

UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA



FACULTAD DE INGENIERÍA DE
SISTEMAS E INFORMÁTICA



**“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.”**

TESIS

Para optar título profesional de:

INGENIERO DE SISTEMAS E INFORMÁTICA.

Presentado por los bachilleres:

JUAN ENRIQUE GARCÍA RIVERA.

CLAUDIO ALBERTO RAÚL DEL ÁGUILA SALAS.

Asesor:

ING. JIMMY MAX RAMÍREZ VILLACORTA.

IQUITOS – PERÚ

2017

DEDICATORIAS.

Dedico este trabajo a Dios, por haberme dado la vida y permitirme llegar a este momento crucial de mi formación profesional. A mi madre por ser el pilar más importante de mi vida y la de mi familia, y por brindarme siempre su apoyo y cariño incondicional. A mi padre quien, con sus consejos y la diferencia de opiniones entre ambos, ha sabido guiarme a lo largo de mi educación, que es el regalo más valioso y preciado que me he podido obtener gracias a él. A mis abuelos tanto padre como de madre que siempre me demuestran su interés y preocupación hacia mi persona.

Claudio Alberto Raúl del Águila Salas.

Dedico este trabajo a aquellos estudiantes y colegas para quienes podrá servirles como punto de referencia la implementación de la Norma ISO 27002.

Juan Enrique García Rivera.

AGRADECIMIENTOS.

A Dios, por haberme dado fuerza y valor, y así poder culminar esta etapa de mi vida.

A mis padres que siempre estuvieron apoyándome y brindándome su confianza.

A la ilustre Universidad Nacional de la Amazonia Peruana, por ser la casa de estudios que me acogió e inculco valores profesionales.

A la Facultad de Sistemas e Informática, su plana docente y administrativa, por brindarme la formación académica y profesional que poseo.

Claudio Alberto Raúl del Águila Salas.

Un agradecimiento al Ingeniero Luis Pita Astengo, responsable de la Oficina General de Informática de la Universidad Nacional de la Amazonia Peruana (OGEIN), quien brindo las herramientas necesarias para realizar este proyecto.

A toda mi familia, por el amor brindado, experiencias y consejos dados sin esperar nada a cambio, los amo.

A la ilustre Universidad Nacional de la Amazonia Peruana, por ser la casa de estudios que me brindo sus conocimientos durante toda mi carrera.

A la Facultad de Sistemas e Informática, su plana docente y administrativo, por brindarme la formación académica y profesional que poseo.

Juan Enrique García Rivera.

RESUMEN.

Mediante la elaboración del análisis de seguridad de la información y seguridad informática basada en la norma ISO/IEC 27002, el presente trabajo tuvo como finalidad conocer las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad.

El análisis estuvo dirigido al centro de datos de la oficina general de informática de la UNAP, teniendo como objetivo principal el estudio de seguridad en los procesos críticos. A través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento del negocio, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información.

La ejecución del análisis de riesgos da a conocer el nivel de impacto que tendría la ocurrencia de las amenazas identificadas en cada activo de la información que pueden afectar datos relevantes utilizados o resultantes de la ejecución de las actividades propias del negocio.

Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información. Pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener la institución.

ABSTRACT

Through the development of the information security and computer security analysis based on ISO / IEC 27002, the present work had as purpose to know the vulnerabilities to which the information is exposed by the lack of application of security controls.

The analysis was directed to the data center of the general office of computer of the UNAP, having as main objective the study of security in the critical processes. Through meetings, review of documentation, consultation, observation, surveys and interviews with executives who have a broad knowledge of the business, it was possible to identify the current risks to which physical, logical and data processing systems are exposed. information.

The execution of the risk analysis reveals the level of impact that the occurrence of the threats identified in each asset of the information that may affect relevant data used or resulting from the execution of the activities of the business.

The results show that, in order to minimize existing risks, it is necessary to implement security controls, which helps to strengthen three important aspects: confidentiality, integrity and availability of information. But the results also show the importance of commitment and teamwork that the institution should have.

INDICE JURADO CALIFICADOR

| | Pag. |
|---------------------------------------|------|
| Historias | 02 |
| Antecedentes | 03 |
| Objetivo | 04 |
| Objetivos | 05 |
| Índice del Contenido | 07 |
| Índice de Tablas | 10 |
| CAPITULO | 12 |
| Introducción | 12 |
| Justificación | 13 |
| Planteamiento del problema | 14 |
| Diseño de la investigación | 14 |
| Objetivos | 15 |
| 1.1. Objetivo general | 15 |
| 1.2. Objetivos específicos | 15 |
| CAPITULO | 15 |
| Marco teórico | 15 |
| 1.1. Antecedentes de la investigación | 15 |
| 1.2. Historia de la ISO | 17 |
| 1.3. Directrices del estándar | 18 |
| 1.4. Certificación | 20 |

ING. ALEJANDRO REATEGUI PEZO
PRESIDENTE

ING. JORGE PUGA DE LA CRUZ
MIEMBRO

ING. RAFAEL VILCA BARBARAN
MIEMBRO

ING. JIMMY MAX RAMÍREZ VILLACORTA
ASESOR

ÍNDICE DEL CONTENIDO.

| | Pag. |
|---|-------------|
| Dedicatorias | 02 |
| Agradecimientos | 03 |
| Resumen | 04 |
| Abstract | 05 |
| Índice del Contenido | 08 |
| Índice de Tablas | 10 |
| I. CAPITULO | 12 |
| 1.1. Introducción | 12 |
| 1.2. Justificación | 13 |
| 1.3. Planteamiento del problema | 14 |
| 1.4. Problema de la investigación | 14 |
| 1.5. Objetivos | 15 |
| 1.5.1. Objetivo general | 15 |
| 1.5.2. Objetivos específicos | 15 |
| II. CAPITULO | 15 |
| 2.1. Marco teórico | 15 |
| 2.1.1. Antecedentes de la investigación | 15 |
| 2.1.2. Historia de la ISO | 17 |
| 2.1.3. Directrices del estándar | 18 |
| 2.1.4. Certificación | 20 |

| | |
|--|----|
| 2.2. Hipótesis de la investigación | 21 |
| 2.3. Variables | 21 |
| III. CAPITULO | 21 |
| 3.1. Metodología | 21 |
| 3.1.1. Tipo de investigación | 21 |
| 3.1.2. Población y muestra | 21 |
| 3.1.2.1. Población | 21 |
| 3.1.2.2. Muestra | 21 |
| 3.1.3. Diseño de la investigación | 22 |
| 3.1.4. Operacionalización de variables | 22 |
| 3.1.5. Técnicas y herramientas utilizados | 23 |
| 3.1.5.1. Plan de recolección de información | 23 |
| 3.1.5.2. Plan de procesamiento de la información | 23 |
| 3.1.5.3. Archivo de la información | 23 |
| 3.1.6. Metodología utilizada | 24 |
| IV. CAPITULO | 27 |
| 4.1. Resultados | 27 |
| 4.1.1. Controles de la norma ISO/IEC 27002 – 2013 aplicables al OGEIN | 27 |
| 4.1.2. Uso de los mecanismos de seguridad de control de la norma ISO/IEC 27002 – 2013 aplicables al OGEIN | 29 |
| 4.1.3. Identificación de medios de seguridad | 40 |
| 4.1.4. Presupuesto de la implementación | 40 |

| | |
|-------------------------------------|----|
| V. CAPITULO | 41 |
| 5.1. Conclusiones | 41 |
| 5.2. Recomendaciones | 41 |
| 5.3. Bibliografía | 44 |
| 5.4. Anexos | 47 |
| Anexo N° 01: Matriz de Consistencia | 48 |

INDICE DE TABLAS.

| | |
|---|----|
| Tabla N° 01: Operacionalización de Variables. | 22 |
| Tabla N° 02: Controles de la Norma ISO aplicados en el OGEIN. | 28 |
| Tablas N° 03: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 29 |
| Tabla N° 04: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 29 |
| Tabla N° 05: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 29 |
| Tabla N° 06: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 30 |
| Tabla N° 07: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 30 |
| Tabla N° 08: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 30 |
| Tabla N° 09: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 30 |
| Tabla N° 10: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 31 |
| Tabla N° 11: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 32 |
| Tabla N° 12: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 33 |
| Tabla N° 13: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 34 |
| Tabla N° 14: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 35 |
| Tabla N° 15: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 36 |
| Tabla N° 16: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 36 |
| Tabla N° 17: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 37 |
| Tabla N° 18: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 37 |
| Tabla N° 19: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 38 |

| | |
|--|----|
| Tabla N° 20: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 38 |
| Tabla N° 21: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 38 |
| Tabla N° 22: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 39 |
| Tabla N° 23: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 39 |
| Tabla N° 24: Uso de los Mecanismos de Seguridad Aplicables al OGEIN. | 39 |
| Tabla N° 25: Identificación de Medios de Seguridad. | 40 |
| Tabla N° 26: Presupuesto de la Implementación. | 40 |

I. CAPITULO.

1.1. INTRODUCCION.

En la actualidad, es un hecho incuestionable que la gran mayoría de los procesos de negocios son soportados, automatizados y gestionados por sistemas informáticos, así como los sistemas de información apoyan la actividad gerencial y la toma de decisiones; incluso muchas veces, es la propia información y el acceso a la misma, el producto / servicio que se intercambia como principal objeto del negocio. La seguridad de la información ya no puede ser concebida como el resultado de un accionar defensivo y reactivo para preservar los activos del negocio, ya que muchas veces, es un activo en sí mismo, una condición para operar y/o competir en el sector, un generador de valor. Requiere un accionar proactivo y su incorporación como elemento estratégico, Por lo tanto, cada vez hay más conciencia y consenso en la importancia de la Seguridad de la Información en las empresas y Organizaciones cualquiera sea el sector de la economía o rol en la sociedad que desempeñen, en particular en las empresas medianas y grandes

Sin embargo, existen diversas industrias y estructuras empresariales que hacen que algunos temas deban ser analizados y estudiados con una estrategia diferente, ya sea por la criticidad de la información que manejan, su dimensión o su estructura empresarial. A modo de ejemplo, pequeñas empresas, con una infraestructura limitada y sistemas informáticos de gestión que no requieran del almacenamiento y procesamiento de información confidencial o crítica ni están sujetos a estrictas normas regulatorias, normalmente van a enfrentar riesgos menores, deben considerar aspectos diferentes al de una gran corporación o grupo empresarial, y también una dimensión del problema diferente, tanto en la problemática como en la de la capacidad de gestión de la solución. Por lo tanto, su estrategia y decisiones responderán a estas diferencias estructurales. Organizaciones más grandes, como pueden ser: empresas del sector financiero, salud, operadoras de telefonía, gubernamentales, etc., deben afrontar la Seguridad de la Información de forma metodológica, planificada y con planes concretos, con un enfoque de continuidad del negocio y mejora continua. Además de parámetros y dimensiones diferentes en su relación costo - beneficio, existen motivos legales, regulaciones y contratos que requieren de la protección de información personal y sensible además de la crítica y estratégica del negocio. De acuerdo a algunas encuestas internacionales, el mayor riesgo a la seguridad de la información, está dado por el factor humano, específicamente errores, conductas inapropiadas y/o negligencia generadas internamente. También existen referencias donde se asegura que la inversión en la gestión de seguridad (de IT) es más efectiva que la

inversión en tecnología para mejorar los niveles de seguridad. El desafío es entonces lograr una metodología que conduzca a una solución eficaz y eficiente, desde el punto de vista técnico y económico, que provea los niveles de seguridad requeridos.

1.2. JUSTIFICACION.

La Información es parte de los activos más importantes de toda empresa, y a su vez es uno de los recursos más propenso a vulnerabilidades, siendo necesario protegerlo de amenazas internas y externas. En la actualidad las empresas necesitan que la información que manejan esté siempre disponible, sin alteraciones en sus datos y sea confiable.

La norma ISO/IEC 27002: Sistemas de Gestión de Seguridad de la Información, proporciona un estándar de calidad de seguridad de la información, ayudando a minimizar los riesgos de daño, robo o fuga de información; permitiendo mantener la integridad, confidencialidad y disponibilidad de la información, además de garantizar la autenticidad y el no repudio de la misma.

Mediante el análisis de seguridad informática y seguridad de la información, podrá conocer y aplicar controles de seguridad en la información que se maneja en la Oficina General de Informática de la UNAP para asegurarse que éste siendo utilizada adecuadamente y solo tenga acceso personas autorizadas.

El desarrollo del análisis de seguridad de la información basada en las Normas ISO/IEC 27002 permitirá conocer las vulnerabilidades existentes en el manejo de la información física, así como la que está contenida en los sistemas de procesamiento de información, de tal forma que se puedan tomar acciones preventivas y correctivas dentro de la empresa, para evitar que se lleguen a comprometer datos confidenciales.

La Oficina General de Informática de la Universidad Nacional de la Amazonia Peruana (OGEIN-UNAP) requiere de una mayor seguridad física, mejor control de acceso y resguardar con mayor eficiencia sus equipos informáticos debido a que debe cumplir estándares internacionales de la norma ISO 27002.

Es indispensable salvaguardar la seguridad física de la Oficina General de Informática debido a que la pérdida o deterioro de los equipos acarrearía:

- Pérdida de Confianza en la Universidad.
- Pérdida de horas de trabajo en reconstruir la información.

- Pérdida de Historial de Notas.
- Pérdida de Acceso al Portal Web.

1.3. PLANTEAMIENTO DEL PROBLEMA.

Durante los últimos años se han presentado incidentes de seguridad que han generado molestias en los usuarios y han sido causa de interrupciones de las actividades que se desarrollan dentro del Centro de Datos de la Universidad Nacional de la Amazonia Peruana, por esta razón se necesita implementar lineamientos de seguridad en las áreas donde se desarrollan los procesos críticos del negocio, de tal forma que puedan garantizar la confidencialidad, disponibilidad e integridad de la información, mitigando riesgos que puedan ocasionar retrasos en las actividades.

El resultado del análisis basado en la norma ISO/IEC 27002, pretende dar a conocer lineamientos de seguridad para prevenir y mitigar vulnerabilidades existentes, proporcionándole controles de seguridad que puedan aplicarse dentro de cada área, en especial de las áreas críticas del centro de datos de la Universidad Nacional de la Amazonia Peruana.

La documentación resultante guiará a dentro del Centro de Datos de la Universidad Nacional de la Amazonia Peruana para que empiece a alinearse en temas de seguridad, ocasionando que se integre a su estructura organizacional un área o persona responsable que se encargue de la seguridad de la información, así como la existencia de una política de seguridad de la información donde se detalle los roles, responsabilidades y controles que se deben aplicar tomando en cuenta desde la seguridad en los sistemas de información hasta la concienciación de sus trabajadores en el manejo de la información.

1.4. PROBLEMA DE LA INVESTIGACION.

¿Cómo se podría minimizar riesgos de pérdida, daño o alteración de la información administrada dentro del Centro de Datos de la Universidad Nacional de la Amazonia Peruana?

1.5. OBJETIVOS.

1.5.1. OBJETIVO GENERAL.

Analizar los mecanismos de seguridad basado en la norma de ISO 27002 para la seguridad física del centro de datos de la Oficina General de Informática – Universidad Nacional de la Amazonía Peruana 2017.

1.5.2. OBJETIVOS ESPECIFICOS.

- Determinar los controles de la norma ISO 27002 respecto a la seguridad física aplicables a Oficina general de Informática de la Universidad Nacional de la Amazonia Peruana 2017.
- Determinar el uso de mecanismos de seguridad para mejorar la gestión de la seguridad brindada por los sistemas de procesamiento, transmisión y almacenamiento en la Oficina general de Informática de la Universidad Nacional de la Amazonia Peruana 2017.
- Identificar los medios de Seguridad en la Oficina general de Informática de la Universidad Nacional de la Amazonia Peruana 2017.
- Realizar el presupuesto de la implementación de los mecanismos de seguridad basado en la norma de ISO 27002 - 2013 para la seguridad física del centro de datos de la Oficina General de Informática – Universidad Nacional de la Amazonía Peruana 2017.

II. CAPITULO.

2.1. MARCO TEORICO.

2.1.1. ANTECEDENTES DE LA INVESTIGACION.

- CRAMM: “CCTA Risk Assessment and Management Methodology” originalmente desarrollado por el gobierno del Reino Unido, dispone de una herramienta que apoya la metodología. Actualmente propiedad de Siemens.

- MAGERIT “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información” desarrollado por el Ministerio de las Administraciones Públicas de España.
- MEHARI: “MEthode Harmonisée d'Analyse de Risque” es una metodología de análisis y gestión de riesgos desarrollada por CLUSIF (“Club de la Sécurité de l'Information Français”).
- NIST (2) SP 800-30: es una Guía de Gestión de Riesgos para los Sistemas y Tecnologías de la Información.
- NIST SP 800-39 “Managing Risk from Information Systems - An Organizational Perspective” (3).
- OCTAVE: “Operationally Critical Threat, Asset, and Vulnerability Evaluation” es un conjunto de métodos, herramientas y técnicas del CERT para la planificación estratégica y evaluación de la seguridad de la información.
- IT GRUNDSCHUTZ: “IT Baseline”, desarrollado por la Oficina Federal de Seguridad de la Información de Alemania.
- ISM3-RA: Es el método de valoración de riesgos propuesto por el modelo de madurez la seguridad de la información ISM3.

Algunas de ellas como CRAMM son antecedentes incluso para la norma BS7799-3 y por ende para la ISO/IEC 27.005 después. Algunas declaran además de ser compatibles, cumplir los requerimientos de la norma ISO/IEC 27.001, otras como Mehari declaran tener objetivos diferentes a los de la norma, pero igualmente ser compatibles con ésta, especialmente en la fase de Planificación, y en las otras fases tener importantes aportes para los procesos y documentos requeridos por la misma.

Por otra parte, en se presenta una metodología de “Análisis y Automatización de la Implantación de SGSI en Empresas Uruguayas”, las cuales son en su amplia mayoría microempresas y PyMEs como se referencia en el mismo. Dicha metodología está enfocada a “a cubrir a aquellas organizaciones que generalmente no poseen metodologías, prácticas, ni requerimientos de seguridad específicos o generales”.

En esa línea de investigación, de una metodología de implantación de SGSI para PyMEs, existen diversos trabajos relacionados como, donde además se incursiona en un tablero integral de mando para la gestión de la seguridad de la información, métricas e indicadores de madurez para las mismas. El modelo es soportado además por una herramienta de software y ha sido mejorada de forma empírica en función de los resultados obtenidos en el sector.

Sin embargo, no hemos encontrado un trabajo específico que abarque las características y necesidades de una empresa como la que nos planteamos en el presente trabajo de tesis, es decir, la de un grupo empresarial constituido por una empresa principal y otra/s subordinada/s, cuyas necesidades son de naturaleza diferente a una PyME, por ejemplo, debido entre otras cosas, a su estructura, dimensión y relacionamiento jerárquico.

En se presenta un artículo con una síntesis parcial de este trabajo, donde se delinea el enfoque, estrategia y principales conclusiones de la metodología para grupos empresariales de relación jerárquica. Artículo que constituye una de las ponencias del “V Congreso Iberoamericano de Seguridad Informática (CIBSI’09)” desarrollado en Montevideo, Uruguay, en noviembre de 2009.

2.1.2. HISTORIA DE LA ISO.

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013.

El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. En el año 2000 la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, con el título de Information Technology - Security Techniques - Code of Practice for Information Security Management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento modificado ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.

En Perú la ISO/IEC 17799:2005 es de uso obligatorio en todas las instituciones públicas desde agosto del 2007, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales, la supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI (www.ongei.gob.pe).

2.1.3. DIRECTRICES DEL ESTANDAR.

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

1. Políticas de Seguridad. Sobre las directrices y conjunto de políticas para la seguridad de la información. Revisión de las políticas para la seguridad de la información.
2. Organización de la Seguridad de la Información. Trata sobre la organización interna: asignación de responsabilidades relacionadas a la seguridad de la información, segregación de funciones, contacto con las autoridades, contacto con grupos de interés especial y seguridad de la información en la gestión de proyectos.
3. Seguridad de los Recursos Humanos. Comprende aspectos a tomar en cuenta antes, durante y para el cese o cambio de trabajo. Para antes de la contratación se sugiere investigar los antecedentes de los postulantes y la revisión de los términos y condiciones de los contratos. Durante la contratación se propone se traten los temas de responsabilidad de gestión, concienciación, educación y capacitación en seguridad de la información. Para el caso de despido o cambio de puesto de trabajo

también deben tomarse medidas de seguridad, como lo es des habilitación o actualización de privilegios o accesos.

4. Gestión de los Activos. En esta parte se toca la responsabilidad sobre los activos (inventario, uso aceptable, propiedad y devolución de activos), la clasificación de la información (directrices, etiquetado y manipulación, manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).

5. Control de Accesos. Se refiere a los requisitos de la organización para el control de accesos, la gestión de acceso de los usuarios, responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones.

6. Cifrado. Versa sobre los controles como políticas de uso de controles de cifrado y la gestión de claves.

7. Seguridad Física y Ambiental. Habla sobre el establecimiento de áreas seguras (perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despacho y recursos, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de acceso público) y la seguridad de los equipos (emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de equipos, salida de activos fuera de las instalaciones, seguridad de equipos y activos fuera de las instalaciones, reutilización o retiro de equipo de almacenamiento, equipo de usuario desatendido y política de puesto de trabajo y bloqueo de pantalla).

8. Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

9. Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.

10. Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.

11. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.

12. Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.

13. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.

14. Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 114 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

2.1.4. CERTIFICACION.

La norma ISO/IEC 17799 es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado para este documento.

La norma ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) sí es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el famoso “Círculo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 y tiene su origen en la norma británica British Standard BS 7799-2 publicada por primera vez en 1998 y elaborada con el propósito de poder certificar los Sistemas de Gestión de la Seguridad de la Información implantados en las organizaciones y por medio de un proceso formal de auditoría realizado por un tercero.

2.2. HIPOTESIS DE LA INVESTIGACION.

Si los controles de seguridad basados en la Norma ISO/IEC 27002, establecen mecanismos adecuados para mitigar riesgos, entonces se pueden presentar en los usos de los sistemas de información y en el manejo de información.

2.3. VARIABLES.

- VARIABLE INDEPENDIENTE (X)

- VARIABLE DEPENDIENTE (Y)

X1. Control de seguridad

Y1. Medios de Seguridad

X2. Mecanismos de Seguridad

III. CAPITULO.

3.1. METODOLOGIA.

3.1.1. TIPO DE INVESTIGACIÓN.

La investigación es de tipo descriptiva.

Tipo de investigación descriptiva: Este tipo de investigación detalla las actividades que se llevan a cabo en los procesos manejados en el objeto de estudio, permitiendo conocer en forma sistemática las falencias que se presentan en los mismos.

3.1.2. POBLACIÓN Y MUESTRA.

3.1.2.1. POBLACIÓN.

La población está conformada por 6 trabajadores que pertenecen a la oficina general de Informática de la Universidad Nacional de la Amazonia Peruana.

3.1.2.2. MUESTRA.

Debido a que la población total involucrada es muy pequeña, la muestra a tomar será el 100% de la población.

3.1.3. DISEÑO DE LA INVESTIGACIÓN.

El diseño de la investigación no experimental: El objeto de estudio de la investigación no se puede modificar deliberadamente, basándose principalmente en la observación de eventos para que puedan ser posteriormente analizados.

3.1.4. OPERACIONALIZACION DE VARIABLES.

| VARIABLES | DIMENSIONES | INDICADORES |
|---|--|---|
| Variable Independiente: X1. Control de seguridad | - Divulgación de las medidas de seguridad | - Políticas de políticas de seguridad que los usuarios deben conocer y aplicar. - Medios determinados para la comunicación de las políticas de seguridad. |
| | - Valoración de las políticas de Seguridad | - Periodicidad en la verificación de la efectividad de las medidas de seguridad. - Periodos determinados para la evaluación interna. |
| X2. Mecanismos de Seguridad | - Seguridad brindada por los sistemas de procesamiento, transmisión y almacenamiento de datos. | - Periodos de revisión de las configuraciones de seguridad de los equipos de almacenamiento de datos. - Periodos de evaluación de seguridad de los sistemas informáticos de procesamiento de datos. - Periodos de revisión de la seguridad en los sistemas de comunicación. |
| Variable Dependiente: Y1. Medios de Seguridad. | - Vulnerabilidades que se conocen y no han podido ser cubiertas | - Histórico de las vulnerabilidades sobre las cuales se han tomado acciones correctivas. - Vulnerabilidades encontradas y reportadas. |

Tabla N° 1: Operacionalización de Variables

3.1.5. TÉCNICAS Y HERRAMIENTAS UTILIZADOS.

Para la selección de las herramientas utilizadas en el proyecto es el siguiente:

3.1.5.1. PLAN DE RECOLECCIÓN DE INFORMACIÓN.

Para desarrollar el análisis de seguridad de la información se utilizará los siguientes mecanismos de recolección de información:

- Entrevistas.
- Consultas.
- Reuniones.
- Observación.
- Revisión de documentación.

3.1.5.2. PLAN DE PROCESAMIENTO DE LA INFORMACIÓN.

Se podrá utilizar el siguiente criterio:

- Levantamiento de Información.
- Clasificación de la Información.
- Registro de la Información.
- Análisis de la información obtenida.
- Verificación de la Información.

3.1.5.3. ARCHIVO DE LA INFORMACIÓN.

El proceso de los datos se realizará sobre la herramienta ofimática de Microsoft, Excel la cual nos permitirá clasificar, verificar y contrastar las variables de la investigación. Con los datos obtenidos se analizará los controles de seguridad que podrá acoger el centro de datos de la UNAP.

Como soporte para la recolección de datos y procesamiento, serán necesarios dos equipos de cómputo portátiles, por movilidad, facilidad para compartir información y poder de procesamiento necesario para detallar resultados y recomendaciones finales.

3.1.6. METODOLOGÍA UTILIZADA.

La metodología a continuación propuesta está alineada a la norma ISO/IEC 27002 y corresponde al análisis de seguridad de la información y seguridad informática realizado, el cual empezó con la identificación de las vulnerabilidades de la situación actual, así como la evaluación de amenazas, vulnerabilidades, impacto y riesgos de los activos de información de las áreas que son consideradas críticas.

Para mitigar las vulnerabilidades encontradas se debe definir y priorizar actividades que conlleven a la aplicación del plan de gestión de la seguridad de la información mediante la implementación de controles de seguridad. Para esto se ha considerado las siguientes fases, en las cuales se detallan un conjunto de actividades a ser realizadas por la empresa.

PRIMERA FASE: DEFINICIÓN:

- Esta primera fase comprende el inicio del plan de gestión de la seguridad de la información, donde se establecen responsabilidades, estándares y procedimientos sobre la dirección del plan de gestión de seguridad.
- Designar formalmente al Responsable de Seguridad de la información y/o Seguridad Informática.
- Definir y establecer las responsabilidades y objetivos del Responsable de Seguridad de la información y/o Seguridad Informática.
- Conformar el Comité de Gestión de la Seguridad de la Información.
- Analizar cada una de las recomendaciones dadas, de tal forma que se dé prioridad de implementación a los controles de seguridad que puedan disminuir el riesgo de mayor impacto.
- Diseñar el manual de políticas de seguridad de la información en base a los controles implementados actualmente y considerando nuevos controles que podrán ser implementados dentro de la empresa.
- Establecer los procedimientos e instructivos de seguridad.
- Designar formalmente a los Propietarios de los activos de información.

- Elaborar un catálogo de Clasificación de la información por área, el cual debe ponerse en conocimiento de todos los funcionarios (categorización: confidencial o pública).
- Evaluar con personal especializado todo lo referente a requerimientos legales, tomando en cuenta organismos de control que regulan a la empresa, leyes ecuatorianas, entre otros.

SEGUNDA FASE: APLICACIÓN:

Esta fase comprende la aplicación de los controles de seguridad anteriormente definidos, se realizan las actividades que han sido diseñadas con el propósito de disminuir el riesgo actual.

- Crear e implementar un programa de capacitación para los trabajadores de la oficina de informática de la UNAP a acerca de temas relacionados con la seguridad informática (charlas, boletines, seminarios, entre otros).
- Implementar los controles de seguridad recomendados en la matriz de situación actual y activos de la información, tomando en cuenta la protección física y lógica de la información y de los sistemas de procesamiento de información.
- Definir y establecer políticas y responsabilidades sobre la administración de accesos de los sistemas de información.
- Estandarizar los USER ID, de tal forma que los responsables del centro de datos de la UNAP utilicen un solo usuario para el ingreso a los diferentes aplicativos.
- Definir y establecer políticas que detallen el buen uso que se le debe dar a los activos del centro de datos de la UNAP.
- Definir procesos que permitan conocer las responsabilidades y obligaciones de los encargados, pasantes, practicantes y terceros en cuanto a la seguridad de la información.
- Gestionar el buen uso de las redes y comunicaciones, generando procedimientos e instructivos.

- Definir el proceso para gestionar los cambios que se necesiten realizar en los aplicativos del centro de datos de la UNAP.
- Incorporar la seguridad de la información en la Gestión de la continuidad del negocio.
- Administrar y registrar los incidentes de seguridad de la información que se presente.
- Analizar la posibilidad de implementación de sistemas de video vigilancia, detectores de humo, sistemas contra incendios.
- Registrar pistas de auditorías en los sistemas de información de la empresa.
- Definir un BACKUP para cada funcionario que desempeñe un rol crítico dentro de las actividades del área de sistemas.

TERCERA FASE: MONITOREO.

- Monitorear la gestión de seguridad de la información, comprobar su eficacia con la finalidad de poder realizar ajustes al plan de seguridad.
- Monitoreo continuo de los controles de seguridad implementados para prevenir incidentes de seguridad.
- Analizar la posibilidad de adquirir herramientas para monitorear las aplicaciones, redes, código malicioso, entre otros.
- Diseñar y ejecutar los indicadores de gestión de seguridad.
- Monitorear el cumplimiento de la gestión del buen uso de los activos.
- Monitorear el acceso y buen uso de redes y comunicación.
- Monitorear el correcto funcionamiento de servicios prestados por terceros.
- Monitorear el cumplimiento de estándares de seguridad del Data-Center.
- Registrar el resultado del monitoreo realizado.

CUARTA FASE: MEJORA.

- Mejorar la gestión de seguridad de la información considerando las vulnerabilidades encontradas luego de monitorear el plan vigente.
- Identificar e incorporar mejoras a la gestión de la seguridad de la información.
- Actualizar el manual de políticas de seguridad de la información cuando ocurran cambios significativos.
- Comprobar la eficacia de las mejoras incorporadas.
- Comunicar las mejoras realizadas a las máximas autoridades.
- Capacitar al personal que maneja la seguridad de la información, así como al personal técnico del centro de datos de la UNAP (administradores, desarrolladores, entre otros).

IV. CAPITULO.

4.1. RESULTADOS.

Al hacer uso de nuestros indicadores de evaluación de la solución, se han obtenido los siguientes resultados:

4.1.1. CONTROLES DE LA NORMA ISO/IEC 27002 - 2013 APLICABLES AL OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|------|------------------------------|---|--|
| 001 | 8. Gestión de Activos. | 8.1. Responsabilidad ligada sobre los activos | 8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos. 8.1.3. Uso aceptable de los activos. 8.1.4. Devolución de activos. |
| 002 | 8. Gestión de Activos. | 8.3. Manejo de los soportes de almacenamiento. | 8.3.1. Gestión de soportes extraíbles. 8.3.2. Eliminación de soportes. 8.3.3. Soportes físicos en tránsito. |

| | | | |
|-----|--------------------------------------|---------------------------------|---|
| 003 | 11. Seguridad Física Y Ambiental. | 11.1. Áreas seguras. | <p>11.1.1. Perímetro de seguridad física.</p> <p>11.1.2. Controles físicos de entrada.</p> <p>11.1.3. Seguridad de oficinas, despachos y recursos.</p> <p>11.1.4. Protección contra las amenazas externas y ambientales.</p> <p>11.1.5. El trabajo en áreas seguras.</p> <p>11.1.6. Áreas de acceso público, carga y descarga.</p> |
| 004 | 11. Seguridad Física Y Ambiental | 11.2. Seguridad de los equipos. | <p>11.2.1. Emplazamiento y protección de equipos.</p> <p>11.2.2. Instalaciones de suministro.</p> <p>11.2.3. Seguridad del cableado.</p> <p>11.2.4. Mantenimiento de los equipos.</p> <p>11.2.5. Salida de activos fuera de las dependencias de la empresa.</p> <p>11.2.6. Seguridad de los equipos y activos fuera de las instalaciones.</p> <p>11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento.</p> <p>11.2.8. Equipo informático de usuario desatendido.</p> <p>11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla.</p> |

Tabla N° 2: Controles de la Norma ISO aplicados en el OGEIN.

4.1.2. USO DE LOS MECANISMOS DE SEGURIDAD DE CONTROL DE LA NORMA ISO/IEC 27002 – 2013 APLICABLES AL OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------|--|-------------------------------|
| 001 | 8. Gestión de activos | 8.1. Responsabilidad ligada sobre los activos. | 8.1.1. Inventario de activos. |
| LABOR: La oficina general de informática ya cuenta con los activos identificados, y mantiene un inventario de los mismos. | | | |

Tabla N° 3: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|------------------------|--|----------------------------------|
| 002 | 8. Gestión de Activos. | 8.1. Responsabilidad ligada sobre los activos. | 8.1.2. Propiedad de los activos. |
| LABOR: Todos los activos están justificados y tienen asignado un propietario el cual tiene la responsabilidad de darle mantenimiento adecuado. | | | |

Tabla N° 4: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|------------------------|--|--------------------------------------|
| 003 | 8. Gestión de Activos. | 8.1. Responsabilidad ligada sobre los activos. | 8.1.3. Uso aceptable de los activos. |
| LABOR: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. | | | |
| RECOMENDACIÓN: Elaborar manuales de uso correspondiente a la información y el uso asociado con los respectivos activos. | | | |

Tabla N° 5: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|------------------------|--|-------------------------------|
| 004 | 8. Gestión de Activos. | 8.1. Responsabilidad ligada sobre los activos. | 8.1.4. Devolución de activos. |
| RECOMENDACIÓN: No se debe permitir el uso de los equipos fuera de la institución. | | | |

Tabla N° 6: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|------------------------|--|--|
| 005 | 8. Gestión de Activos. | 8.3. Manejo de los soportes de almacenamiento. | 8.3.1. Gestión de soportes extraíbles. |
| RECOMENDACIÓN: Elaborar procedimientos respecto a las unidades de almacenamiento extraíble como discos, cintas, USB, Micro SD asegurará los soportes y la información en tránsito no solo físico si no también electrónico contra la divulgación, modificación de datos sensibles o valiosos para el OGEIN. | | | |

Tabla N°7: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|------------------------|---|---------------------------------|
| 006 | 8. Gestión de Activos. | 8.3. Manejo de los soportes de almacenamiento | 8.3.2. Eliminación de soportes. |
| LABOR: Se eliminan los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales a través del envío a patrimonio. | | | |

Tabla N° 8: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|------------------------|--|--------------------------------------|
| 007 | 8. Gestión de Activos. | 8.3. Manejo de los soportes de almacenamiento. | 8.3.3. Soportes físicos en tránsito. |
| RECOMENDACIÓN: Crear procedimientos correspondientes de ser necesario el traslado fuera las oficinas. | | | |

Tabla N° 9: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.1. Áreas seguras. | 11.1.1. Perímetro de seguridad física. |
| RECOMENDACIÓN: Implementar cámaras de seguridad en la entrada de la Oficina General de Informática para el debido control de cada persona que ingrese | | | |
| ACTUAL | | PROPUESTO | |
|  | |  | |

Tabla N° 10: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|------|----------------------------------|----------------------|---------------------------------------|
| 008 | 11. Seguridad Física Y Ambiental | 11.1. Áreas seguras. | 11.1.2. Controles físicos de entrada. |

RECOMENDACIÓN: Se recomienda el uso de un formulario de registro de ingreso y el uso de fotocheck de identificación.



Tabla N° 11: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|-----------------------------------|---|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.1. Áreas seguras. | 11.1.3. Seguridad de oficinas, despachos y recursos. |
| RECOMENDACIÓN: Implementar puertas de fierro para mayor seguridad de los equipos informáticos. | | | |
| ACTUAL | | PROPUESTO | |
|  | |  | |

Tabla N° 12: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.1. Áreas seguras. | 11.1.4. Protección contra las amenazas externas y ambientales. |
| RECOMENDACIÓN: Implementar mampara de vidrio templado con el logo de la Institución y un sensor dactilar para el ingreso a la sala de servidores. | | | |
| ACTUAL | | PROPUESTO | |
|  | |  | |

Tabla N° 13: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|--|--------------------------------------|
| 008 | 11. Seguridad Física Y Ambiental. | 11.1. Áreas seguras. | 11.1.5. El trabajo en áreas seguras. |
| <p>RECOMENDACIÓN: Implementación de Central contra incendio y batería de soporte Pulsador de Emergencia Sensores de Humo y Temperatura Extintores en caso de incendios Implementación de señales de seguridad</p> | | | |
| ACTUAL | | PROPUESTO | |
|  | |  | |
|  | |  | |

Tabla N° 14: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|-----------------------------------|----------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.1. Áreas seguras. | 11.1.6. Áreas de acceso público, carga y descarga. |
| RECOMENDACIÓN: Establecer un punto de acceso para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información. | | | |

Tabla N° 15: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---------------------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.1. Emplazamiento y protección de equipos. |
| LABOR: Los equipos se sitúan donde se pueda proteger para reducir los riesgos de las amenazas y peligros ambientales. | | | |



Tabla N° 16: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|-----------------------------------|---------------------------------|--------------------------------------|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.2. Instalaciones de suministro. |
| <p>Recomendación: Reitero la instalación física adecuada, mantenimiento preventivo y cambio de baterías del equipo ups del centro de datos de la UNAP emitida con Oficio N° 167-2016-OGEIN-UNAP al Rectorado el 26 de septiembre del 2016 y Adjuntado el informe técnico N° 169-16 presentado por Protecline SAC el 19 -09-2016.</p> | | | |
|  | | | |

Tabla N° 17: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---------------------------------|---------------------------------|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.3. Seguridad del cableado. |
| <p>RECOMENDACIÓN: Revisión del cableado eléctrico existente a fin de prever fallos. Además, reitero la solicitud de apoyo técnico para levantar información de los pozos a tierra con los que cuenta la UNAP emitida a la oficina general de mantenimiento con Oficio N° 052-2016-OGEIN.UNAP el 20 de abril del 2016.</p> | | | |

Tabla N° 18: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---------------------------------|---------------------------------------|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.4. Mantenimiento de los equipos. |
| RECOMENDACIÓN: Realización de un plan anual de mantenimiento de los equipos para lograr un control y prevención de posibles fallas. | | | |

Tabla N° 19: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|-----------------------------------|---------------------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.5. Salida de activos fuera de las dependencias de la empresa. |
| RECOMENDACIÓN: Implementar procedimientos de control y documentación donde se registre la salida de los equipos. | | | |

Tabla N° 20: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---------------------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.6. Seguridad de los equipos y activos fuera de las instalaciones. |
| RECOMENDACIÓN: Implementar medidas de seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos. | | | |

Tabla N° 21: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|---|-----------------------------------|---------------------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.7. Reutilización o retirada segura de dispositivos de almacenamiento. |
| RECOMENDACIÓN: Implementar medios de almacenamiento para garantizar que cualquier tipo de datos sensibles de software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización. | | | |

Tabla N° 22: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|-----------------------------------|---------------------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.8. Equipo informático de usuario desatendido. |
| RECOMENDACIÓN: Implementar de políticas de seguridad donde los usuarios se deberían asegurar de que los equipos no supervisados cuentan con protección adecuada. | | | |

Tabla N° 23: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

| ITEM | DOMINIO | OBJETIVO DEL CONTROL | CONTROL |
|--|-----------------------------------|---------------------------------|--|
| 008 | 11. Seguridad Física Y Ambiental. | 11.2. Seguridad de los equipos. | 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla. |
| RECOMENDACIÓN: Adoptar políticas de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procedimiento de información. | | | |

Tabla N° 24: Uso de los Mecanismos de Seguridad Aplicables al OGEIN.

4.1.3. IDENTIFICACION DE MEDIOS DE SEGURIDAD.

| ITEM | MEDIOS DE SEGURIDAD |
|------|--|
| 1 | Puerta de fierro en la entrada de la Oficina Nacional de la amazonia peruana. |
| 2 | Cámaras de seguridad para el control de acceso. |
| 3 | Extintores para la prevención de accidentes. |
| 4 | Sensores de humo para la prevención de accidentes. |
| 5 | Señales de ingreso, aforo, no fumar, prohibido el ingreso de personas no autorizadas, zona segura ante sismos. |

Tabla N° 25: Identificación de Medios de Seguridad.

4.1.4. PRESUPUESTO DE LA IMPLEMENTACION.

| CANT. | DESCRIPCIÓN | PRECIO UNIT. | TOTAL |
|-------|---|--------------|---------------------|
| 02 | Extintor PQS 12 kg. | S/. 295.00 | S/. 590.00 |
| 05 | Señalizaciones | S/. 3.50 | S/. 17.50 |
| 02 | Detectores de humo | S/. 40.00 | S/. 80.00 |
| 01 | Luces de emergencia | S/. 95.00 | S/. 95.00 |
| 01 | Kit de seguridad de cámara de video 8 canales (No incluye DVR y Disco Duro) | S/. 1490.00 | S/. 1490.00 |
| | TOTAL | | S/. 2,272.50 |

Tabla N° 26: Presupuesto de la Implementación.

V. CAPITULO.

5.1. CONCLUSIONES.

- En conclusión, el análisis realizado demuestra que los activos de información de las áreas consideradas críticas y la situación actual de la Oficina general de Informática con respecto a la seguridad de la información, refleja potenciales índices de riesgos, los cuales exponen a la información a daños, robo o modificaciones que pueden causar un impacto negativo dentro de las actividades del negocio.
- Mediante las recomendaciones indicadas, se pretende que la OGEIN -UNAP tome acciones que le permitan prevenir y detectar oportunamente vulnerabilidades a las que están expuestos los sistemas de procesamiento de información, así como la información que es manejada y generada por los trabajadores de la oficina general de Informática.
- La implementación de controles de seguridad basados en la norma ISO/IEC 27002, les permite mejorar tres características importantes como son: la confidencialidad, integridad y disponibilidad de la información.
- El elaborar un manual de políticas de seguridad de la información donde se detallen controles de seguridad acorde a la realidad y necesidades actuales de la OGEIN -UNAP, la constante concienciación a los trabajadores, así como el monitoreo continuo, encamina a la empresa a la correcta gestión de la seguridad de la información.

5.2. RECOMENDACIONES.

- Se debe elaborar un manual de Política de Seguridad de la Información alineada a las mejores prácticas de seguridad, que recoja todos los controles actualmente implementados en la empresa, adicionalmente se debe incluir nuevos controles de seguridad acorde a las necesidades de la empresa.
- Es importante continuar con el compromiso y la comunicación permanente entre el Responsable de Seguridad Informática y la máxima autoridad, para

que así se logren mitigar cualquier tema relacionado con seguridad informática y seguridad de la información de forma oportuna.

- Se deberá designar formalmente al "Responsable de Seguridad informática" y definir claramente las actividades que debe realizar, de tal forma que se encargue de mitigar todos los temas relacionados con la seguridad informática y seguridad de la información.
- Es importante que todos los funcionarios conozcan quien es el "Responsable de Seguridad informática", de tal forma que puedan saber a quién dirigirse oportunamente en casos de incidentes de seguridad.
- Se debe planificar un análisis de riesgos referente al acceso a la información que tienen las terceras, de tal forma que se identifique vulnerabilidades que pueden existir.
- Por temas de seguridad física, se debe considerar la colocación de mecanismos de accesos en las entradas de cada área, de tal forma que se garantice que solo el personal autorizado ingrese a dichas áreas.
- Por temas de seguridad de los funcionarios, seguridad de la información y de los equipos de procesamiento de información, se debe de contar al menos con alarmas que detecte humo para así prevenir daños en casos de incendios.
- Es necesario considerar un back up para el manejo de las llaves del Data Center en caso de no encontrarse el responsable principal.
- De ser posible implementar un mecanismo de acceso al área donde se encuentran estos equipos.
- Adicionalmente se deben considerar todas las medidas de seguridad para el área donde se encuentra el Rack de comunicaciones y UPS.

- Se debe considerar el uso de un UPS que les permita tener electricidad cuando el servicio público tenga fallas, de tal forma que no se paraliquen las actividades normales dentro de la empresa.
- Existe la política de respaldos de información, en la cual detallan tres frecuencias de respaldos que se realizan y la información que se respalda en cada una de ellas. Todas las tareas de respaldos son registradas en el documento "Bitácora Procesos especiales", en se detalla el responsable del respaldo, fecha, hora y observaciones en caso de que se llegue a presentar algún evento durante el proceso de respaldo de información.
- Se recomendó al jefe de la Oficina General de Informática la implementación de estas recomendaciones en el menor tiempo posible para prever situaciones que atenten contra la seguridad física del OGEIN-UNAP.
- Se recomienda a las autoridades proveer los recursos necesarios que faciliten la implementación justificado en dicho informe.

5.3. BIBLIOGRAFIA.

[1]

ISO/IEC. (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Octubre 10, 2014, de ISO/IEC.

Disponible en:

http://www.cva.itesm.mx/biblioteca/pagina_con_formato_version_oct/apaweb.html

[2]

ISOTools Excellence. (2014). ISO 27001. Octubre 10, 2014, de ISOTools Excellence.

Disponible en:

http://www.isotools.org/normas/riesgos-y-seguridad/iso_27001/

[3]

ISOTools Excellence. (2014). La Norma ISO 27001 y la importancia de la gestión de la seguridad de la información. Octubre 10, 2014, de ISOTools Excellence.

Disponible en:

http://www.isotools.org/pdfs/Monografico-ISO-27001_ISOTools.pdf

[4]

Kosutic, D. (2014). La lógica básica de la norma ISO 27001. Noviembre 12, 2014, de 27001 Academy,

Disponible en:

http://www.iso27001standard.com/blog/2014/05/05/the-basic-logic-of-iso_27001-how-does-information-security-work/#

[5]

Kosutic, D. (2014). Qué es norma ISO 27001. Noviembre 15, 2014, de 27001 Academy.

Disponible en:

<http://www.iso27001standard.com/es/que-es-iso-27001/>

[6]

Kosutic, D. (2014). Porque ISO 27001 es importante para su empresa. Noviembre 22, 2014, de 27001 Academy.

Disponible en:

<http://www.iso27001standard.com/es/que-es-iso-27001/>

[7]

Kosutic, D. (2014). Cómo es realmente ISO 27001. Diciembre 8, 2014, de 27001 Academy.

Disponible en:

<http://www.iso27001standard.com/es/que-es-iso-27001/>

[8]

Dirección General de Modernización Administrativa y Procedimientos e Impulso de la Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España, noviembre 15, 2014,

Disponible en:

https://www.cccert.cni.es/publico/herramientas/pilar5/magerit/Libro_1_metodo.pdf

[9]

Xerox. (2012). SO 27001 Certificaciones Seguridad Comprometidos con el más alto nivel de seguridad de la información. Diciembre 18, 2014, de Xerox ISO 27001 security certifications,

Disponible en:

https://www.xerox.com/download/security/white-paper/27b1e0_4b3fde3a23980/ISO-27001-Security-Certification.pdf

[10]

María Eugenia Corti. "Análisis y automatización de la implantación de SGSI en Empresas Uruguayas". Tesis de maestría, Universidad de la República, Facultad de Ingeniería, 2006.
Sandstrom O., "Proceso de implantación de un SGSI, adoptando la ISO 27001". Arsys Internet.

[http://www.borrmart.es/articulo_redseguridad.php?id=1724&numero=33_\(noviembre_de_2009\)](http://www.borrmart.es/articulo_redseguridad.php?id=1724&numero=33_(noviembre_de_2009))

[11]

ISO27000.es. "Sistema de Gestión de la Seguridad de la Información".

[http://www.iso27000.es/doc_sgsi_all.htm_\(octubre_de_2009\)](http://www.iso27000.es/doc_sgsi_all.htm_(octubre_de_2009))

[12]

UNIT - ISO/IEC 27001:2005. "Tecnología de la información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos".

[13]

UNIT - ISO/IEC 27002: 2005. “Tecnología de la información – Código de buenas prácticas para la gestión de la Seguridad de la Información”.

ANEXOS

5.4. ANEXOS: MATRIZ DE CONSISTENCIA.

TITULO "ANALISIS E IMPLEMENTACIÓN DE LA SEGURIDAD DE LA INFORMACION DEL CENTRO DE DATOS DE LA UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA BAJO LA NORMA ISO 27002"

| PROBLEMA | OBJETIVOS | HIPOTESIS | VARIABLES | DIMENSIONES | INDICADORES | METODOLOGIA |
|--|---|--|--|--|--|---|
| ¿Cómo se podría minimizar riesgos de pérdida, daño o alteración de la información administrada dentro del Centro de Datos de la Universidad Nacional de la Amazonia Peruana? | <p>OBJETIVO GENERAL.</p> <ul style="list-style-type: none"> - Proponer mecanismos de seguridad basado en la norma de ISO 27002 para la seguridad física del centro de datos de la Oficina General de Informática - Universidad Nacional de la Amazonía Peruana 2017. <p>OBJETIVOS ESPECÍFICOS.</p> <ul style="list-style-type: none"> - Determinar los controles de la norma ISO 27002 respecto a la seguridad física aplicables a Oficina general de Informática de la Universidad Nacional de la Amazonia Peruana 2017. - Determinar el uso de mecanismos de seguridad para mejorar la gestión de la seguridad brindada por los sistemas de procesamiento, transmisión y | <p>Hipótesis General.</p> <p>A través de controles de seguridad basados en la Norma ISO/IEC 27002 se establecen mecanismos adecuados para mitigar riesgos que se pueden presentar en los usos de los sistemas de información y en el manejo de información</p> | <p>VARIABLE INDEPENDIENTE:</p> <p>X1. Control de seguridad</p> <p>X2.. Mecanismos de Seguridad</p> | <p>- Divulgación de las medidas de seguridad</p> <p>- Valoración de las políticas de Seguridad.</p> <p>-Seguridad brindada por los sistemas de procesamiento, transmisión y almacenamiento de datos.</p> | <p>- Políticas de políticas de seguridad que los usuarios deben conocer y aplicar.</p> <p>- Medios determinados para la comunicación de las políticas de seguridad.</p> <p>- Periodicidad en la verificación de la efectividad de las medidas de seguridad.</p> <p>- Periodos determinados para la evaluación interna.</p> <p>- Periodos de revisión de las configuraciones de seguridad de los equipos de almacenamiento de datos.</p> <p>- Periodos de evaluación de seguridad de los sistemas informáticos de procesamiento de datos.</p> | <p>Tipo de Investigación</p> <p>La investigación es de tipo descriptiva y tecnológica.</p> <p>Diseño de Investigación</p> <p>Teniendo en cuenta la naturaleza del problema, objetivos e hipótesis es un diseño no experimental, transversal.</p> <p>Población</p> <p>La población está conformada por 6 trabajadores que pertenecen a la oficina general de Informática de la Universidad Nacional de la Amazonia Peruana.</p> <p>Muestra.</p> <p>Debido a que la población total involucrada es muy pequeña, la muestra es el 100% de la población.</p> <p>Técnicas e Instrumentos de recolección de datos</p> <p>Plan de recolección de información</p> |

| | | | | | | |
|--|--|--|--|--|---|--|
| | <p>almacenamiento en la Oficina general de Informática de la Universidad Nacional de la Amazonia Peruana 2017.</p> <p>- Identificar los medios de Seguridad en la Oficina general de Informática de la Universidad Nacional de la Amazonia Peruana 2017.</p> <p>- Realizar el presupuesto de la implementación de los mecanismos de seguridad basado en la norma de ISO 27002 - 2013 para la seguridad física del centro de datos de la Oficina General de Informática - Universidad Nacional de la Amazonía Peruana 2017.</p> | | | | - Periodos de revisión de la seguridad en los sistemas de comunicación. | <p>Para desarrollar el análisis de seguridad de la información se utilizará los siguientes mecanismos de recolección de información:</p> <ul style="list-style-type: none"> - Encuestas. - Entrevistas. - Consultas. - Reuniones. - Observación. - Revisión de documentación. <p>Plan de procesamiento de la información</p> <p>Se utilizó el siguiente criterio:</p> <ul style="list-style-type: none"> - Levantamiento de Información. - Clasificación de la Información. - Registro de la Información. - Análisis de la información obtenida. - Verificación de la Información. |
| | | | | | <p>VARIABLE DEPENDIENTE:</p> <p>Y1. Medios de Seguridad</p> | |