UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN SEGURIDAD Y AUDITORÍA INFORMÁTICA

TESIS

DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ALINEADO A LA NORMA ISO/IEC 27001: CASO UNIVERSIDAD NACIONAL DE MOQUEGUA

PRESENTADA POR

BACH. MARIBEL ESTELA COAGUILA MAMANI

ASESOR

DR. ANÍBAL FERNANDO FLORES GARCÍA

PARA OPTAR EL GRADO DE MAESTRO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN SEGURIDAD Y AUDITORÍA INFORMÁTICA

MOQUEGUA – PERÚ

2020

ÍNDICE DE CONTENIDO

PORTADA
PÁGINA DE JURADO i
DEDICATORIA ii
AGRADECIMIENTOS iii
ÍNDICE DE TABLAS vi
ÍNDICE DE FIGURAS vii
RESUMEN viii
ABSTRACT ix
INTRODUCCIÓN x
CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN 1
1.1. Descripción de la Realidad Problemática 1
1.2. Definición del problema 4
1.2.1. Problemas específicos 4
1.3. Objetivo de la Investigación 4
1.3.1. Objetivos específicos 5
1.4. Justificación 5
1.5. Limitaciones 6
1.6. Variables 6
1.7. Hipótesis de la Investigación 7
1.7.1. Hipótesis específicas 7
CAPÍTULO II: MARCO TEÓRICO 8
2.1 Antecedentes de la investigación 8
2.2 Bases teóricas 13
2.2.1 El Sistema de Gestión de Seguridad de la Información 13
2.2.2 ¿Para qué sirve un SGSI? 13
2.2.3 ¿Qué incluye un SGSI? 14
2.2.4 ¿Qué aspectos de seguridad cubre un SGSI? 15
2.2.5 Revisión del SGSI 16
2.2.6 Análisis y Evaluación del Riesgo 16

2.2.7 Tratamiento del Riesgo y la Toma de Decisiones Gerenciales 17
2.2.8 Normas, Guías y Estándares 18
2.2.9 La Norma ISO 27001:2013 19
2.2.10 COBIT 23
2.2.11 Los activos informáticos 26
2.3 Marco conceptual.....28
CAPÍTULO III: MÉTODO 30
3.1 Tipo de Investigación.....30
3.2 Diseño de investigación.....30
3.3 Población y muestra.....31
3.4 Técnicas e instrumentos de recolección de datos 32
3.5 Técnicas de procesamiento y análisis de datos.....33
CAPITULO IV: RESULTADOS DE LA INVESTIGACIÓN.....34
4.1 Descripción de la encuesta a expertos del nivel de validez de la propuesta.....34
4.2 Descripción de los resultados previsibles de la propuesta.....36
4.3 Validación de la propuesta de Plan de Seguridad.....39
4.4 Verificación de la hipótesis general 40
4.5 Plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001: Caso Universidad Nacional de Moquegua.....41
CONCLUSIONES.....178
RECOMENDACIONES.....179
BIBLIOGRAFÍA.....180
ANEXOS.....183

ÍNDICE DE TABLAS

Tabla 1. Variable independiente: Normas ISO/IEC 27001 6
Tabla 2. Variable dependiente: Sistema de Gestión de Seguridad de la Información 6
Tabla 3. Distribución de la muestra 32
Tabla 4. Ficha de validación de la propuesta de seguridad 39
Tabla 5. Cláusulas 4 a 10 de la ISO/IEC 27001:2013 46
Tabla 6. Modelo de madurez y capacidad según la norma ISO / IEC 15504-2:2003 50
Tabla 7. Nivel de madurez y capacidad del SGSI 50
Tabla 8. Nivel de madurez de los documentos obligatorios 52
Tabla 9. Nivel de madurez de los registros obligatorios 53
Tabla 10. Probabilidad de ocurrencia 58
Tabla 11. Nivel de impacto 59
Tabla 12. Nivel de evaluación del riesgo 63
Tabla 13. Nivel de evaluación del apetito del riesgo 64
Tabla 14. Descripción de los campos Formato para el inventario de activos de información del SGSI 66
Tabla 15. Valoración de la disponibilidad de los activos 67
Tabla 16. Valoración de la integridad de los activos 68
Tabla 17. Valoración de la confidencialidad de los activos 68
Tabla 18. Inventario de Activos 71
Tabla 19. Matriz de Riesgos 75
Tabla 20. Tratamiento de Riesgos 79
Tabla 21. Tratamiento del riesgo según el vector de amenaza 81
Tabla 22. Listado de Políticas desarrolladas 88
Tabla 23. Controles seleccionados del Anexo A de la ISO 27001:2013según la evaluación de riesgos 89
Tabla 24. Lista de Controles 90
Tabla 25. Responsables del monitoreo del tratamiento de riesgo 91
Tabla 26. Matriz RACI Valoración de la disponibilidad de los activos 95
Tabla 27. Tiempo de ejecución de los proyectos para la implementación de los controles seleccionados 99

ÍNDICE DE FIGURAS

Figura 1. Riesgos - SGSI..... 14
Figura 2. Documentación del Sistema de Seguridad 14
Figura 3. Aspectos que cubre el SGSI 15
Figura 4. Pasos para la Metodología de Análisis de Riesgos..... 16
Figura 5. Gestión de Riesgos 18
Figura 6. Familia de normas ISO/IEC 27000..... 19
Figura 7. Gráfico resumen de los riesgos identificados: 76
Figura 8. Estrategia para el tratamiento del riesgo..... 78

RESUMEN

La investigación se orienta hacia la elaboración de un Plan de Gestión de Seguridad de la Información alienado la norma ISO/IEC 27001, para fortalecer la seguridad de los sistemas informáticos de la Universidad Nacional de Moquegua. El tipo es aplicada, el diseño es no experimental – transversal, la información fue obtenida a través de la técnica de la encuesta, para esto se utilizó un cuestionario en base a la norma ISO-IEC 27001:2013, la muestra de estudio estuvo conformada por 8 docentes, 81 alumnos y 7 directores de escuela, incluyendo al jefe de DASA, siendo en total 96 encuestados. La propuesta consta de 3 capítulos: Capítulo I el contexto organizacional, el Capítulo II la gestión de riesgos y el Capítulo III el tratamiento de riesgos. Finalmente, la validación de la propuesta se realizó con la participación de 3 expertos, obteniendo un alto nivel de validez, con estos resultados queda demostrada la hipótesis general.

Palabras clave: *Plan de Seguridad, Contexto Organizacional, Gestión de Riesgos, Tratamiento de Riesgos, Norma ISO.*

ABSTRACT

The research is oriented towards the elaboration of an Information Security Management Plan alienated from the ISO / IEC 27001 standard, to strengthen the security of the computer systems of the National University of Moquegua. The type is applied, the design is non-experimental - transversal, the information was obtained through the survey technique, for this a questionnaire was used based on the ISO-IEC 27001: 2013 standard, the study sample was formed by 8 teachers, 81 students and 7 school directors, including the head of DASA, with a total of 96 respondents. The proposal consists of 3 chapters: Chapter I the organizational context, Chapter II risk management and Chapter III risk management. Finally, the validation of the proposal was carried out with the participation of 3 experts, obtaining a high degree of validity, with these results the general hypothesis is demonstrated.

Keywords: *Security Plan, Organizational Context, Risk Management, Risk Treatment, ISO Standard.*

INTRODUCCIÓN

La información se constituye en un activo valioso para las empresas e instituciones, son el insumo en la toma de decisiones, para ello es importante determinar la confiablidad de los controles implementados, identificando las causas que generan problemas en los sistemas de información y estos puedan estar afectando a las actividades que realiza la institución. Hoy en día se generan inmensas cantidades de información, para esto las empresas e instituciones, recurren a la sistematización y utilizan herramientas, equipos informáticos y personal preparado para optimizar los procesos de trabajo, sin embargo, no siempre le dan suficiente importancia a la seguridad y auditoría informática, considerándolo como un gasto y no inversión. La norma ISO/IEC 27001 es una norma internacional auditable que precisa los requisitos que debe cumplir un sistema de gestión de seguridad de la información, ha sido creada para avalar la protección de los activos de información. En este caso la presente investigación consistió en el desarrollo de una propuesta de Plan de Gestión de Seguridad de la Información alienado la norma ISO/IEC 27001 para la Universidad Nacional de Moquegua, con el propósito de alcanzar un conjunto ordenado de lineamientos y que, al implementarse, cumplirán el rol de defensa de la información de la organización académica. La investigación está conformada por: Capítulo I el problema de investigación, Capítulo II el marco teórico, Capítulo III el método, Capítulo IV los resultados de la investigación, Conclusiones, Recomendaciones, Referencias Bibliográficas y Anexos.

La autora

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción de la Realidad Problemática

La Secretaría de Gobierno Digital (SeGDi) es el ente, con atribución técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico.

Existen una serie de normas, como las ISO, estos lineamientos pueden ser aplicados al contexto de las organizaciones que operan en el país, para ello se tiene las normas ISO 27001, cuya finalidad es gestionar la seguridad de la información, la ISO 27002, que suministra lineamientos para mejorar las prácticas referentes a la seguridad de la información y la ISO 27003, enfoca su atención en las exigencias, que se traduce, en un buen diseño e implementación. Las instituciones de diversa índole, utilizan los sistemas y se convierten en activos intangibles, de alta importancia en su funcionamiento, por lo que se vuelven más complejos.

En este contexto se tiene que, una cantidad mayor de usuarios que acceden a la información, ponen en riesgo los datos de la Institución. Además, siempre se debe tener en cuenta, el riesgo que significa la sustracción de la información ya sea a través de los usuarios que acceden a la información, como por terceros que tienen la posibilidad de acceder a ella, mediante algún mecanismo de ataque; para poder minimizar los riesgos a los que son vulnerables. Estas normas técnicas exigen que las organizaciones, implementen estos sistemas, no existiendo un detalle específico dado que las recomendaciones son generales.

El problema radica, en que las instituciones públicas de la región Moquegua, ya sean el Gobierno Regional y los Gobiernos Locales, no cuentan con este sistema, diseñado para proteger la información, debido al alto costo que representa adquirir los equipos especializados, tampoco se cuenta con personal técnico idóneo, teniéndose en cuenta, que para la operatividad del SGSI, se requiere de capital humano permanente, y que no sea cambiado, cada vez que se inicia una nueva gestión (4 años), tampoco se dispone de infraestructura conveniente, para el funcionamiento; todas estas evidencias, ponen en riesgo, la seguridad de la información, que ante un ataque informático, la institución colapsaría y se alteraría su funcionamiento. En esta ocasión, se eligió a la Universidad Nacional de Moquegua, que fue creada por Ley Nº 28520, del 24 de mayo del 2005; mediante Resolución Nro. 204-2007-CONAFU, del 10 de julio del 2007, iniciando su funcionamiento con carreras profesionales relacionadas a la ingeniería y gestión.

Como institución dedicada a la formación académico, gestiona información, sobre sus estudiantes de: pre grado, centro pre universitario, centro de idiomas y centro de capacitación en TICS; permitiendo mantener un historial del rendimiento académico, a través de los certificados de estudio; y debe ser protegida para garantizar el servicio correctamente, evitando la fuga de información que pudiera ser utilizada inadecuadamente por terceros.

Con estas medidas, se resguarda el activo intangible "información", que se encuentra expuesto a una serie de amenazas de diversa índole, evitando en un futuro, desembolsos económicos no planificados, sumado a esto, la alteración de las actividades normales de funcionamiento, que repercute en la atención tanto de los clientes internos como externos. Así mismo, se optará por la norma ISO/IEC 27001:2013, por aumentar sus dominios a 14, con relación al 27001:2005, que solicitaba 11 dominios, mejorando la efectividad de un SGSI; con respecto a los controles, la norma ISO/IEC 27001:2005, contemplaba 133 controles, y la norma ISO/IEC 27001:2013, ha disminuido a 113, eliminando controles, no muy funcionales en un SGSI.

El SGSI a diseñar, se convertirá en una de las decisiones más significativas, para resguardar la información y definir las inspecciones necesarias. La situación de la problemática requiere de diseñar un Sistema de Gestión de Seguridad de la Información en base a la norma ISO/IEC 27001:2013, para su validación en la Universidad Nacional de Moquegua.

1.2. Definición del problema

¿Permitirá el diseño de un Plan de gestión de seguridad de la información alineado a la norma ISO/IEC 27001, fortalecer la seguridad de los sistemas informáticos de las instituciones públicas de la región Moquegua: caso UNAM?

1.2.1. Problemas específicos

- ¿Cómo aplicar la norma ISO/IEC 27001, en la elaboración de un plan de seguridad de la información de las instituciones públicas de la región Moquegua: caso UNAM?

- ¿Cómo validar la propuesta del plan de seguridad de la información para las instituciones públicas de la Región Moquegua: caso UNAM?

1.3. Objetivo de la Investigación

Diseñar un plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001, para fortalecer la seguridad de los sistemas informáticos de las instituciones públicas de la región Moquegua: caso UNAM, orientado a la protección de los activos informáticos.

1.3.1. Objetivos específicos

- Aplicar la norma ISO/IEC 27001, en la elaboración de un plan de seguridad de la información de las instituciones públicas de la región Moquegua: caso UNAM.

- Validar la propuesta del plan de seguridad de la información para las instituciones públicas de la Región Moquegua: caso UNAM.

1.4. Justificación

Se justifica al realizar una propuesta de implementación de un SGSI en la Universidad Nacional de Moquegua, por lo que, se conseguirá minimizar ostensiblemente el riesgo de su funcionamiento. También se justifica, desde la dimensión social, por salvaguardarse la información perteneciente a la región Moquegua, que puede ser utilizada, en proyectos de investigación; desde la dimensión económica, por representar un ahorro sustantivo, a diferencia de lo que pudiese significar, el hecho de destinar recursos en recuperar la información y desde la dimensión tecnológica, por lograr que la institución, se ponga al nivel de otras instituciones de prestigio, tendiente a obtener certificaciones internacionales de calidad y seguridad.

1.5. Limitaciones

Al momento de realizar la encuesta personal, que tenía por finalidad, conocer el contexto de la seguridad de la información de la Universidad Nacional de Moquegua, se pudo detectar que algunos de los encuestados no tenían voluntad de colaborar y que desconocían el tema sobre el cual, cursaba la investigación.

1.6. Variables

Tabla 1.

Variable independiente: Normas ISO/IEC 27001

Variable	Definición conceptual	Definición operativa
Normas ISO/IEC 27001	Es un patrón de referencia para preservar la información, y cuenta con validez internacional.	Es considerado un marco internacional que implica las buenas prácticas para un SGSI.

Fuente: Normas ISO/IEC 27001

Tabla 2.

Variable dependiente: Sistema de Gestión de Seguridad de la Información

Variable	Definición conceptual	Definición operativa	Indicador
Sistema de Gestión de Seguridad de la Información	Lineamientos de políticas referidas a la gestión de la data.	Procesos para administrar adecuadamente la información, asegurando la privacidad, entereza y disposición de la misma.	Políticas Codificación y revisión de activos informáticos Seguridad en la infraestructura Gestión de incidentes Validación del plan SGSI

Fuente: www.ISO27000.es

1.7. Hipótesis de la Investigación

El diseño de un plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001, es el más adecuado, para fortalecer la seguridad de los sistemas informáticos de las instituciones públicas de la región Moquegua: caso UNAM.

1.7.1. Hipótesis específicas

- La norma ISO/IEC 27001, es la más idónea, para la elaboración de un plan de seguridad de la información de las instituciones públicas de la región Moquegua: caso UNAM.

- La propuesta de un plan de seguridad de la información alineado a la norma ISO/IEC 27001 se logrará validar a través de juicio de expertos.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

Talavera, (2015), realizó la tesis: ***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***, en la Facultad de Ciencias e Ingeniería de la Pontificia Universidad Católica del Perú, habiendo llegado a las siguientes conclusiones:

- Se detecta una diferencia referida a la seguridad de la información en el organismo estatal donde se ejecutó el proyecto.
- Las falencias deberían ser resueltas, antes de comprometer a la dirección, en operaciones del plan a definir en la ejecución del SGSI.

Buenaño & Granda, (2009), desarrollaron la investigación: ***Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001-27002***, de la Carrera de Ingeniería de Sistemas de la Universidad Politécnica Salesiana – Sede Guayaquil, arribando a las siguientes conclusiones:

- El servicio de mensajería, que utilizan los trabajadores como los docentes, no dispone de una política que sistematice el uso de estos servicios, que lo convierte en una potencial debilidad.
- La implementación de una política sustentada en documentos, contribuirá en la auditoría a identificar los cambios y examinar las potenciales omisiones a la seguridad, a consecuencia del avance de la tecnología.

Barahona & Garzón, (2014), realizaron la tesis denominada: ***Auditoría de los riesgos informáticos en el Departamento de Tecnología de la empresa KUBIEC usando COBIT 4.1 y la norma ISO/IEC 27001 como marco de referencia***, de la Escuela de Ingeniería de Sistemas de la Escuela Politécnica Nacional de Quito, llegando a las conclusiones:

- RISK IT es un complemento de COBIT y proporcionó una perspectiva integral de los riesgos que pudieran provocar pérdidas económicas y oportunidades en la empresa.

- Es posible determinar los procesos críticos del Departamento de TIC´s, así también el nivel jerárquico no cuenta con capacidad para tomar decisiones que beneficien al Departamento de TIC´s.

Gonzáles & Tenemaza, (2012), realizaron la investigación: ***Análisis de riesgos y vulnerabilidades de la red de datos de la empresa Plywood Ecuatoriana S.A. utilizando el estándar ISO/IEC 27005:2008***, de la Escuela de Ingeniería de Sistemas de la Escuela Politécnica Nacional de Quito, obteniendo las siguientes conclusiones:

- Se identificó y valorizó la exposición de los riesgos de los activos tecnológicos, por establecer los controles adecuados con el fin de atenuar los riesgos identificados.
- Se realizó el respectivo examen de riesgos y debilidades de la seguridad, teniendo en consideración, la determinación de los peligros expuestos, así también, es imprescindible determinar la posibilidad de que pueda presentarse una amenaza y las consecuencias que puede acarrear.

Sandoval, (2014), realizó la tesis: ***Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa,*** de la Maestría en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil, arribando a las conclusiones:

- La implementación de un SGSI, garantizan el desarrollo de los procesos, encargados de gestionar el acceso de la información en la organización.
- En base a un cronograma, se debe cumplir con la revisión de los exámenes para reducir los peligros por pérdida de la data.

Aguirre & Aristizabal, (2013), realizaron la tesis: ***Diseño de un Sistema de Gestión de Seguridad de la Información para El Grupo Empresarial La Ofrenda,*** del Programa de Ingeniería de Sistemas y Computación de la Universidad Tecnológica de Pereira, llegando a las siguientes conclusiones:

- En la actualidad los datos son el principal activo en la mayoría de organizaciones, si llegará a perderse la información, lo más probable, es que no se pueda recuperarla, por no adoptar las medidas anticipadas, siendo muy probable, que se interrumpa sus operaciones.
- Es primordial contar con un sistema que proteja la información, de esta forma, se asegura los datos de la organización.

Villena, (2006), realizó la tesis: ***Sistema de Gestión de Seguridad de Información para una Institución Financiera***, de la Facultad de Ciencias e Ingeniería de la Pontifica Universidad Católica del Perú, logrando las siguientes conclusiones:

- Para la gestión de la seguridad de información se debe contar con el apoyo de todo el personal.
- La tecnología no certifica la seguridad de resguardar la data. Es necesario realizarla en concordancia con los fines de la empresa.
- Concluyendo en que las tecnologías de la información por si sola se garantizan, o el hecho de contar con los últimos adelantos, sino se cuenta con políticas claras de protección de la información.

Pallas, (2009), realizo la tesis: ***Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*****,** del Instituto de Computación – Facultad de Ingeniería de la Universidad de la República de Montevideo, llegando a las siguientes conclusiones:

- La investigación, contribuye una metodología con enfoque global, teniendo en consideración que la empresa, pertenece a un grupo empresarial.
- La flexibilidad y agilidad operativa son condiciones fundamentales para garantizar la seguridad para cada empresa, respetando los lineamientos corporativos de cada empresa.

2.2 Bases teóricas

2.2.1 El Sistema de Gestión de Seguridad de la Información

"Una serie de datos organizados que posee un ente que tienen un alto valor, que no tiene relación necesariamente con la forma de resguardo, su origen o fecha de producción" (ISO 2007.es, 2012).

Según el portal, Gesconsultor.com, (2012), señala que: *"la Información se constituye en un activo primordial para la operación, supervisión y administración de un esquema de negocio, en una organización cualquiera.*

Debe extenderse a en todos los niveles, por haberse convertido en una prioridad, por lo que las empresas destinan recursos para lograrlo; con la adopción de estas medidas por parte de la empresa, existe mayor probabilidad de que las operaciones no sean interrumpidas, o de ser el caso, solucionarlas rápidamente.

2.2.2 ¿Para qué sirve un SGSI?

Su principal utilidad es, definir una serie de políticas y procedimientos en relación a los fines de la empresa, para mantener un control sobre los peligros, que la empresa asuma. (ISO 2007.es, 2012).

Figura 1. Riesgos - SGSI

Fuente: www.ISO27000.es

2.2.3 ¿Qué incluye un SGSI?

En el Sistema de Seguridad:

El nivel 1, el manual de seguridad contiene la explicación del sistema.

El nivel 2, procedimientos, que asegura la planificación.

El nivel 3, instrucciones, checklists y formularios, que explican la realización de las tareas.

El nivel 4, se detallan los registros y documentos, que norman el cumplimiento del SGSI. ISO 27001.

Figura 2. Documentación del Sistema de Seguridad

Fuente: www.ISO27000.es

2.2.4 ¿Qué aspectos de seguridad cubre un SGSI?

Figura 3. Aspectos que cubre el SGSI

Fuente: www.ISO27000.es

Niveles de seguridad:

- **Lógica:** garantiza la privacidad, la entereza y la accesibilidad al software y los datos que conforman el sistema de seguridad.
- **Organizativa:** se enmarca en todo lo relacionado a prevenir, identificar y corregir los riesgos.
- **Física:** se encarga de asegurar los elementos físicos de las instalaciones (servidores, computadoras y otros).
- **Legal:** se enmarca en el cumplimiento de las licencias para operar el Sistema.

2.2.5 Revisión del SGSI

La Dirección de la empresa, se encarga de revisar el SGSI, por lo menos una vez durante el año, por lo que, debe recibir un flujo de informaciones, que permitan tomar decisiones afines a: auditorías y revisiones, observaciones de las áreas implicadas, procedimientos para mejorar el rendimiento y amenazas, y demás cambios que puedan afectar al SGSI.

2.2.6 Análisis y Evaluación del Riesgo

Se considera, a las fases metodológicas que debe desarrollar la organización, y comprende, desde la caracterización de los activos de información, hasta la determinación de la envergadura de las amenazas existentes, y el efecto en los activos informáticos.

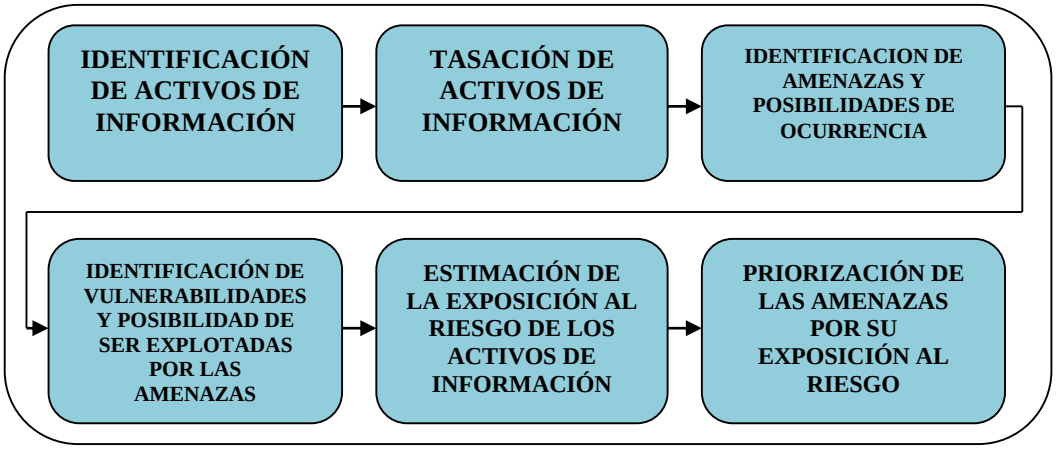


Figura 4. Pasos para la Metodología de Análisis de Riesgos

Fuente: www.centrum.pucp.edu.pe/excelencia

2.2.7 Tratamiento del Riesgo y la Toma de Decisiones Gerenciales

Concluida la evaluación del riesgo, y la empresa haya determinado los activos expuesto a riesgo, se tomará la decisión de elegir la estrategia adecuada.

La gerencia para tomar la decisión debe considerar dos factores: el impacto si el riesgo se materializa y la posibilidad de su ocurrencia.

Al margen del efecto financiero en la empresa, la firma debe contemplar un presupuesto, para actuar sobre alguna de las opciones para controlar el riesgo.

Opciones para el Tratamiento del Riesgo

Reducción del Riesgo

En el caso de los riesgos donde la alternativa de minimizarlos fue elegida, le corresponde implantar los controles para reducirlos a niveles aceptables.

Aceptación del Riesgo

Existen ocasiones en la compañía, que se le presentan circunstancias en las cuales no encuentra controles ni puede diseñarlos.

Transferencia del Riesgo

Es una alternativa válida para la organización, cuando no hay viabilidad técnica ni económica, por lo que se opta, por transferir el riesgo a una empresa aseguradora.

Evitar el Riesgo

Se refiere a cualquier acción para modificar las actividades del negocio, de esta forma evitar el riesgo.

Figura 5. Gestión de Riesgos

Fuente: www.ISO27001.es

2.2.8 Normas, Guías y Estándares

Oliván (2017) indica que existen diversas normas, guías o estándares recomendables para gestión de las TIC. Donde, algunas ponen su énfasis únicamente en la seguridad de la información, y otras realizan algunas referencias a la misma, no obstante, su vital interés forme parte de la estrategia de negocio para la gestión de las TIC. Existiendo, en

alguna de ellas, la posibilidad de obtener una certificación en caso de cumplir con los requisitos exigidos o simplemente se pueden obtener certificados a nivel personal (no a la organización).

2.2.9 La Norma ISO 27001:2013

Oliván (2017) refiere que la familia ISO/IEC 27000 fue desarrollada por la ISO (International Standards Organization) y la IEC (International Electrotechnical Comisión). Este conjunto de guías y estándares están conexos con las TIC en el ámbito de la seguridad.

Es un patrón internacional y se enfoca en administrar de forma integral la seguridad de la información de una organización de cualquier rubro. La finalidad de ISO 27001, es salvaguardar la privacidad, entereza y sobre todo la disposición de la información en una organización, salvaguardando la seguridad de su principal activo: la información.

Las normas están relacionadas de la siguiente forma:

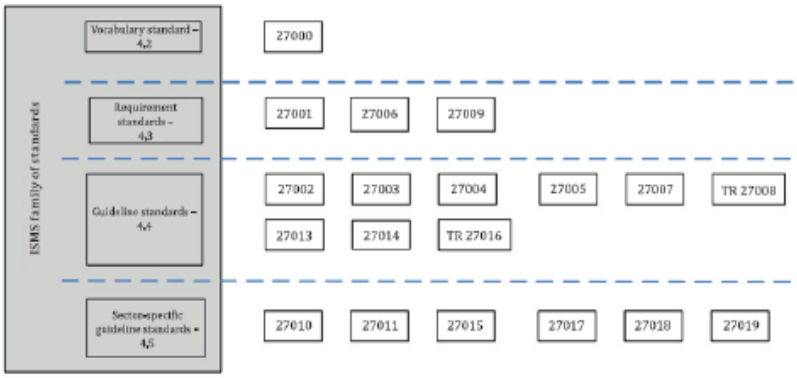


Figura 6. Familia de normas ISO/IEC 27000

Fuente: Oliván (2017)

Los dos estándares más importantes que contienen la lista de controles son:

- ISO/IEC 27001.- Define como establecer un SGSI que servirá para administrar los controles y riesgos de la seguridad de la información dentro de una organización.

  Especifica los requerimientos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI teniendo conocimiento de los riesgos de negocio de la organización. Los objetivos de control y la lista de controles derivan y están alineados con los que están en la lista de la ISO/IEC 27002.
- ISO/IEC 27002.- Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables y comúnmente aceptados en la seguridad de la información y son los que utiliza la norma ISO/IEC 27001.

La norma ISO/IEC 27001:2013 se divide en:

Sección 0, Introducción: explica la finalidad de la norma y la afinidad con otras reglas relacionadas.

Sección 1, Alcance: explica el ámbito de aplicación.

Sección 2, Referencias normativas: se sustenta en una norma, definiendo los requisitos y conceptos.

Sección 3, Términos y conceptos: de nuevo, menciona a la norma.

Sección 4, Contexto de la organización: comprende la fase de Planificación (PDCA) y precisa requerimientos para entender los aspectos externos e internos.

Sección 5, Liderazgo: se precisa las obligaciones, la fijación de funciones y compromisos de la dirección.

Sección 6, Planificación: se precisa los requisitos para el control, el procedimiento de aplicabilidad, la ruta de tratamiento y la fijación de los objetivos, para minimizar riesgos.

Sección 7, Apoyo: se precisa las exigencias sobre la disponibilidad de los recursos, los ámbitos de competencia, la concienciación, la comunicación y la verificación de las documentaciones y archivos.

Sección 8, Funcionamiento: consiste en la ejecución de la valoración y la gestión de riesgos, de la misma forma, los controles y otros procesos básicos.

Sección 9, Evaluación del desempeño: precisa las directrices para efectuar el monitoreo de la auditoría interna y examinación por parte de la gerencia de la empresa.

Sección 10, Mejora: precisa los requisitos para realizar los ajustes, las correcciones y perfeccionamiento del sistema.

Anexo A: esta sección suministra un catálogo de 114 controles organizados en 14 secciones (A.5 a A.18).

Oliván (2017) indica que existen muchas ventajas en caso de implantar un SGSI:

- Minimiza el riesgo de pérdida de información
- Monitorear continuamente los riesgos de forma periódica
- Empleo de técnicas para la gestión de seguridad informática
- Se establece medidas de seguridad para el acceso a la información.
- Complementación con otros sistemas de gestión ya normalizados
- Cumplimiento con la ley vigente
- Brindar confianza interna a la organización
- Minimizar las evaluaciones sobre los productos o servicios de la entidad
- Elemento que diferencia frente a la competencia
- Minimización de auditorías de segundas partes
- Cumplimiento de requisitos del mercado
- Menos costo de las primas de riesgo de seguros
- Dar a conocer medidas de seguridad.

La ISO/IEC 27001 permite el reconocimiento y aceptación a nivel mundial y por lo tanto puede ser utilizada sin límites internacionales.

2.2.10 COBIT

White (2017) refiere que fue lanzado por primera vez en 1996, COBIT (Objetivos de control para la información y tecnologías relacionadas) se diseñó inicialmente como un conjunto de objetivos de control de Tecnologías de la información para ayudar a la comunidad de auditoría financiera a navegar mejor en el crecimiento de los entornos de Tecnologías de la información, en el 2012, se lanzó COBIT 5 y en 2013, ISACA (Information Systems Audit and Control Association) lanzó un 'add-on' para COBIT 5, que incluía más información para las empresas en relación con la gestión de riesgos y la gobernanza de la información.

Oliván (2017) sostiene que el COBIT, es un marco de trabajo de buenas prácticas creado por la Asociación Profesional internacional ISACA para la gestión TIC y la gobernanza TIC. Proporciona una lista de controles sobre las TIC y las ordena en un patrón o marco de trabajo lógico de procesos IT relacionados. Este catálogo no es auditable por sí mismo.

Al igual que la ISO/IEC 27002, COBIT proporciona información sobre lo que se está gestionando. No obstante, mientras la ISO/IEC 27002 se

centra solo en la Seguridad de la Información, COBIT tiene un alcance mucho mayor puesto que engloba todos los procesos de la gestión TIC. Se suele utilizar para la ejecución de políticas y procedimientos clave de la organización, así como para mapear controles, problemas técnicos y riesgos.

Es un estándar aceptado a nivel global que permite implementarse en empresas de todo tipo de tamaño de forma parcial como la ISO/IEC 27002 sin necesitar un análisis completo y compromiso por parte de la administración.

Según el ISACA, COBIT 5 se actualizó para:

- Agilizar el intercambio de información a través de una organización.
- Alcanzar objetivos corporativos incorporando TI en la estrategia.
- Minimizar y controlar la seguridad de la información y la gestión de riesgos.
- Optimizar el coste que rodea TI y tecnología.
- Mejor integración de la investigación de ISACA y el marco COBIT.

Los cinco componentes principales de COBIT 5 incluyen:

Marco: el marco principal de COBIT guía a las organizaciones a través de las mejores prácticas y la estandarización de los procesos de TI y la infraestructura.

Descripciones de los procesos: COBIT incluye un lenguaje que cualquier persona en la organización entenderá, de modo que los gerentes y otros actores clave comprendan fácilmente la terminología, los procesos y las descripciones.

Objetivos de control: esta sección ofrece una descripción general de los requisitos de alto nivel que pueden ayudar a desarrollar y mejorar todos los procesos de TI.

Directrices de gestión: la guía COBIT ofrece mejores prácticas para establecer objetivos, procesar y asignar elementos de tareas o responsabilidades en toda la organización.

Modelos de madurez: los modelos de madurez COBIT ayudan a las empresas a evaluar la madurez de su organización, comprender cómo crecerá el proceso con la organización e identificar cualquier problema potencial que pueda surgir en el futuro.

Principios y beneficios de COBIT

Los 5 principios clave de COBIT 5, según el ISACA:

- Cumplir con las necesidades clave de los interesados.
- Cubrir la empresa de extremo a extremo.
- Integrar múltiples marcos bajo un paraguas.
- Fomentar un enfoque holístico para los negocios.
- Alejar el gobierno de la administración.

2.2.11 Los activos informáticos

Su administración es uno de los puntos primordiales en una empresa o institución, esencialmente si se quiere establecer un sistema enfocado en la seguridad.

Sistemas de información

- Enterprise Resource Planning.
- Customer Relationship Management.
- Inteligencia de Negocios.
- Mail Transfer Agent.

Software

- Sistemas operativos
- Servidor de aplicaciones.

- Aplicaciones cliente
- Software de seguridad
- Aplicaciones de usuario

Hardware

- Computadora Personal.
- Servidores.
- Teléfonos móviles, tablets.

Soportes

- Universal Serial Bus (USB).
- External Hard Drive

Personal

- De planta y por funciones específicas

Redes

- Local Area Network
- Demilitarized Zone.
- Virtual Local Area Network
- Virtual Private Network.

Información

- Documentos de gestión estratégica y Actas.

2.3 Marco conceptual

a) **Análisis,** consiste en identificar, modelar y describir las operaciones de un sistema y su forma de trabajo (McGraw Hill, 2012).

b) **Antispam**, es un instrumento que reconoce y desecha el correo no deseado, con la finalidad de impedir que llegue al destinatario (Welivesecurity.com, 2012).

c) **Captcha**, es una prueba, en la cual se debe responder a una determinada pregunta o también ejecutar una acción y así precisar si el usuario es el correcto (Welivesecurity.com, 2012).

d) **Código malicioso**, más conocido como *malware*, es un programa creado con el fin de causar daño en los sistemas de informáticos (Welivesecurity.com, 2012).

e) **Delito informático**, es una infracción que a través de los mecanismos electrónicos basados en el Internet u otras opciones para llevarlo a cabo (Welivesecurity.com, 2012).

f) **Fingerprinting**, consiste en acumular datos sobre las particularidades del hardware utilizado en la red (Welivesecurity.com, 2012).

g) **Interfaz,** se agrupa en un archivo independiente de bytecode, tal como una clase ordinaria (McGraw Hill, 2012).

h) **Lenguaje de programación,** códigos utilizados por los programadores para elaborar los programas (McGraw Hill, 2012).

CAPÍTULO III: MÉTODO

3.1 Tipo de Investigación

Aplicada, en razón que se orienta a buscar la aplicación o utilización de los conocimientos adquiridos. Está diseñada y orientada para ofrecer soluciones a un problema específico referido. Al respecto, Zorrilla (1993, pág. 43), señala que la investigación aplicada, tiene por finalidad el conocer para hacer, para desenvolverse, para edificar, para transformar.

3.2 Diseño de investigación

Se utilizó el diseño no experimental, según, Hernández, Fernández y Baptista (1991, pág. 245) se refiere a que la información obtenida para cada variable, no se altera o modifica por parte de investigador. Este diseño consiste en observar el fenómeno en estudio y mostrar los resultados tal como fueron obtenidos en el trabajo de campo.

Así también, se aplicó un diseño transversal, al respecto, Hernández, Fernández y Baptista (1991, pág. 247), es decir se obtuvieron los datos en un instante determinado.

3.3 Población y muestra

Son los elementos considerados bajo ciertos criterios de inclusión, al respecto, Valderrama (2016, pág. 183), refiere que, en este caso, lo conforman: la Universidad Nacional de Moquegua, el Gobierno Regional y los 20 Gobiernos Locales de la región Moquegua. Para esta investigación, sólo se eligió a la UNAM, cuya población en estudio, está conformada por: 122 docentes, 1305 estudiantes, 6 directores de Escuela y el jefe de DASA.

Datos:

N = 1427

p = 0,9

q = 0,1

E = 6%

$$n = \frac{z^2 . p . q . N}{E^2 (N - 1) + z^2 . p . q} = \frac{(1.96)^2 \times 0.9 \times 0.1 \times 1427}{(0.06)^2 (1427 - 1) + (1.96)^2 \times 0.9 \times 0.1}$$

n = 89

Tabla 3.

Distribución de la muestra

Categorías	*Total*
Docentes	8
Alumnos	81
Directores de Escuela y jefe de DASA	7
Total	**96**

Fuente: Universidad Nacional de Moquegua.
Elaboración propia.

Valderrama (2016, pág. 184) sostiene que la muestra, es un subconjunto específico de un universo; la muestra inicial, es de 89; sin embargo, se agrega 7 elementos muestrales, que corresponden a los Directores de Escuela y jefe de DASA; resultando el tamaño final de la muestra en 96.

3.4 Técnicas e instrumentos de recolección de datos

Es una fase que consistió en ejecutar el plan de agenciarse la información que responde a la planificación del estudio, así lo sostiene Pino (2016), en este caso, se optó por la técnica de la encuesta para efectuar el análisis del contexto de la seguridad de la información de la Universidad Nacional de Moquegua, para esto se utilizó el cuestionario adecuado a la norma ISO-IEC 27001:2013, utilizado por la Alcaldía Mayor de Bogotá.

3.5 Técnicas de procesamiento y análisis de datos

Consistió en procesar los datos obtenidos de la población objeto de estudio durante el trabajo de campo, y tiene como finalidad generar resultados, como lo refiere Bernal (2010, pág. 198) , en este caso, se contó con el soporte del software SPSS V.23, para agrupar la información obtenida, cuyos resultados se presentan en tablas (Anexo 5). La comprobación de la hipótesis general se realizó a través del método de los expertos.

CAPITULO IV: RESULTADOS DE LA INVESTIGACIÓN

4.1 Descripción de la encuesta a expertos del nivel de validez de la propuesta

Para validar la propuesta del Plan de Seguridad de Información alineado a la Norma ISO/IEC 27001 para la Universidad Nacional de Moquegua, esta se realizó mediante una Encuesta a expertos, conformada por dos bloques de preguntas: datos generales y el nivel de validez de la propuesta, como se detalla a continuación:

- Datos generales: conformado por 2 preguntas
- Nivel de validez de la propuesta: conformado por 7 preguntas

Matriz del instrumento de validación de la propuesta (se encuentra en el Anexo 1)

La encuesta a expertos se ejecutó llevando a cabo las siguientes acciones:

- El primer bloque de preguntas se dirigió a conocer los datos personales de los expertos, específicamente: sus estudios de especialización y los años de experiencia en el tema de investigación; para la formulación de las preguntas del nivel de validez de la propuesta se tomó como tema principal el Plan de Seguridad de Información, con la finalidad de conocer si la propuesta tiene un alto, medio o bajo nivel de validez con puntajes de tres, dos, uno; la cual fue calificada de manera cualitativa por los expertos encuestados y de manera cuantitativa por el investigador.
- Luego se encuestó a 3 profesionales que cumplen con el perfil de expertos, es decir, ingenieros de sistemas, con estudios de especialización en seguridad de la información y como 5 años de experiencia en el área de la investigación.

Expertos

Antonio Arroyo Paz

Ingeniero de Sistemas

CIP 65568

Magister en Ingeniería de Sistemas con mención en Ingeniería del Software

Irenio Chagua Aduviri

Ingeniero de Sistemas

CIP 83044

Maestro en Ciencias: Ingeniería de Sistemas, especialidad: mención en Gerencia en Tecnologías de la Información

Ruso Morales Gonzales

Ingeniero de Sistemas e Informática

CIP 140394

Maestro en Ingeniería de Sistemas e Informática con Mención en Seguridad y Auditoría Informática

4.2 Descripción de los resultados previsibles de la propuesta

Consiste en un Plan de Gestión de Seguridad de Información alineado a la Norma ISO/IEC 27001, como una alternativa para garantizar la seguridad de los sistemas informáticos de las instituciones públicas de la región Moquegua, específicamente para la Universidad Nacional de Moquegua.

a) Reconocimiento de la organización

Es el punto de partida en el plan, en este acápite se realiza la representación de la institución, precisando las actividades, estructura organizacional, asimismo, se especifica la infraestructura existente de la organización. Este proceso es validado por expertos que consideran la profundidad del detalle de la descripción de la organización.

b) Estado actual con respecto a la ISO/IEC 27001

Este acápite permite conocer el análisis realizado en el contexto de la institución, en aspectos relacionados al desempeño, liderazgo, entre otros. Para los expertos este componente tiene un alto nivel de validez, porque permite conocer el estado actual de la norma.

c) Análisis de riesgos

Este acápite, es el primer proceso de la gestión de riesgos, en el cual se determina la ramificación de amenazas y riesgos coligados con los sistemas de Tecnología de la Información, así también, contribuye a precisar controles para minimizar riesgos. El nivel de validación de los expertos es alto porque se caracteriza los riesgos.

d) Gestión de riesgos

Este acápite, permite conocer la priorización, valoración y ejecución de controles que reducen los riesgos en base a las recomendaciones provenientes del análisis de riesgos. El nivel de validación de los expertos es alto, por tratarse de una actividad fundamental y crítica del plan de seguridad.

e) Estrategias para el tratamiento del riesgo

En este acápite, se evalúa el contexto y se fija los casos en los que se sitúa el riesgo. La validación de los expertos es fundamental, por la ubicación del riesgo en la institución y su consideración en el plan de seguridad.

f) Técnicas para el tratamiento del riesgo

En este acápite, se definen las técnicas para el tratamiento del riesgo, en base a las necesidades de la institución y el nivel de inseguridad descubierto. Para los expertos tiene un alto nivel de validez por la información que se brinda en el documento.

g) Plan de tratamiento del riesgo

En este acápite, se establece el plan de tratamiento del riesgo, en el cual se incluyen políticas, controles, monitoreo y asignación de responsabilidades. Para los expertos tiene un alto nivel de validez, por tratarse de un aspecto muy importante que tiene que ver directamente con la seguridad de la información.

4.3 Validación de la propuesta de Plan de Seguridad

La propuesta fue evaluada, en base al nivel de validez, que estimó por conveniente cada experto, colocando el valor 3 si es Alta, el valor 2 si es Media y el valor 1 si es Baja; considerando la evaluación en conjunto de los 3 expertos por dimensión; el valor 3 representa un nivel de validez bajo y el valor 9 representa un nivel de validez alto. A continuación, se detallan los resultados:

Tabla 4.

Ficha de validación de la propuesta de seguridad

Acápite	Experto 1	Experto 2	Experto 3	Total
RECONOCIMIENTO DE LA ORGANIZACIÓN	3	2	3	8
ESTADO ACTUAL CON RESPECTO A LA ISO/IEC 27001	3	3	3	9
ANÁLISIS DE RIESGOS	3	3	3	9
GESTIÓN DE RIESGOS	3	3	3	9
ESTRATEGIAS PARA EL TRATAMIENTO DEL RIESGO	3	3	3	9
TÉCNICAS PARA EL TRATAMIENTO DEL RIESGO	3	3	3	9
PLAN DE TRATAMIENTO DEL RIESGO	3	3	3	9

Fuente: Elaboración propia

Conclusión:

De acuerdo a los resultados por acápites de cada por experto, en su mayoría le otorgan el puntaje de 9; se concluye que el nivel de validez del plan de seguridad de información, es alto, por lo tanto, la propuesta, constituye una alternativa viable en la solución del problema de investigación.

4.4 Verificación de la hipótesis general

La hipótesis general es:

Un plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001, es el más adecuado, para fortalecer la seguridad de los sistemas informáticos de las instituciones públicas de la región Moquegua: Caso UNAM.

En efecto por el alto nivel de validez de los expertos en referencia al Plan de Gestión de Seguridad de Información alineado a la norma ISO/IEC 27001, propuesto para fortalecer los sistemas informáticos de la Universidad Nacional de Moquegua, queda verificada la hipótesis general.

4.5 Plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001: Caso Universidad Nacional de Moquegua

CAPÍTULO I. CONTEXTO ORGANIZACIONAL

En este capítulo se presenta el contexto organizacional, se realiza el reconocimiento de ésta, así mismo se presenta el análisis para describir el estado actual de la seguridad de la información con respecto a la norma ISO/IEC 27001:2013 en la Universidad Nacional de Moquegua, evaluándose el nivel cumplimiento de los dominios descritos en dicha norma.

1.1 RECONOCIMIENTO DE LA ORGANIZACIÓN

En este apartado se realiza la descripción de la organización, describiendo las actividades de la Universidad, así como el organigrama, también se describe la infraestructura actual de la Universidad, teniendo en cuenta la red de comunicaciones, equipos informáticos, diversas aplicaciones y servicios Cloud con los que la Universidad cuenta en la actualidad.

1.1.1 Descripción

La Universidad Nacional de Moquegua es una universidad que se dedica a la formación de profesionales, con aproximadamente 209 empleados, distribuidos en una casa central y tres delegaciones.

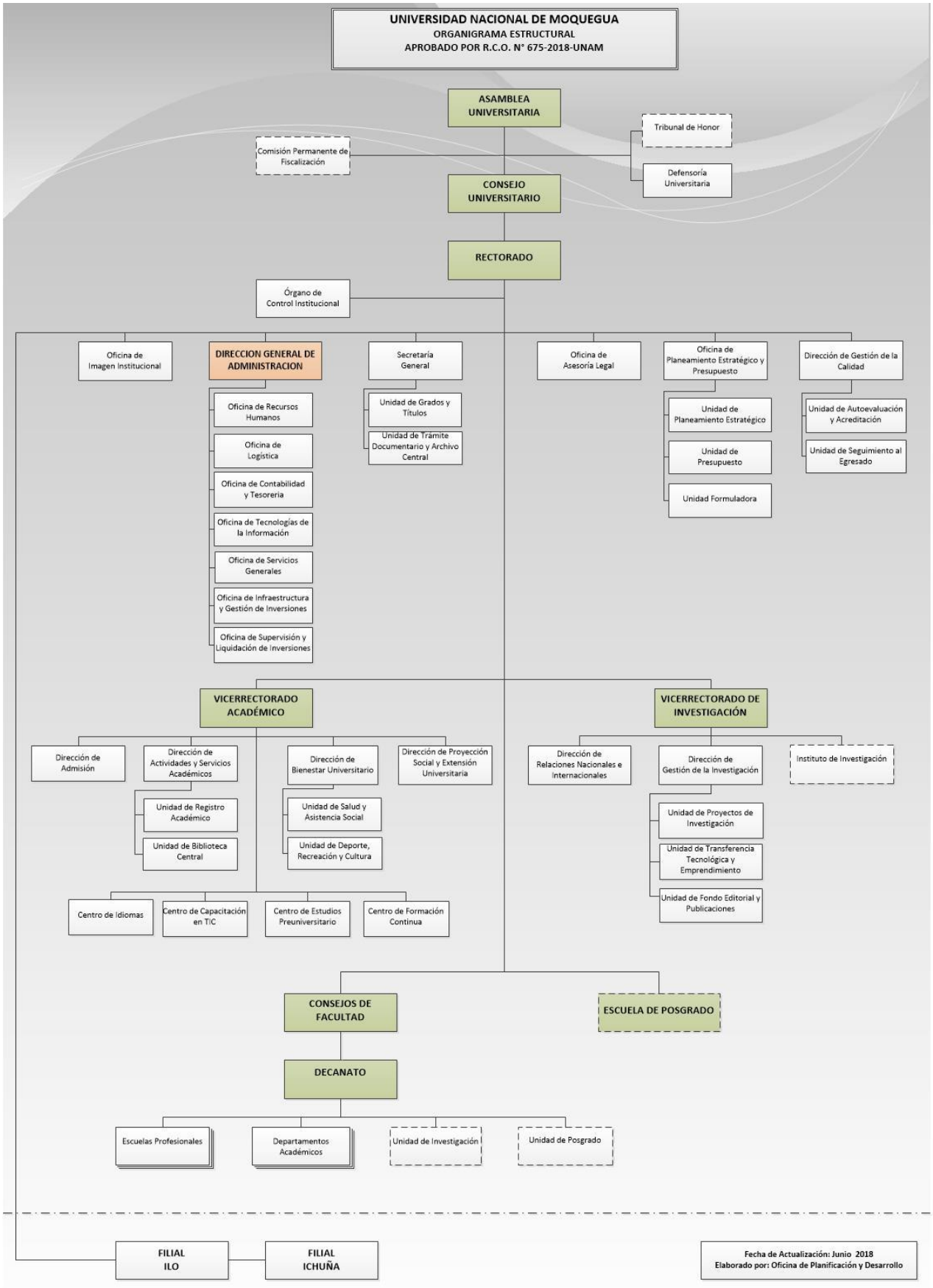
Cuenta con dos filiales una en la ciudad de ILO e Ichuña, además de la sede principal en la ciudad de Moquegua.

La Universidad Nacional de Moquegua tiene como Objetivos Estratégicos:

- Mejorar la formación profesional, con valores humanísticos científicos y tecnológicos al servicio de la región y del país.
- Incentivar una cultura de investigación e innovación en la comunidad universitaria.
- Promover actividades de proyección y extensión con responsabilidad social que aporten al desarrollo social y cultural de la población.

1.1.2 Estructura Organizacional

La estructura organizacional de La Universidad Nacional de Moquegua está dada de forma jerárquica, tal como se muestra a continuación:


UNIVERSIDAD NACIONAL DE MOQUEGUA
ORGANIGRAMA ESTRUCTURAL
APROBADO POR R.C.O. N° 675-2018-UNAM
ASAMBLEA UNIVERSITARIA
Tribunal de Honor
Comisión Permanente de Fiscalización
Defensoría Universitaria
CONSEJO UNIVERSITARIO
RECTORADO
Órgano de Control Institucional
Oficina de Imagen Institucional
DIRECCION GENERAL DE ADMINISTRACION
Secretaría General
Oficina de Asesoría Legal
Oficina de Planeamiento Estratégico y Presupuesto
Dirección de Gestión de la Calidad
Oficina de Recursos Humanos
Oficina de Logística
Oficina de Contabilidad y Tesorería
Oficina de Tecnologías de la Información
Oficina de Servicios Generales
Oficina de Infraestructura y Gestión de Inversiones
Oficina de Supervisión y Liquidación de Inversiones
Unidad de Grados y Títulos
Unidad de Trámite Documentario y Archivo Central
Unidad de Planeamiento Estratégico
Unidad de Presupuesto
Unidad Formuladora
Unidad de Autoevaluación y Acreditación
Unidad de Seguimiento al Egresado
VICERRECTORADO ACADÉMICO
VICERRECTORADO DE INVESTIGACIÓN
Dirección de Admisión
Dirección de Actividades y Servicios Académicos
Dirección de Bienestar Universitario
Dirección de Proyección Social y Extensión Universitaria
Dirección de Relaciones Nacionales e Internacionales
Dirección de Gestión de la Investigación
Instituto de Investigación
Unidad de Registro Académico
Unidad de Biblioteca Central
Unidad de Salud y Asistencia Social
Unidad de Deporte, Recreación y Cultura
Unidad de Proyectos de Investigación
Unidad de Transferencia Tecnológica y Emprendimiento
Unidad de Fondo Editorial y Publicaciones
Centro de Idiomas
Centro de Capacitación en TIC
Centro de Estudios Preuniversitario
Centro de Formación Continua
CONSEJOS DE FACULTAD
ESCUELA DE POSGRADO
DECANATO
Escuelas Profesionales
Departamentos Académicos
Unidad de Investigación
Unidad de Posgrado
FILIAL ILO
FILIAL ICHUÑA
Fecha de Actualización: Junio 2018
Elaborado por: Oficina de Planificación y Desarrollo

1.1.3 Infraestructura

Sistema de Información

- Sistema de Información SIAF
- Sistema de Información SIGA
- Sistema Académico

Servidores

- Servidor SIAF
- Servidor. ACTIVE DIRECTORY
- Servidor. SIGA
- Servidor Repositorio 1
- Servidor Repositorio 2
- Servidor Repositorio 3

Dispositivos de red

- FIREWALL Fortigate 200 D
- SWITCH de distribución externa 1
- SWITCH de distribución interna 1

Equipos terminales

- Impresora Multifuncional Kyocera Eco545 h4132 IDN
- Servicio de Hosting Web
- Pc Portatil DELL
- Pc Portatil HP
- Equipo de escritorio HP Eilito Desk 800-51-SSF
- Tablet Samsung SM-T820
- Equipo Lenovo Think Pad T4705

- Celular LG
- Etiquetadora
- Equipo de escritorio HP Eilito Desk 800-51-SSF
- Equipo de escritorio HP Eilito Desk 800-51-SSF
- Equipo de escritorio HP Eilito Desk 800-51-SSF

Hojas de Coordinación

1.2 ESTADO ACTUAL CON RESPECTO ISO/IEC 27001

El plan de implementación del SGSI basado en ISO/IEC 27001:2013 es el paso inicial que permite evaluar:

- El contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación de desempeño y mejoras

los cuales se convierten en elementos esenciales para actuar según la norma.

Tabla 5.

Cláusulas 4 a 10 de la ISO/IEC 27001:2013

REQUISITOS DE LA NORMA	DETALLE DE COMENTARIOS (Que se tiene y que acciones requiere para cumplir el requisito)
4. CONTEXTO DE LA ORGANIZACIÓN	
4.1. Comprensión de la organización y de su contexto	**Evidencia:** No se ha realizado **Acciones a tomar:** Enunciar las actividades, funciones, servicios y productos. Identificar los problemas internos y externos
4.2. Comprensión de las necesidades y expectativas de las partes interesadas	**Evidencia:** No se ha realizado **Acciones a tomar:** Realizar una identificación de las partes interesadas para determinar sus necesidades y expectativas con la gestión de seguridad de la información
4.3. Determinación del alcance del sistema de gestión de seguridad de la información	**Evidencia:** No se ha realizado **Acciones a tomar:** Revisar y definir el alcance que este se encuentre declarado bajo la norma ISO 27001.
4.4. Sistema de gestión de seguridad de la información	**Evidencia:** No se ha realizado **Acciones a tomar:** Establecer e implementar un sistema de gestión de seguridad de la información, en conformidad con los requisitos de la ISO 27001:2013
5. LIDERAZGO	
5.1. Liderazgo y compromiso	**Evidencia:** No se ha considerado en relación a la Gestión de la Seguridad de la Información **Acciones a tomar:** Generar la política de seguridad de la información y asegurar que los objetivos de seguridad de la información sean establecidos y compatibles con lo establecido por la dirección estratégica de la Universidad y ésta sea patrocinada por las Altas Autoridades
5.2. Política	**Evidencia:** No existe con una Política de seguridad de la información

	Acciones a tomar: Generar una Política de seguridad de la información considerando los elementos requeridos por la norma.
5.3. Roles organizacionales, responsabilidades y autoridades	**Evidencia:** No se cuenta con un organigrama donde se identifique los roles y responsabilidades de las autoridades **Acciones a tomar:** Asignar responsabilidades para documentar la efectividad del sistema de gestión de seguridad de la información dentro de la Universidad con el visto bueno de las altas autoridades
6. PLANIFICACIÓN	
6.1. Acciones para abordar los riesgos y las oportunidades	**Evidencia:** No se ha realizado **Acciones a tomar:** Generar una metodología de evaluación y tratamiento de riesgos donde se identifiquen los activos críticos de información, las amenazas, vulnerabilidades y el impacto. Enunciar una declaración de la aplicabilidad donde se consideren los controles a ser implementados del Anexo A de la norma
6.2. Objetivos de seguridad de la información y planificación para alcanzarlos	**Evidencia:** No se ha realizado **Acciones a tomar:** Implantar los objetivos de SGSI a diferentes niveles y funciones relevantes para la Universidad. Generar un programa de actividades para cumplir los objetivos de Seguridad de la Información
7. SOPORTE	
7.1. Recursos	**Evidencia:** No se ha asignado recursos para la implementación del SGSI **Acciones a tomar:** Para el adecuado funcionamiento del SGSI se requiere asignar puestos de trabajo relacionados en función de las necesidades del sistema.
7.2. Competencia	**Evidencia:** Se cuenta con un MOF que cuenta con el perfil de puesto de trabajo. En todos los puestos se consideran las competencias cardinales. **Acciones a tomar:** Actualizar el MOF considerando al Responsable de cumplimiento y otras cuestiones del proceso de gestión de Seguridad de la Información
7.3. Concienciación	**Evidencia:** En el manual de inducción se cuenta con lineamientos relacionados con la cultura de la organización.

	Acciones a tomar: Considerar en el proceso de inducción: la política de seguridad de información y la cultura organizacional
7.4. Comunicación	**Evidencia:** No se ha realizado
	Acciones a tomar: Determinar comunicaciones internas y externas pertinentes al SGSI considerando, qué, cuándo, a quién, quién y cómo debe ser efectuada el proceso de comunicación.
7.5. Información documentada	**Evidencia:** No se ha realizado
	Acciones a tomar: Actualizar el mecanismo de control de documentos alineándolo a los criterios de las normas en las nuevas de versiones, para hacerlo compatible con la norma ISO 27001.
8. OPERACIÓN	
8.1. Planificación y control operacional	**Evidencia:** No se ha realizado
	Acciones a tomar: Planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1.
8.2. Evaluación de riesgos de seguridad de la información	**Evidencia:** No se ha realizado
	Acciones a tomar: Evaluar los riesgos de seguridad de la información tomando en cuenta los criterios establecidos en 6.1.2
8.3. Tratamiento de riesgos de seguridad de la información	**Evidencia:** No se ha realizado
	Acciones a tomar: Implementar el plan de tratamiento de riesgos de seguridad de la información.
9. EVALUACIÓN DE DESEMPEÑO	
9.1.Monitorización,medición, análisis y evaluación	**Evidencia:** No se ha realizado.
	Acciones a tomar: La organización debe establecer los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar que los resultados sean válidos del sistema de gestión de seguridad de la información
9.2. Auditoría interna	**Evidencia:** No se ha realizado.

	Acciones a tomar: La Universidad debe llevar a cabo auditorías internas periódicamente a fin de proporcionar información acerca del desempeño del sistema de gestión de seguridad de la información
9.3. Revisión de la gerencia	**Evidencia:** No se ha realizado.
	Acciones a tomar: El comité de gestión de seguridad de la información debe revisar el sistema de gestión de seguridad de la información de la organización periódicamente para asegurar su desempeño y efectividad continua.
10. MEJORA	
10.1. No conformidad y acción correctiva	**Evidencia:** No se cuenta con evidencia
	Acciones a tomar: Evidenciar la naturaleza de las no conformidades y cualquier acción subsiguiente tomada; y los resultados de cualquier acción correctiva.
10.2. Mejora continua	**Evidencia:** No se cuenta con evidencia
	Acciones a tomar: La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.

Fuente: https://www.iso.org/home.html

NIVEL DE MADUREZ DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para el cálculo del nivel de madurez del SGSI enunciado en el Sistema de Gestión de Seguridad de la Información se considera el modelo de capacidad de COBIT 5.0 cuyo enunciado se muestra en la Tabla n° 6.

Tabla 6.

Modelo de madurez y capacidad según la norma ISO / IEC 15504-2:2003.

Nivel de Madurez	Descripción
Nivel 0: Proceso incompleto	El proceso no se ejecuta o no logra su propósito. En este nivel, hay poca o ninguna evidencia de algún logro sistemático del propósito del proceso.
Nivel 1: Proceso Ejecutado (un atributo)	El proceso implementado logra su propósito.
Nivel 2: Proceso gestionado (dos atributos)	El proceso realizado descrito previamente está implementado ahora de una manera administrada (planeada, supervisada y ajustada) y sus productos de trabajo están establecidos, controlados y mantenidos adecuadamente.
Nivel 3: Proceso consolidado (dos atributos)	El proceso gestionado descrito anteriormente está implementado ahora utilizando un proceso definido que es capaz de lograr sus resultados.
Nivel 4: Proceso predecible (dos atributos)	El proceso consolidado previamente descrito opera ahora dentro de los límites definidos para lograr sus resultados.
Nivel 5: Proceso optimizado (dos atributos)	Proceso predecible descrito anteriormente se mejora continuamente para satisfacer los pertinentes objetivos de negocios actuales y proyectados.

Fuente: https://www.iso.org/standard/37458.html

En la Tabla n° 7 presenta el resultado del nivel de madurez del SGSI

Tabla 7.

Nivel de madurez y capacidad del SGSI

CRITERIO	Nivel 0 Incompleto	Nivel 1 Ejecutado	Nivel 2 Gestionado	Nivel 3 Establecido	Nivel 4 Predecible	Nivel 5 Optimizado
4. CONTEXTO DE LA ORGANIZACIÓN						
4.1. Comprensión de la organización y de su contexto	**X**					
4.2. Comprensión de las necesidades y expectativas de las partes interesadas	**X**					
4.3. Determinación del alcance del sistema de gestión de seguridad de la información	**X**					
4.4. Sistema de gestión de seguridad de la información	**X**					
5. LIDERAZGO						
5.1. Liderazgo y compromiso	**X**					
5.2. Política	**X**					

5.3. Roles organizacionales, responsabilidades y autoridades	**X**
6. PLANIFICACIÓN	
6.1. Acciones para abordar los riesgos y las oportunidades	**X**
6.2. Objetivos de seguridad de la información y planificación para alcanzarlos	**X**
7. SOPORTE	
7.1. Recursos	**X**
7.2. Competencia	**X**
7.3. Concienciación	**X**
7.4. Comunicación	**X**
7.5. Información documentada	**X**
8. OPERACIÓN	
8.1. Planificación y control operacional	**X**
8.2. Evaluación de riesgos de seguridad de la información	**X**
8.3. Tratamiento de riesgos de seguridad de la información	**X**
9. EVALUACIÓN DE DESEMPEÑO	
9.1. Monitorización, medición, análisis y evaluación	**X**
9.2. Auditoría interna	**X**
9.3. Revisión de la gerencia	**X**
10. MEJORA	
10.1. No conformidad y acción correctiva	**X**
10.2. Mejora continua	**X**

Fuente: Elaboración propia

ANÁLISIS DE MADUREZ DE LOS REQUISITOS ISO 27001:2013

Para la evaluación de los REQUISITOS de la norma (documentos y registros), se realizaron entrevistas con los principales interlocutores y, en la medida de lo posible, se revisó la documentación existente.

Tabla 8.

Nivel de madurez de los documentos obligatorios

DOCUMENTOS OBLIGATORIOS	Cláusulas ISO 27001:2013	Nivel 0 Incompleto	Nivel 1 Ejecutado	Nivel 2 Gestionado	Nivel 3 Establecido	Nivel 4 Predecible	Nivel 5 Optimizado
Alcance del SGSI	4.3	**X**					
Políticas y objetivos de seguridad de la información	5.2 - 6.2	**X**					
Metodología de evaluación y tratamiento de riesgos	6.1.2	**X**					
Declaración de aplicabilidad	6.1.3.d	**X**					
Plan de tratamiento del riesgo	6.1.3.e - 6.2	**X**					
Informe sobre evaluación y tratamiento de riesgos	8.2 - 8.3	**X**					
Definición de funciones y responsabilidades de seguridad	a.7.1.2 - a.13.2.4	**X**					
Inventario de activos	a.8.1.1	**X**					
Uso aceptable de los activos	a.8.1.3	**X**					
Política de control de acceso	a.9.1.1	**X**					
Procedimientos operativos para gestión de TI	a.12.1.1	**X**					
Principios de ingeniería para sistema seguro	a.14.2.5	**X**					
Política de seguridad para proveedores	a.15.1.1	**X**					
Procedimiento para gestión de incidentes	a.16.1.5	**X**					
Procedimientos de la continuidad del negocio	a.17.1.2	**X**					
Requisitos legales, normativos y contractuales	a.18.1.1	**X**					

Fuente: Elaboración propia

Tabla 9.

Nivel de madurez de los registros obligatorios

REGISTROS OBLIGATORIOS	Cláusulas ISO 27001:2013	Nivel 0 Incompleto	Nivel 1 Ejecutado	Nivel 2 Gestionado	Nivel 3 Establecido	Nivel 4 Predecible	Nivel 5 Optimizado
Registros de capacitación, habilidades, experiencia y calificaciones	7.2	**X**					
Resultados de supervisión y medición	9.1	**X**					
Programa de auditoría interna	9.2	**X**					
Resultados de las auditorías internas	9.2	**X**					
Resultados de la revisión por parte de la dirección	9.3	**X**					
Resultados de acciones correctivas	10.1	**X**					
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	a.12.4.1 a.12.4.3	**X**					

Fuente: Elaboración propia

CAPÍTULO II. GESTIÓN DE RIESGOS

En este capítulo se describe la metodología a utilizar para la gestión de riesgos, a fin de que los propietarios de los riesgos y comité de seguridad de la información tomen las medidas adecuadas según los riesgos identificados. Esta metodología se compone de dos fases: la primera fase Análisis de riesgos donde se identifican las amenazas, vulnerabilidades, impacto y el valor de los activos en función de la confidencialidad, integridad y disponibilidad. La segunda fase es el tratamiento de los riesgos donde se toman las decisiones de evitar, mitigar, transferir o aceptar el riesgo.

2.1 METODOLOGÍA

ETAPAS DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS

1. Análisis de Riesgos
2. Tratamiento de Riesgos

2.1.1 Etapa 1: Análisis de riesgos

El análisis de riesgos es el primer proceso de la metodología de gestión de riesgos. El análisis de riesgo implica desarrollar una comprensión del riesgo. Proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento de riesgo más apropiados. También puede proporcionar elementos de entrada para tomar decisiones cuando se deben hacer elecciones y las opciones implican diferentes tipos de niveles de riesgo.

El análisis de riesgo implica la consideración de las cusas y las fuentes del riesgo, sus consecuencias positivas y negativas, y la probabilidad de que estas consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y a la probabilidad. El riesgo se analiza determinando las consecuencias y puede afectar a múltiples objetivos. También se deberían tener en cuenta los controles existentes, así como su eficacia y eficiencia.

La forma de expresar las consecuencias y la probabilidad, así como la manera en que estas se combinan para determinar un nivel de riesgo, debería corresponder al tipo de riesgo, a la información disponible y al objetivo para el que se utiliza el resultado de la apreciación del riesgo. Todos estos datos deberían ser coherentes con los criterios del riesgo. También es importante considerar la interdependencia de los diferentes riesgos y de sus fuentes.

La metodología de análisis de riesgos está compuesta por once (11) pasos primarios:

Paso 1 - Caracterización de sistemas

Paso 2 - Identificación de amenazas

Paso 3 - Identificación de vulnerabilidades

Paso 4 – Determinación del evento del riesgo

Paso 5 - Determinación de probabilidades

Paso 6 - Análisis de impacto

Paso 7 – Calculo del riesgo inherente

Paso 8 – Evaluación de controles existentes

Paso 9 – Calculo del riesgo residual

Paso 10 - Recomendaciones o mejoras de control

Paso 11 - Documentación de resultados

A continuación, se describen cada uno de estos pasos:

Paso 1: Caracterización de Sistemas

En el análisis de riesgos, el primer paso es definir el alcance. En este paso, se identifican los límites de estudio, los objetivos, el análisis interno y externo de la Universidad. Así mismo se consideran los recursos que compone dicho sistema. Se pueden considerar:

- Unidades organizacionales: departamento, oficina, proyecto, sucursales, etc.
- Proceso de negocios: gestión de ventas, compras, contratación de personal, etc.
- Ubicación: sede, sala de servidores o en cualquier otro lugar geográficamente definido para un determinado perímetro.
- Activos: archivos de clientes, bases de datos, nóminas, marca comercial, etc.
- Tecnologías: servidor, aplicación, red, internet inalámbrica, etc.

Paso 2: Identificación de Amenazas

Una amenaza es una causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u Universidad.

La vulnerabilidad es la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

En sí mismo, la presencia de una vulnerabilidad no produce daño, debe existir una amenaza para explotarla. Una vulnerabilidad que no se corresponde con una amenaza puede no requerir la puesta en marcha de un control, pero debe ser identificada y controlada en caso de que se produzcan cambios.

Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.

Amenazas naturales: Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas eléctricas y otros eventos similares.

Amenazas ambientales: Ausencias extendidas de energía eléctrica, polución, químicos, dispersión de líquidos.

Amenazas humanas: Acontecimientos impulsados o generados por las personas, tales como actos no intencionados (errores en la entrada de datos) o malintencionados (ataques a la red, activación de software malicioso, acceso no autorizado a información confidencial).

Paso 3: Identificación de Vulnerabilidades

Las vulnerabilidades pueden ser intrínsecas o extrínsecas. Las vulnerabilidades intrínsecas están relacionadas con las características intrínsecas de los activos y las vulnerabilidades extrínsecas están relacionadas con las características de las circunstancias específicas del activo.

Paso 4: Determinación del Evento del Riesgo

Se describe el evento en el cual la amenaza se materializa debido a la vulnerabilidad existente. Los siguientes pasos evaluaran el evento del riesgo para obtener su cálculo inherente.

Paso 5: Determinación de Probabilidad

Para cada amenaza identificada se realiza el análisis para verificar que podría ser la probabilidad de ocurrencia. Los niveles de posibilidad de que una vulnerabilidad pueda ser explotada se clasifica en Alto, Medio y Bajo.

Tabla 10.

Probabilidad de ocurrencia

Probabilidad de Ocurrencia		Descripción
Bajo		Una vez al año / Un caso entre 6 y 12 meses
Medio		Entre 1 y 3 veces al año / Un caso entre 1 y 6 meses
Alto		Más de 3 veces al año / Entre 1 y 10 casos en 15 días

Fuente: Elaboración propia

Paso 6: Análisis de Impacto

Se hace el cálculo del impacto producto del resultado que una amenaza se materialice a través de una vulnerabilidad existente.

El impacto se puede describir en términos de la degradación de una o varias de los objetivos de seguridad: Integridad, Disponibilidad, Confidencialidad; se puede describir como Alta, Media y Baja.

Tabla 11.

Nivel de impacto

Nivel de Impacto	Descripción
Bajo	– Genera molestias en los usuarios internos – Inoperativo menos de 5 minutos – Sin lesiones o con lesiones leves – Pérdidas económicas menores al 5% del patrimonio.
Medio	– Genera quejas de los usuarios (insatisfacción del cliente externo). – Inoperativo entre 5 minutos y 1 hora – Genera traumas físicos o psicológicos – Pérdidas económicas entre el 5% y 20 % del patrimonio.
Alto	– Genera impacto negativo en la mayoría de los usuarios (externo). – Inoperativo más a 1 hora – Genera pérdidas de vidas humanas e invalidez – Pérdidas económicas superiores al 20 % del patrimonio.

Fuente: Elaboración propia

Paso 7: Calculo del Riesgos Inherente

El riesgo inherente es el riesgo que se obtiene cuando el activo tiene un control de seguridad y se expresa en función de:

- La probabilidad de ocurrencia de que la amenaza explote una vulnerabilidad.
- El impacto producto de que la amenaza aproveche una vulnerabilidad.
- Los controles implementados para reducir o eliminar los riesgos.

Se utiliza la siguiente tabla de valoración del riesgo:

Matriz de valoración de riesgo

		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABI	BAJO			
	MEDIO			
	ALTO			

RIESGO

Siendo el nivel del riesgo:

Muy bajo	Bajo	Medio	Alto	Muy alto

2.1.2 Etapa 2: Tratamiento de riesgos

El tratamiento del riesgo implica la selección y la implementación de una o varias opciones para modificar los riesgos.

Una vez realizada la implementación, los tratamientos proporcionan o modifican los controles. El tratamiento del riesgo supone un proceso cíclico de:

- Evaluar el tratamiento del riesgo
- Decidir si los niveles de riesgo residual son tolerables;
- Si no son tolerables, generar un nuevo tratamiento del riesgo; y
- Evaluar la eficacia de este tratamiento

2.1.3 OPCIONES DE TRATAMIENTO DE RIESGOS

Las opciones de tratamiento del riesgo no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias. Las opciones pueden incluir lo siguiente:

- Evitar el riesgo: Cuando los escenarios de riesgo identificados se consideran demasiado altos, se puede tomar una decisión para evitar el riesgo:
  - Mediante la cancelación de una actividad o conjunto de actividades
  - Modificando las condiciones en las que funciona el negocio

- Mitigar el riesgo: El nivel de riesgo debería ser administrado mediante la introducción, extracción, o modificación de los controles de modo que el riesgo residual se pueda reevaluar como algo aceptable.

  Dos opciones:
  - Cambiar la probabilidad utilizando controles preventivos
  - Cambiar la consecuencia utilizando controles correctivos

- Transferir el riesgo: El riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

  Esta es la mejor opción cuando:

  - Es muy difícil para una Universidad reducir el riesgo a un nivel aceptable
  - La Universidad carece de los conocimientos necesarios para gestionarlo
  - Es más económico transferirlo a un tercero

  Hay dos métodos principales de riesgo compartido:

  - Seguros: Cualquier otra forma de cobertura de los riesgos contratada por una Universidad a cambio de pagar una prima
  - Tercerización: Transferencia de la totalidad o una parte de la actividad de la empresa a un socio externo

- Asumir el riesgo: Si el nivel de riesgo cumple con los criterios de aceptación del riesgo, no es necesario poner en marcha controles adicionales y el riesgo puede ser aceptado de hecho

  La retención del riesgo actual debe, sin embargo, ser documentada.

Tabla 12.

Nivel de evaluación del riesgo

Evaluación del riesgo – Nivel de riesgo	Opciones de Gestión del Riesgo en función del Nivel de riesgo Admisible
– Muy bajo 	– Asumir el riesgo
– Bajo 	– Asumir el riesgo
– Medio	– Mitigar el riesgo
– Alto 	– Mitigar el riesgo – Evitar el riesgo – Transferir el riesgo
– Muy Alto 	– Mitigar el riesgo – Evitar el riesgo – Transferir el riesgo

Elaboración Propia

2.1.4 APETITO DE RIESGO

El comité de seguridad de la información ha considerado que el máximo nivel de riesgo aceptable es MEDIO, en el caso que el cálculo del riesgo sea ALTO o MUY ALTO se tomaran acciones pertinentes, es decir, implementación o mejoras de control para reducir el riesgo a un nivel aceptable.

Tabla 13.

Nivel de evaluación del apetito del riesgo

Evaluación del Apetito del Riesgo	Descripción
– Alto 	– La Universidad **acepta oportunidades** que tienen inherentemente un riesgo alto que puede resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Moderado 	– La Universidad está dispuesta a **aceptar riesgos** que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Tolerable	– La Universidad está dispuesta a **aceptar algunos riesgos en ciertas circunstancias** que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Bajo 	– La Universidad **NO está dispuesta a aceptar riesgos** en la mayoría de las circunstancias que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Cero 	– La Universidad **NO está dispuesta a aceptar riesgos bajo ninguna circunstancia** que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.

Fuente: Elaboración propia

2.1.5 IDENTIFICACIÓN DE NUEVOS RIESGOS

La Universidad puede identificar nuevos riesgos mediante las siguientes fuentes:

- Controles de seguridad de la información deficientes identificadas en los informes de monitoreo.
- Observaciones de auditoria sobre el SGSI y SGCN.

- Incidentes de seguridad de la información.
- Reuniones periódicas trimestrales.
- Riesgos identificados por el área de riesgos, áreas usuarias o por el coordinador de seguridad de la información.

Para cada nuevo riesgo identificado por las fuentes mencionadas se deberá de realizar un análisis y evaluación del mismo, en caso, el riesgo sea intolerable (ALTO o MUY ALTO) se aplicarán nuevos controles o se mejoraran los actuales para disminuirlo.

La Universidad puede asumir un riesgo ALTO o MUY ALTO, en caso, considere que el costo de implementación del control es superior al riesgo evaluado.

2.2 INVENTARIO DE ACTIVOS

Para empezar con la gestión de riesgos se requiere un inventario de activos. Los activos son componentes o funcionalidades de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la Universidad. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

A continuación, se presenta la Descripción de los campos Formato para el inventario de activos de información del Sistema de Gestión de la Seguridad de la Información

Tabla 14.

Descripción de los campos Formato para el inventario de activos de información del SGSI

No.	Identificador del activo. Número consecutivo para ordenar los activos.
Código	Adjunto en la tabla N° 2
Activo	Nombre del activo listado.
Descripción del activo	Breve descripción del activo con el cual se conoce en la Universidad
Ubicación física	Lugar donde se encuentra el activo, puede ser una oficina, almacén, etc.
Tipo de activo	**Hardware (H):** Activo físico disponible, pueden ser: contratos, notificaciones, papeles de trabajo, manuales de usuario, expedientes, servidores, equipos de cómputo, discos removibles, dispositivos ópticos, guías y reglamentos, etc. **Software (S):** Activo no tangible, puede ser: bases de datos, software de aplicación, software de sistema, etc. **Servicio (Ser):** Todo aquel activo que ofrece un servicio a través de un sistema de información, correo electrónico, etc
Clasificación	**Pública (P).** Información accesible para todos y no requiere de un nivel de confidencialidad y su distribución es a través de canales autorizados por la Universidad **Uso interno (UI)**. Información cuya confidencialidad es restringida únicamente al personal autorizado, previa autorización del propietario del activo. **Uso Restringido (UR).** Nivel más alto clasificación de la información y debe ser utilizado sobre la premisa de que la divulgación de la misma está estrictamente limitada y predeterminada a un número muy reducido de personas.
Frecuencia de uso	**Eventual:** el uso del activo se realiza de manera esporádica, se puede aplicar a extintores, alarmas, etc. **Diario:** el uso del activo se realiza al menos una vez al día **Semanal:** el uso del activo se realiza al menos una vez a la semana **Quincenal:** el uso del activo se realiza al menos una vez en la quincena. **Mensual:** El uso del activo se realiza al menos una vez al mes
Propietario del activo	Se enuncia el cargo/nombre de la persona que emite la autorización que se realizan con el activo.
Responsables	Se enuncia el nombre de la persona o grupo que gestionan el activo de información.
Puesto del responsable	Se enuncia el puesto de la persona o grupo que gestiona el activo de información.
Valor del activo y tasación	**Confidencialidad (C)** : 0, 1 (Bajo), 2 (Medio), 3 (Alto), 4 (Muy Alto) **Integridad (I)** : 0, 1 (Bajo), 2 (Medio), 3 (Alto), 4 (Muy Alto) **Disponibilidad (D)** : 0, 1 (Bajo), 2 (Medio), 3 (Alto), 4 (Muy Alto) **Criticidad:** Es el valor del activo obtenido del mayor valor de la confidencialidad, integridad y disponibilidad. **Nivel de tasación:** 1 : Bajo 2 : Medio 3 – Alto 4 - Muy Alto

Fuente: Elaboración propia

2.2.1 VALORACIÓN DE ACTIVOS

Los criterios de valoración de un activo, según las dimensiones de disponibilidad, integridad y confidencialidad, son:

a. Disponibilidad

Responde a la pregunta de cuál sería el impacto que se tendría si el activo no estuviera disponible.

Tabla 15.

Valoración de la disponibilidad de los activos

Valor	Criterio
0	No aplica / no es relevante
1 (Bajo)	No afecta: Información cuya inaccesibilidad no afecta la actividad normal a la Universidad
2 (Medio)	Durante un periodo de tiempo no menor a una semana podría causar pérdidas significativas: Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la Universidad
3 (Alto)	Durante un periodo de tiempo no menor a un día podría causar pérdidas significativas: Información cuya inaccesibilidad permanente durante una jornada laboral podría impedir la ejecución de las actividades de la Universidad
4 (Muy Alto)	Durante un periodo de tiempo no menor a una hora podría causar pérdidas significativas: Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la Universidad

Fuente: Elaboración propia

b. Integridad

Responde a la pregunta de cuál sería la importancia que se tendría si el activo fuera alterado sin autorización ni control:

Tabla 16.

Valoración de la integridad de los activos

Valor	Criterio
0	No aplica / no es relevante
1 (Bajo)	Se puede reparar fácilmente: Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la Universidad
2 (Medio)	Se puede reparar, aunque puede dejar algunas pérdidas: Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para la Universidad o terceros
3 (Alto)	Es difícil su reparación y puede dejar pérdidas significativas: Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la Universidad o terceros.
4 (Muy Alto)	No puede repararse ocasionando pérdidas grandes: Información cuya modificación no autorizada no podría repararse, impidiendo la realización de actividades

Fuente: Elaboración propia

c. Confidencialidad

Responde a la pregunta de cuál sería la importancia que se tendría si se accediera de manera no autorizada.

Tabla 17.

Valoración de la confidencialidad de los activos

Valor	Criterio
0	No aplica / no es relevante
1 (Bajo)	Público: La información puede ser conocida y utilizada sin autorización por cualquier persona fuera y dentro de la Universidad.
2 (Medio)	Reservado (uso interno): Información puede ser conocida y utilizada por todos los agentes de la Universidad.
3 (Alto)	Reservado (confidencial): Información que sólo puede ser conocida y utilizada por un grupo de agentes que la necesiten para realizar su trabajo.
4 (Muy Alto)	Reservado (secreto) : Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes cuya divulgación podría ocasionar un perjuicio a la Universidad o a terceros.

Fuente: Elaboración propia

Criticidad del activo

Bajo (1)	Medio (2)	Alto (3)	Muy alto (4)
			

2.3 APLICACIÓN DE LA METODOLOGÍA DE EVALUACIÓN DE RIESGOS

Se agruparon los activos de la información tal como sigue:

SISTEMA DE INFORMACIÓN

- Sistema de Información SIAF
- Sistema de Información SIGA
- Sistema Académico

SERVIDORES

- Servidor SIAF
- Servidor. ACTIVE DIRECTORY
- Servidor. SIGA
- Servidor Repositorio 1
- Servidor Repositorio 2
- Servidor Repositorio 3

SWITCH

- SWITCH de distribución externa 1
- SWITCH de distribución interna 1

FIREWALL

- FIREWALL Fortigate 200 D

EQUIPOS DE COMPUTO

- Impresora Multifuncional Kyocera Eco545 h4132 IDN, Etiquetadora
- Servicio de Hosting Web
- Pc Portatil DELL, Pc Portatil HP, Equipo Lenovo Think Pad T4705, Equipo de escritorio HP Eilito Desk 800-51-SSF
- Equipo de escritorio HP Eilito Desk 800-51-SSF
- Tablet Samsung SM-T820
- Celular LG

HOJAS DE COORDINACIÓN

Tabla 18.

Inventario de Activos

INVENTARIO DE ACTIVOS																	
N	**Código**	**Activo**	**Descripción del activo**	**Ubicación física**	**Tipo de Activo**			**Clasificación**			**Frec. De uso**	**Propietario del activo (*)**	**Responsables**	**Puesto del responsable**	**Valor del activo y tasación**			
					S	**H**	**Ser**	**P**	**UI**	**UR**					**C**	**I**	**D**	**Criticidad**
1	95-22-8117-0038	FIREWALL Fortigate 200 D	Equipo que se usa para protección de la red tanto interna como externa, filtrado de páginas web, control de aplicaciones	Sala de Servidores		X			X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	1	4	4
2	74-08-9200-0004	Servido SIAF	Administrador del sistema de Información SIAF	Sala de Servidores		X			X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	3	4	4	4
3	74-08-9200-0006	Servidor. ACTIVE DIRECTORY		Sala de Servidores		X			X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	3	4	4	4
4	74-08-9200-0007	Servidor. SIGA	Administrador del sistema de Información SIGA	Sala de Servidores		X			X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	3	4	4	4

5	74-08-9200-0011	Servidor Repositorio 1	Servidor de uso externo e interno de la búsqueda de tesis de los egresados	Sala de Servidores	X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	1	4	4	4
6	74-08-9200-0010	Servidor Repositorio 2	Servidor de uso externo e interno de las revistas publicadas por la Universidad.	Sala de Servidores	X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	1	4	4	4
7		Servidor Repositorio 3	Red interna donde posee los artículos.	Sala de Servidores	X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	1	2	4	4
8		SWITCH de distribución externa 1	Equipo para distribución de Red	Sala de Servidores	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
9		SWITCH de distribución interna 1	Equipo para distribución de Red	Sala de Servidores	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
10		Hojas de Coordinación	Se coordina en un mismo nivel de cargo según organigrama	OTI			X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	1	4	4	4
11	74-22-2358-0142	Impresora Multifuncional Kyocera Eco545 h4132 IDN	Permite imprimir, scanear y fotocopiar.	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	1	1	1	1

12		Servicio de Hosting Web	Provee a los usuarios almacenar información, imágenes, vídeo, otros.		X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	0	4	4	4
13	74-08-0500-0351	Pc Portatil DELL	Uso General	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
14	74-08-0500-0349	Pc Portatil HP	Uso General	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
15	74-08-9950-0338	Equipo de escritorio HP Eilito Desk 800-51-SSF	Uso general	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
16	74-08-9493-0049	Tablet Samsung SM-T820	Uso general	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
17	74-08-0500-0333	Equipo Lenovo Think Pad T4705	Uso General	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2
18	95-22-8325-0025	Celular LG	Uso General	OTI	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	2

19	74-08-0500-0300	Etiquetadora		Sala de Servidores		X		M	OTI	Henry Quispe Mamani	Jefe de la OTI	0	0	0	0
20	74-08-9950-0339	Equipo de escritorio HP Eilito Desk 800-51-SSF	Uso general	OTI	X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	1
21	74-08-9950-0340	Equipo de escritorio HP Eilito Desk 800-51-SSF	Uso general	OTI	X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	1
22	74-08-9950-0341	Equipo de escritorio HP Eilito Desk 800-51-SSF	Uso general	OTI	X	X		D	OTI	Henry Quispe Mamani	Jefe de la OTI	2	2	2	1
23		Sistema de Información SIAF	Realiza la gestión Financiera	Sala de Servidores	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	4	4	4	4
24		Sistema de Información SIGA	Realiza la gestión Administrativa	Sala de Servidores	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	4	4	4	4
25		Sistema Académico	Administra la gestión de datos de los estudiantes	Sala de Servidores	X		X	D	OTI	Henry Quispe Mamani	Jefe de la OTI	4	4	4	4

Elaboración Propia
(*) Oficina de Tecnología de la Información

Tabla 19.

Matriz de Riesgos

N	Activo	Amenaza	Vulnerabilidad	Impacto	Evaluación del Riesgo					
					Probabilidad	Impacto	Valor	C	I	D
1	Sistema de información	- Manejo inadecuado de contraseñas - Uso de software por usuarios no autorizados	- Falta de capacitación al personal - No cuentan con un estándar de desarrollo - Falta de documentación - Uso de parches de software - Administración de configuración inadecuada - Instalación/Desinstalación no controlada	- Malestar en los usuarios por la indisponibilidad del servicio - Modificación de datos	MEDIO	ALTO				X
2	Servidor	- Inhabilitación de Servidores - Servidores comprometidos - Perdida de datos por error hardware - Robo de información	- Falta de mantenimiento no periódico - Falta de actualización de antivirus - Obsolescencia tecnológica - Ubicación física: presencia de humedad	Operativa - Malestar en los usuarios por la indisponibilidad del servicio Imagen: - Porque se deja de brindar los servicios	MEDIO	ALTO			X	X
3	Firewall Fortigate 300D	- Inhabilitación de Firewall - Dependencia a servicio técnico externo - Intrusión a Red interna	- Falla del hardware y sus componentes - Degradación del hardware - Falta de mantenimiento planificado - Falta de contingencia	Operativo - Denegación de servicios - Robo de información de la red interna - Pérdida y modificación de datos	BAJO	ALTO		X	X	X
4	Switch	- Inhabilitación de switch - Dependencia a servicio técnico externo - Intrusión a Red interna	- Falla del hardware y sus componentes - Degradación del hardware - Falta de mantenimiento planificado - Falta de contingencia	Operativo - Denegación de servicios	BAJO	ALTO				X
5	Equipo de Computo	- Ingreso no autorizado y/o por la fuerza con intenciones maliciosas - Robo de información	- Falta de capacitación al personal - Falta de supervisión al personal técnico - Falla del hardware y sus componentes - Degradación del hardware	Operativo - Malestar en los usuarios por la indisponibilidad del servicio - Alteración y/o creación de datos	BAJO	MEDIO		X		X

N	Activo	Amenaza	Vulnerabilidad	Impacto	Evaluación del Riesgo					
					Probabilidad	Impacto	Valor	C	I	D
6	Hojas de coordinación	- Infección de sistemas a través de unidades portables sin escaneo - Pérdida o alteración de la información	- Falta de mantenimiento físico - Perdida de datos por error hardware - Corte de fluido eléctrico constante - Falta de custodia	Operativo - Indisponibilidad de la información	BAJO	BAJO				X

Elaboración Propia

Siendo el nivel del riesgo:

Muy bajo	Bajo	Medio	Alto	Muy alto

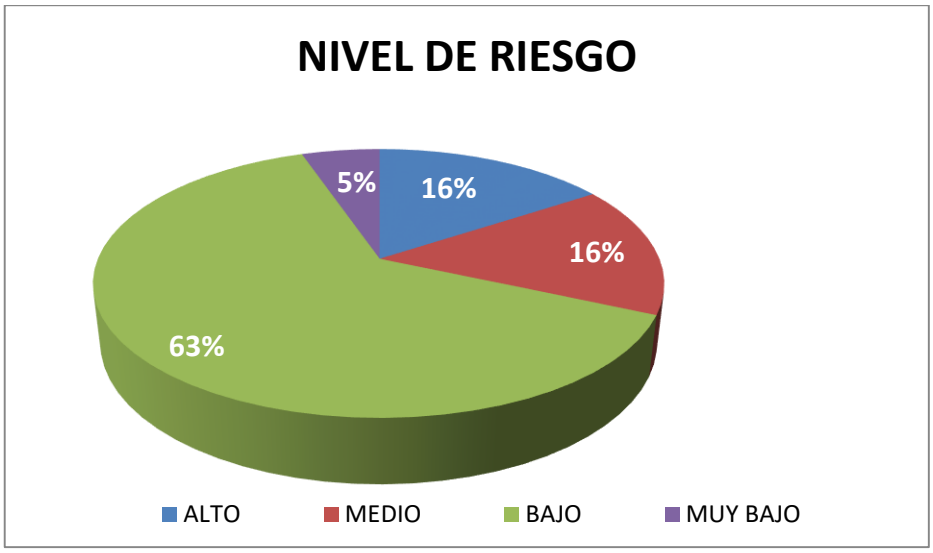


Figura 7. Gráfico resumen de los riesgos identificados:

Elaboración propia

Riesgos	Cantidad
ALTO	3
MEDIO	3
BAJO	12
MUY BAJO	1
Total	**19**

CAPÍTULO III. TRATAMIENTO DE RIESGOS

Se establecerá mediadas de seguridad después de haber estimado el riesgo, también conocidas como de protección que permiten evitar, transferir, mitigar o aceptar los riesgos identificados, para ello el siguiente capítulo se describen las estrategias para el tratamiento de riesgos, estudiando las diferentes situaciones que se presentan en la organización, así como las técnicas como parte del tratamiento de riesgos teniendo en cuenta las prioridades de la organización. Así mismo se establece la política de seguridad, con la finalidad de establecer reglas básicas, para garantizar la confidencialidad, integridad y disponibilidad de la información, así como los controles recomendados, monitoreo y asignación de responsabilidades, teniendo en cuenta la matriz RACI.

3.1 ESTRATEGIAS PARA TRATAMIENTO DEL RIESGO

Se presenta un diagrama de flujo para definir la estrategia de tratamiento del riesgo a fin de enfocarse en el objetivo identificado

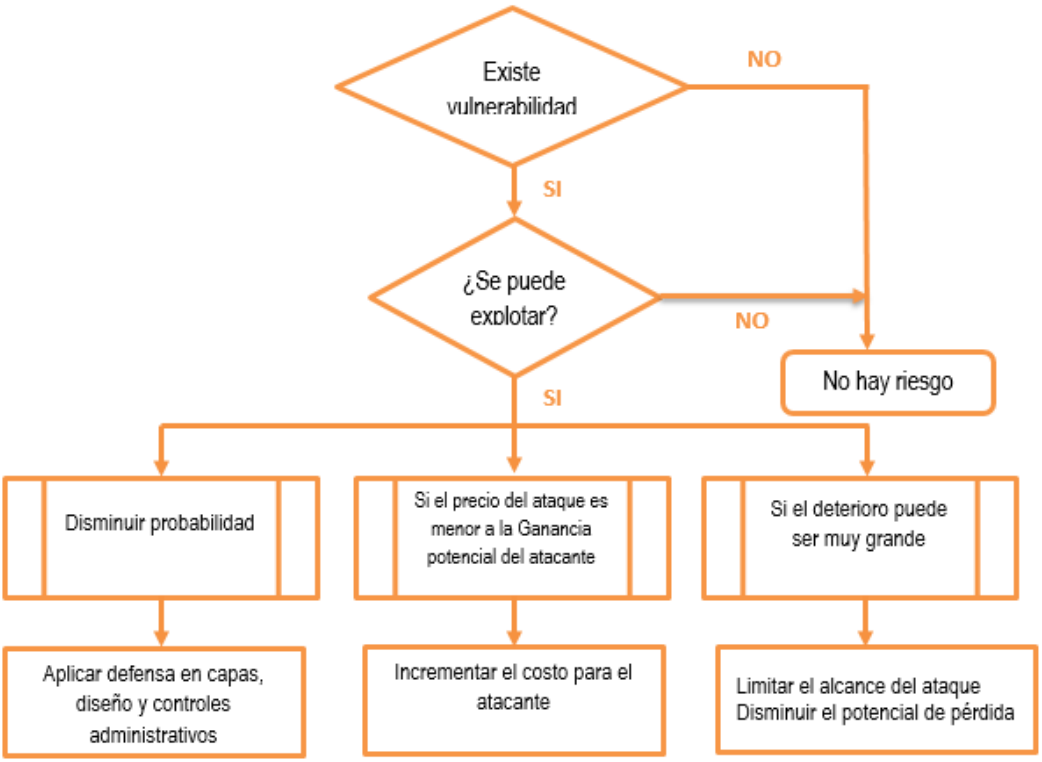


Figura 8. Estrategia para el tratamiento del riesgo.
Fuente: Elaboración propia

- Cuando existe una vulnerabilidad (defecto, debilidad) es necesario implementar técnicas que garanticen la reducción de la probabilidad de que la vulnerabilidad sea explotada.
- Cuando se puede explotar una vulnerabilidad es necesario aplicar protección en capas, diseños arquitectónicos y controles administrativos para minimizar el riesgo.
- Cuando el costo del ataque es menor que la ganancia potencial para el atacante, es necesario aplicar protección para disminuir la motivación aumentando el costo del atacante.
- Cuando la perdida puede ser demasiado grande, es necesario aplicar principios de diseño, técnicas y procedimientos para limitar el alcance del ataque, reduciendo de esta manera el potencial de la perdida.

Luego de realizar la valoración de riesgos se definen el siguiente tratamiento de riesgos:

Tabla 20.

Tratamiento de Riesgos

PROBABILIDAD				
	3 - Alta	**3.Zona de riesgo Medio** Tratamiento: Mitigar el riesgo	**6. Zona de riesgo Alto** Tratamiento: Mitigar el riesgo Evitar el riesgo Transferir el riesgo	**9.Zona de riesgo Muy Alto** Mitigar el riesgo Evitar el riesgo Transferir el riesgo
	2- Medio	**2. Zona de riesgo Bajo** Tratamiento: Asumir el riesgo	**4.Zona de riesgo Medio** Tratamiento: Mitigar el riesgo	**6. Zona de riesgo Alto** Mitigar el riesgo Evitar el riesgo Transferir el riesgo
	1 - Bajo	**1. Zona de riesgo Muy Bajo** Tratamiento: Asumir el riesgo	**2. Zona de riesgo Bajo** Tratamiento: Asumir el riesgo	**3.Zona de riesgo Medio** Tratamiento: Mitigar el riesgo
		1 - Bajo	**2 – Medio**	**3 – Alto**
			IMPACTO	

Elaboración Propia

3.2 TÉCNICAS PARA EL TRATAMIENTO DEL RIESGO

De acuerdo al nivel de riesgo detectado y según las prioridades de la Universidad, se definen diferentes estrategias de tratamiento del riesgo:

Las opciones de tratamiento del riesgo no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias. Las opciones pueden incluir lo siguiente:

- **Evitar el riesgo (E):** Cuando los escenarios de riesgo identificados se consideran demasiado altos, se puede tomar una decisión para evitar el riesgo:

  - Mediante la cancelación de una actividad o conjunto de actividades
  - Modificando las condiciones en las que funciona el negocio

- **Mitigar el riesgo (M):** El nivel de riesgo debería ser administrado mediante la introducción, extracción, o modificación de los controles de modo que el riesgo residual se pueda reevaluar como algo aceptable.

  Dos opciones:

  - Cambiar la probabilidad utilizando controles preventivos
  - Cambiar la consecuencia utilizando controles correctivos

- **Transferir el riesgo (T):** El riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

  Esta es la mejor opción cuando:

  - Es muy difícil para una organización reducir el riesgo a un nivel aceptable
  - La organización carece de los conocimientos necesarios para gestionarlo
  - Es más económico transferirlo a un tercero

Hay dos métodos principales de riesgo compartido:

- Seguros: Cualquier otra forma de cobertura de los riesgos contratada por una organización a cambio de pagar una prima
- Tercerización: Transferencia de la totalidad o una parte de la actividad de la empresa a un socio externo

- **Aceptar el riesgo (A):** Si el nivel de riesgo cumple con los criterios de aceptación del riesgo, no es necesario poner en marcha controles adicionales y el riesgo puede ser aceptado de hecho la retención del riesgo actual debe, sin embargo, ser documentada

Tabla 21.

Tratamiento del riesgo según el vector de amenaza

ID Vector amenaza	Vector Amenaza	Tratamiento del Riesgo			
		A	**E**	**M**	**T**
VA-01	Manejo inadecuado de contraseñas		X	X	X
VA-02	Uso de software por usuarios no autorizados		X	X	X
VA-03	Inhabilitación de Servidores		X	X	X
VA-04	Servidores comprometidos		X	X	X
VA-05	Pérdida de datos por error hardware		X	X	X
VA-06	Robo de información		X	X	X
VA-07	Inhabilitación de Firewall			X	
VA-08	Dependencia a servicio técnico externo			X	
VA-09	Intrusión a Red interna			X	
VA-10	Inhabilitación de switch			X	
VA-11	Ingreso no autorizado y/o por la fuerza con intenciones maliciosas	X			
VA-12	Infección de sistemas a través de unidades portables sin escaneo	X			
VA-13	Pérdida o alteración de la información	X			

Fuente: Elaboración propia

3.3 PLAN DE TRATAMIENTO DEL RIESGO

3.3.1 Política de Seguridad SGSI

Un Plan de implementación del SGSI, requiere de la redacción de una política de seguridad en la se definen las reglas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información en todos los procesos de la organización. En consecuencia, esta debe ser definida, asignada y comunicada a todos los miembros de la institución.

3.3.1.1. Objetivo

El principal objetivo de la política de seguridad del SGSI es definir las reglas básicas que garanticen la confidencialidad, integridad y disponibilidad de la información en los diferentes procesos críticos de la Universidad Nacional de Moquegua

3.3.1.2. Alcance

Está política es aplicable para todos los empleados, personas naturales y jurídicas, contratistas de la Universidad Nacional de Moquegua que tienen acceso a los servicios informáticos disponibles y a la infraestructura de red interna.

3.3.1.3. Responsables

Todos los empleados de la Universidad Nacional de Moquegua, contratistas y terceros externos a la Universidad.

3.3.1.4. Definición

La Universidad Nacional de Moquegua es consciente de que la información con la que opera es un recurso vital para el cumplimiento de sus objetivos, por lo tanto, es esencial garantizar la confidencialidad, integridad y disponibilidad de la misma.

De forma que se comprende con:

- Revisar el cumplimiento de las políticas de seguridad de la información.
- Garantizar los requerimientos legales y de la entidad relativos a la seguridad de la información.
- Asegurar y proteger los activos de información.
- Gestionar los riesgos identificados.
- Desarrollar un plan de concientización sobre seguridad de información para todo el personal.
- Establecer controles de seguridad por medio de implantación de politicas, estándares y procedimientos que permitan proteger los activos de información disponibles.

La UNAM basada en las directrices de seguridad de la información nacional y adaptándolas al caso de la universidad establece que:

- Antes de designar una computadora a un usuario, el oficial de seguridad y el propietario del activo deben asegurar que no existe información confidencial en el activo, en caso contrario, se debe proceder a realizar una copia de la información y realizar un borrado total del equipo.
- El propietario del activo debe establecer las medidas las medidas y mecanismos de control, monitoreo y seguridad de los diferentes servicios que ofrece la organización tales como el correo electrónico y acceso a internet debe ser restringido a contenidos de violencia, etc. o que tengan un origen sospechoso.

- El área de tecnologías de la información deberá planificar pruebas de análisis de vulnerabilidades de los activos de información tanto internas como externas. La frecuencia de evaluación deberá ser mínimo una vez al año.
- El área de tecnologías de la información y el oficial de seguridad deberán autorizar las páginas que por algún motivo fueron bloqueadas siempre en cuando sean autorizadas por el propietario del activo de la información con una justificación documentada.
- El área de tecnologías de la información junto con el área de soporte debe asegurar el correcto funcionamiento de los componentes de red y las configuraciones de los diferentes equipos que conforman la infraestructura tecnológica, deberán considerar la actualización de versiones y parches que indican los proveedores.
- El área de tecnologías de la información y los propietarios de los activos deberán asignar a los usuarios que tendrán un nivel de privilegio de acceso a los diferentes activos de información. Los privilegios de accesos serán revisados cada dos meses.
- El área de tecnologías de la información y los propietarios de los activos deberán elaborar el inventario de activos de la información, clasificándola según su nivel de importancia e indicando su ubicación física. Dicho inventario debe ser actualizado anualmente.
- El área de Recursos humanos y de tecnologías de la información deberán inhabilitar los accesos a los empleados retirados de la organización y éstos

deberán devolver antes la información confidencial que se encuentren bajo su custodia.

- El uso del correo electrónico se utilizará sólo para fines de la Universidad Nacional de Moquegua
- El servicio de internet será de uso sólo a los usuarios autorizados y para fines exclusivos de la organización. Este servicio deberá ser controlado a través de un proxy a fin de evitar que se realice un uso inapropiado.
- El usuario deberá informar al área de tecnologías de la información el cambio de la contraseña si tuviera algún indicio de que haya sido revelada. Las contraseñas no deberán ser enviadas por correo electrónico, deben tener una longitud mínima de 8 caracteres, combinar caracteres alfanuméricos y ser cambiadas máximo cada 90 días.
- Los usuarios deberán realizar un escaneo de los archivos adjuntos con el antivirus antes de ser descargado.
- Las áreas físicas que contengan información confidencial deberán ser de acceso restringido.
- El área de tecnologías de la información deberá asegurar que las claves de usuario serán únicas para cada usuario que solicite el acceso.
- Los activos de información deberán movilizarse fuera o dentro de la organización previa autorización del propietario de la información.
- Las contraseñas de los equipos nuevos deberán cambiarse. Se debe evitar usar las contraseñas predefinidas por el fabricante.
- El área de recursos humanos y tecnologías de la información son los encargados de comunicar al personal las políticas de sistemas de

información antes de la asignación de los activos que se encontrarán bajos su custodia.

- Se debe asegurar la seguridad física de los diferentes activos de información protegiéndolos de amenazas del medio ambiente como: incendios, humedad, polvo, inundación, etc.
- La red inalámbrica deberá tener la siguiente configuración:
    - Establecer el número máximo de dispositivos que pueden conectarse.
    - Administración del filtrado de direcciones MAC de los dispositivos inalámbricos conectados.
    - Uso de encriptación de 256 bits mínimo.
- El área de tecnologías de la información deberá asegurar que los privilegios de los usuarios no serán concedidos como administrador con el fin de que no tenga acceso de configuración de los equipos.
- Los usuarios no deberán compartir las contraseñas ni asegurar que no sean reveladas y tienen la responsabilidad de utilizar su cuenta cumpliendo las políticas de seguridad de la información.
- La infraestructura tecnológica deberá ser asegurada con dispositivos físicos de seguridad como: firewall, IDS, IPS, etc.
- Los equipos de cómputo que contienen información confidencial deberán ser bloqueadas al momento que el usuario abandone dicho equipo, así como por cualquier motivo dejen su lugar de trabajo, por el que deberá apagar su equipo de cómputo al término de la jornada laboral.

- La organización es la responsable de capacitar a sus empleados en temas relacionados a la seguridad de la información con una frecuencia mínima de una vez al año.
- El personal externo y proveedores deberán firmar un acuerdo de confidencialidad si tuvieran acceso a un activo de información confidencial.

3.3.1.5. Sanciones

Cualquier empleado de la UNAM que omita esta política puede estar sujeto a medidas disciplinarias, en las que se puede incluir la culminación del contrato. El incumplimiento de esta política conllevara como primera medida una notificación al superior inmediato, con copia al área de RRHH.

En el caso de terceros, esto conllevara a una nota solicitando explicación al representante legal de la firma.

3.3.2. Controles recomendados

Los controles recomendados se basan en los dominios del Anexo A de la norma ISO/IEC 27001:2013

Documentación de Políticas

Se ha detectado que la Universidad no tienen políticas y/o documentos formales y que en principio son causantes de las vulnerabilidades existentes, por lo que se debe enunciar un conjunto de políticas asociadas a los dominios de la norma ISO/IEC 27001:2013 Anexo A con las cuales se busca disminuir la probabilidad e impacto.

Tabla 22.

Listado de Políticas desarrolladas

ID	Política	Dominio	Vector Amenaza	Nivel de Riesgo
P-01	Política de protección ante virus informáticos y código malicioso	A12	VA-04: Servidores comprometidos	Alto
			VA-12: Infección de sistemas a través de unidades portables sin escaneo	Bajo
P-02	Política de seguridad de información con recursos humanos	A7	VA-06: Robo de información	Alto
			VA-13: Pérdida o alteración de la información	Bajo
P-03	Política de gestión de acceso de usuarios	A9	VA-01: Manejo inadecuado de contraseñas	Alto
			VA-02: Uso de software por usuarios no autorizados	Alto
			VA-03: Inhabilitación de Servidores	Alto
P-04	Política de control de acceso físico y seguridad física	A11	VA-06: Robo de información	Alto
			VA-13: Pérdida o alteración de la información	Bajo
			VA-05: Pérdida de datos por error hardware	Alto
			VA-10: Inhabilitación de switch	Medio
P-05	Política de control de acceso a la red y seguridad lógica	A9 A12	VA-01: Manejo inadecuado de contraseñas	Alto
			VA-03: Inhabilitación de Servidores	Alto
			VA-04: Servidores comprometidos	Alto
			VA-06: Robo de información	Alto
			VA-07: Inhabilitación de Firewall	Medio
			VA-09: Intrusión a Red interna	Medio
			VA-10: Inhabilitación de switch	Medio
P-06	Política de clasificación de la información	A8	VA-06: Robo de información	Alto
			VA-13: Pérdida o alteración de la información	Bajo
P-07	Política de escritorios, pantallas limpias y equipos desatendidos	A11	VA-11: Ingreso no autorizado y/o por la fuerza con intenciones maliciosas	Bajo
P-08	Política de uso y seguridad del correo electrónico	A13	VA-11: Ingreso no autorizado y/o por la fuerza con intenciones maliciosas	Bajo
P-09	Política de uso y seguridad en internet	A13	VA-11: Ingreso no autorizado y/o por la fuerza con intenciones maliciosas	Bajo
P-10	Política de seguridad de información en contratos con terceros	A15	VA-08: Dependencia a servicio técnico externo	Medio
			VA-13: Pérdida o alteración de la información	Bajo

Fuente: Elaboración propia

Tabla 23.

Controles seleccionados del Anexo A de la ISO 27001:2013según la evaluación de riesgos

ID-Riesgo	Riesgo	Vector Amenaza	Nivel Riesgo	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
R-01	Abuso de privilegios de acceso	VA-01: Manejo inadecuado de contraseñas	Alto	X				X			X						
R-02	Afectación de los sistemas de información	VA-02: Uso de software por usuarios no autorizados	Alto	X				X									
R-03	Denegación de servicio	VA-03: Inhabilitación de Servidores	Alto					X			X						
R-04	Caída del sistema por sobrecarga	VA-04: Servidores comprometidos	Alto					X			X						
R-05	Errores de mantenimiento / actualización de equipos (hardware)	VA-05: Pérdida de datos por error hardware	Alto	X						X							
R-06	Información comprometida	VA-06: Robo de información	Alto	X		X	X	X			X						
R-07	Activo comprometido	VA-07: Inhabilitación de Firewall	Medio					X			X						
R-08	Violación de políticas	VA-08: Dependencia a servicio técnico externo	Medio	X										X			
R-09	Hacking interno	VA-09: Intrusión a Red interna	Medio	X				X									
R-10	Activo comprometido	VA-10: Inhabilitación de switch	Medio														
R-11	Acceso de personas no autorizadas	VA-11: Ingreso no autorizado y/o por la fuerza con intenciones maliciosas	Bajo					X		X							
R-12	Actividad ilegal	VA-12: Infección de sistemas a través de unidades portables sin escaneo	Bajo								X						
R-13	Alteración de la información	VA-13: Pérdida o alteración de la información	Bajo	X		X	X	X						X			

Fuente: Elaboración propia

También se enuncian los diferentes controles que permiten reducir el riesgo e identificar el control apropiado según sea el caso. Se resume en la próxima tabla

Tabla 24.

Lista de Controles

Dominio	Control
A7	Aplicación de medidas disciplinarias
	Entrenamiento en seguridad de la información
	Antes de la contratación de personal, definir roles y responsabilidades
	Definir los términos y condiciones del contrato
	Formalizar devolución de recursos y finalización de responsabilidades
	Concienciación con la seguridad de la información
	Finalizado el contrato, revocar los derechos y privilegios asignados
A8	Validar las hojas de vida
	Clasificar y etiquetar la información
	Inventario de Activos
A9	Firewall
	Gestión de Contraseñas
	Gestión (creación, modificación, bloqueado, eliminación) de Usuarios basada en roles
	Reglas de acceso (IP, Protocolo, Puertos)
	VPN
	Firmas digitales
A11	Control del medio ambiente (refrigeración y ventilación)
	Precauciones contra Incendios(extintores)
	Registro de Ingreso de trabajadores y visitantes
	Seguridad Perimetral
	Ubicación y protección de los equipos
A12	Control de software operacional
	Protección contra malware
	Respaldo de la información
	Restricciones sobre la instalación de software
	Segmentación de redes para prevenir la intrusión en la información
	Validación de datos (entrada y salida)
A15	Cláusulas en los contratos de seguridad para proveedores

Fuente: Elaboración propia

3.3.3. Monitoreo

Luego del tratamiento del riesgo y la selección de los controles, es necesario hacer un seguimiento sobre la efectividad de los mismos, caso contrario se pueden ejecutar acciones oportunas que permiten anticiparse a los problemas.

En la siguiente tabla se establecen los riesgos y los responsables a cargo para monitorear:

Tabla 25.

Responsables del monitoreo del tratamiento de riesgo

Riesgo	Nivel	Tratamiento				Plan de Monitoreo	Responsable
		A	E	M	T		
R-01: Abuso de privilegios de acceso	Alto			X		Auditoría interna de las funciones de los empleados	Gerente de proyectos Gerente comercial
R-02: Afectación de los sistemas de información	Alto		X			Evaluación y actualización de activos de almacenamiento Evaluación de activos de respaldo	Gerente de proyectos Coordinador de proyectos
R-03: Denegación de servicio				X		Informes de errores y excepciones	Coordinador de proyectos Analista Desarrollador
R-04: Caída del sistema por sobrecarga	Alto			X		Evaluación periódica de los suministros eléctricos Evaluación al proceso de respaldo externo	Líder de proyectos Soporte
R-05: Errores de mantenimiento / actualización de equipos (hardware)	Alto		X			Informes de errores	Gerente comercial Auxiliar Administrativa
R-06: Información comprometida	Alto		X			Evaluación periódica de la información registrada	Gerente de proyectos Coordinador de proyectos
R-07: Activo comprometido	Medio			X		Evaluación y actualización de activos Evaluación de activos de respaldo	Gerente comercial Auxiliar Administrativa

Riesgo	Nivel	Tratamiento				Plan de Monitoreo	Responsable
		A	E	M	T		
R-08: Violación de políticas	Medio			X		Auditoría interna de las funciones de los empleados y los proveedores	Líder de proyectos Soporte
R-09: Hacking interno	Medio			X		Evaluación de la configuración de la red y encriptación de la información	Coordinador de proyectos Analista Programador
R-10: Activo comprometido	Medio			X		Evaluación y actualización de activos Evaluación de activos de respaldo	Gerente comercial Auxiliar Administrativa
R-11: Acceso de personas no autorizadas	Bajo	X				Registro y evaluación periódica de logs de aplicaciones críticas	Gerente de proyectos Coordinador de proyectos
R-12: Actividad ilegal	Bajo	X				Informes de errores	Analista Programador
R-13: Alteración de la información	Bajo	X				Seguimiento a capacitaciones sobre responsabilidad en el manejo de información	Gerente de proyectos Coordinador de proyectos

Fuente: Elaboración propia

3.3.4. Asignación de Responsabilidades

A partir de los controles del Anexo A de la norma ISO/IEC 27001:2013 se procede a diseñar una matriz RASCI para definir los roles y responsabilidades en relación a la seguridad de la información. Dichos roles se enuncian a continuación:

- **Responsible** (**R**) – **Encargado:** El encargado de la tarea, actividad o proceso
- **Accountable** (**A**) - **Responsable:** El responsable de la tarea, actividad o proceso, es quien rinde cuentas sobre su labor
- **Support (S) – Apoyo:** Se trata de los recursos que se asignan al encargado para cumplir la actividad, tarea o proceso.

- **Consulted (C) - Consultado:** La encargada de suministrar información para la realización de la actividad, tarea o proceso
- **Informed(I) – Informado:** Corresponde a la encargada de informarle sobre el avance de las actividades, tareas o proceso.

Los roles implicados para la implementación del SGSI son:

- **Propietarios de los activos de información**, los responsables de los activos de información.
- **Personal**, todos los usuarios que hacen uso de los activos de información y que tienen una vinculación laboral con la organización.
- **Director General**, quien es el encargado de gobernar el SGSI tanto en el rubro administrativo como financiero.
- **Dirección Ejecutiva**, encargado de la coordinación y verificación de las actividades del SGSI, así como de la correcta administración de los recursos de la institución.
- **Comité Directivo del SGSI**, designado por la Dirección para el Plan de Implementación del SGSI.
- **Líder de seguridad de la información,** encargado de la implementación de técnicas y/o procedimientos para la gestión de incidentes de seguridad de la información, así como, para la mejora de los procesos dentro de la institución.
- **Equipo de seguridad operacional,** encargado de la seguridad de las operaciones y de la implementación de técnicas y/o procedimientos contra

códigos maliciosos, así como el respaldo de la información y el registro de eventos en ambientes de pruebas, desarrollo y operación.

- **Jefe de RRHH**, encargado de la gestión de la documentación que ingresa o sale de la organización tanto de los usuarios internos como con los clientes y/o proveedores, al mismo tiempo atiende las quejas y/o reclamos que podrían suscitarse.
- **Jefe de adquisiciones,** encargado de la gestión de activos, salvaguardando el estado completo de los mismos y manteniendo el inventario actualizado.
- **Jefe del área legal**, encargado de efectivizar los acuerdos confidenciales con los usuarios y los clientes y/o proveedores.
- **Jefe de Finanzas**, encargado de la disposición de los medios y el registro de los hechos económicos, para la generación de informes ante la gerencia.
- **Jefe de infraestructura física**, encargado de la seguridad física y del entorno de la organización, también es el encargado de la implementación de técnicas de aseguramiento para que los empleados laboren en áreas seguras.
- **Jefe de TI**, encargado de la gestión de administración y funcionamiento y el correcto uso de los recursos informáticos.
- **Jefe de I+D,** encargado de las políticas de desarrollo seguro y resguardando la información, en lo que respecta a las aplicaciones y ambientes de desarrollo.

La matriz que define los roles y responsabilidades para la seguridad de la información en la Universidad Nacional de Moquegua se presenta a continuación:

Tabla 26.

Matriz RACI Valoración de la disponibilidad de los activos

R = Responsible –> Encargado **A = Accountable –> Responsable** **S = Supportive –> Apoyo** **C = Consulted –> Consultado** **I = Informed –> Informado**		**Propietario de activo de**	**Personal**	**Director General**	**Dirección ejecutiva**	**Comité Directivo del SGSI**	**Líder de seguridad de la**	**Equipo de seguridad operacional**	**Jefe de RRHH**	**Jefe de adquisiciones**	**Jefe de conformidad legal**	**Jefe de Finanzas**	**Delegado de gestión de las**	**Jefe de TI**	**Jefe de I+D**
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN															
5.1.1	Políticas para la seguridad de la información	C	I	C	A	S	R	S	C	S	C	C	C	S	C
5.1.2	Revisión de las políticas para la seguridad de la información	C		S	A	R	S	C	S	S	S	S	C	S	S
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS															
7.1.1	Selección	A				S			R						
7.1.2	Términos y condiciones del empleo	A	I			S			S		R				
7.2.1	Responsabilidades de la gerencia	A	I		R	S			S						
7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	A	I		S	R			S		C				
7.2.3	Proceso disciplinario	A	I		S				R						
7.3.1	Terminación o cambio de responsabilidades del empleo	A	I			S			S		R			S	
A.8 GESTIÓN DE ACTIVOS															
8.1.1	Inventario de activos	A				S				R				C	
8.1.2	Propiedad de los activos	A			R	S						S	S	C	
8.1.3	Uso aceptable de los activos	A	I			R	S	C	S	C			S		
8.1.4	Retorno de activos	A	I		R	C			S	S		C	S	S	
8.2.1	Clasificación de la información	A	I		S	R	C								
8.2.2	Etiquetado de la información	A	I			S	R		C	C	C	C	S	S	
8.2.3	Manejo de activos	A	I			C	S					C	S	R	
8.3.1	Gestión de medios removibles	A	I			S	S	C					S	R	

R = Responsible –> Encargado
A = Accountable –> Responsable
S = Supportive –> Apoyo
C = Consulted –> Consultado
I = Informed –> Informado

		Propietario de activo de	Personal	Director General	Dirección ejecutiva	Comité Directivo del SGSI	Líder de seguridad de la	Equipo de seguridad operacional	Jefe de RRHH	Jefe de adquisiciones	Jefe de conformidad legal	Jefe de Finanzas	Delegado de gestión de las	Jefe de TI	Jefe de I+D
8.3.2	Disposición de medios	A	I			S						C		R	
8.3.3	Transferencia de medios físicos	A	I			S	C	C						R	
A.9 CONTROL DE ACCESO															
9.1.1	Política de control de acceso	A			S	R	S	S	C	C				S	
9.1.2	Acceso a redes y servicios de red	A	I			S	C	S						R	
9.2.1	Registro y baja de usuarios	A				S	C		R					S	
9.2.2	Aprovisionamiento de acceso a usuario	A				S								R	
9.2.3	Gestión de derechos de acceso privilegiados	A			C	S	R	S	C					S	
9.2.4	Gestión de información de autentificación secreta de usuarios	A				S	C	C						R	
9.2.5	Revisión de derechos acceso de usuarios	A				S	S							R	C
9.2.6	Remoción o ajuste de derechos de acceso	A				S	S	C						R	
9.3.1	Uso de información de autentificación secreta	A	I			S		S						R	
9.4.1	Restricción de acceso a la información	A	I			S	C							R	
9.4.2	Procedimientos de ingreso seguro	A				S	C							R	
9.4.3	Sistema de gestión de contraseñas	A				S	C	S						R	
9.4.4	Uso de programas utilitarios privilegiados	A	I			S	C	S						R	
9.4.5	Control de acceso al código fuente de los programas	A	I			S	C	S						R	
A.11 SEGURIDAD FÍSICA Y AMBIENTAL															
11.1.1	Perímetro de seguridad física	A	I			S	C						R	C	
11.1.2	Controles de ingreso físico	A	I			S	C						R	C	
11.1.3	Asegurar oficinas, áreas e instalaciones	A	I			S	C						R	C	
11.1.4	Protección contra amenazas externas y ambientales	A	I			S	C						R	C	

R = Responsible –> Encargado
A = Accountable –> Responsable
S = Supportive –> Apoyo
C = Consulted –> Consultado
I = Informed –> Informado

		Propietario de activo de	Personal	Director General	Dirección ejecutiva	Comité Directivo del SGSI	Líder de seguridad de la	Equipo de seguridad operacional	Jefe de RRHH	Jefe de adquisiciones	Jefe de conformidad legal	Jefe de Finanzas	Delegado de gestión de las	Jefe de TI	Jefe de I+D
11.1.5	Trabajo en áreas seguras	A	I			S	C						R		
11.1.6	Áreas de despacho y carga	A	I			S	C						R		
11.2.1	Emplazamiento y protección de los equipos	A	I			S	C						R		
11.2.2	Servicios de suministro	A				S	C						R	C	
11.2.3	Seguridad del cableado	A				S	C						S	R	
11.2.4	Mantenimiento de equipos	A				S	C						R		
11.2.5	Remoción de activos	A	I			S	C						R		
11.2.6	Seguridad de equipos y activos fuera de las instalaciones.	A	I			S	C						C	R	
11.2.7	Disposición o reutilización segura de equipos	A	I			S	C						S	R	
11.2.8	Equipos de usuario desatendidos	A	I			S	C						S	R	
11.2.9	Política de escritorio limpio y pantalla limpia	A	I			S	C						S	R	
A.12 SEGURIDAD DE LAS OPERACIONES															
12.1.1	Procedimientos operativos documentados	A					C	S						R	
12.1.2	Gestión del cambio	A	I		S	R	S			S				S	C
12.1.3	Gestión de la capacidad	A			S	R				S			C	S	C
12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	A			S	R	C	S						S	
12.2.1	Controles contra códigos maliciosos	A			S		C	S		C				R	C
12.3.1	Respaldo de la información	A			R	S	C			S				S	
12.4.1	Registro de eventos	A			S	S	C	S		S				R	
12.4.2	Protección de información de registros.	A			S	S	R	C		S				S	
12.4.3	Registros del administrador y del operador	A				S	R	S						S	
12.4.4	Sincronización de reloj	A					C	S						R	

R = Responsible –> Encargado **A = Accountable –> Responsable** **S = Supportive –> Apoyo** **C = Consulted –> Consultado** **I = Informed –> Informado**		**Propietario de activo de**	**Personal**	**Director General**	**Dirección ejecutiva**	**Comité Directivo del SGSI**	**Líder de seguridad de la**	**Equipo de seguridad operacional**	**Jefe de RRHH**	**Jefe de adquisiciones**	**Jefe de conformidad legal**	**Jefe de Finanzas**	**Delegado de gestión de las**	**Jefe de TI**	**Jefe de I+D**
12.5.1	Instalación de software en sistemas operacionales	A	I			S	C			C				R	
12.6.1	Gestión de vulnerabilidades técnicas	A				S	S	S						R	
12.6.2	Restricciones sobre la instalación de software	A	I			S	S	S						R	
12.7.1	Controles de auditoría de sistemas de información	A			S	S	R	S						S	C
A.15 RELACIONES CON LOS PROVEEDORES															
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	A			C	R	S								
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	A				S	R				S			S	
15.1.3	Cadena de suministro de tecnología de información y comunicación	A				S	R							S	
15.2.1	Monitoreo y revisión de servicios de los proveedores	A					S	C						R	
15.2.2	Gestión de cambios a los servicios de proveedores	A				S	S							R	

Fuente: Elaboración propia

3.3.5. Propuesta de Proyecto

En este apartado se da a conocer la planeación momentánea de 8 meses para su ejecución y que están ligados con el análisis de riesgos y la identificación del nivel de madurez en seguridad de la información.

Tabla 27.

Tiempo de ejecución de los proyectos para la implementación de los controles seleccionados

Breve Descripción de Plan de Mitigación	Responsable	Tiempo
Proyecto: Documentar metodología de desarrollo, estándar de desarrollo funcional y seguro que sea aplicado por personal interno y por proveedores	Líder de seguridad de la información	2 Meses
Proyecto: Implementar un sistema de continuidad de negocio que incluya análisis de impacto, tiempos de recuperación, estrategias de recuperación, planes de contingencia y pruebas	Líder de seguridad de la información	8 Meses
Proyecto: Documentar procedimiento de control de cambio operativo y capacitar sobre el mismo.	Líder de seguridad de la información	1 Mes
Proyecto: Rediseño de gestión de acceso y programa de concientización	Líder de seguridad de la información	1 Mes
Proyecto: Hardening o aseguramiento de servidores mediante buenas prácticas NIST	Líder de seguridad de la información	6 Meses
Proyecto: Implementación de sistemas de certificados	Líder de seguridad de la información	5 Meses
Segregar funciones de TI. Contratación de Personal.	Líder de seguridad de la información	3 Meses
Proyecto de "documentación de un sistema de gestión de seguridad de la información: políticas y procedimientos"	Líder de seguridad de la información	2 Meses
Proyecto: Establecer políticas de password en sistemas de información bajo los mismos requisitos de la política de seguridad	Líder de seguridad de la información	1 Mes
Proyecto: Segregación de red TI y Administrativa	Líder de seguridad de la información	1 Mes
Proyecto: Implementación de Sistema de Gestión de respaldo adquirido y establecer política de respaldo insite y offsite	Líder de seguridad de la información	3 Meses
Proyecto: Implementar un sistema manual o automatizado de control de versiones como SUBVERSION.	Líder de seguridad de la información	1 Mes
Actualización del organigrama de TI y establecer un comité de seguridad de la información. El responsable de red debe monitorear tanto el firewall como las anomalías de red	Líder de seguridad de la información	1 Mes
Proyecto: Adquisición e implementación de controles físicos para centro de datos (Cámaras, Controles ambientales)	Líder de seguridad de la información	4 Meses
Proyecto: Adquisición e implementación de sistema de capacidad de servidores y aplicaciones (CPU, Memoria, Disco)	Líder de seguridad de la información	8 Meses

Elaboración Propia

ANEXOS:

ANEXO A:

POLÍTICA DE PROTECCIÓN ANTE VIRUS INFORMÁTICOS Y CÓDIGO MALICIOSO

1. OBJETIVO

La Política de Protección ante Virus Informáticos y Código Malicioso tiene por objetivo definir los requerimientos mínimos, que garanticen una adecuada protección ante posibles infecciones de virus informáticos y/o códigos maliciosos, que pudieran afectar negativamente la integridad, disponibilidad y confidencialidad de la información de la empresa. Cabe resaltar que esta política fue desarrollada de acuerdo con lo indicado en la ISO/IEC 27001:2013 Anexo A

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de la Universidad Nacional de Moquegua y de todas aquellas personas que mantienen un vínculo laboral con la Universidad de manera temporal o permanente y bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

a. La organización deberá establecer mecanismos para prevenir y detectar la introducción de software malicioso (antivirus). Los usuarios son conocedores desde su incorporación en la compañía de un “Reglamento de Uso de PC”, donde se les indica cómo hacer uso eficiente de los recursos informáticos.

b. El software antivirus deberá ser actualizado y habilitado en todas las computadoras y servidores de la UNAM. No está permitido el uso de otro tipo de software antivirus que no esté aprobado por el Comité de Seguridad de la Información en adelante CSI y el Oficial de Seguridad de la Información en adelante OSI.

c. El usuario que perciba la existencia de algún malware como virus, troyano, etc. deberá comunicar al área de Seguridad de Información en adelante SI mediante el buzón de seguridad (seguridad.informacion@unam.edu.pe) y al área de Soporte e Infraestructura TI. Lo mismo aplica a cualquier medida de protección que se considere desactualizada, que no esté funcionando correctamente o cuando se detecte algún comportamiento sospechoso en los sistemas.

d. Los equipos móviles de terceros que sean autorizados, por el OSI y el Jefe de Soporte e Infraestructura TI, a ingresar en la red de la UNAM deben ser escaneados previamente con el software antivirus vigente de la UNAM.

e. Todo colaborador que sospeche o identifique algún equipo infectado con virus, deberá desconectarlo de la red de la organización y notificado al área de Soporte e Infraestructura TI y Seguridad de la Información.

f. Todo servidor, computador personal, equipo portátil y cualquier otro equipo informático, propiedad de La UNAM debe tener instalado el software antivirus corporativo aprobado por el CSI, y validado por el OSI.

g. Queda prohibida la conexión a la red de datos de la UNAM, de cualquier equipo informático que no cuente con el software antivirus corporativo instalado y actualizado previamente.

h. Los equipos informáticos, propiedad de los colaboradores, proveedores y/o terceros, que requieran conectarse a la red de datos de la UNAM, deberán ser evaluados y autorizados por la Jefatura de Soporte e Infraestructura TI y el área de SI, con la finalidad de verificar que cuenten con un antivirus, que cumpla los requerimientos y estándares de seguridad informática de la empresa. Solo se brindará acceso en caso sea estrictamente necesario para las labores del personal.

i. Todo medio magnético, debe ser analizado previamente a su lectura/escritura, por el software antivirus corporativo de la UNAM.

j. Los archivos y software que se descarguen de fuentes externas a la UNAM, utilizando el internet u otra red pública, deberán ser analizados por un antivirus antes de que el archivo se descargue o se ejecute el software.

k. El usuario debe analizar mediante el software antivirus corporativo cualquier archivo antes de descomprimirlos, así mismo al software descargado de fuentes externas a la UNAM.

l. Los colaboradores, deberán verificar periódicamente, que el software antivirus instalado en su estación de trabajo, se encuentre actualizado, caso contrario, informar inmediatamente al Jefe de Soporte e Infraestructura TI.

m. Los archivos que serán almacenados en un medio de respaldo deberán ser analizados por un antivirus.

- **Requerimientos del software antivirus corporativo**

a. El antivirus corporativo de la UNAM, deberá contemplar como mínimo las siguientes características:
   - ✓ Detección y protección en tiempo real
   - ✓ Las definiciones y librerías de virus, deberán actualizarse como mínimo una vez al día.
   - ✓ Contar con facilidades que incluyan, como mínimo, medidas que protejan contra amenazas de red y software espía.
   - ✓ Permitir la programación de tareas de revisión y búsqueda automática de virus informáticos y código malicioso.

b. Es responsabilidad del Jefe de Soporte e Infraestructura TI de la UNAM, el asegurar que se mantenga actualizado, el antivirus

corporativo en todo servidor, computador personal, equipo portátil y cualquier otro equipo informático propiedad de la UNAM.

- **Restricciones y limitaciones**

  a. Los Colaboradores de la UNAM:

  - ✓ No deberán copiar o descargar archivos provenientes de fuentes, y/o sitios web desconocidos o de bajo nivel de confiabilidad.
  - ✓ No se debe utilizar el software adquirido por fuentes externas a la Universidad. Sólo se utilizará el software que haya sido autorizado y verificado por el Jefe de Soporte e Infraestructura de TI en conjunto con el oficial de seguridad.
  - ✓ Los virus informáticos serán eliminados sólo con la asistencia del Jefe de soporte e Infraestructura de TI o a quien éste designe como responsable.
  - ✓ No deberán efectuarse actualizaciones automáticas en línea del software instalado en los equipos informáticos de la UNAM, a menos que el software utilizado, haya sido aprobado por el OSI, o por el Jefe de Soporte e Infraestructura TI de la UNAM.

  b. El usuario no debe tener la posibilidad de deshabilitar la ejecución de los sistemas antivirus y no deben ejecutar sistemas y/o aplicaciones que sospechen posee un contenido malicioso o cuya fuente de origen no es confiable. Asimismo, los usuarios quedan prohibidos de participar en la distribución de malware.

4. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos de infección y daño de los equipos informáticos, así como la propagación de virus a través de la red interna de la UNAM.

b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN CON RECURSOS HUMANOS

1. OBJETIVO

La Política de Seguridad de Información con Recursos Humanos de La UNAM tiene por objetivo definir los requisitos de Seguridad de la Información antes, durante y al finalizar el empleo. Asimismo, coordinar la concientización y entrenamiento de los colaboradores de La UNAM y brindar los lineamientos para la definición de los procesos disciplinarios. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013 Anexo A

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de La UNAM y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo cualquier modalidad de contrato.

3. DESCRIPCIÓN

3.1 Requisitos de Seguridad antes del Empleo

a. Las responsabilidades de los empleados que tienen acceso a información confidencial o altamente confidencial de la Universidad deben ser definidas en

el MOF (Manual de Organización y Funciones) y en el Reglamento Interno de Trabajo (RIT) de la empresa.

b. La Gerencia de GDH es responsable de obtener y resguardar los compromisos de confidencialidad y/o consentimientos para el tratamiento de datos personales de colaboradores que se incorporarán a la compañía.

c. Como parte de los documentos de ingreso, los colaboradores de La UNAM reciben y/o firman lo siguiente:

    - Reglamento Interno de Uso de Computadoras Personales: Considera las normas correspondientes al uso de computadoras personales.
    - Código de Ética: Define los lineamientos básicos a considerar como parte de una conducta y comportamiento ético del colaborador, a fin de cumplir con las políticas y procedimientos de La UNAM.
    - Convenio de Confidencialidad: Define las cláusulas de confidencialidad entre el colaborador y la empresa.
    - Ley de Protección de Datos Personales: Define el consentimiento por parte del colaborador para obtener sus datos personales y sensibles, como parte del proceso de vinculación a la compañía.
    - Manual Corporativo de Prevención de Lavado de Activos y Financiamiento del Terrorismo: Considera las políticas, responsabilidades, mecanismos y procedimientos que constituyen el sistema de prevención del Lavado de Activos y del financiamiento del Terrorismo de la UNAM.

- Reglamento Interno de Seguridad y Salud en el trabajo: Define las normas y procedimientos de Seguridad y Salud en el trabajo que rigen en la UNAM.
- Reglamento Interno de Trabajo: Establece los derechos, obligaciones, prohibiciones y otras disposiciones sobre ética laboral, orden, disciplina, higiene y seguridad.

d. Todos los candidatos a ser contratados como empleados deben ser adecuadamente seleccionados considerando lo siguiente:
    - Validación de datos personales.
    - Validación de datos profesionales.
    - Validación de referencias laborales.
    - Evaluaciones psicotécnicas.
    - Dinámica de evaluaciones de competencias (según el proceso de selección). No todos los puestos pasan por dinámica.
    - Validación de record crediticio.

3.2 Requisitos de Seguridad durante el Empleo

a. Las áreas de GDH y Seguridad de la Información son responsables de asegurar que los colaboradores entiendan sus responsabilidades y la relación con el proceso de seguridad de la información a fin de reducir los riesgos de hurto, fraude o mal uso de las instalaciones y sus activos de información. Para lo cual los nuevos colaboradores reciben como parte del programa de inducción, temas relacionados a seguridad de la información, lavado de activos, entre otros.

b. El personal de La UNAM, no debe interceptar o divulgar el contenido de las comunicaciones o contribuir a que otros lo hagan. El contenido de las comunicaciones, ocasionalmente, puede ser revisado o auditado, en caso sea necesario para actividades de mantenimiento, seguridad, auditoría o en la resolución de algún problema.

c. La violación o el no cumplimiento de alguna política de la seguridad de información, podrá derivar en la aplicación de sanciones disciplinarias, que en su mayor grado pueden alcanzar la desvinculación y/o aplicación de las acciones legales que correspondan, según se indica en el Reglamento Interno de Trabajo y Código de Ética de la institución.

d. Cualquier colaborador que tenga conocimiento de una violación de alguna política de seguridad de la información, debe informarla al OSI y Gerencia de División de Gestión y Desarrollo Humano.

e. La Gerencia de Gestión y Desarrollo Humano en coordinación con la Gerencia Legal, es responsable de la definición de términos y condiciones para los contratos de empleo. El área de SI es responsable de comunicar y concientizar a los colaboradores lo referente a las políticas de seguridad de la información vigentes a la fecha.

f. El OSI en coordinación con la Gerencia de Gestión y Desarrollo Humano efectuarán programas de inducción a los nuevos colaboradores y sesiones de capacitación a los colaboradores. Dicha actividad está a cargo del OSI y son dictadas en forma anual en cada local (administrativo y comercial), para asegurar el cumplimiento de las políticas y procedimientos de seguridad de la información.

3.3 Requisitos de Seguridad al finalizar el Empleo

a. La Gerencia de Gestión y Desarrollo Humano debe informar a las área de Soporte de TI, Administración, Desarrollo Organizacional, Comercial, Inteligencia Comercial y al OSI, sobre la culminación del vínculo laboral con los empleados con la finalidad de asegurar el retorno de los activos de la empresa, la restricción de los accesos a las instalaciones y a los sistemas de información de La UNAM.

b. En el caso de un cese de un colaborador que maneje información Altamente Confidencial, el jefe inmediato deberá notificar a las áreas de TI, GDH, Administración y SDI esta decisión a fin de retirarle los accesos físicos y lógicos correspondientes de inmediato.

4. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico no autorizado a los activos de información de la compañía (sistemas, carpetas compartidas, correo electrónico, servicios), fuga de información altamente confidencial, daños en la reputación de la compañía, entre otros; pudiendo afectar la confidencialidad, integridad y disponibilidad de la información en la empresa.
b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes al Reglamento Interno de Trabajo de La UNAM.
c. Las acciones disciplinarias no se limitarán sólo a la pérdida de privilegios de acceso a la información, también se podrá considerar la cancelación de contratos u otras acciones apropiadas según lo establecido en el Manual de Funciones y Responsabilidades de la Universidad.

POLÍTICA DE GESTIÓN DE ACCESO DE USUARIOS

1. OBJETIVO

La política de gestión de accesos de usuarios de la UNAM tiene por objetivo describir los lineamientos que nos permitan gestionar adecuadamente los accesos de usuarios y sus contraseñas de los colaboradores evitando el acceso no autorizado a la red y sistemas de información. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013 Anexo A.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de la UNAM.

3. DESCRIPCIÓN

3.1 Gestión de Usuarios

a. Todo colaborador que ingresa a laborar a la UNAM recibirá un usuario para su acceso a la red y a los sistemas, esto con el propósito de vincularlo a los usuarios y a los perfiles asociados a los sistemas, para responsabilizarlo de sus acciones. Dichos accesos tendrán un nivel de permiso o privilegio asignado, correspondientes a sus funciones desempeñadas en la

Universidad. El oficial de seguridad de la Información revisará con frecuencia (indicado en el Manual de Procedimientos del SGSI) los niveles de acceso a los diversos sistemas de la compañía.

b. La Gerencia de Gestión y Desarrollo Humano debe informar oportunamente los cambios de puesto de los colaboradores (Ascensos y Movimientos Internos) a través de un correo a la Gerencia de Tecnologías de la Información y al nuevo jefe del colaborador, para que inicien el proceso de altas o bajas de accesos de acuerdo al Instructivo de gestión de altas, modificaciones y bajas de usuarios.

c. Los privilegios especiales del personal de la Gerencia de Tecnología de la Información – Jefatura de Soporte e Infraestructura TI, tal como el acceso a los archivos de otros usuarios y/o modificar el estado de seguridad de los sistemas deberán ser restringidos únicamente a los responsables directos del manejo del sistema y/o temas de seguridad definidos por cada vicepresidencia responsable.

d. Las cuentas de usuarios (dominio) que no han sido utilizadas en más de un año o que nunca han sido utilizadas serán desactivadas previa revisión de Seguridad de la Información (Indicado en el Manual de Procedimientos del SGSI, Capitulo 7), salvo excepciones que serán previamente aprobadas por el Oficial de Seguridad de Información de la compañía (p.e. cuentas requeridas para la ejecución de aplicaciones y servicios).

e. Las cuentas de usuario creadas para el desarrollo y pruebas de los diversos sistemas deben ser utilizadas únicamente para los fines descritos, siendo responsabilidad de la Jefatura de Desarrollo el cumplimiento de este

lineamiento. El OSI en coordinación con el Jefe de Desarrollo evaluarán la eliminación de las cuentes de desarrollo y pruebas que no sean necesarias luego de culminado el proceso de desarrollo.

f. Las cuentas de altos privilegios tales como: administración del sistema operativo o de la base de datos, serán utilizadas exclusivamente para estos fines y no para labores diarias.

g. Por ningún motivo, se efectuarán reasignaciones a otros usuarios de las cuentas y privilegios existentes. Las cuentas de acceso y privilegios de los usuarios que dejen de laborar en la compañía, serán desactivados previa comunicación de la Gerencia de División de Gestión y Desarrollo Humano. En caso que se requiera que las cuentas de red y acceso a los sistemas de un colaborador cesado se mantengan activas por un tiempo determinado, se deberá solicitar la autorización correspondiente al OSI, indicando el tiempo que permanecerá activa (debe ser el mínimo indispensable), la persona responsable de las cuentas y el sustento correspondiente.

h. La Gerencia de División de Gestión y Desarrollo Humano comunicará en un plazo no mayor a un día útil el cese del colaborador para la desactivación de accesos. Lo comunicará a las áreas de Seguridad de la Información, Soporte e Infraestructura TI, Administración y a la Área de pertenencia del colaborador, esto de acuerdo al Manual de procedimientos de Gestión y Desarrollo Humano.

i. Toda cuenta de usuario debe tener asociada obligatoriamente una contraseña. Dicha contraseña debe ser exigida en el proceso de autenticación y no puede estar en blanco. Toda cuenta de usuario debe establecerse acorde a la nomenclatura estándar definida en la UNAM.

j. Se prohíbe el uso de cuentas genéricas, que permitan el acceso de varios usuarios haciendo uso de una misma identificación. En aquellos casos en que sea absolutamente necesario y justificado el uso de éstas, su creación deberá contar con una aprobación explícita del OSI, asignar un responsable único y registrar dicha asignación y responsabilidad. No se debe permitir la utilización de cuentas de usuarios duplicadas, que correspondan a personas diferentes, en los sistemas de la UNAM.

k. Todo colaborador que se percate de una mala asignación de privilegios a alguna cuenta de usuario deberá notificarlo inmediatamente como incidente al área de Soporte e Infraestructura TI y Seguridad de la Información para que tomen acción al respecto.

l. Las cuentas de administrador de las PCs de la UNAM deben contar con contraseñas basadas en los lineamientos de seguridad de la empresa y ser cambiadas por lo menos 2 veces al año.

m. El OSI debe revisar de manera anual o cuando lo considere pertinente, el cumplimiento del procedimiento de “Altas, Bajas y Modificaciones de Cuentas” del área de Soporte e Infraestructura TI. La creación de cuentas de usuarios se realizará según lo estipulado en el procedimiento de Altas, Bajas y Modificaciones de cuentas descrito en el Manual de TI. Para el caso de los ceses, el OSI debe revisar de manera mensual o cuando lo considere

conveniente, que se hayan restringido los accesos o deshabilitado (en el Directorio Activo) al personal cesado. Para el caso de cuentas que manejen información sensible de la empresa, el jefe directo debe notificar la desactivación de las cuentas inmediatamente ocurra el cese del colaborador.

3.2 Gestión de Contraseñas

a. Las contraseñas son personales e intransferibles. No se deben transmitir las contraseñas verbalmente a través de líneas telefónicas, ni a través del correo electrónico. Compartir la contraseña está considerada una "Falta Grave", la cual será sancionada de acuerdo a lo estipulado en el Reglamento Interno de Trabajo.

b. Los usuarios no deben anotar las contraseñas de acceso en lugares visibles y/o públicos o de fácil localización, tales como: debajo del teclado o teléfono, detrás de una foto, etc. Cualquier contraseña encontrada en estos medios, debe notificada al área de SI como un incidente.

c. El usuario debe efectuar el cambio de sus contraseñas cada vez que considere que éstas han sido vulneradas o divulgadas a terceros, ello, independientemente del cambio automático solicitado por el sistema y de la notificación al área de seguridad de la información. Al crearse una cuenta de usuario se le asignará una contraseña temporal que deberá ser cambiada en el primer inicio de sesión. Las cuentas de usuarios quedarán bloqueadas

automáticamente después de 3 intentos fallidos (por un lapso de tiempo 30 minutos) y sólo podrá ser desbloqueada por el personal del área de Soporte e Infraestructura de TI durante ese lapso de tiempo.

d. Cada persona es totalmente responsable de las acciones efectuadas con sus cuentas de usuario asignadas. Por tal motivo, ninguna persona debe alejarse de su puesto de trabajo dejando su PC sin bloquear, toda vez que las acciones que se realicen durante su ausencia son de su total responsabilidad, sin importar si puede demostrar que no estaba frente a su PC.

e. Las contraseñas deben estar conformadas por caracteres alfanuméricos y con un largo mínimo de 8 caracteres. Es recomendable que el usuario, al registrarlas, considere que esta debe ser fácil de recordar, difícil de adivinar y que cumpla con las siguientes características:

- En el proceso de cambio de contraseñas, esta no se debe ser igual a las últimas 5 contraseñas utilizadas.
- La contraseña no debe estar en Blanco.
- La vigencia de la contraseña es de 30 días.

f. Las contraseñas, no deben ser visibles por pantalla al momento de ser ingresadas. No deben ser identificadas en el momento de la transmisión y deben viajar por la red encriptados, con algoritmos no reversibles.

g. Las cuentas de usuario (dominio) cuyas contraseñas no tienen fecha de expiración son:

- Cuentas especiales (Directores, Gerencia General) y algunos casos excepcionales, debidamente justificados.
- Usuarios requeridos para la ejecución de Software tales como cuentas de sistemas/aplicaciones, servicios y bases de datos.
- Usuarios para el uso de recursos (Salas, Buzón, Equipos, entre otros)

h. Para los administradores de sistemas:

- Las contraseñas deben permanecer encriptados con algoritmos y residir en archivos ocultos y protegidos en los sistemas.
- Toda vez que se asigne una contraseña, ésta deberá ser no trivial y asignada en forma aleatoria y siempre que el sistema lo permita, obligar en forma automática el cambio de la contraseña en el primer ingreso al sistema (primer “LOGIN”).

- Debe obligarse el cambio automático de la contraseña por primera vez cuando se le otorga el acceso al usuario y luego cada 30 días, forzando que la nueva contraseña considere las exigencias indicadas en este documento.

i. En la medida de lo posible, se debe:

- Evitar que las contraseñas, sean escritas o pasadas como parámetro, en archivos, programas, shell, procesos batch o log de procesos en forma visible.
- Incorporar en las aplicaciones a ser desarrolladas por personal interno o por empresas externas, un mecanismo que permita desconectar al usuario y la ejecución de su trabajo realizado en la aplicación, después de un tiempo prudente de inactividad de este usuario de acuerdo a lo requerido por el área de SI.
- Toda contraseña, provista por el fabricante a cualquier sistema, debe ser cambiada de acuerdo a los estándares de la UNAM. De igual forma cualquier contraseña provista por un proveedor, de hardware o software, debe ser cambiada.

j. El OSI debe revisar que los requerimientos descritos para la conformación de las contraseñas, sean configurados y ejecutados por el Gerencia de TI.

4. INCUMPLIMIENTO

- El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico a los activos de información de la compañía (sistemas, correo electrónico, servicios) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la empresa.
- El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes al Reglamento Interno de Trabajo de La UNAM.

POLÍTICA DE CONTROL DE ACCESO FÍSICO Y SEGURIDAD FÍSICA

1. OBJETIVO

La Política de Control de Acceso Físico y Seguridad Física de la UNAM tiene por objetivo evitar el acceso de forma física no autorizada, daños e indisponibilidad de las áreas y a la información de la Universidad, evitar pérdidas, daños, robo o exposición al peligro de los activos de información y la interrupción de las actividades de la Universidad. Esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013

2. ALCANCE

La presente política considera a áreas sensibles que abarcan a los medios de procesamiento de información, clasificada como altamente confidencial en la UNAM. Asimismo, es de estricto cumplimiento de todos los colaboradores y terceros que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1 Áreas Sensibles

a. Las áreas sensibles de la UNAM son aquellas oficinas y/o áreas en las cuales se procesa, almacena y/o accede a información catalogada como altamente confidencial. En este sentido, las áreas sensibles son:

CENTRO DE DATOS

- Sala de servidores
- Cuartos de comunicaciones
- Zonas de acceso al edificio

b. Los propietarios del(los) activo(s) de información con el apoyo del área de Seguridad de la Información deben identificar las áreas sensibles dentro de la empresa para protegerlas de manera eficiente y oportuna.

c. El CSI de la UNAM deberá validar y aprobar la relación de áreas sensibles de la empresa. El OSI debe monitorear la implementación de controles de acceso apropiados para las áreas sensibles.

Categoría	Nivel de Criticidad	Áreas	Medidas de control
Nivel 1	Muy alta	Centros de Datos	• Mecanismos de control de acceso físico (lectores de acceso, vidrio blindado) • Mecanismos de control ambientales (detectores de humo, extintores) • Bitácoras de ingreso y salida de personas. • Monitoreo externo e interno (cámaras de seguridad)
Nivel 2	Alta	Cuartos de Comunicaciones Sala de Servidores	• Mecanismos de control de acceso físico (puertas con llave) • Mecanismos de control ambientales (detectores de humo, extintores)

Nivel 3	Alta	Zonas de acceso al edificio	• Barreras perimétricas (naturales o físicas) • Bitácoras de ingreso y salida de personas. • Monitoreo externo e interno (cámaras de seguridad)

Cuadro 1. Clasificación de áreas sensibles

3.1.1. Perímetro de seguridad física

a. Los perímetros de seguridad se utilizan para proteger las áreas que contienen información y medios de procesamientos de información, estos son controlados y restringidos únicamente a personas autorizadas.

b. El perímetro de las áreas sensibles está delimitado por elementos de protección, tales como: Puertas, Cerraduras (mecánicas o automatizadas), Lectores de acceso, Bitácoras de ingreso y salida de personas (en caso sea necesario), Vidrio blindado, Personal de seguridad

3.1.2 Controles físicos de entrada

a. El acceso a las áreas donde se procesa o almacena información sensible de La UNAM debe protegerse mediante controles de ingreso apropiados para asegurar que solo se le permita el acceso al personal autorizado. Soporte e Infraestructura TI es responsable del control de acceso a la Sala de Servidores y cuarto de comunicaciones; y el área de administración es responsable del control de accesos a las oficinas.

b. El acceso a las áreas sensibles debe estar delimitado por elementos de protección, tales como:

- Bitácora de accesos: Se registra fecha y hora de entrada, salida de los visitantes, estos debieran ser supervisados a no ser que su acceso haya sido previamente aprobado; solo se les deberá permitir el acceso para propósitos específicos y autorizados. Principalmente para los centros de datos, sala de servidores y zona de acceso al edificio.

- Tarjeta de control de acceso: Se autoriza y valida todos los accesos a áreas donde se procesa o almacena información sensible.

- Identificación visible: Se requiere que todos los colaboradores, contratistas y terceros utilicen alguna forma de identificación visible.

- Monitoreo interno: El acceso a las áreas seguras o los medios de procesamiento de información confidencial deber ser restringida a los terceros, solo cuando sea estrictamente necesario este acceso será autorizado por la Vicepresidencia correspondiente o con quien este designe, en coordinación con el Oficial de Seguridad de la Información. Este acceso debe ser monitoreado.

c. Todo colaborador de La UNAM, deberá contar con Fotocheck de identificación (intransferible y deberá colocarlo en un lugar visible durante toda su jornada laboral) y una tarjeta magnética que le habilite el ingreso al área donde generalmente desarrolla sus labores.

d. En caso de extravío y/o robo del fotocheck personal y tarjeta magnética, se deberá notificar a las áreas de GDH y administración a fin de tomar las acciones pertinentes.

e. El área de Administración deberá velar por el correcto registro y declaración de equipos de cómputo, equipos informáticos y/o electrónicos de los colaboradores al momento del ingreso y salida de las instalaciones de La UNAM.

f. Las jefaturas directas, ante la situación de un cambio de cargo de un colaborador, deben revisar sus permisos de accesos físicos asignados y verificar que estos sigan siendo válidos de acuerdo a su nueva función.

g. En el caso de un cese de un colaborador que maneje información altamente confidencial, el jefe inmediato deberá notificar a las áreas de TI, GDH, Administración y Seguridad de la Información esta decisión a fin de retirarle los accesos físicos correspondientes en el momento. Posteriormente, el área de GDH envía una notificación con una frecuencia quincenal.

3.1.3 Protección contra amenazas externas e internas

a. A fin de evitar daños y/o pérdidas que afecten la seguridad de los activos de información de la UNAM, se tiene implementado controles para evitar el daño por fuego, inundaciones, explosión y otras formas de desastres naturales o causados por el hombre:

- Se debe evitar el almacenamiento de los suministros a granel como papelería en las áreas seguras.
- Los medios de respaldo de información deben ubicarse a una distancia segura para evitar el daño colateral.
- Controles de Amenaza contra incendios (detectores de humo, detectores de calor, alarma audible, extintores)

b. Se deben establecer las condiciones ambientales básicas de temperatura, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo a los requerimientos específicos de los equipos de cómputo. Se deben instalar sistemas automáticos de detección y respuesta automática ante condiciones ambientales que afecten el correcto funcionamiento de los equipos. Cuando no se pueda disponer de un sistema de extinción automática de incendios, deben contarse con extintores manuales revisados y vigentes.

c. El centro de procesamiento de datos (datacenter) debe contar con mecanismos de control de acceso físico tales como:

- ✓ Controles de Amenaza contra incendios (detectores de humo, detectores de calor, alarma audible, extintores)
- ✓ Controles de Amenaza contra inundación (detector de humedad)
- ✓ Controles de Aire Acondicionado (sistema de aire acondicionado
- ✓ Controles de Sistema Eléctrico (grupo electrógeno, banco de baterías)
- ✓ Controles de Seguridad Física (Control biométrico, tarjetas magnéticas, panel de identificación, vigilancia a través de cámaras CCTV)

d. No se deben ingerir alimentos o bebidas, así como colocar o manipular líquidos cerca de los equipos o dispositivos de procesamiento de información en la sala de servidores y cuartos de comunicaciones.

e. Las instalaciones eléctricas y de gas de los lugares del trabajo deben ser construidas, instaladas, protegidas y mantenidas orientándose técnicamente según lo que establecen las normas vigentes establecidas.

3.1.4 Trabajo en áreas sensibles

a. El acceso de terceras personas a áreas sensibles debe ser autorizado, supervisado y solo cuando sea requerido.

b. No se permite el trabajo no supervisado, de igual manera, no se permite las grabaciones ni fotografías (equipo fotográfico, video, audio y cámaras) en las áreas sensibles.

c. El Oficial de Seguridad de la Información debe revisar de manera anual o cuando lo considere conveniente, el cumplimiento del procedimiento relacionado al acceso físico a áreas sensibles de la UNAM. Dicho procedimiento se detalla en el Manual de TI.

3.1.5 Áreas de acceso público

a. Toda persona ajena a la UNAM deberá anunciarse formalmente ante el área de recepción del edificio e indicar el propósito de su visita.

b. Los visitantes y/o personal externo deberán entregar un documento de identidad válido y deberán contar con una autorización formal, previa al ingreso a las instalaciones de la UNAM.

c. Todo colaborador, visitante y/o personal externo deberán declarar al personal de Seguridad, al momento de ingreso a las instalaciones, oficinas y/o ambientes de la UNAM, cualquier equipo de cómputo u otro equipo informático con el que vayan a ingresar.

d. El desplazamiento de visitante y/o personal externo dentro de las instalaciones debe ser restringido sólo a las áreas que están involucradas en su visita, el jefe del área visitada deberá monitorear permanentemente su actividad. En caso un colaborador identifique una persona desconocida sin pase de visitante deberá comunicar inmediatamente al personal de Seguridad.

e. Los visitantes y/o personal externo deberán mantener el pase de visitante de manera visible durante el ingreso y desplazamiento a las oficinas y/o ambientes autorizados de la UNAM, bajo ningún motivo, prestar y/o intercambiar el pase de visitante proporcionado por la UNAM.

f. Los visitantes y/o personal externo deberán devolver el pase de visitante proporcionado, al término de sus actividades en las oficinas y/o ambientes de la UNAM.

g. En caso de extravío y/o robo del pase de visitante, se deberá notificar al personal de seguridad de la UNAM.

h. Los colaboradores y personal externo que extiendan su permanencia en nuestras instalaciones fuera del horario laboral, deberá cumplir con el "Procedimiento de Colaboradores fuera del Horario de Trabajo" establecido en el Manual de Administración. El personal de seguridad solamente permitirá la estancia y/o ingreso a las oficinas a las personas que se encuentren debidamente autorizadas según el Procedimiento descrito. La permanencia en las instalaciones de Lunes a Viernes será máximo hasta las 11:00pm y los fines de semana 5:00pm.

i. En caso el personal de Seguridad tenga que ausentarse de la Recepción del 1er Piso pasadas las 7:30pm, ya sea por rondas rutinarias o algún requerimiento específico, la puerta principal será cerrada con llave para evitar el riesgo de ingreso de una persona no autorizada. Por este motivo, en caso un colaborador desee retirarse deberá esperar al personal de Seguridad para aperturar la puerta y registrar su salida.

j. En caso que algún proveedor posea un objeto extraño a su salida, este deberá ser revisado y registrado por personal de seguridad.

3.1.6 Monitoreo interno

a. Todas las áreas sensibles que contengan información altamente confidencial, deberán contar con monitoreo y grabación constante e ininterrumpida, para lo cual, se deberá implementar y monitorear un circuito cerrado de TV.

b. Las cintas y/o los medios magnéticos de grabaciones del Circuito Cerrado de TV, deberán ser conservados por lo menos 1 mes y deberán estar disponibles ante cualquier solicitud de revisión y/o auditoría.

c. El circuito cerrado de TV deberá estar en óptimas condiciones por lo que su mantenimiento será incluido en el Cronograma de Mantenimientos Críticos incluido en el Manual de Administración.

3.2 Equipos de seguridad

3.2.1 Ubicación y protección del equipo

a. Todo ingreso de visitantes y/o personal externo a áreas sensibles de la UNAM, deberá ser autorizado por el jefe o gerente del área visitada. Adicionalmente, se deberá llevar una bitácora de ingreso a dichas áreas sensibles en la cual deberá indicarse de manera expresa: nombre del visitante y/o personal externo, motivo de ingreso, fecha y hora de ingreso y nombre del propietario de la información que autorizó el mencionado ingreso para las áreas sensibles (nivel 1 y nivel 3).

b. Todos los computadores portátiles de la UNAM deberán asegurarse a los escritorios de los usuarios con dispositivos y/o mecanismos de seguridad proporcionados por el área de Administración.

c. Los equipos de cómputo u otro equipo informático, los equipos que pertenecen a los colaboradores, los equipos que ingresan a las oficinas de la UNAM por visitantes y/o personal externo, sólo podrán salir de las instalaciones acompañado de una autorización firmada por el propietario del activo junto con el Gerente del área y/o por el personal responsable designado por el mismo para tales efectos.

d. Para las conexiones a la red de datos de la UNAM, se deberá tener en consideración lo indicado en la "Política de Control de Acceso y Seguridad Lógica".

3.2.2 Servicios públicos de soporte

a. Todos los servidores, computadores personales, equipos de comunicación y otros equipos de las oficinas de la UNAM, deben usar controles que regulen el voltaje. Para tales efectos, se emplearán pozos a tierra, líneas exclusivas y/o equipos de estabilización eléctrica.

b. Los servidores de producción deben poseer UPS (sistemas de energía ininterrumpida), autorizados por el CSI de la UNAM.

3.2.3 Seguridad del cableado

a. El acceso a los ambientes de equipos de comunicaciones y cableado, deberá estar permitido sólo al personal autorizado por el comité de Seguridad.

b. El cableado deberá estar ubicado y protegido físicamente con gabinetes cerrados. Las llaves de los mencionados gabinetes, deberán estar bajo custodia del Jefe de Soporte e Infraestructura TI o por el personal designado por el mismo, para tales efectos.

3.2.4 Mantenimiento de equipo en áreas sensibles

a. El acceso a la sala de servidores, a los ambientes de equipos de comunicaciones y cableado, deberá estar permitido sólo al personal autorizado por la Gerencia de TI de la UNAM.

b. Todo ingreso y egreso a la sala de servidores, deberá ser registrado de manera formal en una bitácora de ingreso.

c. Los servidores, equipos de comunicaciones y el cableado deberán estar ubicados y protegidos físicamente con gabinetes cerrados.

3.2.5 Seguridad de la eliminación o reutilización del equipo

a. Previo a la eliminación (destrucción física) de equipos que almacenen información altamente confidencial de la UNAM, se debe eliminar, destruir o sobre-escribir la información utilizando técnicas que no hagan posible la recuperación de la información original.

3.2.6 Autorización para trasladar equipos de cómputo

a. Los equipos informáticos de los colaboradores y otros equipos que hayan sido traídos a las oficinas de la UNAM por visitantes y/o personal externo, no deben salir de las instalaciones sin la autorización firmada por el gerente del área y/o por el personal responsable designado por el mismo para tales efectos.

4. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos tales como robo o pérdida de activos, fuga de información, acceso no autorizado, entre otros; pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la UNAM.

b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

POLÍTICA DE CONTROL DE ACCESO A LA RED Y SEGURIDAD LÓGICA

1. OBJETIVO

La política de Control de Acceso y Seguridad Lógica a la Información de la UNAM tiene como objetivo controlar el acceso a los principales sistemas de información y activos críticos de la compañía. Esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1 Control de acceso a la red

a. Los accesos a los servicios de red, son asignados por el área de Soporte e Infraestructura de TI en la creación de los usuarios

b. Todos los usuarios de la UNAM deben acceder a los Servicios de Red (impresión, carpetas compartidas, servidores, internet, entre otros) de la empresa a través de una cuenta en el dominio. Esto es requerido mediante la Solicitud de Autorización de Accesos a Sistemas y Asignación de Equipos.

c. El acceso a las herramientas tecnológicas se realizará solamente a través de equipos de la empresa y/o configurados por personal de la UNAM, a excepción de las aplicaciones web. Asimismo, el acceso a dichas herramientas considera la sensibilidad de los datos a los que se accede por lo que se realizará una autenticación mediante contraseña fuerte o de ser el caso mediante una doble autenticación. El área de SI deberá definir los lineamientos bajo los cuales se basará el área de Soporte e Infraestructura TI para la ejecución de controles de acceso.

d. La habilitación de los accesos a los servicios de Internet a través de dispositivos móviles (Smartphone, laptops, tablets, entre otros) se destinarán sólo al personal debidamente autorizado y de acuerdo con el perfil aprobado. Es responsabilidad del OSI y el Jefe de Soporte e Infraestructura TI validar estos perfiles.

e. Los usuarios pueden utilizar sus PCs o los servicios de red para visualizar, descargar, guardar, recibir o enviar archivos de video, música, imágenes o similares, siempre y cuando no esté relacionado con:

- ✓ Contenido ofensivo de cualquier clase, incluyendo material pornográfico.
- ✓ Promover la discriminación sobre la base de raza, género, nacionalidad, edad, estado civil, orientación sexual, religión o discapacidad.
- ✓ Comportamiento violento o intimidante, apuestas, juegos o beneficio económico personal.

f. Se restringe el acceso a la red a través de equipos de terceros (proveedor). En caso de requerirlo por asuntos de negocio, se deberá solicitar la autorización a las áreas de SI y Soporte e Infraestructura de TI, indicando el sustento correspondiente.

g. Los usuarios no deben participar en juegos de entretenimiento en línea o de manera local. Asimismo, no deben acceder a servicios de radio ni de TV por demanda y no deben tratar de violar la seguridad de las computadoras, servidores y equipos de comunicaciones de la empresa.

h. El OSI es responsable del control de los accesos a los servicios de red, y la realización de pruebas de intrusión y evaluación de vulnerabilidades de forma periódica. Es responsabilidad del área de Soporte e Infraestructura TI el monitoreo de la red interna y externa de la UNAM, de acuerdo a lo estipulado en la Política de

Administración de las Operaciones y Comunicaciones.

i. Es responsabilidad del OSI en coordinación con las Gerencias respectivas el monitoreo periódico de los accesos para sincerar su autorización y correcta asignación a los usuarios.

j. En el caso de un cese de un colaborador que maneje información Altamente Confidencial, el jefe inmediato deberá notificar a las áreas de TI, GDH, Administración y Seguridad de la Información esta decisión a fin de retirarle los accesos lógicos correspondientes de inmediato. En caso excepcional que se desee mantener activo algún acceso (personal cesado) el jefe inmediato debe informar esto a Soporte e Infraestructura TI y Seguridad de la Información indicando el sustento correspondiente del requerimiento y fecha de caducidad del pedido (esta fecha no deberá exceder los 30 días).

3.2 Gestión de acceso de usuarios

a. Cualquier tipo de acceso a recursos de la red proporcionados por la UNAM obliga la configuración de una contraseña de acceso al equipo bajo los lineamientos indicados en la Política de Gestión de Acceso de Usuarios.

b. Todo sistema de información de la UNAM requiere de una cuenta de acceso y contraseña en el momento en que se inicia una sesión,

así como después de cierto periodo de inactividad. Los parámetros específicos dependerán de lo definido entre las áreas de Soporte e Infraestructura TI y Seguridad de la Información. La complejidad de la contraseña inicial de acceso al equipo debe considerar lo establecido en la Política de Gestión de Acceso de Usuarios.

c. La gestión y administración operativa de los accesos de usuarios a los sistemas de información de la UNAM, son responsabilidad del área de Soporte e Infraestructura TI o del personal que la misma designe como responsable para tales efectos.

d. Los privilegios especiales se deben restringir a aquellas personas que administran los sistemas, pudiendo existir excepciones cuando tanto el propietario del activo, así como el OSI las autorice formalmente. Todo privilegio especial debe ser debidamente registrado y monitoreado mediante la creación de un GTI formalmente aprobado por el responsable de área, el propietario del activo en referencia y el OSI.

e. Los cambios en la configuración del sistema operativo y en actividades relacionadas a los privilegios del sistema, deben ser realizados por los administradores del sistema, no por los usuarios finales de la UNAM.

f. Los nuevos accesos de usuario y modificaciones en los privilegios deberán ser solicitados y autorizados por el responsable o gerente de área, por el(los) propietario(s) de los activos involucrados y el área de SI antes de ser ejecutadas por el área de Soporte e Infraestructura TI. Los registros de las solicitudes se conservarán por el periodo definido por el área de SI.

g. A los visitantes y/o terceros de la UNAM no se les debe habilitar accesos de usuario ni privilegios para el uso de equipos o redes de la UNAM, a menos que obtengan la autorización formal del gerente de área y en caso se requiera accesos a sistemas por el(los) propietario(s) de los activos involucrados y el área de SI.

h. Los privilegios que se otorguen a los colaboradores de la UNAM deben tener validez por períodos no mayores a un año. Los privilegios otorgados a los visitantes y/o terceros de la UNAM deben tener validez por períodos que dure el contrato.

i. El propietario del activo (gerentes) en coordinación con el área de SI son responsables de coordinar una revisión anual de los privilegios

otorgados a los usuarios de su área, registrando a través del GTI, las revocaciones o modificaciones de privilegios que resulten de la revisión.

j. Al momento del cese de la relación laboral, la Gerencia de División de Gestión y Desarrollo Humano, debe de emitir una notificación a los involucrados en el proceso de ceses (Soporte e Infraestructura TI, seguridad de la información, administración y DO) de acuerdo a lo estipulado en el Procedimiento de altas, bajas y modificaciones de cuentas del manual de TI.

k. En el caso de un cese de un colaborador que maneje información confidencial, el jefe inmediato deberá notificar a las áreas de TI, GDH, Administración y SDI esta decisión a fin de retirarle los accesos lógicos correspondientes de inmediato.

l. El jefe de área deberá informar acerca de los cambios por ascensos o movimientos a las aéreas involucradas. El área de Soporte e Infraestructura TI realiza de acuerdo a los procedimientos definidos los cambios y/o actualizaciones que sean necesarios para el colaborador. GDH, debe informar sobre los nuevos ingresos a las áreas involucradas y validar los ascensos o movimientos de los colaboradores de la empresa.

m. En caso excepcional que se desee mantener algunos accesos (limitados) el jefe inmediato debe solicitar el permiso

correspondiente al OSI y a la Jefatura de Soporte e Infraestructura TI, indicando el tiempo que se requerirán estos accesos (debe ser el tiempo mínimo indispensable) y el sustento correspondiente.

3.3 Responsabilidades de usuario y gestión de contraseña de usuario

a. Es responsabilidad de los propietarios de los activos (gerencias), establecer los accesos a los diferentes tipos de información de la compañía para el personal a su cargo. Asimismo, es su responsabilidad revisar y/o evaluar periódicamente los privilegios de los colaboradores a su cargo y solicitar se restrinja o revoque cualquier privilegio en caso sea necesario.

b. La sesión de usuario quedará bloqueada automáticamente luego de un periodo de inactividad que será definido por las áreas de Soporte e Infraestructura TI y Seguridad de la Información. Al crearse una cuenta de usuario se le asignará una contraseña temporal que deberá ser cambiada en el primer inicio de sesión. Las cuentas de usuarios quedarán bloqueadas automáticamente después de 3 intentos fallidos (por un lapso de tiempo 30 minutos) y sólo podrá ser desbloqueada por el personal del área de Soporte e Infraestructura TI durante ese lapso de tiempo.

c. EI área de SI, es responsable de informar a los usuarios que es obligatorio el cambio de su contraseña inicial y que debe ser compleja.

d. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas. El OSI y el Jefe de Soporte e Infraestructura TI evaluarán los casos excepcionales relacionados a la presente política.

e. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo vía telefónica indicando si es de acceso a la red o a los sistemas de información, a fin que se le proporcione una nueva contraseña temporal. Cabe resaltar que esta contraseña temporal deberá ser cambiada inmediatamente por el usuario.

f. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

g. Se debe de considerar el monitoreo de eventos relacionados a la seguridad en el uso de sesiones en la red de la UNAM. Algunos de estos eventos son:

- ✓ Inicios de sesión fallidos.
- ✓ Principales motivos de fallas en el proceso de logueo.
- ✓ Cambios en la definición de políticas de red
- ✓ Creación, modificación y eliminación de usuarios de red.
- ✓ Actividad de cuentas con privilegios de administrador.

h. La Jefatura de Soporte e Infraestructura TI es responsable del cambio de contraseñas por defecto (fabricante) en los productos o equipos adquiridos por la UNAM. Para el caso de Software recién adquirido, la Jefatura de Soporte e Infraestructura TI deberá modificar las cuentas especiales que vienen por defecto luego de su instalación, esto con el objetivo de evitar accesos no autorizados.

3.4 Control de acceso remoto

a. Los controles referidos al acceso remoto a la red de la UNAM, se encuentran especificados en la Política de Acceso Remoto y Computación Móvil.

4. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico a los activos de información de la compañía (sistemas, correo electrónico, servicios de red) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la UNAM.

b. El incumplimiento de la presente política, que ocasione cualquier riesgo o pérdida para la compañía, pueden conllevar a una acción disciplinaria o legal, según lo definido en el documento “Reglamento Interno de Trabajo”.

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

1. OBJETIVO

La política de clasificación de la información tiene por objetivo establecer los lineamientos requeridos para la clasificación de la información de la UNAM teniendo en cuenta para ello, la criticidad y sensibilidad de la misma, para las operaciones de la UNAM. Cabe resaltar que esta política ha sido desarrollada de acuerdo a lo establecido en la ISO/IEC ISO/IEC 27001:2013 Anexo A.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de la UNAM y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1. Responsabilidades para con la información

a. Todo activo de información que utilice un proceso y/o área de la UNAM debe tener un propietario asignado.

b. Los propietarios del(los) activo(s) de información tienen la responsabilidad de asignar la clasificación apropiada, según la criticidad de la información, tal y como se define en la presente política. Autorizan y brindan privilegios de acceso a la información, asi mismo realizan coordinaciones con el área de seguridad de la información a fin de asegurar que se utilicen los controles apropiados para el cumplimiento del ciclo de vida de la información.

c. El área de SI tiene la potestad de recomendar y asesorar a los propietarios del(los) activo(s) de información respecto a la clasificación, acceso y uso adecuado de ésta.

3.2. Etiquetado

a. La clasificación de la información se encuentra especificada en la Política de Inventario de Activos.

b. La información en formato impreso, manuscrito u otro tipo de información Altamente confidencial, deberá portar la etiqueta "Altamente confidencial" en la parte superior derecha de cada página. En caso estuviera encuadernado, se deberá etiquetar apropiadamente en la carátula "Altamente confidencial", así como en la página del título y en la contra caratula.

c. Todo USB, Disco Externo, CD-ROM, DVD o cualquier otro medio magnético de almacenamiento, que contenga información “Altamente Confidencial”, debe ser etiquetado externamente con su clasificación apropiada.

d. La información clasificada como “Altamente Confidencial”, se debe etiquetar de manera apropiada desde el momento en que se crea hasta su eliminación o cambio de clasificación.

e. Los colaboradores de la UNAM, no deberán retirar ni cambiar las etiquetas de clasificación de datos a la información sin el permiso previo del propietario de la información y del Oficial de Seguridad de la Información de la UNAM.

f. Toda agrupación, y/o recolección de información debe etiquetarse con la clasificación más crítica de la información agrupada. Para tal efecto, si se crea un reporte y/o base de datos, y la misma contiene información sólo para “Pública”, “Interna”, “Confidencial” y “Altamente Confidencial”, todo el reporte y/o base de datos debe clasificarse y etiquetarse como “Altamente confidencial”.

g. Toda información que no esté etiquetada, será clasificada como “Información Interna”.

3.3.Otras etiquetas

a. Pueden existir otras etiquetas en la clasificación de la información específica para las áreas y/o gerencia de la UNAM, pero éstas deben concordar con el sistema de clasificación de la información definida en esta política.

3.4.Distribución de la información

a. Los propietarios del(los) activo(s) de información "Altamente Confidencial" deben asegurarse que las copias impresas, lógicas y/o medios magnéticos se encuentren adecuadamente etiquetados, con su clasificación de "Altamente Confidencial" antes de proceder a su distribución.

b. Los colaboradores de la UNAM tienen prohibida la distribución de la información "Altamente Confidencial", en cualquiera de los medios impresos, lógicos y/o magnéticos, en los que esta pueda encontrarse, sin el conocimiento y autorización del propietario de la información.

3.5.Desclasificación de la información

a. Si se define una fecha de vencimiento de la información "Altamente Confidencial", ésta debe señalarse de manera clara, en todos los medios en que esta información se manifieste.

b. Los colaboradores que utilicen información “Altamente Confidencial”, nominada para desclasificación en una fecha ya vencida, deben comunicar de manera formal, al propietario de la información para su desclasificación definitiva.

c. El propietario de la información tiene la potestad de desclasificar cuando lo considere necesario la clasificación actual de la información siempre que la fecha de desclasificación esté vigente. Así mismo el propietario de la información debe cambiar la etiqueta de clasificación que aparece en el documento original y notificar al Oficial de Seguridad de la Información de la UNAM y a todos los destinatarios y/o usuarios actuales de la información desclasificada.

d. Por lo menos una vez al año, los propietarios del(los) activo(s) de información deben revisar la información clasificada como confidencial en la UNAM con el fin de determinar si la información puede o no ser desclasificada.

3.6.Eliminación de la información

a. Toda información “Altamente Confidencial” de la UNAM, debe eliminarse de manera segura, cuando ésta ya no se utilice. Para tal efecto, los propietarios del(los) activo(s) de información, deben evaluar la criticidad y utilidad de la información periódicamente.

b. Toda información “Altamente Confidencial”, que no vaya a utilizarse nuevamente debe ser colocada en cajas lacradas hasta el momento que sea trasladada para su disposición por personal de la UNAM o por una empresa externa contratada para tal fin.

c. La eliminación de información Altamente Confidencial impresa en papel debe realizarse a través del uso de máquinas trituradoras u otro mecanismo de similar efectividad.

d. Los colaboradores de la UNAM no deben eliminar información, ni archivos importantes para la UNAM, sin autorización previa del propietario de la información.

e. Los discos duros interno y otros medios magnéticos, no pueden ser donados, desechados, reutilizados, antes de ser sometidos a un proceso de eliminación de información según lo indicado en el Procedimiento de Eliminación de Medios de Información del Manual de Procedimientos del SGSI.

3.7.Extravío y/o divulgación de la información

a. En caso que la información “Altamente Confidencial” se perdiera y/o se divulgará a partes no autorizadas, se notificará al propietario de la información y al OSI de la UNAM.

4. INCUMPLIMIENTO

a. El cumplimiento de esta política involucra a todo el personal y terceros que tengan acceso a la información y recursos informáticos de la compañía. Esto puede afectar la confidencialidad, integridad y disponibilidad de la información de la UNAM

b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

POLÍTICA DE ESCRITORIOS, PANTALLAS LIMPIAS Y EQUIPOS DESATENDIDOS

1. OBJETIVO

La Política de Escritorios y Pantallas limpias de la UNAM tiene como objetivo describir los lineamientos que nos permitan proteger la información capturada, almacenada y emitida a través de impresoras, fax, fotocopiadores, escáner, equipos multifuncionales y cámaras digitales. Esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013 Anexo A

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

a. Los usuarios deben guardar los documentos y medios de almacenamiento de información (laptop sin cable de seguridad, CD's, DVD's, memorias USB, discos externos y otros) cuando no se estén utilizando. Asimismo, la información altamente confidencial debe ser guardada bajo llave (gavetas, archivadores con llave y caja fuerte) cuando no está siendo utilizada o cuando la oficina se encuentra vacía.

b. Cuando los usuarios se retiren o suspendan sus labores, deben dejar los equipos bloqueados (Alt+Ctrl+Supr y Enter, en Windows) o cerrar su sesión de trabajo.

c. Los usuarios deben evitar la grabación de archivos importantes en el escritorio de la computadora para evitar su divulgación, alteración o pérdida en caso de que un tercero obtenga acceso no autorizado al equipo. La información de carácter altamente confidencial debe ser almacenada y tratada en un ambiente seguro de almacenamiento (servidor de archivos o fileserver).

d. Las estaciones de trabajo asignadas deberán ser apagadas por el usuario al término de sus labores o culminado el día de trabajo, con el fin de que otras personas no puedan acceder a su información.

e. Las fotocopiadoras, escáner, cámaras digitales y otras tecnologías de reproducción utilizados por el personal de la UNAM deben ser aquellas proporcionadas y autorizadas por la empresa. Por otra parte los documentos que contienen información de carácter altamente confidencial debieran retirarse inmediatamente de la impresora. Es responsabilidad de todos los colaboradores de la UNAM el cumplimiento de este lineamiento.

f. Los usuarios deben destruir las impresiones que dejen de utilizar y que contengan información altamente confidencial, usando las trituradoras de papel disponibles en las oficinas o algún otro mecanismo de eliminación segura que no permita recuperar la información.

g. Es responsabilidad del área de Seguridad de la Información, la verificación del cumplimiento de la presente política y de tomar las acciones correctivas para mitigar el riesgo de pérdida, manipulación, fuga de la información o suplantación.

4. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos de accesos y/o modificaciones no autorizadas, pérdida, fuga y uso no adecuado de la información considerada como altamente confidencial en la UNAM.

b. El incumplimiento de la presente política, dependiendo del tipo y la gravedad de la infracción podrá seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

POLÍTICA DE USO Y SEGURIDAD DEL CORREO ELECTRÓNICO

1. OBJETIVO

La política de Uso y Seguridad de Usuarios del Correo Electrónico de la UNAM tiene por objetivo definir los requerimientos mínimos acordes con la política de Seguridad de la Información de la UNAM que garanticen un adecuado uso del correo electrónico corporativo, sin que este exponga a la empresa a riesgos de información innecesarios. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013 Anexo A

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de la UNAM y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo cualquier modalidad de contrato.

3. DESCRIPCIÓN

3.1 Gestión de usuarios

Responsabilidad del usuario

a. En caso de recibir mensajes con asuntos sospechosos y/o de origen desconocido, correos no deseados, los colaboradores destinatarios de la UNAM deberán reenviar estos al buzón de seguridad de la información (seguridad.informacion@unam.edu.pe) para su solución. Por ningún motivo se debe responder directamente al remitente.

b. Para impedir el acceso de partes no autorizadas a los correos electrónicos de la organización, las contraseñas generadas por los usuarios deben tener una complejidad adecuada, la cual es la misma utilizada para el acceso a la red. Los usuarios no deben considerar en la contraseña palabras que se encuentren en diccionarios, datos personales, nombres o relacionado con las actividades laborales. Para este punto, se debe tener en cuenta lo contemplado en la "Política de gestión de acceso de usuarios".

c. Todos los usuarios son responsables de la información tratada desde su cuenta de correo electrónico. Cualquier opinión expresada en los mensajes pertenece únicamente al autor remitente, y no representa la opinión de la UNAM. La divulgación, difusión, copia y/o adulteración de un correo electrónico de la empresa se encuentra estrictamente prohibida.

d. La información proveniente de Internet no es confiable hasta que haya sido respaldada y/o confirmada por una fuente confiable. Los colaboradores que utilicen los sistemas de correo electrónico de la UNAM deben acatar los siguiente:

- ✓ Sólo una vez obtenido el permiso de la fuente correspondiente, reenviar o reproducir material.
- ✓ No revelar información interna de la UNAM.

e. Los colaboradores de la UNAM no deben usar frases inadecuadas, comentarios peyorativos, palabras obscenas en los mensajes de correo electrónico destinado a los colaboradores, clientes u otras personas, debido a que estos pueden tener implicancias legales negativas para la empresa. Las comunicaciones electrónicas de la UNAM, deben utilizarse por parte de los colaboradores, únicamente para asuntos relacionados de tipo laboral. Como parte de las buenas prácticas que rige La Universidad, todas las comunicaciones realizadas, deben alinearse a las normas de conducta y ética.

f. Cuando un correo electrónico contiene información confidencial de la compañía, éste se debe almacenar en un espacio diferente. Los usuarios deben descargar archivos adjuntos con información confidencial a carpetas compartidas (acceso a un grupo limitado de personas) o en su respectiva PC. No debe almacenarse información Confidencial en la bandeja de entrada del correo electrónico.

g. Todos los mensajes que se transmitan a través del activo correo electrónico son de propiedad de la UNAM. El Reglamento Interno de Uso de Computadoras personales es de conocimiento de todos los usuarios, forma parte del File Personal y es firmado al ingreso de cada nuevo colaborador a la organización. Los usuarios deberán cumplir con procesos disciplinarios que se indican en el Reglamento Interno de Trabajo.

h. Todo documento de carácter confidencial que se transmita a través del correo electrónico deberá protegerse mediante una contraseña de apertura para evitar la exposición de la información contenida en el archivo, en caso sea accedido por personal no autorizado, esto es responsabilidad del usuario que transmite esta información. Todos los mensajes deben incluir en el asunto su respectiva clasificación, esta etiqueta ayudará a distinguir a los destinatarios acerca de la confidencialidad y privacidad de la información.

i. Cuando los colaboradores de la UNAM adjunten archivos en el correo electrónico, deberán pasar a un formato de texto amplio si es que fuera posible, así mismo los clientes y/o proveedores deberán utilizar el mismo formato cuando se considere práctico y razonable. Todo archivo adjunto debe ser examinado con un antivirus autorizado antes de ser abierto o ejecutado. Siempre que sea posible, los archivos adjuntos deben descomprimirse antes de que se realice la verificación de virus.

Los colaboradores de la UNAM deben tener cuidado con todos los archivos adjuntos que sean recibidos de terceros aun siendo conocidos las fuentes y se confíen en ellos.

3.2 Privacidad de la Información

j. La UNAM respeta los derechos de sus trabajadores y es responsable del mantenimiento y protección de la infraestructura tecnológica incluyendo el respeto a la privacidad. Asimismo, la UNAM se reserva el derecho de desactivar y/o deshabilitar cualquier cuenta de correo electrónico que por uso indebido atente contra lo establecido en el presente documento.

k. Queda prohibida la revisión, sin sustento, del contenido de las comunicaciones electrónicas y/o correos electrónicos de los colaboradores de la UNAM. Dicha restricción, se extiende igualmente al personal involucrado en la gestión de los sistemas (personal de la Jefatura de Soporte e Infraestructura TI).

l. Bajo ninguna circunstancia, las contraseñas individuales deben ser compartidas ni reveladas con ninguna persona, a excepción del usuario autorizado. Soporte e Infraestructura TI no debe solicitar a los usuarios revelar su contraseña de correo electrónico o sistemas. Cuando se comparten datos que se encuentren en la PC del colaborador deberán utilizar las opciones de reenvío de mensajes, carpetas compartidas en el File Server, acceso USB (en caso este permitido) u otros mecanismos autorizados para compartir la información.

m. En caso estrictamente necesario, la UNAM cuenta con la potestad de divulgar a las autoridades pertinentes, toda la información requerida que ha sido almacenada en el correo electrónico institucional. Este consentimiento lo brindan los usuarios al hacer uso del sistema de correo electrónico de la UNAM. Todo proceso de investigación forense que se realice sobre el sistema de correo electrónico, deberá ser solicitado al Comité de Seguridad de la Información y realizado por el equipo de soporte tecnológico o un tercero especializado en el rubro, evidenciando las actividades realizadas a nivel de filtros de búsqueda.

n. Únicamente cuando se tenga indicios y/o evidencias materiales que el contenido de las comunicaciones electrónicas de los colaboradores de la UNAM pueda estar comprometiendo las políticas y/o los objetivos de negocio, el OSI, previa autorización del Comité, podrá solicitar las revisiones pertinentes. El OSI debe contar con la asesoría y opinión previa del Área Legal de la UNAM.

3.3 Privilegios a nivel de correo electrónico

o. Sólo el personal autorizado por el Comité y el OSI podrá enviar correos electrónicos a las listas Grupales de la organización.

p. Es responsabilidad de Soporte e Infraestructura TI otorgar únicamente los privilegios necesarios para que el colaborador desempeñe su trabajo, de acuerdo a lo registrado en la “Solicitud de autorización de accesos y asignación de equipos”. Al momento de culminada la relación entre el colaborador de la UNAM, se deberá eliminar todos los privilegios del empleado en cualquier sistema de comunicación electrónica y/o correo

electrónico de la UNAM. Cualquier pedido ajeno a lo estipulado en la presente política debe ser evaluado por el OSI y Soporte e Infraestructura TI.

3.4 Mecanismos de seguridad a nivel de correo electrónico

q. Es responsabilidad de Soporte e Infraestructura TI velar para que el sistema de correo electrónico cuente con mecanismos de cifrado automático para la transmisión de correos a fin de evitar riesgos de intercepción o vulnerabilidad en los mismos, se debe emplear un proceso de cifrado autorizado por el Oficial de Seguridad de la Información.

r. Para cualquier tipo de acceso al sistema de correo electrónico, ya sea a través de una red externa a la empresa o dispositivos móviles, se deberá realizar el acceso a través de un protocolo seguro (HTTPS/IMAP). Para esto Soporte e Infraestructura TI facilita un certificado digital a todos los colaboradores de la UNAM, este deberá ser instalado en las PC's desde donde se acceda al correo electrónico.

3.5 Condiciones de Uso del correo electrónico

a. El sistema de correo electrónico de la UNAM, debe usarse exclusivamente para fines laborales. El uso es de carácter personal y se permitirá sólo cuando el consumo sea mínimo en cuanto a los recursos del sistema y no tenga injerencia en la productividad del trabajador. No está permitido el uso del servicio para fines de recaudación de fondos para obras benéficas, etc. No acordes con la labor de la organización.

b. Está prohibido suplantar la identidad de un usuario para dar un mal uso del servicio de correo electrónico tales como afiliarse a organizaciones y reenviar anuncios electrónicos que no sean de interés de la organización.

c. Es obligatorio el uso de firmas en el envío de correos electrónicos al exterior de la UNAM, indicando el nombre, cargo, teléfono y dirección.

d. En caso se requiera una cuenta de uso grupal o genérica, se deberá solicitar el acceso respectivo a Soporte e Infraestructura TI y Seguridad de la Información, indicando:

- ✓ Justificación de uso.
- ✓ Nombre tentativo de la misma, la cual será evaluada y validada por el Oficial de Seguridad de la Información.
- ✓ Personas que utilizarán la cuenta.

e. Queda prohibido el reenvío y/o re-direccionamiento general de los correos electrónicos a terceros fuera de la UNAM, a menos que se haya obtenido un permiso del OSI y el Jefe de Soporte e Infraestructura TI de La UNAM. Los mensajes enviados por terceros que contengan información Confidencial no deben reenviarse a terceras personas a no ser que el remitente tenga un objetivo específico y que el envío sea de beneficio a los objetivos laborales.

4. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico a los activos de información de la compañía (sistemas, correo electrónico, servicios) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la UNAM.

b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

POLÍTICA DE USO Y SEGURIDAD EN INTERNET

1. OBJETIVO

La Política de Uso y Seguridad en Internet de la UNAM tiene por objetivo definir los requerimientos mínimos que garanticen un adecuado uso de los beneficios de Internet, sin que este exponga a la empresa a riesgos de información innecesarios. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013 Anexo A

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

a. El acceso a Internet, deberá ser otorgado únicamente a aquellos colaboradores de la UNAM que hagan uso para fines de la organización.
b. Si un empleado de la UNAM no cuenta con el adecuado servicio a internet y es necesario para realizar un proyecto, el gerente del área responsable deberá evaluar, y rechazar o autorizar dicho requerimiento.

c. En casos considerados de riesgo, el acceso a Internet deberá ser evaluado por el OSI.

3.1 Integridad de la información

a. Toda la información adquirida de Internet debe considerarse no confiable.

b. Los archivos que se descargan de Internet y otras fuentes que no pertenezcan a la UNAM, deberán ser escaneados con el antivirus antes de usarlos.

c. Si un proveedor externo utiliza un software que no es confiable debe probarse en una máquina aislada de la red de la UNAM, y excluida del ambiente de producción, que haya sido respaldada recientemente.

d. Se debe utilizar firmas digitales a fin de garantizar la integridad de la información.

- **Instalación de Software**

a. Los colaboradores de la UNAM no están autorizados para instalar software en los equipos de cómputo suministrados por la UNAM, toda instalación debe coordinarse a través de un SRI a Soporte Tecnológico.

b. Es necesario considerar en este punto lo contemplado en la "Política de Adquisición, Desarrollo, Instalación, actualización y cambios a los Sistemas Informáticos"

- **Tecnología de actualización automática**

a. El software del proveedor que haya sido aprobado por el OSI de la UNAM se autorizará la actualización automática.

- **Información del usuario**

a. La identidad del usuario tiene que estar plenamente registrada, no está permitido falsificar, sustituir u ocultar dicha identidad en cualquier sistema de comunicación de la UNAM. Debe conocerse: nombre del usuario, dirección de correo electrónico, nombre de la organización a la que pertenece y otros detalles que permitan identificar al verdadero autor de los mismos.

b. Queda prohibido el re-direccionamiento de correo y otras facilidades anónimas. Se prohíbe el anonimato en las conexiones haciendo uso de los diferentes servicios tales como FTP, HTTP, HTTPS y otros métodos de acceso remoto, por ejemplo, sin los mecanismos de seguridad correspondientes. Ante la necesidad explícita de negocio u operación se deberá evaluar a nivel de CSI este tipo de conexiones.

c. Se prohíbe realizar monitoreo de red no autorizada que permita conocer la navegación de los usuarios y/o acceder a información altamente confidencial o de uso personal.

- **Cambios en páginas web**

a. Los colaboradores de la UNAM no están autorizados para crear, modificar páginas de internet, a no ser que existiera una autorización del área de tecnologías de la información.

3.2 Uso personal

a. Los colaboradores de la UNAM que tienen acceso a internet y la usan para uso personal que no estén relacionadas con las labores de la organización, deberán utilizarlo en sus horas libres mas no en el horario laboral.

- **Sitios ofensivos de internet**

a. Está terminantemente prohibido el ingreso a sitios cuyo contenido sea censurable, como, por ejemplo: material de tipo violento, sexista, racista, sexualmente explícito o potencialmente ofensivo.

- **Bloqueo de sitios y filtros de contenido**

a. La Jefatura de Soporte e Infraestructura TI es responsable del control de las licencias de software y/o recursos informáticos. En la UNAM, únicamente está permitido el uso de software licenciado y autorizado por la Jefatura de Soporte e Infraestructura TI.

b. La organización deberá establecer mecanismos para prevenir y detectar el ingreso de software malicioso. Los usuarios, desde su incorporación en la compañía, tienen conocimiento del “Reglamento de Uso de PC”, donde se les indica cómo hacer uso eficiente de los recursos informáticos.

c. Es responsabilidad del área de Soporte e Infraestructura TI la actualización y habilitación del software antivirus en todas las computadoras y servidores de la UNAM.

d. Todas las descargas realizadas de Internet, los mails entrantes y los archivos introducidos por cualquier medio en la red de la UNAM deben ser examinados por el software de antivirus.

e. Los usuarios que identifiquen la existencia de algún virus deberán comunicar al área de SI mediante el buzón de seguridad (seguridad.informacion@unam.edu.pe) y al área de Soporte e Infraestructura TI. Lo mismo aplica a cualquier medida de protección que se considere desactualizada, que no esté funcionando correctamente o cuando se detecte algún comportamiento sospechoso en los sistemas.

f. La UNAM puede restringir o bloquear el acceso a sitios de Internet, así como impedir la descarga de ciertos tipos de archivo, incluyendo los archivos gráficos y de música, que contravengan la presente política.

g. El Oficial de Seguridad de la Información deberá supervisar y mantener una lista de los elementos bloqueados de Internet, la misma que debe ser actualizada automáticamente o expandible según el nivel de riesgo aceptable en la empresa. Dicha lista deberá ser de conocimiento de las Vicepresidencias y de los propietarios del(los) activo(s) de información.

3.3 Confidencialidad de la Información

- **Intercambio de Información**

a. El intercambio de software o de datos por Internet, exceptuando el correo electrónico, entre la UNAM y otra entidad no deberá realizarse, a menos que exista un acuerdo por escrito que especifique los términos del intercambio y el modo de protección del software y los datos.
b. No se debe utilizar el internet para el envío de información Confidencial de la UNAM, a menos que haya sido encriptada y autorizado por el CSI de la UNAM y validados por el OSI.
c. Es necesario considerar en este punto lo contemplado en la "Política de Uso y Seguridad del Correo Electrónico"

- **Exposición de información**

a. Los colaboradores de la UNAM no deben colocar información Altamente Confidencial de la UNAM en ningún equipo informático accesible por Internet, que soporte el servicio FTP anónimo o servicios similares, a no ser que la exposición de éstos datos haya sido autorizada por el CSI.

- **Eliminación de mensajes**

a. Los mensajes enviados por colaboradores de la UNAM a los grupos de discusión, a boletines electrónicos y otros de la internet, que incluyan una afiliación implícita o explícita con la UNAM, pueden eliminarse por iniciativa de las Gerencias de la UNAM, si esta considera que los mismos no están alineados con los intereses de la universidad o con la política vigente de la UNAM.

b. Divulgación de información Confidencial

a. Los colaboradores de la UNAM no deben divulgar información Altamente Confidencial de la Universidad a través de Internet, si se identifica la publicación de este tipo de información en los medios se procederá con la aplicación de la política de sanciones.

c. Divulgación Involuntaria

a. Está prohibida la divulgación de Información Altamente Confidencial en Internet por los colaboradores de la UNAM.

d. Uso de Redes sociales desde las estaciones de trabajo

a. El uso de redes sociales debe ser utilizado responsablemente y en horario no laborable. Se encuentra prohibido divulgar información confidencial o que perjudique la reputación de la empresa en las redes sociales.

4. INCUMPLIMIENTO

d. El incumplimiento de esta política puede generar la materialización de riesgos de infección de equipos informáticos, fuga o exposición de información altamente confidencial de la compañía, entre otros; pudiendo afectar la confidencialidad, integridad y disponibilidad de la información confidencial de la empresa.

e. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN EN CONTRATOS CON TERCEROS

1. OBJETIVO

La política de seguridad de información en contratos con terceros tiene por objetivo definir y establecer los roles y responsabilidades de terceros, así como establecer controles que permitan reducir los riesgos de seguridad de la información asociados a los servicios brindados por terceros a la UNAM. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2013 Anexo A

2. ALCANCE

Esta política tiene alcance de aplicación a todos los contratos o acuerdos existentes entre la UNAM y terceros (proveedores de servicios, outsourcing, asesores, contratistas, entre otros).

3. REQUISITOS DE SEGURIDAD ANTES DE LA CONTRATACÍON

a. Cuando la empresa requiera la contratación de terceros, el Oficial de Seguridad de la Información en coordinación con el Gestor de Servicios y el área Legal deben realizar la evaluación de riesgo de seguridad de

información a fin de definir principalmente: el tipo de acceso requerido, sustento del acceso solicitado, clasificación de la información / evaluación de impacto, medidas de mitigación y control. Lo definido en la evaluación de riesgos deberá documentarse en el contrato.

b. El acceso de terceros a la información, sistemas de información, instalaciones de procesamiento, instalaciones administrativas u otras áreas de servicios críticos se aplicará sólo luego de la implementación de controles apropiados y la firma respectiva del contrato y/o acuerdo que defina las condiciones para la conexión o el acceso. Asimismo, es responsabilidad del Gestor de Servicios solicitar a las áreas pertinentes (Soporte e Infraestructura TI, Seguridad de la Información, Administración) estos accesos. No está permitido el acceso a los datos personales (información sensible[1]) y datos de titulares de tarjetas, las alternativas a este acceso tendrán que ser evaluado por el Oficial de Seguridad de la Información y Soporte e Infraestructura TI.

c. Los terceros que presten servicios a la UNAM, deben firmar el respectivo contrato y acuerdo de confidencialidad. El contrato debe definir el tipo de información tratada (intercambiada, transferida, almacenada) y el objetivo de hacerlo. Si la información que se intercambia, transfiere, almacena o trata entre las partes es confidencial o sensible, el acuerdo de confidencialidad puede formar parte del mismo contrato (cláusula) o como un acuerdo separado.

[1] Datos de la esfera más íntima de la persona (p.e. huella digital, ingresos económicos, entre otros)

d. Los terceros que como parte del servicio traten datos personales de clientes, proveedores, empleados, entre otros; deberán firmar un acuerdo (p.e. cláusula) respecto al conocimiento de las medidas requeridas por la Ley N° 29733 - Ley de Protección de Datos Personales y su adecuación o alineamiento.

e. La información involucrada en el servicio del tercero debe ser clasificada y controlada de acuerdo a la política de clasificación de información de la UNAM. Para el intercambio o transferencia de información entre La UNAM y el tercero, esta deberá estar adecuadamente clasificada y etiquetada.

f. La conexión entre sistemas de la UNAM y los sistemas de terceros deberá ser aprobada por el OSI a fin de comprometer la seguridad de la información.

4. REQUISITOS DE SEGURIDAD DURANTE EL SERVICIO

a. El Gestor de Servicio deberá validar que las condiciones de entrega de servicio del tercero se den según lo definido antes de la contratación.

b. El área de SI es responsable de realizar una visita anual a los proveedores que realicen el tratamiento de información sensible (datos sensibles de clientes, datos de titulares de tarjetas, entre otros) de la UNAM con el objetivo de validar el cumplimiento de los requisitos de seguridad exigidos a nivel contractual (referentes a la Ley de Protección de Datos Personales). Al respecto se emitirá un informe con los resultados de la evaluación.

5. REQUISITOS DE SEGURIDAD AL TÉRMINO DEL VÍNCULO CONTRACTUAL

a. Todo Gestor de Servicio debe informar al área de Soporte e Infraestructura TI, Administración y al OSI, sobre la culminación del vínculo contractual con el tercero y/o sus empleados con la finalidad de asegurar el retorno de los activos de la empresa, la restricción de los accesos a las instalaciones y a los sistemas de información de la UNAM.

b. El área de SI debe registrar en una bitácora los terceros que brindan algún tipo de servicio a la UNAM y que como parte del servicio se considere el tratamiento (intercambio, transferencia, almacenamiento) de información Confidencial (p.e. datos personales).

6. INCUMPLIMIENTO

a. El incumplimiento de esta política puede generar la materialización de riesgos asociado a los servicios de terceros con la UNAM, lo cual compromete los activos de información de la compañía (sistemas, correo electrónico, servicios) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la empresa.

b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Reglamento Interno de Trabajo de la UNAM.

CONCLUSIONES

Primera

Se comprobó la idoneidad de la norma ISO/IEC 27001 por su versatilidad en la aplicación de cada uno de sus lineamientos y que son altamente compatibles con la realidad de la institución que fue sujeta de investigación.

Segunda

La propuesta del plan de seguridad de información alineado a la norma ISO/IEC 27001 para la Universidad Nacional de Moquegua, fue validado satisfactoriamente por 03 expertos, logrando altos niveles de validez en cada uno de los acápites evaluados.

RECOMENDACIONES

Primera

Realizar charlas de capacitación al personal docente, administrativo y estudiantes sobre la norma ISO/IEC 27001, explicando que la Universidad Nacional de Moquegua cuenta con un plan de seguridad alienado a la mencionada norma y que los procedimientos que se establecen en los diferentes trámites académicos y administrativos, responden al mencionado plan.

Segunda

El plan de seguridad de información alineado a la norma ISO/IEC 27001 para la Universidad Nacional de Moquegua, debe ser revisado anualmente por expertos en seguridad informática, con la finalidad de implementar medidas que permitan mejorar y reforzar los procesos, teniendo en consideración la rapidez de los cambios en el contexto actual.

BIBLIOGRAFÍA

Aguirre, J., & Aristizabal, C. (2013). *Diseño de Sistema de Gestion de Seguridad de la Informacion para el Grupo Empresarial La Ofrenda.* Pereira: Universidad Tecnológica de Pereira.

Barahona, J., & Garzón, E. (2014). *Auditoría de los riesgos informáticos en el Departamento de Tecnología de la empresa KUBIEC usando COBIT 4.1 y la norma ISO/IEC 27001 como marco de referencia.* Quito: Escuela Politécnica Nacional.

Bernal, C. (2010). *Metodología de la investigación.* Bogotá: Pearson.

Buenaño, J., & Granda, M. (2009). *Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001-27002.* Guayaquil: Universidad Politécnica Salesiana.

Gesconsultor.com. (2012). *Gobierno T.I. Riesgo Cumplimiento* . Recuperado el 15 de Enero de 2016, de http://www.gesconsultor.com/iso-27001.html

Gonzáles, A., & Tenemaza, D. (2012). *Análisis de riesgos y vulnerabilidades de la red de datos de la empresa Plywood Ecuatoriana S.A. utilizando el estándar ISO/IEC 27005:2008.* Quito: Escuela Politécnica Nacional.

Hernández, R., Fernández, C., & Baptista, P. (1991). *Metodología de la investigación.* México DF: Mc Graw Hill Interamericana .

ISO 2007.es. (2012). *El Portal ISO 2007 en español*. Recuperado el 8 de Setiembre de 2015, de http://www.iso27000.es/download/doc_sgsi_all.pdf

McGraw Hill. (2012). *Glosario de términos de programación*. Recuperado el 8 de Setiembre de 2015, de https://www.mhe.es/universidad/informatica/8448136640/archivos/apendice_general_4.pdf

Oliván, A. (10 de Diciembre de 2017). *Guía de controles de ciberseguridad para la protección integral de la Pyme.* Obtenido de UOC/UAB/URV/UIB: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73066/6/aolivan1TFM0118memoria.pdf?fbclid=IwAR1d4e5kOPpvRmLSqi74NrsDXlAc1jIkCPxh8QXsKNxZz40FCjTtzcT8QdE

Pallas, G. (2009). *Metodlogia de Implantacion de un SGSI en un grupo empresarial jerarquico.* Montevideo: Instituto de Computación – Facultad de Ingeniería. Universidad de la República.

Pino, R. (2016). *Metodología de la investigación.* Lima: San Marcos.

Sandoval, C. (2014). *Analisis de la Norma ISO/IEC 27001. Diseño de Implementacion en la red de una empresa.* Guayaquil: Universidad Católica de Santiago de Guayaquil.

Talavera, V. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la norma ISO/IEC 27001:2013.* Lima: Pontificia Universidad Católica del Perú.

Valderrama, S. (2016). *Pasos para elaborar proyectos de investigación científica.* Lima: San Marcos.

Villena, M. (2006). *Sistema de Gestion de Seguridad de Informacion para una Institucion Financiera.* Lima: Pontificia Universidad Católica del Perú.

Welivesecurity.com. (2012). *Glosario*. Recuperado el 6 de Setiembre de 2015, de http://www.welivesecurity.com/la-es/glosario/#Z

White, S. (26 de Diciembre de 2017). *Network World España*. Obtenido de ¿Qué es COBIT? Un marco para la alineación y la gobernanza: https://www.networkworld.es/archive/que-es-cobit-un-marco-para-la-alineacion-y-la-gobernanza

Zorrila, S. (1993). *Introducción a la metodología de la investigación.* México DF: León y Cal.