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	S	N
	18.2.3 Comprobación del cumplimiento.	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	S	N

ANEXO N° 6 – Ficha de observación para el indicador Nivel de Riesgo en fase Post Test

<table>
<tr><td rowspan="3"></td><td colspan="3">FICHA DE OBSERVACIÓN N° 01:
INDICADOR: NIVEL DEL RIESGO (SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES)
FASE: POST TEST</td></tr>
<tr><td>CÓDIGO:
FO-003-HN PNP “LNS” OFAD/UT</td><td>VERSIÓN:
2.0</td><td>PÁGINA:
1/9</td></tr>
<tr><td>CLASIFICACIÓN:
CONFIDENCIAL</td><td>FECHA DISEÑO:
03-2017</td><td></td></tr>
<tr><td>Proceso:</td><td colspan="3">Gestión de riesgos</td></tr>
<tr><td>Investigador:</td><td colspan="3">Miguel Angel Ayala Medrano</td></tr>
<tr><td>Fecha de recolección:</td><td colspan="3">26 al 30 de Junio de 2017</td></tr>
<tr><td>Puesto:</td><td colspan="3">Jefe (e) de la Unidad de Telemática</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
</table>

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES
FASE: POST TEST

ACTIVO CRÍTICO				AMENAZAS POTENCIALES		VULNERABILIDADES IMPORTANTES		EVALUACIÓN DEL RIESGO						
N°	CÓDIGO ACTIVO	ACTIVO	VALOR DEL ACTIVO		AMENAZA		VULNERABILIDAD	DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO
								C	I	D				
1	A-01	Base de datos de Titulares	4		Alteración de la Información		Falta de capacitación y educación en seguridad de la información	4	4	4	4	4.0	2	3.00
					Introducción de información Incorrecta		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.0	4	4.00
					Divulgación de La información		Carencia de toma de conciencia en seguridad	3	4	4	4	4.0	3	3.50
					Manipulación de la Configuración		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.0	2	3.00
					Acceso no autorizado		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.0	1	2.50
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.0	1	2.50
					Corrupción de la información		Carencia de backup o respaldo de la información	4	4	4	4	4.0	1	2.50
2	A-02	Base de datos de Pacientes	5		Alteración de la Información		Falta de capacitación y educación en seguridad de la información	3	4	4	5	5.0	3	4.00
					Introducción de información Incorrecta		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.50	3	3.75
					Divulgación de La información		Carencia de toma de conciencia en seguridad	4	4	4	4	4.50	3	3.75
					Manipulación de la Configuración		Falta de restricción del acceso a la información para usuarios	4	3	4	4	4.50	2	3.25
					Acceso no autorizado		Falta de restricción del acceso a la información para usuarios	3	3	4	4	4.50	1	2.75
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	3	3	3	4.00	1	2.50
					Corrupción de la información		Carencia de backup o respaldo de la información	4	4	4	4	4.50	1	2.75
3	A-02	Base de datos de Farmacia	4		Alteración de la Información		Falta de capacitación y educación en seguridad de la información	3	3	4	4	4.0	3	3.50
					Introducción de información Incorrecta		Falta de restricción del acceso a la información para usuarios	3	3	4	4	4.0	2	3.00

					Divulgación de La información		Carencia de toma de conciencia en seguridad	4	4	5	5	4.5	3	3.75
					Manipulación de la Configuración		Falta de restricción del acceso a la información para usuarios	3	3	4	4	4.0	2	3.00
					Acceso no autorizado		Falta de restricción del acceso a la información para usuarios	3	3	4	4	4.0	2	3.00
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.0	2	3.00
					Corrupción de la información		Carencia de backup o respaldo de la información	3	4	4	4	4.0	1	2.50
4	E-01	Sistema de Gestión de Salud	5		Errores de Usuario		Falta de capacitación	3	3	4	4	4.5	4	4.25
					Errores de Administrador		Falta de capacitación	3	4	4	4	4.5	3	3.75
					Errores de Configuración		Falta de capacitación	3	3	3	3	4.0	3	3.50
					Escape de Información		Carencia de toma de conciencia en seguridad	3	3	4	3	4.0	3	3.50
					Vulnerabilidad del Sistema		Falta de procedimientos para el monitoreo de sistemas	4	4	4	4	4.5	3	3.75
					Caída del Sistema		Carencia de sistema de contingencia	3	3	3	3	4.0	4	4.00
					Error en Actualización del Sistema		Incumplimiento de las políticas para la protección de los sistemas de información	3	3	4	4	4.5	4	4.25
					Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	4	4	4.5	3	3.75
					Suplantación de Identidad de Usuario		Falta de restricción del acceso a la información para usuarios	3	4	4	4	4.5	3	3.75
					Abuso de Privilegios de Acceso		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.5	3	3.75
					Uso no previsto		Falta de restricción del acceso a la información para usuarios	3	3	3	3	4.0	3	3.50
					Difusión de Software dañino		Falta de registro de fallas e incidencias	4	3	4	4	4.5	3	3.75
					Acceso no Autorizado		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.5	2	3.25
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	3	3	3	4.0	2	3.00
					Manipulación de Programas		Incumplimiento de las políticas para la protección de los sistemas de información	3	3	3	3	4.0	3	3.50
5	E-02	Sistema de Farmacia	4		Errores de Usuario		Falta de capacitación	3	4	4	4	4.0	3	3.50
					Errores de Administrador		Falta de capacitación	3	4	4	4	4.0	4	4.00
					Errores de Configuración		Falta de capacitación	3	3	4	4	4.0	4	4.00
					Escape de Información		Carencia de toma de conciencia en seguridad	3	4	4	4	4.0	3	3.50

					Vulnerabilidad del Sistema		Falta de procedimientos para el monitoreo de sistemas	4	4	4	4	4.0	3	3.50
					Caída del Sistema		Carencia de sistema de contingencia	3	3	3	3	3.5	4	3.75
					Error en Actualización del Sistema		Incumplimiento de las políticas para la protección de los sistemas de información	3	3	4	4	4.0	3	3.50
					Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas de información	4	4	4	4	4.0	3	3.50
					Suplantación de Identidad de Usuario		Falta de restricción del acceso a la información para usuarios	3	3	4	4	4.0	3	3.50
					Abuso de Privilegios de Acceso		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.0	3	3.50
					Uso no previsto		Falta de restricción del acceso a la información para usuarios	2	2	3	3	3.5	3	3.75
					Difusión de Software dañino		Falta de registro de fallas e incidencias	3	3	4	4	4.0	3	3.50
					Acceso no Autorizado		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.0	3	3.50
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	3	3	3	3	3.5	2	2.75
					Manipulación de Programas		Incumplimiento de las políticas para la protección de los sistemas de información	3	3	3	3	3.5	3	3.25
6	E-03	Servicio web Acreditación de Derecho Habientes	5		Errores de Usuario		Falta de capacitación	3	3	4	4	4.5	4	4.25
					Errores de Configuración		Falta de capacitación	4	4	4	4	4.5	4	4.25
					Escape de Información		Carencia de toma de conciencia en seguridad	3	3	4	4	4.5	4	4.25
					Vulnerabilidad del Sistema		Falta de procedimientos para el monitoreo de sistemas	3	4	4	4	4.5	3	3.75
					Caída del Sistema		Carencia de sistema de contingencia	4	4	4	4	4.5	3	3.75
					Error en Actualización del Sistema		Incumplimiento de las políticas para la protección de los sistemas de información	2	3	4	4	4.5	3	3.75
					Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas de información	3	4	4	4	4.5	3	3.75
					Suplantación de Identidad de Usuario		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.5	3	3.75
					Abuso de Privilegios de Acceso		Falta de restricción del acceso a la información para usuarios	4	3	4	4	4.5	3	3.75

					Uso no previsto		Falta de restricción del acceso a la información para usuarios	4	4	4	4	4.5	4	4.25
					Difusión de Software dañino		Falta de registro de fallas e incidencias	3	3	4	4	4.5	4	4.25
					Acceso no Autorizado		Falta de restricción del acceso a la información para usuarios	3	3	4	4	4.5	3	3.50
					Interceptación de Información		Falta de restricción del acceso a la información para usuarios	4	4	5	5	5.0	3	4.00
					Manipulación de Programas		Incumplimiento de las políticas para la protección de los sistemas de información	4	5	5	5	5.0	4	4.50
7	E-04	MS Windows Server 2008, MS SQL Server 2008 R2	5		Caída de aplicaciones o del sistema operativo		Falta de registro de fallas e incidencias	4	3	4	4	4.50	4	4.25
					Errores de mantenimiento o actualización de programas		Falta definir responsabilidades de seguridad	4	4	4	4	4.50	4	4.25
8	E-04	Antivirus Corporativo NOD32	3		Caída de aplicaciones o del sistema operativo		Falta de registro de fallas e incidencias	3	3	3	3	3.0	4	3.50
					Difusión de software dañino		Falta o falla de controles contra código malicioso	3	3	3	3	3.0	3	3.00
					Errores de mantenimiento o actualización de programas		Incumplimiento de las políticas para la protección de los sistemas de información	3	3	3	3	3.0	3	3.00
9	D-01	Sub Director del Hospital	5		Deficiencias en la organización		Falta de control y supervisión en la organización	3	4	4	4	4.5	4	4.25
					Indisponibilidad del personal		Falta de personal para desempeñar el rol	3	3	4	4	4.5	3	3.75
					Segregación responsabilidades		Falta de control y supervisión en la organización	2	3	3	3	4.0	2	3.00
10	D-02	Jefe de la Oficina de administración	4		Deficiencias en la organización		Falta de control y supervisión en la organización	4	4	4	4	4.5	4	4.25
					Indisponibilidad del personal		Falta de personal para desempeñar el rol	4	4	5	5	5.0	4	4.50
					Segregación responsabilidades		Falta de control y supervisión en la organización	3	3	3	3	4.0	2	3.00
11	D-03	Jefe de la Unidad de Telemática	5		Deficiencias en la organización		Falta de control y supervisión en la organización	3	3	3	3	4.0	3	3.50
					Indisponibilidad del personal		Falta de personal para desempeñar el rol	3	4	4	4	4.5	3	3.75
					Segregación responsabilidades		Falta de control y supervisión en la organización	2	3	3	3	4.0	2	3.00
12	D-04	Programador	5		Indisponibilidad del personal		Falta de personal para desempeñar el rol	3	3	3	3	4.0	3	3.50

					Introducción de información incorrecta		Falta de capacitación y educación en seguridad de información	3	3	3	3	4.0	2	3.00
					Fraudes		Carencia de toma de conciencia en seguridad	3	3	3	3	4.0	2	3.00
13	S-01	Servidor de producción	5		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	3	4	3	4	4.5	3	3.75
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	3	3	3	3	4.0	3	3.50
					Caída de servidor		Carencia de sistema de contingencia	3	3	4	4	4.5	3	3.75
14	S-02	Servidor Backup	4		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	3	3	3	3	3.5	3	3.25
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	3	3	3	4	4.0	3	3.50
					Caída de servidor		Carencia de sistema de contingencia	3	3	4	4	4.0	3	3.50
15	S-03	Servidor de Antivirus	3		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	3	2	2	3	3.0	3	3.00
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	2	2	2	2	2.5	3	2.25
					Caída de servidor		Carencia de sistema de contingencia	3	2	2	3	3.0	3	3.00
16	S-04	Servidor de Desarrollo	2		Errores de mantenimiento o actualización de equipos		Inadecuado mantenimiento de equipos	2	3	3	3	2.5	3	2.25
					Manipulación de hardware y/o equipos		Falta de políticas y procedimientos operativos específicos	2	2	2	2	2.0	3	2.50
					Caída de servidor		Carencia de sistema de contingencia	2	2	3	3	2.5	3	2.75
17	S-05	Switch Capa 3	4		Manipulación de la Configuración		Falta de políticas y procedimientos operativos específicos	2	2	2	2	3.0	2	2.50
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	2	2	3.0	2	2.50
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	2	2	3.0	2	2.50
18	S-06	Web Filter	2		Manipulación de la Configuración		Falta de políticas y procedimientos operativos específicos	2	2	2	2	2.0	2	2.00
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	2	2	2.0	2	2.00

					Errores de monitorización		Falla de mecanismos de monitoreo	1	2	2	2	2.0	1	1.50
19	S-07	Firewall	3		Manipulación de la Configuración		Falta de políticas y procedimientos operativos específicos	2	2	2	2	2.5	1	1.75
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	2	2	2.5	1	1.75
					Errores de monitorización		Falla de mecanismos de monitoreo	1	1	2	2	2.5	1	1.75
20	H-01	Datacenter	5		Acceso no Autorizado		Falta de restricción del acceso a áreas críticas	4	4	3	4	4.5	2	3.25
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	4	4	3	4	4.5	2	3.25
					Pérdida de energía eléctrica		Falta o deficiencia en protección contra amenazas externas y ambientales	3	3	3	3	4.0	3	3.50
21	H-02	Centro de Energía	4		Manipulación de la Configuración			3	3	3	3	3.5	3	3.25
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	2	3	3	3.5	3	3.25
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	2	2	3.0	3	3.00
					Pérdida de energía eléctrica		Falta o deficiencia en protección contra amenazas externas y ambientales	2	2	2	2	3.0	3	3.00
22	H-03	Aire Acondicionado de Precisión	4		Manipulación de la Configuración		Incumplimiento de las políticas para la protección de los sistemas	3	3	3	3	3.5	3	3.25
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	3	3	3	3.5	3	3.25
					Errores de monitorización		Falla de mecanismos de monitoreo	2	2	2	2	3.0	2	2.50
23	H-04	Grupo Electrógeno	4		Avería de origen físico		Falla en la seguridad de la eliminación o reutilización del equipo	3	3	3	3	3.5	3	3.25
					Errores de mantenimiento		Inadecuado mantenimiento de equipos	2	3	3	3	3.5	2	2.75
					Interrupción de otros servicios y suministros esenciales		Inadecuadas medidas de control de seguridad para equipos fuera del local	1	2	2	2	3.0	2	2.50
													NIVEL DE RIESGO	**3.09**

ANEXO N° 7 – Ficha de observación para el indicador Número de Controles Aplicados en fase Post Test

<table>
<tr><td rowspan="3"></td><td colspan="3">FICHA DE OBSERVACIÓN N° 02:
INDICADOR: NÚMERO DE CONTROLES APLICADOS
(DECLARACIÓN DE APLICABILIDAD DE CONTROLES)
FASE: POST TEST</td></tr>
<tr><td>CÓDIGO:
FO-004-HN PNP “LNS” OFAD/UT</td><td>VERSIÓN:
2.0</td><td rowspan="2">PÁGINA:
1/9</td></tr>
<tr><td>CLASIFICACIÓN:
CONFIDENCIAL</td><td>FECHA DISEÑO:
03-2017</td></tr>
<tr><td>Proceso:</td><td colspan="3">Gestión de riesgos</td></tr>
<tr><td>Investigador:</td><td colspan="3">Miguel Angel Ayala Medrano</td></tr>
<tr><td>Fecha de recolección:</td><td colspan="3">26 al 30 de Junio de 2017</td></tr>
<tr><td>Puesto:</td><td colspan="3">Jefe (e) de la Unidad de Telemática</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
</table>

FICHA DE OBSERVACIÓN: INDICADOR NÚMERO DE CONTROLES APLICADOS DECLARACIÓN DE APLICABILIDAD DE CONTROLES FASE: POST TEST				
OBJETIVOS DE CONTROL		CONTROLES	¿APLICA? SI/NO	¿EXISTE? SI/NO/PARCIAL
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
5.1 Directrices de la Dirección en seguridad de la información.				
	5.1.1 Conjunto de políticas para la seguridad de la información	Control: La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.	S	S
	5.1.2 Revisión de las políticas para la seguridad de la información.	Control: Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas.	S	S
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
6.1 Organización interna				
	6.1.1 Asignación de responsabilidades para la segur. de la información.	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	S	S
	6.1.2 Segregación de tareas.	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	S	S
	6.1.3 Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes	S	S
	6.1.4 Contacto con grupos de interés especial.	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	S	S
	6.1.5 Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto	S	S
6.2 Dispositivos para movilidad y teletrabajo.				
	6.2.1 Política de uso de dispositivos para movilidad.	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	N	N
	6.2.2 Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	N	N
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.				
7.1 Antes de la contratación.				
	7.1.1 Investigación de antecedentes.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	S	S
	7.1.2 Términos y condiciones de contratación.	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	S	S
7.2 Durante la contratación.				
	7.2.1 Responsabilidades de gestión.	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de	S	S

		acuerdo con las políticas y procedimientos establecidos por la organización.		
	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	S	S
	7.2.3 Proceso disciplinario.	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	S	S
7.3 Cese o cambio de puesto de trabajo.				
	7.3.1 Cese o cambio de puesto de trabajo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	S	S
8. GESTIÓN DE ACTIVOS.				
8.1 Responsabilidad sobre los activos.				
	8.1.1 Inventario de activos.	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	S	S
	8.1.2 Propiedad de los activos.	Control: Los activos mantenidos en el inventario deberían tener un propietario.	S	S
	8.1.3 Uso aceptable de los activos.	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	S	S
	8.1.4 Devolución de activos.	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	S	S
8.2 Clasificación de la información.				
	8.2.1 Directrices de clasificación.	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	S	S
	8.2.2 Etiquetado y manipulado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	S	S
	8.2.3 Manipulación de activos.	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	S	S
8.3 Manejo de los soportes de almacenamiento				
	8.3.1 Gestión de soportes extraíbles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	S	S
	8.3.2 Eliminación de soportes.	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	S	S
	8.3.3 Soportes físicos en tránsito.	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte	S	S
9. CONTROL DE ACCESOS.				
9.1 Requisitos de negocio para el control de accesos.				
	9.1.1 Política de control de accesos.	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	S	S
	9.1.2 Control de acceso a las redes y servicios asociados.	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	S	S

9.2 Gestión de acceso de usuario.				
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso	S	S
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	S	S
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	S	S
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	S	S
	9.2.5 Revisión de los derechos de acceso de los usuarios.	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	S	P
	9.2.6 Retirada o adaptación de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	S	S
9.3 Responsabilidades del usuario.				
	9.3.1 Uso de información confidencial para la autenticación.	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta	S	S
9.4 Control de acceso a sistemas y aplicaciones.				
	9.4.1 Restricción del acceso a la información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	S	S
	9.4.2 Procedimientos seguros de inicio de sesión	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	S	P
	9.4.3 Gestión de contraseñas de usuario	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	S	S
	9.4.4 Uso de herramientas de administración de sistemas	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	S	P
	9.4.5 Control de acceso al código fuente de los programas	Control: Se debería restringir el acceso a los códigos fuente de los programas	S	S
10 CIFRADO				
10.1 Controles criptográficos.				
	10.1.1 Política de uso de los controles criptográficos.	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	N	N
	10.1.2 Gestión de claves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	N	N
11. SEGURIDAD FÍSICA Y AMBIENTAL.				
11.1 Áreas seguras.				
	11.1.1 Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información	S	P
	11.1.2 Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado	S	P

	11.1.3 Seguridad de oficinas, despachos y recursos.	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	S	P
	11.1.4 Protección contra las amenazas externas y ambientales.	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	S	P
	11.1.5 El trabajo en áreas seguras.	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	S	P
	11.1.6 Áreas de acceso público, carga y descarga.	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado	S	P
11.2 Seguridad de los equipos.				
	11.2.1 Emplazamiento y protección de equipos.	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado	S	S
	11.2.2 Instalaciones de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	S	S
	11.2.3 Seguridad del cableado.	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño	S	P
	11.2.4 Mantenimiento de los equipos.	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	S	S
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	S	S
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones	N	N
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	S	S
	11.2.8 Equipo informático de usuario desatendido.	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	S	S
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	S	S
12. SEGURIDAD EN LA OPERATIVA.				
12.1 Responsabilidades y procedimientos de operación				
	12.1.1 Documentación de procedimientos de operación.	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	S	S
	12.1.2 Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	S	S
	12.1.3 Gestión de capacidades	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	S	S

	12.1.4 Separación de entornos de desarrollo, prueba y producción	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	S	S
12.2 Protección contra código malicioso				
	12.2.1 Controles contra el código malicioso	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos	S	S
12.3 Copias de seguridad.				
	12.3.1 Copias de seguridad de la información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	S	S
12.4 Registro de actividad y supervisión				
	12.4.1 Registro y gestión de eventos de actividad.	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	S	S
	12.4.2 Protección de los registros de información.	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	S	S
	12.4.3 Registros de actividad del administrador y operador del sistema.	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	S	S
	12.4.4 Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	S	S
12.5 Control del software en explotación.				
	12.5.1 Instalación del software en sistemas en producción	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	S	S
12.6 Gestión de la vulnerabilidad técnica.				
	12.6.1 Gestión de las vulnerabilidades técnicas.	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	S	S
	12.6.2 Restricciones en la instalación de software.	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	S	S
12.7 Consideraciones de las auditorías de los sistemas de información.				
	12.7.1 Controles de auditoría de los sistemas de información.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	S	S
13. SEGURIDAD EN LAS TELECOMUNICACIONES				
13.1 Gestión de la seguridad en las redes				
	13.1.1 Controles de red.	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	S	S
	13.1.2 Mecanismos de seguridad asociados a servicios en red	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	S	S
	13.1.3 Segregación de redes.	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes	S	S
13.2 Intercambio de información con partes externas.				
	13.2.1 Políticas y procedimientos de intercambio de información.	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	N	N

	13.2.2 Acuerdos de intercambio.	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	N	N
	13.2.3 Mensajería electrónica.	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	S	S
	13.2.4 Acuerdos de confidencialidad y secreto.	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	S	S
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.				
14.1 Requisitos de seguridad de los sistemas de información.				
	14.1.1 Análisis y especificación de los requisitos de seguridad.	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	S	S
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	S	S
	14.1.3 Protección de las transacciones por redes telemáticas.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	S	S
14.2 Seguridad en los procesos de desarrollo y soporte.				
	14.2.1 Política de desarrollo seguro de software.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	S	S
	14.2.2 Procedimientos de control de cambios en los sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	S	S
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización	S	S
	14.2.4 Restricciones a los cambios en los paquetes de software.	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	S	S
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	S	S
	14.2.6 Seguridad en entornos de desarrollo.	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	S	S
	14.2.7 Externalización del desarrollo de software.	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	N	N
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	S	S
	14.2.9 Pruebas de aceptación.	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	S	S
14.3 Datos de prueba.				

	14.3.1 Protección de los datos utilizados en pruebas.	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	S	S
15. RELACIONES CON SUMINISTRADORES.				
15.1 Seguridad de la información en las relaciones con suministradores.				
	15.1.1 Política de seguridad de la información para suministradores.	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	S	S
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	S	S
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	S	S
15.2 Gestión de la prestación del servicio por suministradores.				
	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	S	N
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	S	N
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.				
16.1 Gestión de incidentes de seguridad de la información y mejoras.				
	16.1.1 Responsabilidades y procedimientos.	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	S	S
	16.1.2 Notificación de los eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	S	S
	16.1.3 Notificación de puntos débiles de la seguridad.	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios	S	S
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	S	S
	6.1.5 Respuesta a los incidentes de seguridad.	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	S	S
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	S	S
	16.1.7 Recopilación de evidencias.	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	S	S
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.				
17.1 Continuidad de la seguridad de la información.				
	17.1.1 Planificación de la continuidad de la seguridad de la información.	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la	S	S

		seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		
	17.1.2 Implantación de la continuidad de la seguridad de la información.	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	S	S
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.	S	S
17.2 Redundancias.				
	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	S	S
18. CUMPLIMIENTO				
18.1 Cumplimiento de los requisitos legales y contractuales.				
	18.1.1 Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	S	P
	18.1.2 Derechos de propiedad intelectual (DPI).	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	S	P
	18.1.3 Protección de los registros de la organización.	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	S	S
	18.1.4 Protección de datos y privacidad de la información personal.	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	S	S
	18.1.5 Regulación de los controles criptográficos.	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	N	N
18.2 Revisiones de la seguridad de la información.				
	18.2.1 Revisión independiente de la seguridad de la información.	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	S	S
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	S	S
	18.2.3 Comprobación del cumplimiento.	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	S	S

ANEXO N° 8 – Tabla resumen para el indicador Nivel de Riesgo en fases Pre y Post Test

TABLA RESUMEN: INDICADOR: EVALUACIÓN DEL RIESGO FASES: PRE Y POST TEST				
N°	**CÓDIGO ACTIVO**	**ACTIVO**	**RIESGO PROMEDIO PRE TEST**	**RIESGO PROMEDIO POST TEST**
1	A-01	Base de datos de Titulares	3.75	3.13
2	A-02	Base de datos de Pacientes	3.82	3.25
3	A-03	Base de datos de Farmacia	3.86	3.11
4	E-01	Sistema de Gestión de Salud	4.28	3.68
5	E-02	Sistema de Farmacia	4.45	3.53
6	E-03	Servicio web Acreditación de Derecho Habientes	4.52	3.98
7	E-04	MS Windows Server 2008, MS SQL Server 2008 R2	4.50	3.25
8	E-05	Antivirus Corporativo NOD32	3.42	3.1
9	D-01	Sub Director del Hospital	3.92	3.17
10	D-02	Jefe de la Oficina de administración	3.92	3.67
11	D-03	Jefe de la Unidad de Telemática	3.67	3.42
12	D-04	Programador	3.92	3.17
13	S-01	Servidor de producción	4.08	3.67
14	S-02	Servidor Backup	4.08	3.42
15	S-03	Servidor de Antivirus	3.33	2.75
16	S-04	Servidor de Desarrollo	3.33	2.50
17	S-05	Switch Capa 3	3.25	2.50
18	S-06	Web Filter	2.75	1.83
19	S-07	Firewall	2.75	1.75
20	H-01	Datacenter	3.75	3.33
21	H-02	Centro de Energía	3.56	3.13
22	H-03	Aire Acondicionado de Precisión	3.33	3.00
23	H-04	Grupo Electrógeno	3.33	2.83
		NIVEL DE RIESGO	**3.72**	**3.09**

Fuente: Elaboración propia

ANEXO N° 9 – Tabla resumen para el indicador Número de Controles Aplicados en fases Pre y Post Test

TABLA RESUMEN: INDICADOR: NÚMERO DE CONTROLES APLICADOS FASES: PRE Y POST TEST							
		TOTAL PRE TEST			TOTAL POST TEST		
N° CONTROLES QUE APLICAN /EXISTEN	TOTAL	NO EXISTENTE	PARCIALMENTE EXISTENTE	SI EXISTENTE	NO EXISTENTE	PARCIALMENTE EXISTENTE	SI EXISTENTE
SI APLICA /EXISTE	105	78	16	11	2	12	91
	100%	74.28%	15.24%	10.48%	1.90%	11.43%	86.67%
	DIFERENCIA				-72.38%	-3.81%	76.19%
NO APLICA	9						

Fuente: Elaboración propia

Anexo N° 10 – Políticas de seguridad de la información

<table>
<tr><td rowspan="2"></td><td colspan="3">DOCUMENTO</td></tr>
<tr><td>CÓDIGO:
N° 001- 2017-OFAD/UT/001</td><td>VERSIÓN:
01
FEC.:
MAY 2017</td><td>PÁGINA:
1/10</td></tr>
<tr><td></td><td colspan="3">POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL Hospital Nacional PNP. ”Luis N. Sáenz”</td></tr>
<tr><td></td><td colspan="3">PRIMERA VERSIÓN
Revisado por: Miguel A. Ayala Medrano</td></tr>
</table>

I. Objetivo

Establecer la Política de Seguridad de la Información en el Hospital Nacional PNP “Luis N. Sáenz”.

II. Descripción: Políticas de Seguridad de la Información

En el Hospital Nacional PNP “Luis N. Sáenz”, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad de su servicio de atención de salud, la administración de riesgos y la consolidación de una cultura de seguridad en la institución.

Consciente de las necesidades actuales, se implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de servicio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información, deben adoptar los lineamientos contenidos en la presente Política de Seguridad de la Información y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política de Seguridad de la Información se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la institución. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control de la norma internacional ISO 27001:2013.

Se establecerá el Comité de Seguridad de la Información que tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

III. Objetivos de la Política de Seguridad de la Información

- Proteger, preservar y administrar objetivamente la información de la Unidad de Telemática del Hospital Nacional PNP “Luis N. Sáenz”, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos para asegurar su permanencia y nivel de eficacia.
- Definir las directrices para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

IV. Declaración General de Políticas de Seguridad de la Información:

Acerca de la seguridad de la información

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- Confidencialidad: Los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

- Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.

- Eventos de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- Protección a la duplicación: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- Confiabilidad de la Información: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

V. Organización para la Seguridad de la Información

El Hospital Nacional PNP "Luis N. Sáenz" garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Sub Director del Hospital (Presidente) o su representante
- Jefe del Estado Mayor del Hospital o su representante
- Jefe de la Oficina de Administración o su representante
- Jefe de la Unidad de Telemática (Coordinador)
- Jefe de Operaciones y Seguridad de la Unidad de Telemática
- Asesor especialista en Seguridad de la Información

Dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de la institución para su aprobación mediante una Directiva Institucional.

Los jefes de División, Oficinas, Unidades o Áreas, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad de la Información y por tanto, deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados por las Directiva Institucional.

Sanciones para las violaciones a las Políticas de Seguridad de la Información

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los directores, funcionarios, personal asistencial y administrativo del Hospital Nacional PNP “Luis N. Sáenz”. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde proceso administrativo disciplinario, hasta acciones de orden civil o penal, de acuerdo con las circunstancias, si así lo ameritan.

Identificación, clasificación y valoración de activos de Información

Cada Unidad, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Unidad de Telemática brindar herramientas que permitan la administración del inventario por cada Unidad, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

La Unidad de Telemática en coordinación con la División de Almacén del Hospital tienen la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

Seguridad de la información en el Recurso Humano

Todo el personal del Hospital Nacional PNP “Luis N. Sáenz”, cualquiera sea su situación contractual, la Unidad a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Unidad de Telemática debe mantener un directorio completo y actualizado de tales perfiles y determina cuales son los atributos que deben definirse para los diferentes perfiles.

El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de “Responsabilidades Personales para la Seguridad de la Información en el Hospital Nacional PNP “Luis N. Sáenz”.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento; en todo caso el proceso de cambio en la cadena de custodia de la información o relevo, debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

Seguridad Física y del entorno

Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores en producción y desarrollo, de contingencia y a los cuartos de comunicaciones. La Unidad de Telemática elaborará y mantendrá las normas, controles y registros de acceso a dichas áreas.

Seguridad en los equipos

Los servidores que contengan información y servicios institucional deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Unidad de Telemática. El Comité de Seguridad de la Información define el límite de responsabilidades de las dependencias. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.

Los equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La Unidad de Telemática debe asegurar que la infraestructura de servicios de TI este cubierta por mantenimiento y soporte adecuados de hardware y software.

Administración de las comunicaciones y operaciones

Reporte e investigación de incidentes de seguridad

El personal del Hospital debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de Unidad a la Unidad de Telemática. En casos especiales dichos reportes podrán realizarse directamente al Comité de Seguridad de la Información, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

Protección contra software malicioso y hacking

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

Como control mínimo, las estaciones de trabajo del Hospital deben estar protegidas por software antivirus con capacidad de actualización automática en

cuanto a firmas de virus. Los usuarios de la estaciones no están autorizados a deshabilitar este control.

La Unidad de Telemática podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las Unidades del Hospital deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

La Unidad de Telemática debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad.

Las copias de seguridad de información crítica deben ser mantenidas de acuerdo a cronogramas definidos y publicados por la Unidad de Telemática.

Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Unidad de Telemática.

Internet y Correo Electrónico

Las normas de uso de Internet serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

Los servicios de correo electrónico institucional están administrados por la Dirección de Tecnologías de Información y Estadística PNP, por lo que todo usuario deberá ceñirse a las disposiciones que dicha Dirección establezca.

Uso de Software

Todas las instalaciones de software que se realicen sobre sistemas del Hospital deben ser aprobadas por la Unidad de Telemática, de acuerdo a los procedimientos elaborados para tal fin por dichas Unidades. No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor.

Control de Acceso

Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

Corresponde a la Unidad de Telemática elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal.

La Unidad de Telemática debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.

El control de las contraseñas de red y uso de equipos es responsabilidad de la Unidad de Telemática. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por la jefatura de la Unidad de Telemática y deben ser cambiadas en intervalos regulares de tiempo y en todo caso, cuando el personal adscrito al cargo cambie.

Computación Móvil

El Hospital reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc).

Corresponde a la Unidad de Telemática elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Todo dispositivo móvil que requiera ser conectado a la intranet PNP del Hospital deberá ser autorizado por la Unidad de Telemática.

Previa autorización de la Unidad de Telemática, puede generarse redes inalámbricas de la intranet PNP del Hospital, en casos excepcionales (eventos de capacitación, charlas, conferencias, etc.).

Acceso Remoto

El acceso remoto a servicios de red ofrecidos por el Hospital debe estar sujeto a medidas de control definidas por la Unidad de Telemática, las cuales deben incluir acuerdos escritos de seguridad de la información. Todo acceso será realizado vía VPN con las medidas de seguridad establecidas para tal fin. Dichos accesos serán autorizados por la Jefatura de la Unidad de Telemática sólo en casos de asistencia remota para el uso del Sistema de Gestión de Salud y en horarios que no haya personal de servicio. Todo acceso remoto deberá informarse por escrito y en detalle en un Informe dirigido a la Jefatura de la Unidad de Telemática y deberá ser presentado el siguiente día útil.

Adquisición, Desarrollo y Mantenimiento de Sistemas Software

Para apoyar los procesos de servicios de atención de salud y estratégicos del Hospital debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

La Unidad de Telemática debe elegir, elaborar, mantener y difundir la "Metodología de Desarrollo de Sistemas Software en el Hospital Nacional PNP "Luis N. Sáenz", que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad. Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. El Hospital no debe emprender procesos de desarrollo o mantenimiento de sistemas software que tengan asociados riesgos altos no mitigados.

Cumplimiento

Todo uso y seguimiento de uso a los recursos de TI en el Hospital Nacional PNP "Luis N. Sáenz" debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional en materia de tecnologías de la información y comunicaciones.

Anexo N° 11 – Declaración de Aplicabilidad

	DOCUMENTO		
	CÓDIGO: **N° 002- 2017-OFAD/UT/001**	**VERSIÓN:** **01** **FEC.:** **MAY 2017**	**PÁGINA:** **1/9**
	DECLARACIÓN DE APLICABILIDAD DEL Hospital Nacional PNP. ”Luis N. Sáenz”		
	PRIMERA VERSIÓN **Revisado por: Miguel A. Ayala Medrano**		

DECLARACIÓN DE APLICABILIDAD

OBJETIVOS DE CONTROL	CONTROLES	¿APLICA? SI/NO	¿EXISTE? SI/NO/PARCIAL	DESCRIPCIÓN DE IMPLEMENTACIÓN INDICADOR
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
5.1 Directrices de la Dirección en seguridad de la información.				
5.1.1 Conjunto de políticas para la seguridad de la información	Control: La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
5.1.2 Revisión de las políticas para la seguridad de la información.	Control: Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Propuesta para integrar en el MOF del Estado Mayor del Hospital
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
6.1 Organización interna				
6.1.1 Asignación de responsabilidades para la segur. de la información.	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
6.1.2 Segregación de tareas.	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	S	S	Porcentaje de cumplimiento: 80% Meta: 100%
6.1.3 Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
6.1.4 Contacto con grupos de interés especial.	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
6.1.5 Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Propuesta para integrar en en todo expediente técnico de contrataciones.
6.2 Dispositivos para movilidad y teletrabajo.				
6.2.1 Política de uso de dispositivos para movilidad.	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	N	N	---
6.2.2 Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	N	N	---
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.				
7.1 Antes de la contratación.				
7.1.1 Investigación de antecedentes.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
7.1.2 Términos y condiciones de contratación.	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%

					Documento elaborado: Políticas de Seguridad de la Información
7.2 Durante la contratación.					
	7.2.1 Responsabilidades de gestión.	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	7.2.3 Proceso disciplinario.	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	S	S	Porcentaje de cumplimiento: 50% Meta: 100%
7.3 Cese o cambio de puesto de trabajo.					
	7.3.1 Cese o cambio de puesto de trabajo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
8. GESTIÓN DE ACTIVOS.					
8.1 Responsabilidad sobre los activos.					
	8.1.1 Inventario de activos.	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	8.1.2 Propiedad de los activos.	Control: Los activos mantenidos en el inventario deberían tener un propietario.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	8.1.3 Uso aceptable de los activos.	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	8.1.4 Devolución de activos.	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
8.2 Clasificación de la información.					
	8.2.1 Directrices de clasificación.	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento a cumplir: Reglamento de documentación policial
	8.2.2 Etiquetado y manipulado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento a cumplir: Reglamento de documentación policial
	8.2.3 Manipulación de activos.	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
8.3 Manejo de los soportes de almacenamiento					
	8.3.1 Gestión de soportes extraíbles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	8.3.2 Eliminación de soportes.	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	8.3.3 Soportes físicos en tránsito.	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
9. CONTROL DE ACCESOS.					

9.1 Requisitos de negocio para el control de accesos.					
	9.1.1 Política de control de accesos.	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	9.1.2 Control de acceso a las redes y servicios asociados.	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Permiso de Acceso a Sistemas
9.2 Gestión de acceso de usuario.					
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.5 Revisión de los derechos de acceso de los usuarios.	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	S	P	Porcentaje de cumplimiento: 80% Meta: 100%
	9.2.6 Retirada o adaptación de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
9.3 Responsabilidades del usuario.					
	9.3.1 Uso de información confidencial para la autenticación.	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
9.4 Control de acceso a sistemas y aplicaciones.					
	9.4.1 Restricción del acceso a la información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Permiso de Acceso a Sistemas
	9.4.2 Procedimientos seguros de inicio de sesión	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	S	P	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Permiso de Acceso a Sistemas
	9.4.3 Gestión de contraseñas de usuario	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Permiso de Acceso a Sistemas
	9.4.4 Uso de herramientas de administración de sistemas	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	S	P	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	9.4.5 Control de acceso al código fuente de los programas	Control: Se debería restringir el acceso a los códigos fuente de los programas	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
10 CIFRADO					
10.1 Controles criptográficos.					
	10.1.1 Política de uso de los controles criptográficos.	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	N	N	---

	10.1.2 Gestión de claves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	N	N	---
11. SEGURIDAD FÍSICA Y AMBIENTAL.					
11.1 Áreas seguras.					
	11.1.1 Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
	11.1.2 Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
	11.1.3 Seguridad de oficinas, despachos y recursos.	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
	11.1.4 Protección contra las amenazas externas y ambientales.	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
	11.1.5 El trabajo en áreas seguras.	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
	11.1.6 Áreas de acceso público, carga y descarga.	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
11.2 Seguridad de los equipos.					
	11.2.1 Emplazamiento y protección de equipos.	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.2 Instalaciones de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.3 Seguridad del cableado.	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño	S	P	Porcentaje de cumplimiento: 50% Meta: 100%
	11.2.4 Mantenimiento de los equipos.	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones	N	N	---
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	11.2.8 Equipo informático de usuario desatendido.	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Propuesta de recomendaciones de seguridad de información para usuarios.
12. SEGURIDAD EN LA OPERATIVA.					
12.1 Responsabilidades y procedimientos de operación					
	12.1.1 Documentación de procedimientos de operación.	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	12.1.2 Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	12.1.3 Gestión de capacidades	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%

	12.1.4 Separación de entornos de desarrollo, prueba y producción	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
12.2 Protección contra código malicioso					
	12.2.1 Controles contra el código malicioso	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
12.3 Copias de seguridad.					
	12.3.1 Copias de seguridad de la información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
12.4 Registro de actividad y supervisión					
	12.4.1 Registro y gestión de eventos de actividad.	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento: Reporte de los logs de los servidores
	12.4.2 Protección de los registros de información.	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	12.4.3 Registros de actividad del administrador y operador del sistema.	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento: Reporte de los logs de los servidores
	12.4.4 Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
12.5 Control del software en explotación.					
	12.5.1 Instalación del software en sistemas en producción	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Acción: Configurar nivel de usuario de equipo de cómputo sin derechos de instalación de software
12.6 Gestión de la vulnerabilidad técnica.					
	12.6.1 Gestión de las vulnerabilidades técnicas.	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	S	S	Porcentaje de cumplimiento: 80% Meta: 100%
	12.6.2 Restricciones en la instalación de software.	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Acción: Configurar nivel de usuario de equipo de cómputo sin derechos de instalación de software
12.7 Consideraciones de las auditorías de los sistemas de información.					
	12.7.1 Controles de auditoría de los sistemas de información.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	S	S	Porcentaje de cumplimiento: 80% Meta: 100%
13. SEGURIDAD EN LAS TELECOMUNICACIONES					
13.1 Gestión de la seguridad en las redes					
	13.1.1 Controles de red.	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	S	S	Porcentaje de cumplimiento: 80% Meta: 100%
	13.1.2 Mecanismos de seguridad asociados a servicios en red	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	S	S	Porcentaje de cumplimiento: 80% Meta: 100%
	13.1.3 Segregación de redes.	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes	S	S	Porcentaje de cumplimiento: 80% Meta: 100%
13.2 Intercambio de información con partes externas.					
	13.2.1 Políticas y procedimientos de intercambio de información.	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	N	N	---
	13.2.2 Acuerdos de intercambio.	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	N	N	---
	13.2.3 Mensajería electrónica.	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	S	S	Porcentaje de cumplimiento: 50% Meta: 100%

	13.2.4 Acuerdos de confidencialidad y secreto.	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento a cumplir: Reglamento de documentación policial
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.					
14.1 Requisitos de seguridad de los sistemas de información.					
	14.1.1 Análisis y especificación de los requisitos de seguridad.	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.1.3 Protección de las transacciones por redes telemáticas.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
14.2 Seguridad en los procesos de desarrollo y soporte.					
	14.2.1 Política de desarrollo seguro de software.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.2 Procedimientos de control de cambios en los sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.4 Restricciones a los cambios en los paquetes de software.	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.6 Seguridad en entornos de desarrollo.	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Acción: Generar DB para desarrollo
	14.2.7 Externalización del desarrollo de software.	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	N	N	---
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.9 Pruebas de aceptación.	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%
14.3 Datos de prueba.					
	14.3.1 Protección de los datos utilizados en pruebas.	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Acción: Generar DB para desarrollo
15. RELACIONES CON SUMINISTRADORES.					
15.1 Seguridad de la información en las relaciones con suministradores.					
	15.1.1 Política de seguridad de la información para suministradores.	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Propuesta para integrar en en todo expediente técnico de contrataciones.
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Propuesta para integrar en en todo expediente técnico de contrataciones.
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Propuesta para integrar en en todo expediente técnico de contrataciones.
15.2 Gestión de la prestación del servicio por suministradores.					

	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	S	N	Porcentaje de cumplimiento: 0% Meta: 100% Documento elaborado: Propuesta para integrar en en todo expediente técnico de contrataciones. Obs. No se tiene proveedores
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	S	N	Porcentaje de cumplimiento: 0% Meta: 100% Documento elaborado: Propuesta para integrar en en todo expediente técnico de contrataciones. Obs. No se tiene proveedores
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.					
16.1 Gestión de incidentes de seguridad de la información y mejoras.					
	16.1.1 Responsabilidades y procedimientos.	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	16.1.2 Notificación de los eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	16.1.3 Notificación de puntos débiles de la seguridad.	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	6.1.5 Respuesta a los incidentes de seguridad.	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	S	S	Porcentaje de cumplimiento: 50% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	16.1.7 Recopilación de evidencias.	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.					
17.1 Continuidad de la seguridad de la información.					
	17.1.1 Planificación de la continuidad de la seguridad de la información.	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	17.1.2 Implantación de la continuidad de la seguridad de la información.	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	S	S	Porcentaje de cumplimiento: 100% Meta: 100%

					Documento elaborado: Políticas de Seguridad de la Información
17.2 Redundancias.					
	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
18. CUMPLIMIENTO					
18.1 Cumplimiento de los requisitos legales y contractuales.					
	18.1.1 Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	S	P	Porcentaje de cumplimiento: 50% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	18.1.2 Derechos de propiedad intelectual (DPI).	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	S	P	Porcentaje de cumplimiento: 50% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	18.1.3 Protección de los registros de la organización.	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	18.1.4 Protección de datos y privacidad de la información personal.	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	S	S	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	18.1.5 Regulación de los controles criptográficos.	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	N	N	---
18.2 Revisiones de la seguridad de la información.					
	18.2.1 Revisión independiente de la seguridad de la información.	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	S	S	Porcentaje de cumplimiento: 80% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	S	S	Porcentaje de cumplimiento: 80% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información
	18.2.3 Comprobación del cumplimiento.	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	S	S	Porcentaje de cumplimiento: 80% Meta: 100% Documento elaborado: Políticas de Seguridad de la Información

Anexo N° 12 – Validación del instrumento por juicio de expertos

INFORME DE VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

I. **Datos Generales**

1.1 Apellidos y nombres del validador:

Pérez Rojas Even Deyser

1.2 Institución donde labora/cargo:

Universidad César Vallejo

1.3 Especialidad del validador:

Magister en Gestión de Tecnologías de la Información

1.4 Nombre del instrumento y finalidad de su aplicación:

Instrumento 01: Ficha de Observación. Evaluación del riesgo según los activos de información, amenazas y vulnerabilidades. (Ver Anexo 01).

Finalidad: Recopilar información para evaluar el nivel de riesgo de seguridad de la información pre y post test en el Hospital Nacional PNP "Luis N. Sáenz".

Instrumento 02: Ficha de observación. Declaración de aplicabilidad de controles pre y post test. (Ver Anexo 02).

Finalidad: Recopilar información para determinar la aplicación de controles pre y post test en el Hospital Nacional PNP "Luis N. Sáenz".

1.5 Título de la investigación: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN HOSPITAL NACIONAL, 2017

1.6 Autor del Instrumento: Miguel Angel Ayala Medrano

1

II. Definición conceptual de las variables y sus dimensiones

Variable: Proceso de gestión del riesgo

Para Peltier (2014), "El proceso de gestión de riesgos consiste en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable. Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo). A continuación, identifique los controles que llevarían el efecto a un nivel aceptable." (p. xxi).

AUTOR: Thomas R. Peltier.
TÍTULO: Information Security Fundamentals.
2da. Edición. Florida: CRC Press, 2014. 375 pp.
ISBN 13: 978-1-4398-1063-7

Dimensiones de las variables:

Para ISO/IEC 27005:2011, "La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable." (p. 6).

AUTOR: Organización Internacional de Normalización
TÍTULO: Norma ISO/IEC 27005. Tecnología de la Información – Técnicas de seguridad – Gestión de riesgos de seguridad de la información. ISO, 2011.

Dimensión 1: Evaluación del riesgo

Dimensión 2: Tratamiento del riesgo

III. **Matriz de operacionalización de las variables**

Variable: Proceso de gestión del riesgo

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento	Escala de Medición
Proceso de gestión del riesgo	Para Peltier (2014), "El proceso de gestión de riesgos consiste en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable. Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo). A continuación, identifique los controles que llevarían el efecto a un nivel aceptable." (p. xxi).	Para ISO/IEC 27005:2011, "La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, **evaluar los riesgos**, **tratar los riesgos** utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable." (p. 6).	Evaluación del riesgo	Nivel de riesgo	Ficha de Observación	Nominal
			Tratamiento del riesgo	Número de controles aplicados	Ficha de Observación	Nominal

UCV UNIVERSIDAD CÉSAR VALLEJO

sube

IV. Matriz de Consistencia

Título: Sistema de Gestión de Seguridad de Información para mejorar el proceso de gestión del riesgo en un Hospital Nacional

Problemas de investigación	Objetivos de investigación	Hipótesis	Variables	Dimensiones	Indicadores	Metodología y Diseño
Problema General	**Objetivo General**	**Hipótesis General**				
¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional?	Evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional.	La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva en el proceso de gestión del riesgo de un Hospital Nacional.	V.I.: Sistema de Gestión de Seguridad de la Información	▪ Alcance del SGSI. ▪ Políticas de seguridad de información. ▪ Identificación de activos. ▪ Mecanismos de control SGSI. ▪ Análisis y evaluación del riesgo ▪ Plan de tratamiento del riesgo. ▪ Documentación de procedimientos. ▪ Declaración de aplicabilidad.		**Metodología:** SGSI: ISO/IEC 27001:2013 Análisis de riesgos: Magerit v3.0 Aplicación de controles: ISO/IEC 27002:2013 **Tipo de investigación:** Aplicada **Tipo de Diseño:** Pre experimental.
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicas**				
PE1: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional?	OE1: Evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.	HE1: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva reduciendo el nivel de riesgo en el proceso de gestión del riesgo en un Hospital Nacional.	V.D. Proceso de Gestión del riesgo	Evaluación del riesgo	Nivel de riesgo	**Instrumento:** - Ficha de Observación
PE2: ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional?	OE2: Evaluar la manera en que la implementación del sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.	HE2: La implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional.		Tratamiento del riesgo	Número de controles aplicados	

UCV UNIVERSIDAD CÉSAR VALLEJO

sube

V. Certificado de validez de contenido del instrumento

Nº	DIMENSIONES / indicadores	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Evaluación del riesgo	Si X	No	Si X	No	Si X	No	
1	Nivel de riesgo							
	DIMENSIÓN 2: Tratamiento del riesgo	Si X	No	Si X	No	Si X	No	
2	Número de controles aplicados							

Observaciones (precisar si hay suficiencia): Si hay Suficiencia.

Opinión de aplicabilidad: **Aplicable** [X] **Aplicable después de corregir** [ ] **No aplicable** [ ]

Apellidos y nombres del juez validador. Dr/ Mg: Magister Pérez Rojas Evan Deysa. **DNI:** 43776847

Especialidad del validador: Magister en Gestión de Tecnologías de la Información

30 de 05 del 2017

[1]**Pertinencia:** El indicador corresponde al concepto teórico formulado.
[2]**Relevancia:** El indicador es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los indicadores planteados son suficientes para medir la dimensión

Firma del Experto Informante.
CIP. 155873

UCV UNIVERSIDAD CÉSAR VALLEJO

sube

INFORME DE VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

I. Datos Generales

1.1 Apellidos y nombres del validador:

Cortes Alvarez Erika Patricia

1.2 Institución donde labora/cargo:

UCV

1.3 Especialidad del validador:

Mg Educación

1.4 Nombre del instrumento y finalidad de su aplicación:

Instrumento 01: Ficha de Observación. Evaluación del riesgo según los activos de información, amenazas y vulnerabilidades. (Ver Anexo 01).

Finalidad: Recopilar información para evaluar el nivel de riesgo de seguridad de la información pre y post test en el Hospital Nacional PNP "Luis N. Sáenz".

Instrumento 02: Ficha de observación. Declaración de aplicabilidad de controles pre y post test. (Ver Anexo 02).

Finalidad: Recopilar información para determinar la aplicación de controles pre y post test en el Hospital Nacional PNP "Luis N. Sáenz".

1.5 Título de la investigación: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN HOSPITAL NACIONAL, 2017

1.6 Autor del Instrumento: Miguel Angel Ayala Medrano

UCV UNIVERSIDAD CÉSAR VALLEJO

sube

V. Certificado de validez de contenido del instrumento

Nº	DIMENSIONES / indicadores	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Evaluación del riesgo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Nivel de riesgo	X		X		X		
	DIMENSIÓN 2: Tratamiento del riesgo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	Número de controles aplicados	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Erika Cortes Alvarez **DNI:** 000851216

Especialidad del validador: Mg de Educación

27 de Junio del 2017

[1]**Pertinencia:** El indicador corresponde al concepto teórico formulado.
[2]**Relevancia:** El indicador es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los indicadores planteados son suficientes para medir la dimensión

Firma del Experto Informante.

5

UCV UNIVERSIDAD CÉSAR VALLEJO

sube

INFORME DE VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

I. Datos Generales

1.1 Apellidos y nombres del validador:

HUAMANI CUBAS ARTHUR

1.2 Institución donde labora/cargo:

UCV

1.3 Especialidad del validador:

Seguridad de la información / ciberseguridad.

1.4 Nombre del instrumento y finalidad de su aplicación:

Instrumento 01: Ficha de Observación. Evaluación del riesgo según los activos de información, amenazas y vulnerabilidades. (Ver Anexo 01).

Finalidad: Recopilar información para evaluar el nivel de riesgo de seguridad de la información pre y post test en el Hospital Nacional PNP "Luis N. Sáenz".

Instrumento 02: Ficha de observación. Declaración de aplicabilidad de controles pre y post test. (Ver Anexo 02).

Finalidad: Recopilar información para determinar la aplicación de controles pre y post test en el Hospital Nacional PNP "Luis N. Sáenz".

1.5 Título de la investigación: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN HOSPITAL NACIONAL, 2017

1.6 Autor del Instrumento: Miguel Angel Ayala Medrano

UCV UNIVERSIDAD CÉSAR VALLEJO

sube

V. Certificado de validez de contenido del instrumento

Nº	DIMENSIONES / indicadores	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Evaluación del riesgo	Si	No	Si	No	Si	No	
1	Nivel de riesgo	X		X		X		
	DIMENSIÓN 2: Tratamiento del riesgo	Si	No	Si	No	Si	No	
2	Número de controles aplicados	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable** [X] **Aplicable después de corregir** [ ] **No aplicable** [ ]

Apellidos y nombres del juez validador. Dr/ Mg: HUDHANI CUBA ARTHUR **DNI:** 41233380

Especialidad del validador: Seguridad de la información / Ciberseguridad

28 de junio del 2017

[1]**Pertinencia:** El indicador corresponde al concepto teórico formulado.
[2]**Relevancia:** El indicador es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los indicadores planteados son suficientes para medir la dimensión

Firma del Experto Informante.

5