

FACULTAD DE INGENIERÍA



Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO IEC/27002, PARA OPTIMIZAR LA GESTIÓN EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA”

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Ruben Eduardo Rumiche Huamani

Asesor:

Mg. Ing. Jorge Alfredo Bojórquez Segura

Lima - Perú

2021

Tabla de contenido

DEDICATORIA	2
AGRADECIMIENTO	3
ÍNDICE DE TABLAS.....	6
ÍNDICE DE FIGURAS.....	7
RESUMEN EJECUTIVO	8
ABSTRACT	9
CAPÍTULO I.....	10
1.1. <i>Introducción</i>	10
1.2. <i>Estructura de los órganos jurisdiccionales de la Corte Superior de Justicia de Lima</i>	11
1.3. <i>ORGANIGRAMA ESTRUCTURAL – CORTE SUPERIOR DE JUSTICIA QUE OPERA COMO UNIDAD EJECUTORA</i>	12
1.1. <i>Realidad problemática</i>	13
1.4. <i>Antecedentes</i>	15
1.4.1. Antecedentes Nacionales	15
1.4.2. Antecedentes Internacionales	24
CAPÍTULO II.....	32
2.1. <i>Marco Teórico</i>	32
2.1.1. Sistema de Gestión	34
2.1.2. Norma ISO/IEC 27001:2013	35
2.1.3. Norma ISO/IEC 27002:	35
2.1.4. Seguridad de la Información	37
2.1.5. Seguridad Informática	38
2.1.6. Objetivo de la Seguridad Informática	39
2.1.7. Ingeniería Social	39
2.1.8. Políticas de Seguridad de la Información.....	40
2.1.9. Amenazas.....	40
2.1.10. Vulnerabilidad.....	41
2.1.11. Activo	42
2.1.12. Riesgo.....	42
2.1.13. Análisis de riesgos.....	43
2.1.14. Justificación del proyecto de investigación	45
2.2. <i>Formulación del problema</i>	47
2.2.1. Problemas Específicos.....	47
2.3. <i>Objetivos</i>	47
2.3.1. Objetivo general	47
2.3.2. Objetivos específicos	47

2.4.	<i>Hipótesis</i>	48
2.4.1.	Hipótesis general	48
2.4.2.	Hipótesis específicas	48
2.5.	<i>MATRIZ DE CONSISTENCIA</i>	49
CAPÍTULO III		50
3.1.	<i>Descripción de la Experiencia</i>	50
3.2.	<i>METODOLOGÍA</i>	51
3.3.	<i>Variables de Estudio</i>	54
3.4.	<i>POBLACIÓN Y MUESTRA</i>	54
3.4.1.	Población	54
3.4.2.	Muestra.....	55
3.5.	<i>Técnicas e instrumentos de recolección y análisis de datos</i>	55
3.5.1.	Instrumentos.....	56
3.5.2.	Cuestionario.....	56
3.6.	<i>Procedimiento</i>	58
CAPÍTULO IV		70
4.1.	<i>Resultados</i>	70
CAPÍTULO V		80
5.1.	<i>Conclusiones y recomendaciones</i>	80
5.1.1.	Conclusiones	80
5.1.2.	Recomendaciones.....	81
LECCIONES APRENDIDAS		83
REFERENCIAS		85
ANEXOS		91

ÍNDICE DE TABLAS

Tabla 1.- <i>Contratación de los Sistemas de apoyo a SGSI existentes</i>	15
Tabla 2.- <i>Matriz de Consistencia</i>	49
Tabla 3.- <i>Objetivos de Control y Controles ISO 27002:2013</i>	53
Tabla 4.- <i>Procedimiento - Fase Diagnóstico</i>	59
Tabla 5.- <i>Procedimiento - Fase Planificación</i>	60
Tabla 6.- <i>Procedimiento - Fase Implementación</i>	63
Tabla 7.- <i>Procedimiento - Fase Evaluación</i>	68

ÍNDICE DE FIGURAS

<i>Figura 1</i> .- Estructura de los Órganos Jurisdiccionales de la CJLIMA.....	11
<i>Figura 2</i> .- Organigrama Estructural CSJLIMA.....	12
<i>Figura 3</i> .- Los 3 pilares de la Seguridad Informática.....	33
<i>Figura 4</i> .- Círculo de Deming	34
<i>Figura 5</i> .- Propiedades fundamentales de la Seguridad	38
<i>Figura 6</i> .- Tipos de Amenazas - Fuente: Alberto G. Alexander 2007	41
<i>Figura 7</i> .- Áreas Vulnerables	42
<i>Figura 8</i> .- Escala de Likert	57
<i>Figura 9</i> .- Políticas de Seguridad	70
<i>Figura 10</i> .- Organización de la Seguridad de la Información	71
<i>Figura 11</i> .- Seguridad relativa a los recursos humanos	71
<i>Figura 12</i> .- Gestión de activos	72
<i>Figura 13</i> .- Control de acceso	72
<i>Figura 14</i> .- Criptografía	73
<i>Figura 15</i> .- Seguridad física y del entorno	73
<i>Figura 16</i> .- Seguridad de las operaciones.....	74
<i>Figura 17</i> .- Seguridad de las telecomunicaciones.....	75
<i>Figura 18</i> .- Adquisición, desarrollo y mantenimiento de los sistemas de información	76
<i>Figura 19</i> .- Relación con los proveedores	76
<i>Figura 20</i> .- Aspectos de la seguridad de la información para la gestión de continuidad del negocio.....	77
<i>Figura 21</i> .- Cumplimiento	78

RESUMEN EJECUTIVO

El trabajo de investigación realizado en la Corte Superior de Justicia de Lima, tuvo la intención de conocer los riesgos y vulnerabilidades y posteriormente tuvo el objetivo de implementar un plan de Seguridad Informática en la institución, tomando como referencia la norma internacional ISO IEC 27002:2013, la cual encierra políticas y lineamientos que permitirá mejorar el nivel y establecer una cultura en la seguridad de la información.

Para obtener mejores resultados sobre la situación tecnológica, se utilizó la técnica de encuesta para reunir información por las constantes fallas de los sistemas informáticos, a fin de evaluar la necesidad de implementar un plan de seguridad informática.

El resultado de dicha encuesta es que no se aplica una política interna en la seguridad informática, así como no cuenta con controles permanentes en el parque informático y desconocimiento en el uso de la norma ISO 27002:2013.

Las vulnerabilidades y riesgos que se presentan en los sistemas de información que administra la Corte Superior de Justicia de Lima, son muy frecuentes, y se espera que, cumpliendo con políticas y estrategias adecuadas, se podrá afrontar cualquier eventualidad o ataque futuro, siendo conscientes de la importancia que representa la información en toda institución pública o privada.

Palabras claves:

Seguridad de la información, ISO 27002, SGSI, Seguridad Informática.

ABSTRACT

The research project carried out at the Corte Superior de Justicia de Lima, intend to know risks and vulnerabilities and the subsequent objective of implementing a Computer Security plan in the institution, taking as reference the international standard ISO IEC 27002: 2013, that contains policies and guidelines that will improve the level and establish a culture of information security.

To obtain better results on the technological situation, the survey technique was used to gather information for the frequent failures of the computer systems, in order to evaluate the need to implement a computer security plan.

The result of this survey shows that the internal policy on computer security is not applied, as well as it does not have permanent controls in the computer park and unawareness in the use of ISO 27002: 2013.

The vulnerabilities and risks that arise in the information systems managed by the Corte Superior de Justicia de Lima are very frequent and it is expected that fulfilling with appropriate policies and strategies, any eventuality or future attack can be faced, being aware of the importance of information in any public or private institution.

KEY WORD:

Security of the information, ISO 27002, SGSI, Informatic security.

NOTA DE ACCESO

No se puede acceder al texto completo pues contiene datos confidenciales

REFERENCIAS

- Alexander, a. G. (2007). Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001:2005. Bogotá: Alfaomega Colombiana.
- Talavera Álvarez, V. R. (2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la Iso/Iec 27001: 2013.
- Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL, 28(5).
- (2018 - Jaime Vásquez Escalante – Implementación del sistema de gestión ISO – UNMSM).
- Bertolín, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo.
- Luis Castro (2019) Análisis y diseño de un sistema de gestión de seguridad informática para la empresa star audio.
- Muñoz, j. (2018). Diseño de un plan estratégico para la seguridad de la información de cias & profesionales sas.
- Michel Miranda Cairo ; Osmany Valdés Puga ; Iván Pérez Mallea ; RenierPortelles Cobas ; Raúl Sánchez Zequeira ; Revista Cubana de Ciencias Informáticas 2016, 10 (2)
- Vallejo, M. R. L. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. Revista Publicando, 4(10 (1)), 31-51.

Alexander, Alberto.: Diseño de un Sistema de Gestión de Seguridad de la Información – óptica

ISO 27001:2005. Alfaomega. Bogotá - Colombia (2007)

Metodología de la Investigación - Roberto Hernández Sampieri – 6ta edición

Knapp, K. J., Franklin Morris Jr., R., Marshall, T. E., & Byrd, T. A. (2009).

Informationsecuritypolicy: Anorganizational-levelprocessmodel. Computers Security, 28(7),
493-508. Elsevier Ltd.

Escalante Terán, O. M. (2018). Conflictos entre la gobernabilidad y la soberanía en
organizaciones multilaterales: Estudio de la implementación de políticas de seguridad
informática entre los años 2004 - 2016 en la Unión Europea.

Celis Figueroa, L. A. (2018). Plan de seguridad de la información aplicado a la central
hidroeléctrica Carhuaquero.

Aguilera, P. (2011). Redes seguras (Seguridad informática). Madrid, España: Editex.

Huancá Suaquita, J. R. (2018). La falsa percepción en la seguridad de los sistemas informáticos.

Guevara Pérez, O., & Miranda Zelada, A. A. (2014). Diseño de una red de datos para el
policlínico Señor de los Milagros S.R.L., usando metodología Top Down Network Design y
aplicando estándares ISO/IEC 27002.

Acevedo Gutiérrez, A. (2017). Propuesta de implementación de tecnología Sandbox en una
entidad financiera para la prevención de presencia de Ransomware en la red interna y mitigación
de incidentes.

García Paredes, A. (2016). Implementación de un sistema de gestión de Seguridad de la información, aplicado a los Riesgos asociados a los activos de información En la empresa Net – Consultores S.A.C.

Gil Izurraga, J. E., & Maihuiri Vargas, L. A. (2018). Implementación de un Data Center Virtual en Cloud Computing para mejorar los servicios del departamento de TI en la Empresa Venus peruana S.A.C.

Cortéz Rodríguez, A. I., & Santiago Cueva, W. J. (2018). Plan de seguridad informática basado en la norma Iso 27002 para mejorar la gestión tecnológica del colegio carmelitas – Trujillo.

Gavidia Mamani, S., & Torres Torres, L. D. (2018). Implementación de los controles de la ISO/IEC 27002: 2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.

Angulo Castillo, A. M. (2014). Plan de seguridad informático para mejorar la calidad en el servicio del call center de la empresa telsat Perú sac.

López Sovero, C. E. (2015). Sistema de Control basado en COBIT para la certificación SOX. Caso: AFP en Perú.

Martínez Borja, J. J. (2014). Controles de seguridad para reducir la cantidad de incidencias de seguridad de la información del año 2012 en el servicio de administración tributaria de Huancayo.

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

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (22), 73-88.

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017, July). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002: 2013 para la Cooperativa Codelcauca. In Memorias de Congresos UTP (pp. 88-95).

Aliaga Flores, L. C. (2013). Diseño de un sistema de gestión de seguridad de información para un instituto educativo.

Camelo, L., de Negocios, A. D. I., del Negocio, C., de Aplicabilidad, D., Informáticos, D., & Externos, D. (2010). Seguridad de la Información en Colombia. Obtenido de <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-deseuridad-de-la.html>.

Tasinchana, C., & Maribel, S. (2017). Análisis e Implantación de la norma ISO/IEC 27002: 2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos).

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et technica, 22(2).

Infante Moro, A., Infante Moro, J. C., Martínez López, F. J., & García Ordaz, M. (2016). Percepción de la importancia de la seguridad informática en la industria hotelera española. El turismo y la experiencia del cliente: IX jornadas de investigación en turismo (2016), p 77-89.

- Pinto, M. G. H., & Sánchez, B. A. N. (2016). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. Obtenido de Escuela Superior Politécnica del Litoral: <https://www.dspace.espol.edu.ec/retrieve/94448/D-71165.pdf>.
- Haro, C. A. R. (2015). La Seguridad Informática. Ciencia Unemi, 4(5), 26-33.
<https://www.calameo.com/books/0040572544de9b12d95ed>
- Antúñez Pajuelo, J. M. (2012). Plan de contingencia para casos de emergencia tienda Cassinelli - Surquillo.
- Ortiz (2013) Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de Seguridad de la información en la universidad Nacional agraria de la selva.
- Leiva Peña, R. (2017). Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.
- Sandoval Fernández, L. R. (2019). Modelo de buenas prácticas aplicando ISO 27002 para gestión de incidencias de la red Wncor.
- Palomino Palomino, K. (2017). Buenas Prácticas en Seguridad de la Información Basada en Iso 27002 en la Asociación Para el Desarrollo Empresarial en Apurímac – ADEA.
- García Rivera, J. E., & Del Águila Salas, C. A. R. (2017). Análisis e implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonía Peruana bajo la norma ISO 27002.
- Rodríguez Barbarán, L. V. (2019). Implementación de un sistema de gestión de la calidad basado en la norma ISO 9001 en el proyecto: “Construcción de Viviendas Masivas”.

Calderón Juárez, F. A. (2018). Desarrollo e implementación de un sistema de información online usando dispositivos móviles para optimizar la gestión de recaudación de efectivo en el área de cobranza diaria de la cooperativa de ahorro y crédito san francisco, Huánuco, 2015.

Ingunza Lastra, K. Y., & Valdivia Jaimes, J. A. (2018). Implementación del modelo "Arsi" para optimizar la seguridad de la información en la cooperativa de ahorro y crédito san francisco Ltda. 289.

González, M. A., & Vásquez, L. M. (2013). Impacto del uso de Genexus para la optimización del servicio en la empresa Compañía Monterrico de Movilidad y Mensajería SAC (Tesis de licenciatura). Repositorio de la Universidad Privada del Norte. Recuperado de <http://hdl.handle.net/11537/193>

Veites, A. G. (2001). Enciclopedia de la seguridad Informática 2da Edición. Alfaomega.

https://alicia.concytec.gob.pe/vufind/Record/UDHR_6ec9e24a13451e416a8d557e5604e18f

Sánchez Sánchez, R. M. (2007). Análisis de riesgos en seguridad informática caso UNMSM