“Responsabilidad con pensamiento positivo”

UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN

CARRERA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

TEMA:

“PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON LA NORMA ISO/IEC 27001 – 27002 VER. 2013, PARA EL DEPARTAMENTO DE SISTEMAS Y RECURSOS TECNOLÓGICOS DE LA UNIVERSIDAD ISRAEL”

AUTOR:

Edison Rolando Reinoso Diaz

TUTOR:

Msc. Wilmer Valle

TUTOR TÉCNICO:

Msc. Tannia Mayorga

AÑO 2017

UNIVERSIDAD TECNOLOGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Graduación certifico:

Que el Trabajo de Graduación **"Propuesta de Sistema de Gestión de Seguridad de la Información con la norma ISO/IEC 27001 – 27002: 2013, para el Departamento de Sistemas y recursos tecnológicos de la Universidad Israel",** presentado por Edison Rolando Reinoso Diaz, estudiante de la carrera de Ingeniería de Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, julio 2017

TUTOR

Msc. Wilmer Valle

CC: 1709343071

AUTORIA DE TESIS

El presente Proyecto de Investigación titulado: **"Propuesta de Sistema de Gestión de Seguridad de la Información con la norma ISO/IEC 27001 – 27002: 2013, para el Departamento de Sistemas y recursos tecnológicos de la Universidad Israel"**, es de manera original, y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Quito, julio 2017

AUTOR

Edison Rolando Reinoso Diaz

CC: 1712790623

DERECHOS DE AUTOR

Autorizo a la Universidad Tecnológica Israel, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Quito, julio 2017

AUTOR

Edison Rolando Reinoso Diaz

CC: 1712790623

DEDICATORIA

El presente trabajo se lo dedico a Dios por darme la oportunidad de estar rodeado de gente maravillosa, porque día a día me ha dado las fuerzas para seguir adelante, por bendecirme con una familia hermosa.

También se la dedico a mi esposa e hija, quienes han estado conmigo en todo momento, brindándome su apoyo.

A toda mi familia, que de forma directa o indirecta han colaborado con la finalización de una meta en mi vida.

Edison Rolando Reinoso Diaz

AGRADECIMIENTO

Agradezco a Dios, a mis padres, esposa e hija por no dejarme desmayar y seguir adelante para culminar la meta propuesta.

A la Universidad Israel por permitirme terminar la carrera de Ingeniería en Sistemas e infundir los conocimientos para seguir con la vida profesional, a los docentes que me brindaron sus conocimientos.

Mi más sincero agradecimiento a todos quienes fueron participes de la culminación de este trabajo.

Edison Rolando Reinoso Diaz

PÁGINAS PRELIMINARES

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN EJECUTIVO

La Dirección de Recursos Tecnológicos de la Universidad Tecnológica Israel en adelante UISRAEL, es la encargada de implementar y mantener toda la infraestructura tecnológica y activos de información de la universidad.

Con el fin de que todos los activos de la información se encuentren protegidos se propone un Sistema de Gestión de Seguridad de la información basado en la norma ISO 27000:2013, la misma que permitirá proteger la integridad, disponibilidad y confidencialidad de la información.

Para el desarrollo del presente proyecto se realizó un análisis de la situación actual de la Dirección de Recursos Tecnológicos, mediante entrevistas y cuestionarios realizadas a la persona responsable de las diferentes áreas de la dirección, y un análisis a la red interna de la universidad, lo que ayudo a tener una visión de la protección que se le da a la información.

La fase del análisis se basó en la norma ISO 27001:2013, donde se realizó el desarrollo de las matrices de riesgos que se estipulan a partir del capítulo III, para determinar la probabilidad e impacto de las vulnerabilidades, lo siguiente fue el desarrollar políticas de seguridad basándonos en la norma ISO 27002:2013 como son: control de acceso, perímetros de seguridad, proceso de contratación y cesación de actividades de empleados entre las más importantes, luego de realizar las políticas de seguridad los dos últimos dominios tratan específicamente sobre la continuidad del negocio y cumplimiento de las políticas de seguridad creadas en los dominios anteriores las cuales están anexadas en el manual de buenas prácticas.

SUMMARY

The Technological Resources Department of the Israel Technological University -UISRAEL- is in charge of implementing and maintaining the technological infrastructure and information assets of the university.

In order for all information assets to be protected, an Information Security Management System based on ISO 27000: 2013 is proposed, which will protect the integrity, availability and confidentiality of information.

For the development of this project, an analysis of the current situation of the Technological Resources Department was carried out. It used interviews and questionnaires made to the person responsible for the different areas of management, and an analysis to the internal network of the university, which helped to have a vision of the protection that is given to the information. The analysis period began with the development of risk matrices to determine the likelihood and impact of vulnerabilities, which allowed the development of security policies based on ISO 27002: 2013, among the most important policies that were developed are: access control, security perimeters, hiring process and cessation of employee activities. After conducting security policies, the last two domains deal specifically with business continuity and compliance with security policies created in previous domains, which are annexed in the manual of good practices

CAPITULO I

1 Introducción

Debido a la gran evolución de la tecnología y la poca capacitación que se realiza a los usuarios para su desenvolvimiento profesional, día a día crece las amenazas, vulnerabilidades y riegos contra la seguridad de la información de una institución, por lo tanto, es necesario proteger uno de sus activos más valiosos “la información”, a fin de garantizar la confidencialidad, integridad y disponibilidad.

En la actualidad, el panorama está lleno de diversos escenarios de riesgos tales como: la fuga de información, el mal uso de la información, ingeniería social, entre otros, que van apareciendo con el fin de obtener información confidencial y hacer mal uso de la misma.

Para poder garantizar un nivel de protección de los activos de información se debe realizar un análisis adecuado de gestión de riesgos bajo normas y estándares sugeridos en la norma ISO 27001:2013 y así identificar esfuerzos hacia aquellos elementos que se encuentran más expuestos.

El propósito de un sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001 y 27002:2013 es, por lo tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Con estas normas se guiará para la propuesta de implementación de un Sistema de Gestión de Seguridad de la Información, conjuntamente con los controles de seguridad para la institución y de las buenas prácticas para gestionar la seguridad de la información.

1.2 Planteamiento del problema

En el departamento de Sistemas de la Universidad Tecnológica "Israel", se puede observar y detectar la falta de estándares, políticas o normas de Seguridad de la información, en tal razón se plantea el presente proyecto con el fin de realizar el análisis para la implementación de la normativa ISO/IEC 27001 – 27002:2013, la cual ayudará al departamento de sistemas con la protección de los activos de la información en la institución.

Para argumentar el proyecto se tendría que formular estas interrogantes:

- ✓ ¿La universidad tiene estrategias preventivas y planes de contingencia para minimizar los riesgos en el manejo de la información ante incidentes?
- ✓ ¿Cuáles son los beneficios de la gestión de seguridad de la información en los activos de la universidad?
- ✓ ¿Cómo generar conciencia de seguridad en los trabajadores, estudiantes y docentes sobre la información que procesa y difunde la universidad?

Con estas pocas interrogantes aclaradas podremos empezar con la investigación de los activos de información y con el respaldo de las autoridades responsables se realizará el estudio y análisis para optimizar los recursos tecnológicos y humanos de la institución.

Organigrama de la Universidad Tecnológica Israel

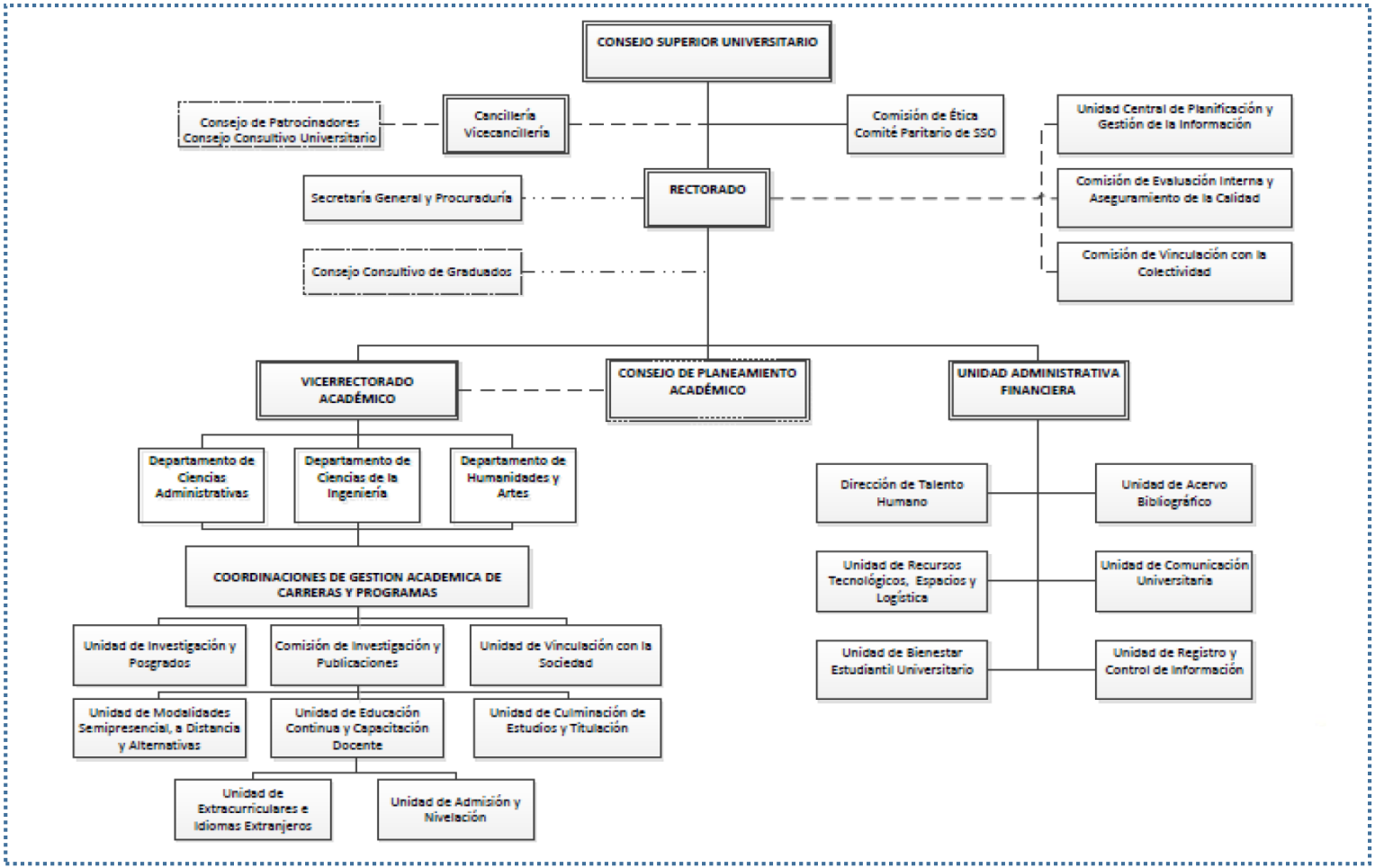

Gráfico No. 1: Estructura Orgánica de la UISRAEL
Elaborado por: Universidad Tecnológica Israel
Fuente: https://uisrael.edu.ec/wp-content/uploads/2016/05/PEDI-2014-2017.pdf

1.3 Solución del Problema

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos, con la información recabada el presente proyecto reúne la información necesaria para la propuesta de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2013 para así garantizar la protección de los activos de información y otorgar confianza a cualquiera de las partes interesadas.

La correcta implementación de un SGSI dentro de la institución, ayudará a prevenir incidentes de seguridad, que generan pérdidas económicas e interrupciones en la continuidad del negocio, mediante la reducción de las probabilidades o impactos que los riesgos identificados pudieran ocasionar a su información.

1.4 Objetivos

1.4.1 Objetivo general

Realizar la propuesta de Sistema de Gestión de Seguridad de la Información con las Normas ISO/IEC 27001 – 27002: 2013 para el Departamento de Sistemas y Recursos Tecnológicos de la UISRAEL.

1.4.2 Objetivos específicos

- ✓ Analizar la información que se transmita de manera física o lógica

- ✓ Desarrollar una cultura en Seguridad de la Información orientada a la identificación y análisis de riesgos, promoviendo a través de las buenas prácticas y estándares de seguridad (formatos de requerimientos, bitácoras, publicidad, concientización entre otros).

- ✓ Establecer controles, minimizando los riesgos significativos y de alto impacto para la institución, como el robo o fuga de información, accesos no autorizados mal uso y/o cualquier otro daño que afecte a la divulgación indebida de la información confidencial, la alteración o modificación de la misma, y en general la continuidad de las operaciones y la reputación de la institución.

- ✓ Registrar la revisión de los problemas, fallas, eventos e incidentes de seguridad reportados, identificar las lecciones aprendidas para utilizarlas como fuente de mejora continua en las políticas de seguridad.

1.5 Hipótesis

Las políticas de seguridad de la información, minimizan los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios, entre otros factores.

La gestión de seguridad de la información contribuye a la calidad en el servicio y en la protección más segura de los activos de información como, por ejemplo: la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios, laboratorios de computación, infraestructura tecnológica, personal docente, administrativo, estudiantes y entre otros activos de la institución.

Los programas y talleres de capacitación de seguridad de la información crean conciencia de seguridad en los trabajadores, docentes, alumnos y terceros para un buen uso de la información.

1.5.1 Señalamiento de variables

a) Variables Independientes

- ✓ Control de seguridad
- ✓ Nivel de compromiso
- ✓ Infraestructura tecnológica
- ✓ Madurez de procesos

b) Variables Dependientes

- ✓ Madurez de la seguridad de la información
- ✓ Vulnerabilidades en los procedimientos
- ✓ Amenazas

1.6 Alcance y limitaciones

1.6.1 Alcance

El alcance del proyecto abarca en la Propuesta de un Sistema de Gestión de Seguridad de la información con normas ISO/IEC 27001 y 27002:2013, para la Universidad Tecnológica Israel, el cual se aplicará al Departamento de Tecnología, el cual está orientado a cubrir la propuesta de un Sistema de Gestión de Seguridad de la Información, el proceso de análisis se basará en la clasificación de activos de información y valoración de riesgos.

En el transcurso del desarrollo del proyecto se realizará el manual de políticas basado en la norma ISO 27002:2013 para la institución.

1.6.2 Limitaciones

El proyecto consistirá solo en el análisis y desarrollo de políticas del Sistema de Gestión de Seguridad de la Información para la Universidad Tecnológica Israel, basado en la norma ISO-IEC 27001 y 27002:2013, pero no abarca las fases de implementación, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

CAPITULO II

2 Marco teórico

Al mencionar información nos referimos, sin importar la forma que esta adopte, como documentación impresa o escrita, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Este activo se debería proteger de forma correcta mediante los controles de seguridad independientemente de la forma que este tome o los medios por los que se comparta o almacene, las políticas y procedimientos de seguridad de la información surgen como una herramienta a la necesidad de la institución para concientizar a cada uno de los miembros de la institución sobre la importancia a la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la misma.

Para el proyecto propuesto nos basaremos en las normas: ISO/IEC 27001 y 27002: 2013.

La norma 27001 de BSI (British Standards Institution) BS7799-Parte 2, fue publicada por primera vez en 1998 y ya era un estándar certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005, la cual ha ido realizando los cambios evolutivos para que no sea redundante con los requerimientos de implementación, ya que en actualidad tenemos la ISO/IEC 27001 :2013. [1]

La norma ISO 27001:2013 es una norma internacional que permite el aseguramiento de la confidencialidad e integridad de los datos y de la información de cualquier organización, así como de los sistemas que la procesan. Esto permite a las organizaciones salvaguardar la información que

custodian, sobre todo en la red y formatos digitales, evaluando objetivamente los riesgos y definiendo una serie de medidas para eliminarlos o reducirlos al máximo.

El estándar internacional ISO/IEC 27001 y 27002:2013, están orientados a establecer un sistema de gestión que permite identificar, atender y minimizar el riesgo, protegiendo la información en las empresas, de amenazas internas y externas, garantizando así la disponibilidad, confidencialidad e integridad. [1]

Precisamente por ello, la presente investigación se orienta a demostrar que una gestión de seguridad de la información basada en el análisis de vulnerabilidades y en políticas de seguridad, resultará exitosa si se toma muy en cuenta todas las necesidades concretas de la Universidad en la Dirección de Tecnología para que contribuya con eficacia y calidad en los servicios críticos de la institución, ya que por el creciente ambiente interconectado de negocios (correos, blogs, VoIP, etc.) la información está expuesta en el medio, es por eso que va aumentando los riesgos en sus diferentes activos y se exponen a nuevas amenazas y vulnerabilidades, razón por la cual la institución debe prever los medios necesarios para evitar el robo y manipulación de sus datos confidenciales ya sean estos por accesos no autorizados o fuga de información. [2]

La norma ISO/IEC 27001 nos recalca que "La información es un activo que, como otros activos comerciales importantes, tiene valor para la institución y, en consecuencia, necesita ser protegido adecuadamente". [2]

La norma internacional proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la

Información, en adelante lo abreviaremos como SGSI. La adopción de un SGSI debería ser fruto de una decisión estratégica de la institución. El diseño y la implementación del SGSI dependen de las necesidades y objetivos de cada institución, así como de sus requisitos de seguridad, sus procesos, su tamaño y estructura.

Esta norma internacional sigue el modelo Planificar-hacer-verificar-actuar (Plan-Do-Check-Act conocido como modelo PDCA), que se aplica para estructurar todos los procesos del SGSI. La figura 1 muestra cómo un SGSI, partiendo de los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios, produce los elementos de salida de seguridad de la información que responden a dichos requisitos y expectativas. [3]

Es previsible que estos factores y los sistemas que lo soportan cambien con el tiempo. Lo habitual es que la implementación de un SGSI se ajuste a las necesidades de la institución.

Esta norma internacional sirve para cualquier parte interesada, ya se interna o externa a la institución, pueda afectar una evaluación de la conformidad.

La institución tiene que definir y gestionar numerosas actividades para funcionar con eficacia. Cualquier actividad que utiliza recursos y se gestiona de modo que permite la transformación de unos elementos de entrada en unos elementos de salida puede considerarse un proceso. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente.

La aplicación de un conjunto de procesos en la institución, junto con la identificación de éstos y sus interacciones y su gestión, puede calificarse de enfoque por proceso.

El enfoque por proceso para la gestión de la seguridad de la información que se describe en esta norma internacional anima a los usuarios a enfatizar la importancia de:

a) Comprender los requisitos de seguridad de la información de una institución y la necesidad de establecer una política de seguridad de la información y sus objetivos.

b) Implementar y operar los controles para administrar los riesgos de seguridad de la información de una institución en el marco de sus riesgos empresariales generales.

c) Supervisar y revisar el rendimiento y la eficacia del SGSI.

d) Asegurar la mejora continua sobre la base de la medición objetiva.

La norma ISO/IEC 27002:2013 ofrece una guía de buenas prácticas para la implementación de controles que permiten gestionar de manera adecuada la seguridad de la información. La norma en cuestión fue publicada originalmente con el nombre de ISO 17799 describiendo los dominios de control y los mecanismos que pueden ser implementados dentro de una institución siguiendo las directrices que pauta la norma.

Esta norma consta de 14 dominios, 35 objetivos de control y 114 controles, los cuales estas alineados para la correcta gestión de la seguridad de la información de la institución, hay que

recalcar algo muy importante ya que esta norma no es certificable y la aplicación total o parcial en cada institución se realiza de forma totalmente libre y sin necesidad de una supervisión regular externa. Esta norma se la aplicará cuando el Honorable Consejo Directivo conjuntamente con la Dirección de Tecnología apruebe el Manual de Políticas que se adjunta al proyecto de investigación para la institución.

Entre los Controles de Seguridad dela norma 27002: 2013 podemos citar los siguientes:

- ✓ **Políticas de Seguridad**

Un documento denominado "política" es aquel que expresa una intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la institución. El contenido de las políticas se basa en el contexto en el que opera una institución y suelen ser considerados en su redacción los fines y objetivos de la institución, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la institución, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores (legales de obligado cumplimiento, del sector al que pertenece la institución, de la propia institución de niveles superiores o más amplios, ...) relacionadas. [5]

- ✓ **Aspectos Organizativos de la Seguridad de la Información**

El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la institución. Para ello se debería definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades. Para una actualización adecuada en materia de seguridad se debería

contemplar la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información. Las protecciones físicas de las organizaciones son cada vez más reducidas por las actividades de la institución requiere por parte del personal interno/externo que acceden a información desde el exterior en situación de movilidad temporal o permanente. En estos casos se considera que la información puede ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información. [6]

- ✓ **Seguridad Ligada a los recursos humanos**

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. [7]

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren

capacitados para respaldar la Política de Seguridad de la institución en el transcurso de sus tareas normales.

Suele ser responsabilidad del Área de Recursos Humanos incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarios respecto a las necesidades actuales en seguridad.

El Responsable del Área Jurídica participa en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las Políticas en seguridad y en el tratamiento de incidentes de seguridad que requieran de su intervención. [7]

- ✓ **Gestión Activos**

El objetivo del presente dominio es que la institución tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. [7]

Algunos ejemplos de activos son:

- ✓ Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- ✓ Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- ✓ Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBX, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- ✓ Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada por la propia institución. Se debería considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

- ✓ **Control de Accesos**

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. [7]

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

- ✓ **Cifrado**

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas. [7]

- ✓ **Seguridad física y Ambiental**

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la institución.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la institución, contra accesos físicos no autorizados. [8]

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la institución esté físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud). [9]

- ✓ **Seguridad en la Operativa**

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento. [9]

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permite garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada institución. [9]

Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la institución. [9]

Finalmente, se deberían verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

- ✓ **Seguridad en las Telecomunicaciones**

El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección. [9]

Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

- ✓ **Adquisición, desarrollo y Mantenimiento de los sistemas de información**

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. [10]

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Aplica a todos los sistemas informáticos, tantos desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la institución en donde residan los desarrollos mencionados. [10]

- ✓ **Relaciones con Suministradores**

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

La institución debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas. [10]

- ✓ **Gestión de Incidentes**

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno. [11]

Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

- ✓ **Aspectos de la SI en la Gestión de la Continuidad de Negocio**

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. [12]

Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

Minimizar los efectos de las posibles interrupciones de las actividades normales de la institución asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones

deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan, los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales.

- ✓ **Cumplimiento**

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la institución y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

- ✓ **Análisis de riesgos de seguridad de la información**

Antes de definir lo que es un análisis de riesgos, tenemos que considerar lo que es un riesgo, a continuación, se exponen las siguientes definiciones:

- **Riesgo:** Incidente o situación que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos.

- **Análisis de riesgo:** es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

  La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar.

  Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.

  Dentro del tema de análisis de riesgo se ven reflejados cinco elementos muy importantes dentro del concepto estos son los siguientes: probabilidad, amenazas, vulnerabilidades, activos e impactos.

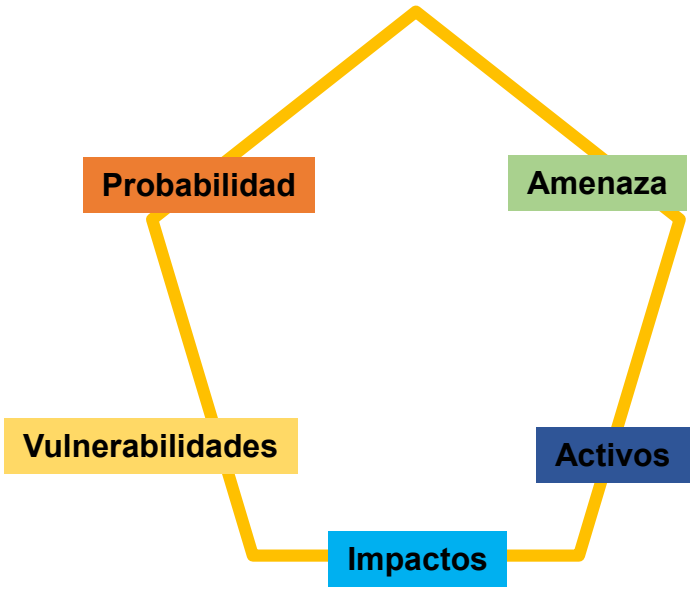

Gráfico No. 2: Análisis de Riesgos
Elaborado por: El Autor

- **Probabilidad:** establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

  Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con razonable objetividad su probabilidad de ocurrencia. Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad. Por ejemplo, el acceso no autorizado a datos; dónde se hacen estimaciones sobre la base de experiencias.

- **Amenazas:** las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

  Las amenazas pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

- **Vulnerabilidades:** son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

  Estas vulnerabilidades son de naturaleza variada. A modo de ejemplo se citan las siguientes: falta de conocimiento del usuario, tecnología inadecuadamente probada ("testeada"), transmisión por redes públicas, etc.

  Una vulnerabilidad común es contar con antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.

- **Activos:** Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

- **Impactos:** las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

  Se puede establecer que las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio. Otras no tan comunes, felizmente, son la pérdida de vidas humanas, afectación del medio ambiente, etc.

✓ **Identificación de Vulnerabilidades**

Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinan vulnerabilidades a nivel del sistema operativo y firewall.

✓ **Limitantes del análisis de riesgo**

En general, a pesar de que se han desarrollado muchas soluciones a los problemas de la seguridad en los sistemas de información, la apreciación general es que la inseguridad es un problema que no ha sido resuelto. La perspectiva parece poco optimista, principalmente debido a que los atacantes han pasado de ser aficionados en busca de notoriedad a criminales en busca de lucro.

- ✓ **Priorización de Riesgos**

En este paso de la estimación de riesgos, se estiman su prioridad de forma que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico se puede dejar en un segundo plano.

Sin importar cuál sea el proceso que se siga, el análisis de riesgos comprende los siguientes pasos:

1. Definir los activos informáticos a analizar.
2. Identificar las amenazas que pueden comprometer la seguridad de los activos.
3. Determinar la probabilidad de ocurrencia de las amenazas.
4. Determinar el impacto de las amenazas, con el objeto de establecer una priorización de las mismas.
5. Recomendar controles que disminuyan la probabilidad de los riesgos.
6. Documentar el proceso

Cuando ya hemos realizado este análisis no tenemos más que presentar nuestras cuentas a los responsables de la institución (o adecuarlas al presupuesto que un departamento destina a materias de seguridad), siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza ha de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Hemos de tener siempre presente que los riesgos se pueden minimizar, pero nunca eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención ante un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas

proactivas (aquellas que se toman para prevenir un problema) y medidas reactivas (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

El proceso de análisis debe ser el más importante de la gestión de seguridad de la gestión de seguridad de la información de la institución, ya que por medio de esto se decide la toma de decisiones en eliminar, ignorar, mitigar y controlar, e decir aplicar la gestión de riesgos basados en la compleja tarea de determinar, analizar, evaluar y clasificar los activos de la información más importantes según la criticidad de los mismos.

CAPITULO III

3 Metodología

Para el desarrollo del proyecto y dar cumplimiento al primer objetivo, el modelo a emplearse será PHVA (Planear, Hacer, Verificar, Actuar), basado en la norma ISO/IEC 27001:2013.

Este modelo nos guiara para poder realizar el análisis y estudio de los activos de información que son parte de la institución.

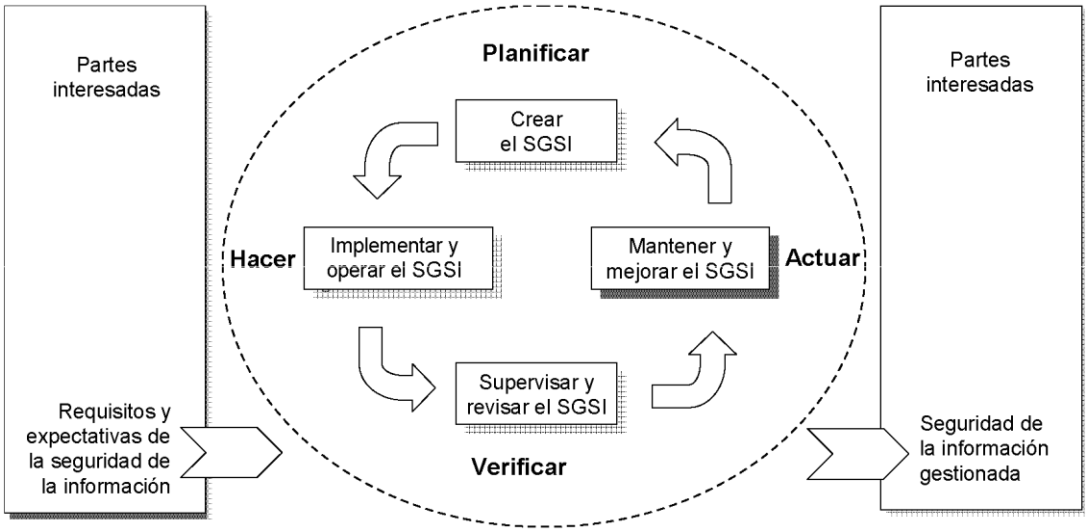

Gráfico No. 3: Modelo PDCA aplicado a los procesos del SGSI
Elaborado por: Norma ISO/IEC 27001:2005
Fuente: https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

- ✓ **Planificar (creación del SGSI):** Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la institución.

- ✓ **Hacer (implementación y operación del SGSI)**: Implementar y operar la política, controles, procesos y procedimientos del SGSI.

- ✓ **Verificar (supervisión y revisión del SGSI):** Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.

- ✓ **Actuar (mantenimiento y mejora del SGSI):** Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.

3.1 Modalidad de la investigación

La presente investigación considera las siguientes modalidades:

- ➢ *De campo.* - Para esta investigación de procedió a realizar encuestas a los estudiantes y al departamento de tecnología de la institución para poder fundamentar la propuesta del proyecto.

- *Bibliografía documentada.* - A través de libros, internet, tesis, las cuales han servido como sustentó de fuentes para recolectar información, que sirvió para la realización del proyecto.

3.2 Recolección de Información

La recolección de información se realizó a través de entrevistas y cuestionarios al personal encargado de la administración del departamento de tecnología de la institución, adicional se investigó mediante libros físicos y digitales, artículos científicos, internet.

3.3 Procesamiento de análisis de información

Para el procesamiento y análisis de la información se necesitó de los siguientes pasos:

- ✓ Elaboración de cuestionarios para el personal de tecnología y estudiantes
- ✓ Organizar la información
- ✓ Tabulación de la información suministrada
- ✓ Informe de resultados

3.4 Servicio crítico de la institución

Se considera servicio crítico a : Matrícula, Admisión y Registros, grados y títulos, tesorería, ya que estas áreas tienen y manejan información muy sensible, es por esto que los sistemas de información están en constante amenaza de intrusos tanto internos como externos y es necesario evaluar el riesgo que tienen, por tal razón se recomienda la implementación de un sistema de gestión de seguridad de la información para adoptar las políticas que ayudaran a la institución a

mejorar sus servicios con calidad y la seguridad para los alumnos, docentes y los mismos empleados.

3.5 Población y Muestra

3.5.1 El Universo

Las unidades básicas objeto de investigación la conforman los empleados y los estudiantes de la institución:

- ✓ Honorable Consejo Directivo
- ✓ Directores
- ✓ Coordinadores
- ✓ Personal Administrativo
- ✓ Personal Docente
- ✓ Estudiantes

Cuya población se totaliza en:

Personal Docente:	63
Personal Administrativo:	47
Estudiantes:	1945

Datos tomados de la página web de la universidad:

- ✓ https://uisrael.edu.ec/wp-content/uploads/2017/07/Padr%C3%B3n-Electoral-elecciones-agosto-2017-Proofesores-e-Investigadores-1.pdf

- ✓ https://uisrael.edu.ec/wp-content/uploads/2017/07/Padr%C3%B2n-Electoral-elecciones-agosto-2017-Servidores-y-Trabajadores-1.pdf

- ✓ https://uisrael.edu.ec/wp-content/uploads/2017/07/padron-electoral-estudiantes-estudiantes.pdf

3.5.2 Muestra

Para el estudio y análisis de datos, se realizó un muestreo intencional de los criterios para la selección dentro de la población consistieron:

- ✓ Director y o Coordinador, posee un amplio conocimiento de los procesos y actividades que deben realizar y que mantenga un rol de ejecutor en la toma de decisiones.

- ✓ Estudiante de la institución que realiza actividades en los laboratorios de cómputo para llevar a cabo las actividades que su rol exige.

Es factible que un número de 25 personas entre personal administrativo, docente y estudiantil a entrevistar y encuestar se puede lograr una apreciación muy real de la situación actual, ya que el análisis se centra sobre el grupo de personas que cumplen un papel relevante en los procesos de la institución.

3.6 Operacionalización de variables e indicadores

Variable	Definición Conceptual	Dimensiones	Indicadores
Controles de Seguridad	Los controles de seguridad ayudan a regular las actividades realizadas sobre la información	Divulgación de las medidas de seguridad	Políticas de seguridad que los usuarios deben conocer y aplicar
			Medios determinados para la comunicación de las políticas de seguridad
		Valoración de las políticas de seguridad	Periodicidad en la verificación de la efectividad de las medidas de seguridad
			Periodos determinados para la evaluación interna
Nivel de compromiso	Es el nivel de apoyo que se brinda a los sistemas de seguridad de la información	Inversión realizada en la adquisición de recursos que permitan el control y monitoreo continuo de las políticas de seguridad	Adquisición de herramientas tecnológicas y/o contratación de personal especializado en gestión de la seguridad de la información
		Cumplimiento de los procedimientos y controles de la seguridad	Revisiones periódicas de las actividades establecidas de acuerdo al rol del usuario
Infraestructura Tecnológica	Es el conjunto de Software y Hardware que dan soporte al procesamiento y almacenamiento de datos	Seguridad brindada por los sistemas de procesamiento, transmisión y almacenamiento de datos	Periodos de revisión de la configuración de seguridad de los equipos de almacenamiento de datos.
			Periodos de evaluación de seguridad de los sistemas informáticos de procesamiento de datos
			Periodos de revisión de la seguridad en los sistemas de comunicación
Madurez de los procesos	La madurez de los procesos se refiere a la definición, estandarización, automatización y regulación de los procesos	Nivel de procesos de la institución	Evaluación del estado actual del proceso
Madurez de la seguridad de la información	La madurez de la seguridad de la información, implica el cumplimiento e implementación de los controles establecidos	Establecimiento de controles de seguridad de la información	Capacitaciones del personal
			Incidentes detectados sobre las políticas de seguridad
			Auditorías realizadas en las áreas administrativas
		Seguridad de la información a nivel de tecnologías de la información	Incidentes reportados en los equipos de cómputo de los usuarios
			Criterios determinados en las evaluaciones de los sistemas de información.
Vulnerabilidad en los procedimientos	Las vulnerabilidades se consideran como una falencia que puede ser explotada	Vulnerabilidades que se conocen y no han podido ser cubiertas	Histórico de las vulnerabilidades sobre las cuales se ha tomado acciones correctivas
			Vulnerabilidades encontradas y reportadas.

Variable	Definición Conceptual	Dimensiones	Indicadores
Amenazas	Es el conjunto de vulnerabilidades que se han detectado y significan un riesgo para la seguridad de la información	Identificación de las amenazas existentes	Reporte de amenazas detectadas
		Gestión sobre las amenazas	Procedimientos definidos para la gestión y control de amenazas
			Seguimiento sobre las amenazas criticas gestionadas.
			Histórico de la gestión de amenazas.

Tabla Nº 1.- Matriz de Operacionalización de Variables
Elaborado por: El Autor

3.7 Análisis e interpretación de resultados

Este proceso se realiza a través de las encuestas realizadas al personal de la institución dentro de las instalaciones, a continuación, el detalle:

1. *¿En la Universidad Tecnológica Israel se tiene implementadas políticas de seguridad de la información?*

Opción	Frecuencia
Si	0
No	10

Tabla Nº 2.- Políticas de Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

En esta encuesta se interpreta que 100% de los encuestados responden que no, la institución no cuenta con políticas de seguridad de la información

2. *¿Cuál sería el beneficio que tendría la institución al contar con políticas de Seguridad de la Información?*

Opciones	Frecuencia	%
Mayor seguridad en los medios de almacenamiento de información	8	50
Aumenta la productividad a través de consultas confiables	4	25
Calidad en el servicio para los alumnos, docentes y terceros	4	25
Otros	0	0
Total	**16**	**100**

Tabla Nº 3.- Beneficios de las Políticas de Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

Del total de repuestas marcadas el 50% considera que la mayor seguridad de los medios de almacenamiento de información es uno de los beneficios de usar políticas de seguridad de la información, un 25% apuesta por la calidad en el servicio a los alumnos y docentes y el otro 25% consideran que aumenta la productividad a través de consultas confiables.

3. *¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la Información?*

Medidas en la Gestión de seguridad de la información	Frecuen	%
Desarrollo de políticas de seguridad	10	37
Clasificación del acceso de la información	4	15
Capacitación de usuarios	4	15
Monitoreo y reportes de la actividades en la red	4	15
La continuidad del negocio después de incidentes	5	18
Otros	0	0
Total	**27**	**100**

Tabla Nº 4.- Prioridades de la Gestión de Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

Sobre qué medidas de seguridad de la información son las más prioritarias, un 37% considera el desarrollo de políticas de seguridad, un 18% opina que la continuidad del negocio es muy importante y en un 15% consideran a la capacitación de usuarios, clasificación y acceso a la información y monitoreo de las actividades de la red informática de la UISRAEL.

4. ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?

Errores más comunes cuando se usa Internet y el correo electrónico	Frecuenc	%
Omitir la seguridad como un aspecto fundamental de configuración del Servidor	4	25
Transmisión en pleno texto de contraseñas	4	25
Uso inadecuado de herramientas de seguridad, o no uso alguno	3	19
Obtener y mantener programas y aplicaciones (software) que son vulnerables	5	31
Otros	0	0
Total	**16**	**100**

Tabla Nº 5.- Errores más comunes en el uso de Internet y Correo
Elaborado por: El Autor

Análisis de interpretación

Podemos apreciar que todos los errores mencionados son muy comunes cuando se usa Internet, pero sobresale con un 31% el obtener y mantener programas que son vulnerables. Le siguen como errores más frecuentes el omitir la seguridad al momento de configurar el servidor y la transmisión en pleno texto de contraseñas con un 25% y finalmente, otro error común es el uso inadecuado de herramientas de seguridad.

5. ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?

MF = Muy Frecuentes RF = Regularmente frecuentes PF = Poco frecuentes

Riesgos	MF	%	RF	%	PF	%
Fenómenos Naturales (Terremotos, Inundaciones)	0	0	0	0	10	38
Fallas mecánicas (Cortes de fluido eléctrico, incendios)	1	11	5	20	4	15
Divulgación ilícita de la información por el personal	0	0	7	28	3	12
Destrucción o modificación de la información	1	11	2	8	7	27
Intrusos al sistema de la red	2	22	6	24	2	8
Virus informáticos, gusanos, spam	5	56	5	20	0	0
Otros (Especifique)	0	0	0	0	0	0
Total	**9**	**100**	**25**	**100**	**26**	**100**

Tabla Nº 6.- Riesgos y frecuencia
Elaborado por: El Autor

Análisis de interpretación

Según el cuadro expuesto, los riesgos más frecuentes (MF) que se presentan en la UISRAEL son los virus informáticos, gusanos y spam "con un 56%, en segundo lugar, están "los intrusos al sistema de la red" con un 22% y el tercer lugar lo comparten "las fallas mecánicas" como los cortes de fluido eléctrico y "la destrucción y/o modificación de la información" con un 11%.

Los riesgos regularmente frecuentes (RF) se presentan en su mayoría por: divulgación ilícita de la información (28%), por los intrusos al sistema de la red (24%), por los cortes de fluido eléctrico (20%), por los virus informáticos (20%) y una minoría considera como riesgo regularmente frecuente la destrucción o modificación de la información por parte del personal (8%).

Los riesgos poco frecuentes (PF) se presentan ocasionalmente por fenómenos naturales como terremotos o inundaciones (38%), por la destrucción de la información por parte del personal (27%) y en algunos casos por los cortes de fluido eléctrico (15%).

6. *¿Sus equipos de cómputo en su oficina tienen fuente de poder interrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?*

Protección de equipos cómputo	Frecuencia	%
Si	6	80
No	4	20
Total	**10**	**100**

Tabla Nº 7.- Fuentes de energía interrumpible
Elaborado por: El Autor

Análisis de interpretación

Según la tabla del total de encuestados un 80% cuenta con equipos en sus oficinas para protegerse ante cortes de energía eléctrica y hay un considerable 20% que no tienen estos equipos de protección.

7. *¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?*

Incidencias que se dan con más frecuencia	Frecuencia	%
Saturación de la red por programas indebidos (música, video)	5	29
Uso del correo electrónico de la Universidad para otros fines	6	35
Olvido de contraseña	2	12
No realizar copias de respaldo	3	18
Otros: No organizar la información para mayor seguridad	1	6
Total	17	100

Tabla Nº 8.- Incidencias de usuarios
Elaborado por: El Autor

Análisis de interpretación

Del total de respuestas recogidas las incidencias más frecuentes son: el uso del correo electrónico de la Universidad para fines personales con 35% , la saturación de la red e Internet por programas indebidos (29%); y menos frecuentes pero que tampoco dejan de ser preocupantes son: los usuarios que no realizan copias de seguridad (18%) y el olvido de sus contraseñas (12%) y en la opción otros un 6% de respuestas coincidieron que existen usuarios que no organizan sus archivos, lo que genera también problemas de seguridad.

8. *¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?*

Ultima vez que participó a eventos	Frecuencia	%
Aproximadamente 3 meses	1	10
Aproximadamente 6 meses	3	30
Aproximadamente 1 año	4	40
Nunca	2	20
Total	10	100

Tabla Nº 9.- Asistencia a talleres de Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

El 20% del personal de Tecnología de la UISRAEL nunca ha asistido a eventos o talleres de seguridad de la información, pero también hay personas que conscientes del problema de seguridad han asistido de alguna manera a talleres o seminarios de seguridad de información, así un 40% ha asistido aproximadamente hace 1 año, un 30% ha participado aproximadamente hace 6 meses y un 10% ha asistido aproximadamente hace 3 meses.

9. ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

Disposición a talleres de Capacitación	Frecuencia	%
Muy interesado	8	80
Poco interesado	2	20
Nada interesado	0	0
Total	**10**	**100**

Tabla Nº 10.- Interés en asistir a talleres de Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

Del personal encuestado un 80% está muy interesado si se realizan programas y talleres de capacitación de seguridad de la información, existe un 20% que está poco interesado debido a que no consideran a la seguridad como una prioridad dentro de la universidad. Lo positivo es que no hay ningún personal que esté ajeno a la capacitación de seguridad.

10. ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad? ¿Por qué?

	Frecuencia	%
Si	7	70
No	3	30
Total	10	100

	Razones
Si	• No había Internet y por ende no había riesgos a la información • La Universidad como centro de investigación no debe tener restricciones en el acceso a la información
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

Tabla Nº 11.- Redes diseñadas en la Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

Sobre si las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad un 70% considera que sí, y las razones se han consolidado en el cuadro anterior. Por otra parte, un 30% opina lo contrario.

11. *¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?*

Impacto económico	Frecuencia	%
Muy beneficioso	6	60
Poco beneficioso	0	0
Nada beneficioso	4	40
Total	**10**	**100**

Tabla Nº 12.- Impacto económico de un plan de Gestión de Seguridad de la Información
Elaborado por: El Autor

Análisis de interpretación

Con respecto al impacto económico de implementar un plan de gestión de seguridad de la información en la gestión integral de la Universidad las apreciaciones se encuentran divididas pues si bien hay un 60% que lo considera muy beneficioso existe un 40% que piensa que es poco beneficioso. Por otro lado, no hay ningún personal que opina que el impacto económico no es beneficioso.

Mediante esta pequeña encuesta se pudo determinar que si la institución implementa un SGSI se beneficiará de manera inmediata con la calidad.

3.8 Evaluación de riesgos, vulnerabilidades y estrategias de seguridad

En este cuadro se muestran los riesgos y vulnerabilidades identificadas y las estrategias o medidas de seguridad necesarias para mitigar dichos riesgos.

Riesgos / Vulnerabilidades	Estrategias o medidas de seguridad a Aplicar
• Interés en obtener información estratégica de la Universidad por parte de la competencia, tales como información de postulantes para examen de admisión, información de alumnos regulares, planilla de pagos de docentes, etc. • Personal que trabaja la Universidad que se puede prestar para estas actividades desleales.	• Estándares de seguridad para servidores con sistemas operativos Windows y Linux. • Restricciones en el manejo de la información enviada por correo electrónico hacia redes externas. • Revisiones periódicas de los registros de los sistemas y operaciones realizadas por los usuarios.
• Pérdida de información ocasionada por la infección de virus informático.	• Adecuada arquitectura e implementación del sistema antivirus. • Verificación periódica de la actualización del antivirus de computadoras personales y servidores. • Generación periódica de reporte de virus detectados.
• Ausencia o exceso de contraseñas manejadas por los usuarios	• Uniformizar dentro de lo posible la estructura de las contraseñas empleadas y sus fechas de renovación • Implementar un sistema de Servicio de Directorio, el cual permita al usuario identificarse en él, y mediante un proceso automático, éste lo identifique en los sistemas en los cuales posee acceso.
• Falta de conciencia en seguridad de la información por parte del personal de la Universidad.	• Programa de capacitación de la Universidad en temas relacionados a la seguridad de la información.
• Arquitectura de red inapropiada para controlar accesos desde redes externas. • Posibilidad de acceso no autorizado a sistemas por parte de personal externo a la Universidad.	• Diseño de arquitectura de seguridad de red. • Adecuada configuración de elementos de control de conexiones (Firewalls). • Implementación y administración de herramientas de seguridad.

Riesgos / Vulnerabilidades	Estrategias o medidas de seguridad a Aplicar
• No existen controles con respecto a las copias de seguridad. Se realizan copias de seguridad, pero muchas veces no se ha probado que se puede recuperar la información.	• Establecimiento de un procedimiento formal que contemple la generación de una copia de respaldo para los usuarios. • Asegurar que la información del usuario se almacene en el servidor y estén protegidas por contraseñas.
	• Enviar fuera de la oficina una copia de seguridad completa una vez por semana.
• No existe un control de protección sobre los correos electrónicos no solicitados por los usuarios.	• Implementación y administración de herramientas para la inspección del contenido de los correos electrónicos recibidos
• Acceso abierto a redes inalámbricas por parte de intrusos	• Separación del segmento de red Inalámbrico mediante un firewall. • Configuración la red inalámbrica para permitir el tráfico sólo de los equipos de escritorio y portátiles de la oficina.
• Personal deja expuesto sus documentos	• Implementar la política de control para poder resguardar la información del usuario en sitios seguros. • Concientizar a los usuarios del uso de información.
• Identificación del Personal	• El 99% del personal no consta con un carnet el cual identifique si es empleado o no de la institución. • Se debería uniformar a la persona de administrativo y docente para mitigar el riesgo reputacional de la institución.

Tabla Nº 13.- Evaluación de riesgos, vulnerabilidades y estrategias de seguridad
Elaborado por: El Autor

3.9 Clasificación de activos de la institución

Mediante esta tabla identificamos los tipos de activos:

Tipo de activo	Descripción
Servicios	Contempla servicios prestados por el sistema
Datos / información	Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad.
Software	Programas, aplicativos, desarrollos, software base, sistema de información
Equipos informáticos	Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la institución
Personal	Personas relacionadas con los sistemas de información.
Redes de comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente
Equipamiento auxiliar	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones

Tabla Nº 14.- Clasificación de los activos
Elaborado por: El Autor

A continuación, se detallará el inventario de los activos de información que se pudieron identificar en la Dirección de Tecnología:

3.10 Inventario de activos de información de tecnología

No	Nombre del Activo	Descripción del Activo	Tipo de activo	Contenedor
A1	Centro Principal de Procesamiento	Centro Principal de procesamiento donde reside la infraestructura que soporta la operación del negocio	Instalaciones	Data Center
A2	Cuartos de comunicaciones	Instalación física donde residen los rack de comunicaciones	Instalaciones	Cuartos de rack
A3	Área administración de plataforma	Instalación física donde están ubicados los administradores de plataforma	Instalaciones	Área administración de plataforma
A4	Red LAN	Red LAN corporativa de la institución	Redes de comunicaciones	Red LAN
A5	Red WAN	Red WAN de la entidad	Redes de comunicaciones	Red WAN
A6	Red WIFI corporativa	Red Wifi utilizada por los equipos móviles para acceder a los recursos de la red corporativa de la institución	Redes de comunicaciones	Red LAN
A7	Red WIFI invitados	Red Wifi para invitados	Redes de comunicaciones	Red LAN
A8	Servidores de administración	Servidores que soportan los servicios bases de administración	Equipos informáticos	Data Center
A9	Servidores de bases de datos de producción	Servidores de producción que soportan los motores e instancias de bases de datos	Equipos informáticos	Data Center
A10	Servidores de aplicaciones de producción	Servidores de producción que soportan las aplicaciones y sistemas de información	Equipos informáticos	Data Center
A11	Plataforma de Correo	Servidores que soportan la plataforma y servicio de correo corporativo	Equipos informáticos	Data Center
A12	Servidores de Pruebas	Servidores que soportan los ambientes de prueba de la entidad	Equipos informáticos	Data Center
A13	Servidores de Desarrollo	Servidores que soportan los ambientes de desarrollo de la entidad	Equipos informáticos	Data Center
A14	SAN	Unidades de almacenamiento donde reside la información de la entidad	Equipos informáticos	Data Center

No	Nombre del Activo	Descripción del Activo	Tipo de activo	Contenedor
A15	Solución de Backup	Solución de Backup para el respaldo de información del negocio	Equipos informáticos	Data Center
A16	Dispositivos de red	Equipos y dispositivos de red activos (switch, router)	Equipos informáticos	Cuartos de rack
A17	Computadores Administradores	Computadores que utilizan los administradores de plataforma	Equipos informáticos	Área administración de plataforma
A18	Computadores de escritorio usuarios	Computadores de escritorio asignados a los colaboradores de la entidad	Equipos informáticos	Computadores
A19	Portátiles	Computadores portátiles de la entidad	Equipos informáticos	Portátiles
A20	Impresoras	Impresoras de la entidad ubicada en diferentes áreas	Equipos informáticos	Impresoras
A21	Equipos de seguridad perimetral	Equipos informáticos destinados a proteger la seguridad perimetral de la entidad	Equipos informáticos	Equipos de seguridad perimetral
A22	Aplicación Mesa de Ayuda	Aplicación utilizada por la mesa de ayuda para la gestión de requerimientos e incidentes	Software	Servidores de administración
A23	Sistema Monitoreo de servicios	Aplicaciones utiliza para monitorear el rendimiento y disponibilidad de los servicios de TI	Software	Servidores de administración
A24	Sistema de Control de Acceso	Sistema para controlar el acceso a las áreas de la entidad	Software	Servidores de administración
A25	Herramienta de Virtualización	Herramienta utilizada para la virtualización de servidores	Software	Servidores de administración
A26	Sistema Gestor Base de Datos	Sistema de gestión y administración de las bases de datos de la entidad	Software	Servidores de bases de datos
A27	Antivirus	Software de administración de seguridad para el control de virus	Software	Servidores de administración
A28	Sistema de control de versiones	Sistema de administración para el control de versiona-miento de software	Software	Servidores de administración
A29	Aplicativo de nómina	Aplicativo para la gestión de recursos humanos	Software	Servidores de aplicaciones
A30	Sistema de Gestión Documental	Sistema de Gestión documental de la institución	Software	Servidores de aplicaciones
A31	Sistema de Gestión de Calidad	Aplicativo para el Sistema de Gestión de Calidad	Software	Servidores de aplicaciones
A32	Página WEB	Página Web de la institución	Software	Servidores de aplicaciones
A33	Aplicativos seguimiento proyectos	Página Web de la institución	Software	Servidores de aplicaciones
A34	Directorio activo	Servicio establecido donde están los objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red	Servicios	Servidores de administración

No	Nombre del Activo	Descripción del Activo	Tipo de activo	Contenedor
A35	Correo Electrónico	Correo electrónico corporativo de la institución	Servicios	Plataforma de Correo
A36	Bases de datos	Bases de datos que almacenan la información de la entidad	Servicios	Servidores de bases de datos
A37	File Server	Almacenamiento de los documentos electrónicos que manejan las áreas de la institución	Servicios	Servidores de administración
A38	Video Conferencia	Corresponde al servicio de videoconferencia de la institución	Servicios	Servidores de administración
A39	Gestión de privilegios	Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones.	Servicios	Directorio activo
A40	Identidad del Usuario	Información que identifica a un funcionario (nombre, cedula, datos biométricos como la huella, código del usuario, etc.)	Datos / Información	Directorio activo
A41	Datos de autenticación	Usuario y Contraseña que utiliza los usuarios para ingresar a los recursos tecnológicos y aplicaciones.	Datos / Información	Directorio activo
A42	Usuarios genéricos	Usuario genéricos que utilizan las aplicaciones para conectarse a las bases de datos	Datos / Información	Bases de datos
A43	Log de evento de seguridad	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones	Datos / Información	Log de eventos
A44	Registro de incidentes de seguridad	Registro de incidentes de seguridad reportados por la herramienta de mesa de ayuda	Datos / Información	Bases de datos
A45	Manuales técnicos de administración	Corresponde a los documentos, manuales y procedimientos relacionadas con la administración de la plataforma	Datos / Información	File Server
A46	Bitácora de control de acceso al centro de computo	Registro de acceso al centro de computo	Datos / Información	Carpetas
A47	Plan estratégico de tecnología	Documento que contiene el plan estratégico de tecnología	Datos / Información	File Server
A48	Documentos del proceso	Corresponde a los documentos del proceso que están publicados en el sistemas de gestión de calidad	Datos / Información	Bases de datos

Tabla Nº 15.- Inventario de los activos de información
Elaborado por: El Autor

Identificados los activos de información se procedió a valorar su grado de importación y criticidad para la institución, para lo cual, se valoró la afectación o perdida que le puede generar a la entidad en cuanto aspectos financieros, legales y de imagen, en caso dado que al materializarse una amenaza afecte su disponibilidad, integridad o confidencialidad. Para tal efecto, se utilizaron los siguientes criterios para realizar la respectiva valoración:

3.11 Tabla para valoración activos de información

Aspecto	Criterio de valoración	Criterio de valoración	Valor a
Financiero	Pérdidas económicas para la empresa (porcentaje calculado sobre la utilidad operacional)	Menor o igual a 0.25%	1
		Mayor a 0.25% y menor o igual a 5%	2
		Mayor a 5% y menor o igual a 20%	3
		Mayor a 20% y menor o igual a 50%	4
		Mayor al 50%	5
Legal	Incumplimiento de normatividad y legislación	No tiene repercusión frente a normatividad y contratos.	1
		Genera llamados de atención por parte de los entes de control.	2
		Genera posibles sanciones menores por parte de los entes de control y/o reclamos por parte de terceros.	3
		Genera sanciones económicas por parte de los entes de control y/o demandas por parte de terceros.	4
		Genera sanciones mayores por parte de entes de control, cancelación de contratos, suspensión de licencias, cierre de líneas de negocios.	5
Imagen	Afectación de la imagen de la empresa	Conocido solo de manera interna de la empresa pero no de interés publico	1
		Atención de algunas partes interesadas a nivel local que potencialmente puede afectar a la empresa	2
		Media atención de las partes interesadas a nivel local y regional.	3
		Alta Atención de las partes interesadas a nivel local, regional y nacional.	4
		Conocimiento general a nivel nacional e internacional.	5

Tabla Nº 16.- Inventario de los activos de información
Elaborado por: El Autor

Para poder sacar el análisis de la puntuación en la criticidad del activo se realizó las siguientes preguntas:

3.12 Preguntas para definir la criticidad del activo

Criterio	Factor Afectado	Pregunta
Disponibilidad	Financiero	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad?
Integridad	Financiero	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Confidencialidad	Financiero	¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entes de control o puede generar demandas de terceros?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?

Tabla Nº 17.- Criticidad del activo
Elaborado por: El Autor

Por último, para determinar el nivel de criticidad del activo se valoró y utilizó los criterios de valoración de la siguiente tabla:

3.13 Nivel de criticidad del activo

Criterio de Evaluación	Valor criticidad activo	Nivel criticidad
La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	>= 4	**Alto**
La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	> 2 y < 4	**Medio**
La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	> 0 y <= 2	**Bajo**
La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la información de la empresa	Igual a 0	No aplica

Tabla Nº 18.- Nivel de criticidad del activo
Elaborado por: El Autor

De acuerdo a la metodología planteada que está del presente proyecto, la siguiente es la valoración del nivel de criticidad de los activos de la dirección de tecnológica que se identificaron:

3.14 Valoración nivel criticidad activos información de tecnología

Resumen Valoración de nivel de criticidad del activo

Confidencialidad			Integridad			Disponibilidad		
Alto	**Medio**	**Bajo**	**Alto**	**Medio**	**Bajo**	**Alto**	**Medio**	**Bajo**
20	10	15	21	21	15	16	19	10

Tabla Nº 19.- Valoración de nivel de criticidad del activo
Elaborado por: El Autor

Para realizar este análisis de riesgos de los activos de información de la institución, se optó por seleccionar los activos de información con el nivel de criticidad Alto y Medio y agruparlos en la medida de lo posible por contener. Aquellos contenedores que incluyeran más de un activo de información se utilizaron para la valorización de riesgos en lugar de hacerlo sobre el activo.

De lo antes mencionado, los siguientes fueron los contenedores y/o activos de información que se seleccionaron para el proceso de valoración de riesgos.

Activo de Información	Nivel de criticidad	Contener y/o activo seleccionado para valoración de riesgos
A3. Área administración de plataforma	Alto	Área administración de plataforma
A17. Computadores Administradores	Alto	
A44. Registro de incidentes de seguridad	Alto	Bases de datos
A42. Usuarios genéricos	Alto	
A18. Computadores de escritorio usuarios	Medio	Computadores
A16. Dispositivos de red	Alto	Cuartos de rack
A2. Cuartos de comunicaciones	Medio	
A1. Centro Principal de Procesamiento	Alto	Servidores de administración
A14. SAN	Alto	
A8. Servidores de administración	Alto	
A10. Servidores de aplicaciones de producción	Alto	
A9. Servidores de bases de datos de producción	Alto	
A11. Plataforma de Correo	Medio	
A15. Solución de Backup	Medio	
A41. Datos de autenticación	Alto	Directorio activo
A39. Gestión de privilegios	Alto	
A34. Identidad del Usuario	Alto	
A21. Equipos de seguridad perimetral	Alto	Equipos de seguridad perimetral
A43. Log de evento de seguridad	Alto	Log de eventos
A35. Correo Electrónico	Medio	Plataforma de Correo
A19. Portátiles	Medio	Portátiles
A4. Red LAN	Alto	Red LAN
A6. Red WIFI corporativa	Alto	
A7. Red WIFI invitados	Medio	
A6. Red WAN	Alto	Red WAN
A43. Directorio activo	Alto	Servidores de administración
A37. FileServer	Alto	
A25. Herramienta de Virtualización	Alto	
A24. Sistema de Control de Acceso	Medio	
A31. Sistema de Grabación de llamadas	Medio	
A33. Aplicativos CORE del negocio	Alto	Servidores de aplicaciones

Activo de Información	Nivel de criticidad	Contener y/o activo seleccionado para valoración de riesgos
A29. Aplicativo de nomina	Medio	
A32. Página WEB	Medio	
A36. Bases de datos	Alto	Servidores de bases de datos
A26. Sistema Gestor Base de Datos	Alto	

Tabla Nº 20.- Valoración de nivel de criticidad por nivel
Elaborado por: El Autor

3.15 Valoración de Riesgos Activos de Tecnología

Se procedió a realizar la valoración de los riesgos a los cuales están expuestos los activos de información que se identificaron para el proceso de tecnología, para lo cual, se desarrolló las siguientes actividades:

- Identificación de riesgo
- Análisis del riesgo inherente
- Elaboración matriz de riesgo inherente
- Valoración de controles existentes para mitigar el riesgo inherente
- Determinación de riesgos residual
- Elaboración matriz de riesgo residual

NOTA: El detalle de los riesgos del proceso de tecnología se encuentra en el Anexo E del presente trabajo, el cual además de esta información contiene los parámetros, la formulación y los cálculos se utilizaron para determinar el riesgo inherente y el residual.

3.16 Identificación de amenazas

Se identificaron las amenazas a las que estos están expuestos los activos de información de la dirección de tecnología que fueron seleccionados para la valoración de riesgos, para lo cual, se planearon las siguientes preguntas:

- ¿Cuál es la probabilidad de ocurrencia de la amenaza?
- ¿Cuál sería el impacto en caso de que ocurriera?
- ¿Cuáles de los criterios de seguridad afectaría, si la confidencialidad, la integridad o la disponibilidad?

Para facilitar esta labor de identificación, se elaboró la siguiente lista que contiene una serie de riesgos de seguridad que en términos generales pueden afectar a cualquier tipo de institución y los principios de seguridad que se ven afectos, relacionados con la *confidencialidad, disponibilidad* e *integridad* de la información:

Lista de riesgos y principios de seguridad afectados

RIESGOS	PRINCIPIOS AFECTADOS		
	C	I	D
Abuso de privilegios de acceso	X	X	
Acceso no autorizado	X	X	
Auditorias débiles	X	X	X
Denegación de Servicio			X
Divulgación o robo de información de autenticación	X		
Divulgación no autorizada de información del negocio	X		
Ejecución de ingeniería social	X		
Errores del administrador	X	X	X
Instalación de software no autorizado		X	X
Intercepción no autorizada de información en tránsito	X		

RIESGOS	PRINCIPIOS AFECTADOS		
	C	I	D
Manipulación de la configuración	X		
Modificación sin autorización		X	
Pérdida o robo de información	X		X
Suplantación de identidad	X	X	
Uso inadecuado de sistema para generar fraudes	X	X	
Uso inadecuado de sistemas que generan interrupción			X

Tabla Nº 21.- Lista de riesgos y principios afectados
Elaborado por: El Autor

Con base en esta información se identificaron las siguientes amenazas a las cuales están expuestos los activos de información de la Dirección de Tecnología seleccionados para el proceso de valoración de riesgos:

3.17 Amenazas que pueden afectar los activos de tecnología

Amenazas	Activos de tecnología que pueden ser afectados	
Acceso no autorizado	• Área administración de plataforma • Bases de datos • Cuartos de Rack • Data Center • Directorio Activo • Equipos de seguridad perimetral	• Servidores de Administración • Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Ataques externos / internos (hacking no ético)	• Bases de datos • Equipos de seguridad perimetral • Servidores de Administración • Plataforma de Correo	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Data Center
Cambio de privilegios sin autorización	• Bases de Datos	• Servidores de bases de datos de producción

Amenazas	Activos de tecnología que pueden ser afectados	
Autorización	• Directorio Activo • Servidores de Administración	• Servidores de aplicaciones de producción • Plataforma de Correo
Desastres naturales	• Data Center del proveedor	
Divulgación de información de autenticación	• Bases de Datos • Directorio Activo	• Servidores de Administración
Error del administrador	• Bases de datos • Data Center • Directorio Activo • Red LAN • Red WAN	• Servidores de Administración • Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo • Equipos de seguridad perimetral
Instalación de software no autorizado	• Directorio Activo • Computadores	• Portátiles
Interceptación no autorizada de información en tránsito	• Red LAN • Red WAN	• Servicio de Correo
Interrupción en los servicios	• Bases de datos • Data Center del proveedor • Directorio Activo	• Red LAN • Red WAN • Servidores de Producción
Modificación sin autorización	• Bases de datos • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Robo de equipos	• Área administración de plataforma • Cuartos de Rack	• Data Center del proveedor
Robo de información	• Bases de datos • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Plataforma de Correo

Amenazas	Activos de tecnología que pueden ser afectados	
Suplantación de identidad de usuarios	• Directorio Activo	• Servicio de Correo
Uso inadecuado de sistemas para generar fraudes	• Bases de datos • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Uso inadecuado de sistemas que generan interrupción	• Bases de datos • Data Center del proveedor • Directorio Activo • Red LAN • Red WAN	• Servidores de Administración • Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Abuso de privilegios	• Data Center del proveedor • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo

Tabla Nº 22.- Amenazas que pueden afectar los activos
Elaborado por: El Autor

Las siguientes son vulnerabilidades asociadas a las diferentes amenazas identificadas y que están relacionados con las características de los activos de la dirección de tecnología o de sus contenedores**:**

Vulnerabilidad asociados a las amenazas de los activos

AMENAZA	VULNERABILIDADES
Acceso no autorizado	• Inadecuada Administración de Seguridad • Ausencia o Inadecuada plataforma de Seguridad Perimetral • Inadecuada Administración o Asignación de roles y permisos • Ausencia de una configuración segura de la red • Contraseñas no seguras • Configuración incorrecta de las cuentas de usuario • Falta de seguridad de los puertos de red • Políticas no aplicada o no existencia de seguridad

AMENAZA	VULNERABILIDADES
Ataques externos / internos (hacking no ético)	• Inadecuada Administración de Seguridad • Ausencia o Inadecuada plataforma de Seguridad Perimetral • Ausencia de una configuración segura de la red • Falla de seguridad en los componentes de red
Cambio de privilegios sin autorización	• Contraseñas no seguras • Inadecuada Administración o Asignación de roles y permisos • Inadecuada Administración de Seguridad • Políticas no aplicada o no existencia de seguridad
Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	• Ausencia de un sistema de continuidad de negocio • Ubicación física de los equipos • Ubicación física del centro de cómputo • Políticas no aplicada o no existencia de seguridad física
Divulgación de información de autenticación	• Inadecuada Administración de Seguridad • Contraseñas no seguras • Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado
Error del administrador	• Ausencia de capacitación permanente • Ausencia o inadecuado procedimiento de control de cambios • Desmotivación del personal
Instalación de software no autorizado	• Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos
Interceptación no autorizada de información en tránsito	• Políticas no aplicada o no existencia de seguridad • Inadecuado mecanismo de cifrado
Interrupción en los servicios	• Inadecuada Configuración y Capacidad de los ambientes • Ausencia o inadecuado procedimiento de control de cambios • Falta de mantenimiento de equipos
Modificación sin autorización	• Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado
Robo de equipos	• Políticas no aplicada o no existencia de seguridad • Ausencia o inadecuado plataforma de vigilancia física • Inadecuado inventario de activos físicos • Ubicación física de los equipos
Robo de información	• Inadecuada Administración de Seguridad • Ausencia o Inadecuada plataforma de Seguridad Perimetral • Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado • Inexistencia de Logs de eventos de seguridad
Suplantación de identidad de usuarios	• Contraseñas no seguras • Cuentas de usuario sin auditar • Ausencia o inadecuado plataforma de vigilancia física • Inadecuado mecanismo de cifrado
Uso inadecuado de sistemas para generar fraudes	• Inadecuada Administración de Seguridad • Cuentas de usuario sin auditar • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos

AMENAZA	VULNERABILIDADES
Uso inadecuado de sistemas que generan interrupción	• Inadecuada Administración de Seguridad • Cuentas de usuario sin auditar • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos • Políticas no aplicada o no existencia de seguridad
Abuso de privilegios	• Cuentas de usuario sin auditar • Contraseñas no seguras • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos • Políticas no aplicada o no existencia de seguridad

Tabla Nº 23.- Vulnerabilidad asociadas a las amenazas de los activos
Elaborado por: El Autor

3.18 Análisis de Riesgo Inherente

Por medio del análisis de riesgos se estableció la probabilidad de ocurrencia de los riesgos y el impacto de los mismos, con el fin de obtener el nivel de riesgo inherente, el cual, nos permitió establecer el nivel de riesgo propio de la actividad sin tener en cuenta las medidas y controles de seguridad que actualmente existen en la entidad para mitigar o minimizar los riesgos. Para determinar la probabilidad de ocurrencia de una amenaza sobre cada uno de los activos, se utilizó los siguientes criterios de valoración:

Valoración probabilidad de ocurrencia

Probabilidad de ocurrencia en un (1) año	Valor Cualitativo	Valor Asignado
Una vez cada año	Raro	1
Una vez cada seis (6) meses	Baja (Improbable)	2
Una vez cada tres (3) meses	Media (Posible)	3
Una vez cada mes	Alta (Probable)	4
Más de una vez al mes	Muy Alta	5

Tabla Nº 24.- Valoración de probabilidad de ocurrencia
Elaborado por: El Autor

Para determinar el impacto que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad sobre los activos de información se utilizó los siguientes criterios de valoración:

3.19 Valoración del impacto

Impacto	Impacto cuantitativo (Porcentaje sobre utilidad operacional)	Impacto Cualitativo (Uno o más factores)	Valor
Insignificante	Genera pérdidas financieras pequeñas no significativas. (Perdida Menor o igual a 0.25%)	• No afecta la seguridad de la información de la entidad. • No afecta la imagen de la entidad ante las partes interesadas. • Genera reprocesos insignificantes. • La información se puede recuperar rápidamente con la misma calidad.	1
Menor	Genera pérdidas financieras menores no significativas. (Perdida Mayor a 0.25% y menor o igual a 5%)	• No afecta la seguridad de la información de la entidad. • Afecta en menor grado la imagen de la entidad ante las partes interesadas. • Genera reprocesos menores. • La información se puede recuperar en un tiempo moderado con la misma calidad.	2
Moderado	Genera pérdidas financieras moderadas. (Mayor a 5% y menor o igual a 20%)	• Afecta en menor grado la seguridad de la información de la entidad. • Afecta medianamente la imagen de la entidad ante las partes interesadas. • Genera reprocesos moderados. • La información se puede recuperar pero no con la misma calidad	3
Mayor	Genera pérdidas financieras mayores. (Perdida mayor o igual a 20% y menor a 50%)	• Afecta en mayor grado la seguridad de la información de la entidad. • Afecta altamente la imagen de la entidad ante las partes interesadas. • Genera reprocesos mayores. • Es difícil recuperar la información	4
Catastrófico	Genera pérdidas financieras críticas. (Perdidas Mayores a 50%)	• Afectar seriamente la seguridad de la información de la entidad. • Afecta gravemente la imagen de la empresa ante las partes interesadas • Puede generar pérdida masiva de clientes. • Genera alto nivel de reprocesos. • Es difícil y costoso recuperar la información. • Afecta la continuidad del negocio	5

Tabla Nº 25.- Valoración del impacto
Elaborado por: El Autor

El nivel de riesgo inherente es igual a el valor de la probabilidad x valor del impacto.

Para clasificar el riesgo ya se inherente o residual dependiente de su nivel de riesgo, se utilizó los siguientes criterios de valoración que determinan el tipo de riesgo:

Valoración de los riesgos

Tipo de riesgo	Valor Nivel Riesgo	Acción requerida
Riesgo Extremo	Nivel Riesgo mayor o igual a 15 puntos	Requiere acciones inmediatas que permitan reducir y compartir el riesgo, transferirlo o incluso evitarlo
Riesgo Alto	Nivel Riesgo mayor o igual a 10 y menor a 15 puntos	Requieren atención urgente e implementar medidas para reducir el nivel del riesgo
Riesgo Medio	Nivel Riesgo mayor o igual a 5 y menor a 10 puntos	Requiere de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual
Riesgo Bajo	Nivel Riesgo mayor o igual a 3 y menor a 5 puntos	El riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo
Riesgo Inusual	Nivel Riesgo Menor a 3 puntos	Se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes.

Tabla Nº 26.- Valoración de los riesgos
Elaborado por: El Autor

El siguiente es el resultado del proceso de valoración del riesgo inherente de las amenazas asociados a los activos de información de la Dirección de Tecnología:

3.20 Valoración de riesgos inherentes de la Dirección de Tecnología

RIESGOS	VALORACION IMPACTO			Probabilidad	ESTIMACION DE RIESGO			Nivel de Riesgo
	D	I	C		D	I	C	
R1. Acceso no autorizado		Mayor	Catastrófico	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo
R2. Ataques externos / internos (hacking no ético)	Mayor		Mayor	Alta	Riesgo Extremo		Riesgo Extremo	Riesgo Extremo
R3. Cambio de privilegios sin autorización	Moderado	Moderado	Moderado	Alta	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto
R4. Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	Mayor			Raro	Riesgo Bajo			Riesgo Bajo
R5. Divulgación de información de autenticación			Moderado	Media			Riesgo Medio	Riesgo Medio
R6. Error del administrador	Moderado			Alta	Riesgo Alto			Riesgo Alto
R7. Instalación de software no autorizado		Menor		Media		Riesgo Medio		Riesgo Medio
R8. Interceptación no autorizada de información en tránsito		Mayor	Mayor	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo
R9. Interrupción en los servicios	Moderado			Media	Riesgo Medio			Riesgo Medio
R10. Modificación sin autorización		Moderado		Media		Riesgo Medio		Riesgo Medio
R11. Robo de equipos	Moderado			Media	Riesgo Medio			Riesgo Medio
R12. Robo de información	Mayor		Mayor	Media	Riesgo Alto		Riesgo Alto	Riesgo Alto
R13. Suplantación de identidad de usuarios			Moderado	Baja			Riesgo Medio	Riesgo Medio

RIESGOS	VALORACION IMPACTO			Probabilidad	ESTIMACION DE RIESGO			Nivel de Riesgo
	D	I	C		D	I	C	
R14. Uso inadecuado de sistemas para generar fraudes			Mayor	Baja			Riesgo Medio	Riesgo Medio
R15. Uso inadecuado de sistemas que generan interrupción	Mayor			Baja	Riesgo Medio			Riesgo Medio
R16. Abuso de privilegios		Mayor	Mayor	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo

D: Disponibilidad, I: Integridad, C: Confidencialidad

Tabla Nº 27.- Valoración de riesgos inherentes
Elaborado por: El Autor

3.21 Riesgos inherentes de Tecnología por tipo de riesgo

RIESGO	Probabilidad	Impacto	Nivel de Riesgo Probabilidad x impacto	
R1. Acceso no autorizado	4. Alta	5. Catastrófico	20	Riesgo Extremo
R2. Ataques externos / internos (hacking no ético)	4. Alta	4. Mayor	16	Riesgo Extremo
R8. Interceptación no autorizada de información en tránsito	4. Alta	4. Mayor	16	Riesgo Extremo
R16. Abuso de privilegios	4. Alta	4. Mayor	16	Riesgo Extremo
R3. Cambio de privilegios sin autorización	4. Alta	3. Moderado	12	Riesgo Alto
R6. Error del administrador	4. Alta	3. Moderado	12	Riesgo Alto
R12. Robo de información	3. Media	4. Mayor	12	Riesgo Alto
R5. Divulgación de información de autenticación	3. Media	3. Moderado	9	Riesgo Medio
R9. Interrupción en los servicios	3. Media	3. Moderado	9	Riesgo Medio
R10. Modificación sin autorización	3. Media	3. Moderado	9	Riesgo Medio
R11. Robo de equipos	3. Media	3. Moderado	9	Riesgo Medio
R14. Uso inadecuado de sistemas para generar fraudes	2. Baja	4. Mayor	8	Riesgo Medio
R15. Uso inadecuado de sistemas que generan interrupción	2. Baja	4. Mayor	8	Riesgo Medio
R7. Instalación de software no autorizado	3. Media	2. Menor	6	Riesgo Medio
R13. Suplantación de identidad de usuarios	2. Baja	3. Moderado	6	Riesgo Medio
R4. Desastres naturales	1. Raro	4. Mayor	4	Riesgo Bajo

Tabla Nº 28.- Riesgos inherentes
Elaborado por: El Autor

3.22 Mapa de Calor

El mapa de calor permite representar de forma gráfica un plano conformado por zonas donde se ubicación los riesgos de acuerdo a su probabilidad y su impacto. Cada zona dentro del mapa de calor corresponde a un tipo de riesgo, el cual indica las acciones que se deben realizar para el tratamiento del riesgo.

El siguiente es el mapa de calor que tuvo en cuenta para determinar la ubicación de los riesgos inherentes que fueron identificados:

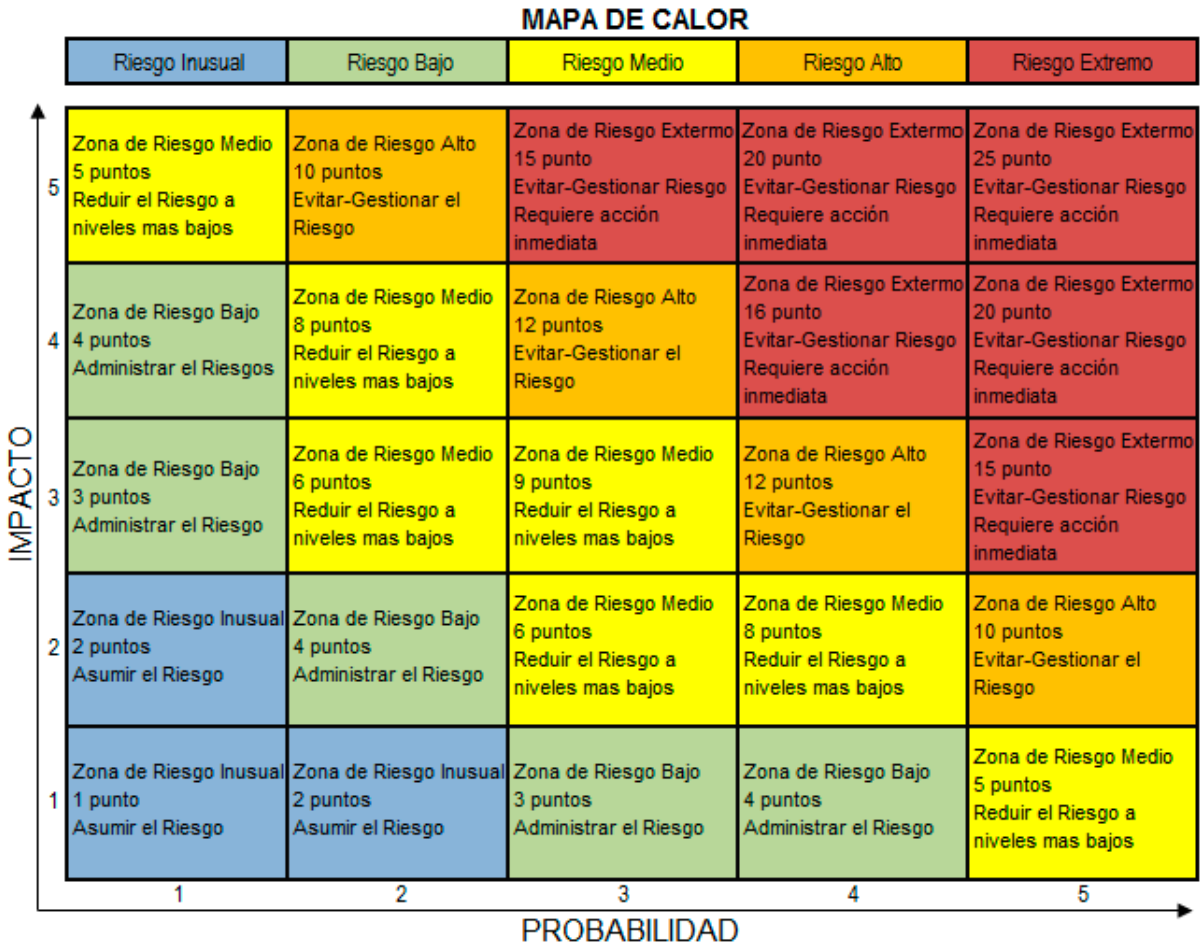

Tabla Nº 29.- Valoración de nivel de criticidad por nivel
Elaborado por: Norma ISO/IEC 27001:2013, ISO 31000:2009

Se utilizó una matriz de 5x5 para el mapa de calor, debido a que las metodologías de riesgos de la ISO 31000:2009 utilizan este tipo de matrices para la valoración de los diferentes tipos de riesgos.

3.23 Mapa de Riesgo Inherente

Los siguientes son los mapas de riesgo inherente del proceso de tecnología:

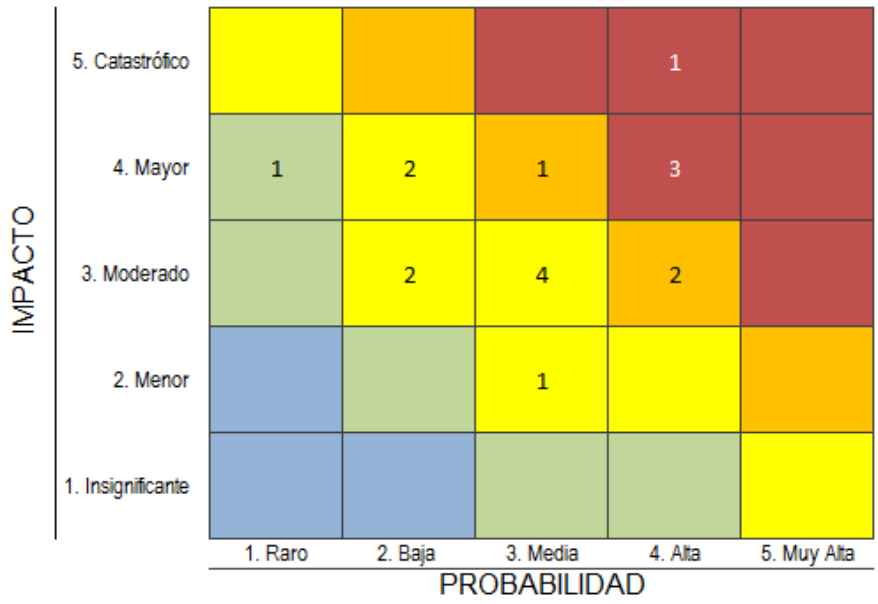

Gráfico No. 4: Mapa de Riesgo inherente

3.24 Mapa Riesgo inherentes detallado proceso de tecnología

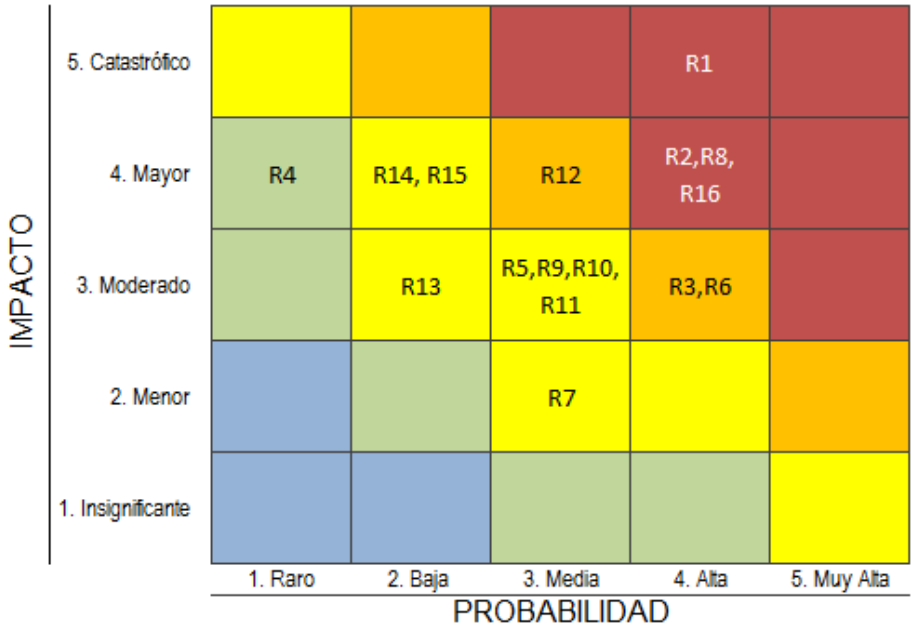

Gráfico No. 5: Mapa de Riesgo inherente

3.25 Valoración de Controles

Una vez generada la matriz de riesgo inherente se procedió a valorar la efectividad de los controles existentes, con el objetivo determinar el nivel de desplazamiento que estos pueden genera sobre el mapa de calor de riesgo, lo cual determina, el mapa de calor del riesgo residual

Criterios para evaluar la efectividad del control

Aspectos a evaluar	Opciones de respuesta	Peso
Afecta impacto o probabilidad. Permite establecer el movimiento que genera sobre la matriz, si sobre el eje X (probabilidad) o sobre el eje Y (impacto)	Impacto	
	Probabilidad	
Categoría del control	Control Preventivo	20
	Control Detectivo	15
	Control Correctivo	5
Herramientas para ejercer el control	SI	15
	NO	0
Están definidos los responsables de la ejecución del control y del seguimiento	SI	15
	NO	0
La frecuencia de la ejecución del control y seguimiento es adecuada.	SI	20
	NO	0
El tiempo que lleva el control ha demostrado ser efectivo	SI	20
	NO	0
Está documentado los pasos para el manejo del control	SI	10
	NO	0

Tabla Nº 30.- Criterios para evaluar la efectividad del control
Elaborado por: Norma ISO/IEC 27001:2013

La pregunta relacionada con ‘Afecta impacto o probabilidad’, permite establecer el movimiento que genera la efectividad del control sobre el mapa de calor, si sobre el eje X (probabilidad) o sobre el eje Y (impacto).

Con base en los anteriores criterios, el siguiente es el resultado de la valoración de la efectividad de los controles existentes:

Valoración de controles

RIESGO \ AMENAZA	DESCRIPCION DEL CONTROL	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	TOTAL PUNTAJE
R1. Acceso no autorizado	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	El acceso de los usuarios a los recursos tecnológicos se controla por el directorio activo	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
	Se cuenta con un esquema de privilegios sobre el FileServer	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
R2. Ataques externos / internos (hacking no ético)	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	SI	NO	90
			20	15	15	20	20	0	
R3. Cambio de privilegios sin autorización	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	

RIESGO \ AMENAZA	DESCRIPCION DEL CONTROL	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	TOTAL PUNTAJE
R4. Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	Simulacros de evacuación	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
			Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R5. Divulgación de información de autenticación	Se tiene implementada la política de contraseña segura	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
R6. Error del administrador	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
R8. Interceptación no autorizada de información en tránsito	Los canales de comunicaciones con las regionales utilizan protocolos de encripción para la transmisión de datos.	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
R9. Interrupción en los servicios	Se cuenta con una plataforma en alta disponibilidad	Impacto	Correctivo	SI	SI	NO	SI	NO	55
			5	15	15	0	20	0	
	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
R10. Modificación sin autorización	El acceso de los usuarios a los recursos tecnológicos se controla a través del directorio activo	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	

RIESGO \ AMENAZA	DESCRIPCION DEL CONTROL	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	TOTAL PUNTAJE
R11. Robo de equipos	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	SI	SI	SI	SI	SI	100
			20	15	15	20	20	10	
	Existe guardias de seguridad que revisan a los equipos que entran y salen de la entidad	Probabilidad	Preventivo	SI	SI	SI	NO	SI	80
			20	15	15	20	0	10	
	Existen pólizas contra robo de equipos	Impacto	Correctivo	SI	SI	SI	SI	SI	85
			5	15	15	20	20	10	
R12. Robo de información	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Existe un esquema de premisos implementado en el FileServer y en las aplicaciones	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
R13. Suplantación de identidad de usuarios	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	SI	SI	SI	SI	SI	100
			20	15	15	20	20	10	
R14. Uso inadecuado de sistemas para generar fraudes	Los aplicativos críticos de la entidad tienen un esquema de autenticación integrado con el dominio y basado en roles y permisos	Probabilidad	Preventivo	SI	NO	SI	NO	NO	55
			20	15	0	20	0	0	
			20	15	15	0	0	10	
	Se cuenta con un esquema de privilegios sobre el FileServer	Impacto	Correctivo	SI	SI	NO	NO	NO	35
			5	15	15	0	0	0	

Tabla Nº 31.- Valoración de controles
Elaborado por: El Autor

3.26 Determinación del Riesgo Residual

Una vez determinado el nivel de desplazamiento que genero el control por disminución de la probabilidad o del impacto, se procedió a elaborar la matriz de riesgos residual, para lo cual, se ubicó el riesgo residual dentro del mapa de riesgos teniendo en cuenta el nuevo valor de su probabilidad y de su impacto.

El desplazamiento que se generó dentro de la matriz de riesgos determino la opción de tratamiento para el riesgo.

La siguiente es la distribución de riesgo residual asociados a los activos de la dirección de tecnología:

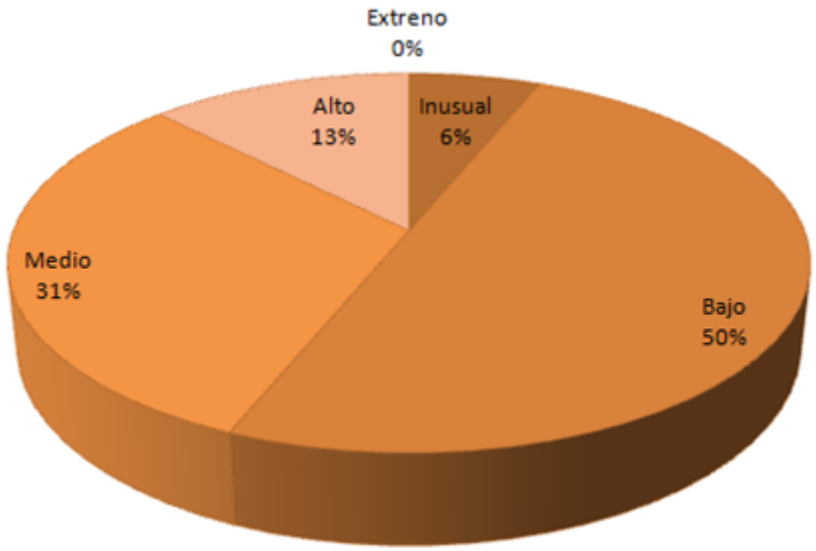

Gráfico No. 6: Distribución del riesgo residual activos Dirección de Tecnología
Elaborador por: El autor

3.26.1 Mapa de Riesgo Residual

Los siguientes son los mapas de riesgo residual una vez valorada la efectividad de los controles identificados:

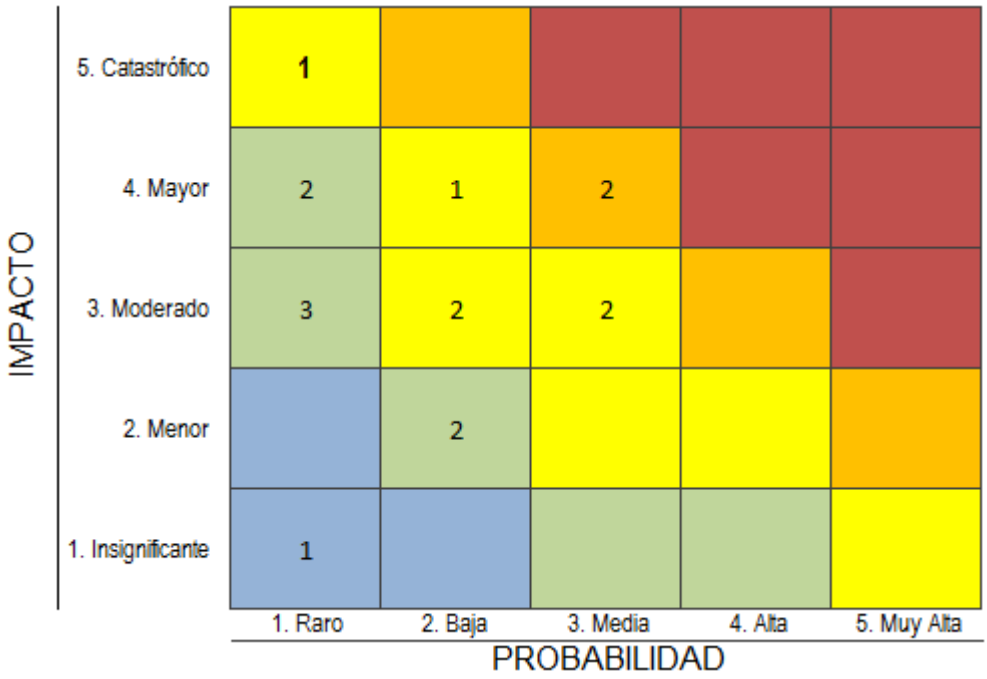

Gráfico No. 7: Mapa Riesgo residual general proceso de tecnología
Elaborador por: El autor

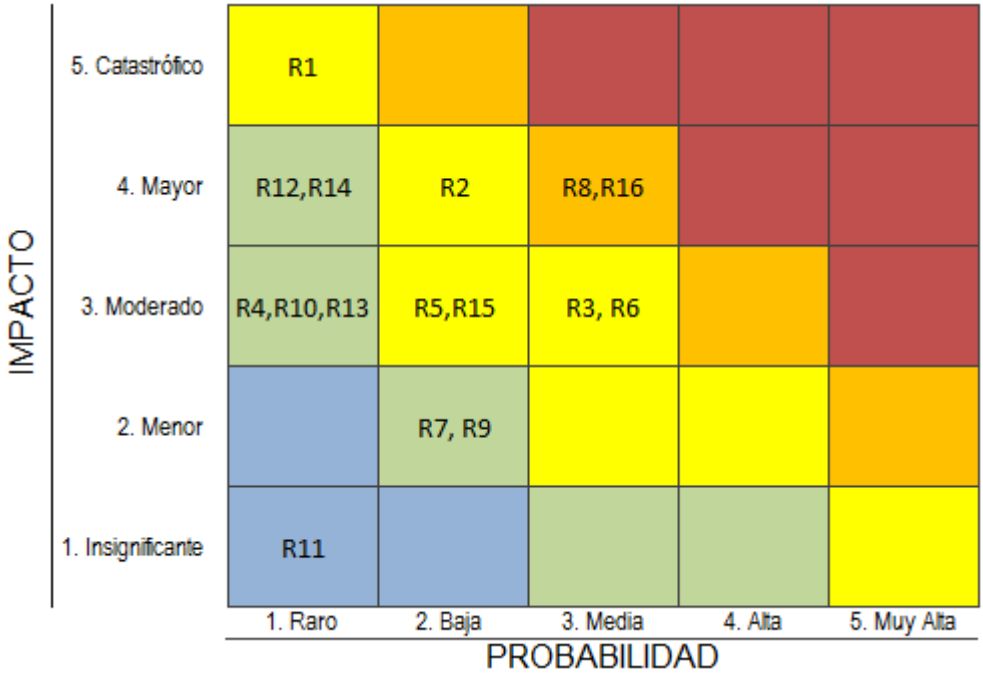

Gráfico No. 8: Mapa Riesgo residual detallado proceso de tecnología
Elaborador por: El autor

3.26.2 Comparativa mapas de calor

Los siguientes son los comparativos entre el mapa de riesgo inherente y el riesgo residual:

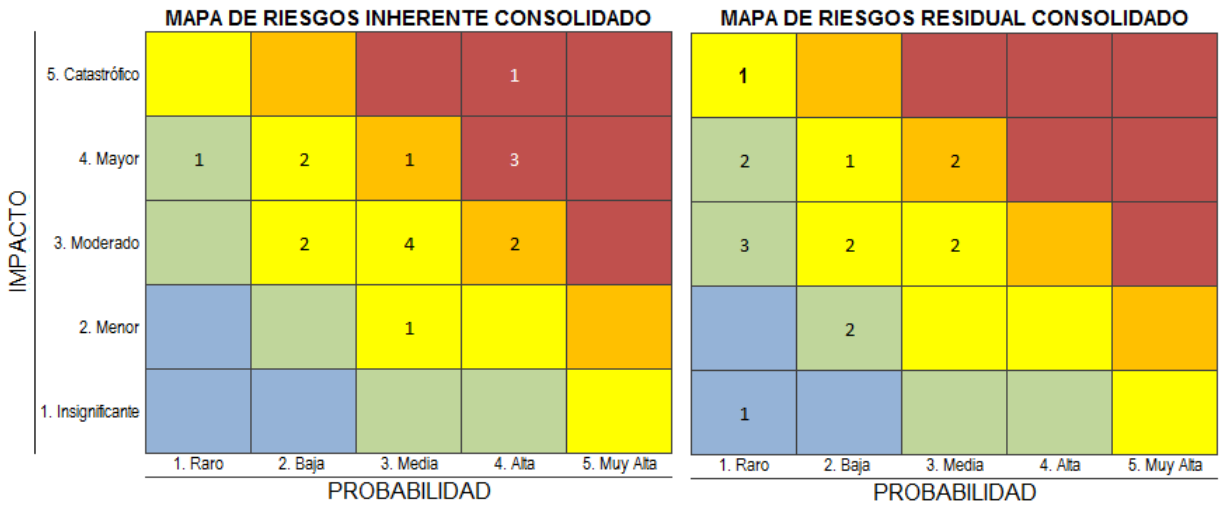

Gráfico No. 9: Comparativo Mapas de Calor Consolidadas
Elaborador por: El autor

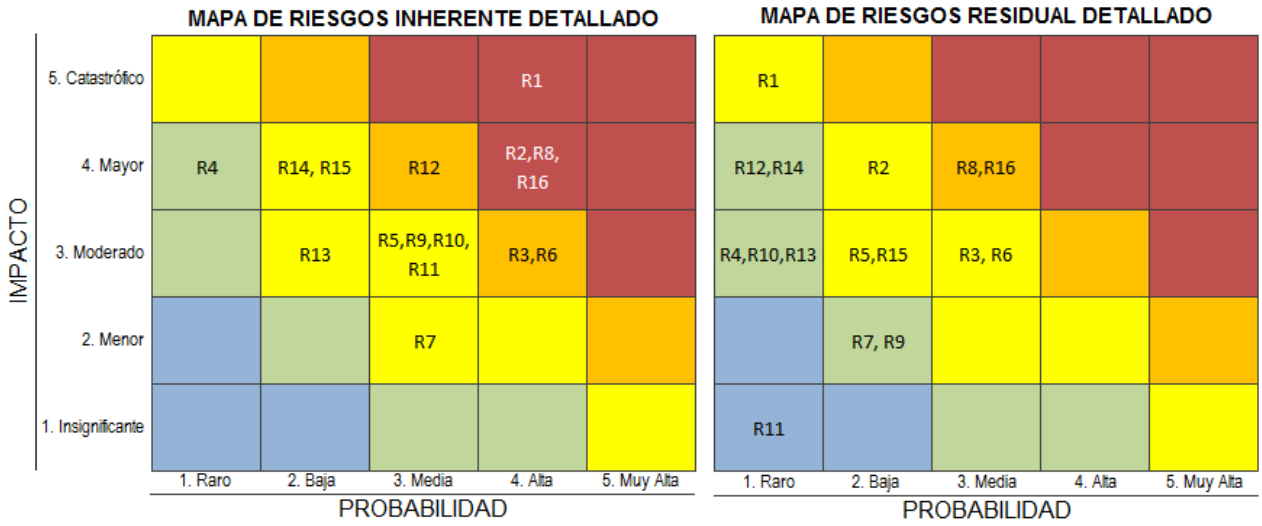

Gráfico No. 10: Comparativo Mapas de Calor Detalladas
Elaborador por: El autor

3.27 Plan de tratamiento del riesgo

Con el objetivo de gestionar el riesgo residual se establecieron los planes de tratamiento orientados a preservar las características de confidencialidad, integridad y disponibilidad de los activos de información de tecnología seleccionados para la respectiva valoración de riesgos. Para determinar la opción para el tratamiento del riesgo, se utilizó la siguiente tabla de criterios:

Opción	Acción de seguir
Evitar	Establecer las medidas orientadas a prevenir su materialización.
Reducir	Establecer medidas encaminadas a disminuir tanto la probabilidad mediante medidas de prevención, como el impacto mediante medidas de protección.
Transferir	Si es posible, reducir su efecto a través del traspaso del riesgo a otras organizaciones (ej. Seguros, tercerización de servicios).
Asumir	Si al mitigar el riesgo este queda como un riesgo residual, se puede aceptar el riesgo sin necesidad de tomar otras medidas de control.

Tabla Nº 32.- Plan de tratamiento de riesgo
Elaborado por: Norma ISO/IEC 27001:2013

Las siguientes son las opciones que se establecieron para el tratamiento de los riesgos residuales de acuerdo a su a posición en la matriz de 5x5:

Riesgos	Riesgo	Opción de tratamiento
Acceso no autorizado	Riesgo Medio	Disminuir el riesgo
Ataques externos / internos (hacking no ético)	Riesgo Medio	Disminuir el riesgo
Cambio de privilegios sin autorización	Riesgo Medio	Disminuir el riesgo
Desastres naturales	Riesgo Bajo	Reducir el riesgo
Divulgación de información de autenticación	Riesgo Medio	Disminuir el riesgo
Error del administrador	Riesgo Medio	Disminuir el riesgo
Instalación de software no autorizado	Riesgo Bajo	Reducir el riesgo
Interceptación no autorizada de información en tránsito	Riesgo Alto	Prevenir el riesgo.
Interrupción en los servicios	Riesgo Bajo	Reducir el riesgo
Modificación sin autorización	Riesgo Bajo	Reducir el riesgo
Robo de equipos	Riesgo Inusual	Aceptar el riesgo

Riesgos	Riesgo	Opción de tratamiento
Robo de información	Riesgo Bajo	Reducir el riesgo
Suplantación de identidad de usuarios	Riesgo Bajo	Reducir el riesgo
Uso inadecuado de sistemas para generar fraudes	Riesgo Bajo	Reducir el riesgo
Uso inadecuado de sistemas que generan interrupción	Riesgo Medio	Disminuir el riesgo
Abuso de privilegios	Riesgo Alto	Prevenir el riesgo.

Tabla Nº 33.- Plan de tratamiento de riesgo
Elaborado por: Norma ISO/IEC 27001:2013

Los siguientes son los planes de tratamiento que se definieron para evitar, disminuir o mitigar los riesgos residuales del proceso de tecnología:

3.27.1 Plan de tratamiento de riesgos residuales proceso de Tecnología

Riesgos	Riesgo Residual	Plan de Tratamiento	Afecta			Descripción plan de acción	Responsable
			D	I	C		
R1. Acceso no autorizado	**Riesgo Medio**	Disminuir el riesgo		I	C	Realizar periódicamente pruebas de Hacking Ético para establecer el nivel de protección de la infraestructura de TI, sobre todo, los servicios publicados hacia la web	Departamento de Tecnología
						Adquirir una solución para el monitoreo de Logs y correlación de eventos	Departamento de Tecnología
						Monitorear periódica los Logs de eventos de seguridad y las bitácoras de entrada a las áreas de la entidad.	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Departamento de Tecnología
						Realizar permanentemente campañas de seguridad	Departamento de Tecnología
R2. Ataques externos / internos (hacking no ético)	**Riesgo Medio**	Disminuir el riesgo	D	I	C	Realizar periódicamente prueba de Hacking Ético con el objetivo de establecer el nivel de protección de la infraestructura de TI, sobre todo, los servicios de la entidad publicados hacia la web	Departamento de Tecnología
R3. Cambio de privilegios sin autorización	**Riesgo Medio**	Disminuir el riesgo	D	I		Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Departamento de Tecnología
						Garantizar que este implementada la política de contraseña segura	Departamento de Tecnología

Riesgos	Riesgo Residual	Plan de Tratamiento	Afecta			Descripción plan de acción	Responsable
			D	I	C		
R4. Desastres naturales	**Riesgo Bajo**	Reducir el riesgo	D			Garantizar la debida ejecución de las pruebas de continuidad	Departamento de Tecnología
R5. Divulgación de información de autenticación	**Riesgo Medio**	Disminuir el riesgo			C	Garantizar que este implementada las políticas de contraseña segura y bloqueo automático de pantallas.	Departamento de Tecnología
						Realizar permanentemente campañas de seguridad	Departamento de Tecnología
R6. Error del administrador	**Riesgo Medio**	Disminuir el riesgo	D	I	C	Monitorear periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Garantizar la debida capacitación del personal de TI	Departamento de Tecnología
						Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Departamento de Tecnología
R7. Instalación de software no autorizado	**Riesgo Bajo**	Reducir el riesgo		I		Garantizar que la política que restringe instalación de software por parte de las usuarios está debidamente implementada	Departamento de Tecnología
R8. Interceptación no autorizada de información en tránsito	**Riesgo Alto**	Evitar el riesgos Atención inmediata		I	C	Implementar un portal de intercambio seguro que garantice la integridad, confidencialidad, autenticidad y no repudio de la información que se intercambió con terceros	Departamento de Tecnología
						Implementar mecanismos que garanticen el cifrado de la información que se intercambia con terceros a través del correo electrónico	Departamento de Tecnología
R9. Interrupción en los servicios	**Riesgo Bajo**	Reducir el riesgo	D			Monitorear periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Departamento de Tecnología
						Garantizar que todos los contratos con los proveedores de TI tengan Acuerdos de niveles de servicio	Departamento de Tecnología
						Garantizar la debida ejecución de las pruebas de contingencia de TI	Departamento de Tecnología
R10. Modificación sin autorización	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo		I		Monitorear periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema	Departamento de Tecnología
R11. Robo de equipos	**Riesgo Inusual**	Aceptar el riesgo			C		
R12. Robo de información	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo			C	Monitorear periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos los sistemas.	Departamento de Tecnología
						Implementar mecanismo de cifrado de disco duro de los dispositivos móviles y portátiles de la entidad	Departamento de Tecnología

Riesgos	Riesgo Residual	Plan de Tratamiento	Afecta			Descripción plan de acción	Responsable
			D	I	C		
						Garantizar la implementación del bloqueo de dispositivos externos en los computadores de la entidad	Departamento de Tecnología
						Clasificar la información de la entidad, de acuerdo a si es pública, privada o confidencial	Departamento de Tecnología
R13. Suplantación de identidad de usuarios	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo		I	C	Monitorear periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Departamento de Tecnología
						Revisar periódicamente la efectividad de la solución de anti spam	Departamento de Tecnología
						Garantizar que este implementada las políticas de contraseña segura y bloqueo automático de pantallas.	Departamento de Tecnología
						Realizar permanentemente campañas de seguridad	Departamento de Tecnología
R14. Uso inadecuado de sistemas para generar fraudes	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo		I	C	Monitorear periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Departamento de Tecnología
						Garantizar la debida segregación de funciones	Departamento de Tecnología
R15. Uso inadecuado de sistemas que generan interrupción	**Riesgo Medio**	Medidas prontas y adecuadas para disminuir el riesgo	D			Monitorear de manera periódica los Logs de eventos de seguridad.	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Departamento de Tecnología
R16. Abuso de privilegios	**Riesgo Alto**	Atención inmediata	D	I	C	Monitorear de manera periódica los Logs de eventos de seguridad y las actividades que realizan los administradores	Departamento de Tecnología
						Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Departamento de Tecnología
						Eliminar (si es posible) o bloquear las cuentas de súper administradores. En caso de bloqueo la contraseña de la misma deberá ser administrado por el oficial de seguridad	Departamento de Tecnología
						Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Departamento de Tecnología

Tabla Nº 34.- Plan de tratamiento de riesgos residuales
Elaborado por: El Autor

3.28 Políticas de seguridad de la información

Se elaboró el manual de Políticas de Seguridad de la información, que corresponde al documento que contiene las políticas, normas y lineamientos que regirán la seguridad de la información en la institución, las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información de la institución.

El debido cumplimiento de las políticas de seguridad de la información por parte todos los colaboradores y de terceros que tienen relación alguna con la entidad, permite minimizar al máximo los riesgos asociados con la seguridad de la información, pero para alcanzar este propósito, es necesario que la política del sistema de gestión de seguridad de la información sea impulsada por la alta directiva de la entidad.

En el presente trabajo se definido la política del Sistema de Gestión de Seguridad de la información y política que lo soportan, las cuales demuestran que existe un compromiso expreso por parte del Honorable Consejo Directivo con relación a la seguridad de la información. Adicional, a estas políticas es necesario contar con políticas relacionadas de seguridad involucren aspectos administrativos, físicos y tecnológicos orientadas a proteger los activos de información a través de los cuales se gestiona la información del negocio

Es fundamental divulgar en la entidad de forma adecuada el propósito de las políticas de seguridad de la información antes de su aplicación, con el objetivo de que los colaboradores y terceros comprendan como estas políticas ayudan a proteger la confidencialidad, integridad y disponibilidad de la información del negocio. Esta labor es esencial, para que los usuarios no vean en estas políticas como una serie de restricciones que les complicaran sus labores diarias,

sino por el contrato, lo que se busca con una adecuada socialización es conseguir que los usuarios entiendan los riesgos a los cuales está expuesta la entidad y las necesidades de tener unas normas para evitarlos.

El manual de Políticas de Seguridad de la Información desarrollado se basa en los objetivos del proyecto propuesto del Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001:2013, y para efecto del presente trabajo se documentaron las siguientes políticas de seguridad en un manual anexado a este trabajo de investigación:

NORMA ISO 27001:2013	A.5.	Política General de Seguridad de la Información
	A.6.	Organización de Seguridad de la Información
	A.7.	Seguridad de los Recursos Humanos
	A.8.	Gestión de Activos
	A.9.	Control de Acceso
	A.10.	Criptografía
	A.11.	Seguridad Física y del Entorno
	A.12.	Seguridad de las Operaciones
	A.13.	Seguridad de las Comunicaciones
	A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas
	A.15.	Relaciones con los Proveedores
	A.16.	Gestión de Incidentes de Seguridad de la Información
	A.17.	Seguridad de la Información en la Continuidad del Negocio
	A.18.	Cumplimiento de Requisitos Legales

Gráfico No. 11: Anexo de Norma ISO/IEC 27001:2013
Elaborado por: ISO/IEC 27000
Fuente: https://www.iso.org/stage-codes.html

3.29 Desarrollo de políticas de seguridad

La gran diversidad de amenazas internas y externas a las que está sometida la información son conocidas, la política de seguridad busca minimizar los riesgos, el éxito total se conseguirá con el compromiso de las autoridades de la universidad, con la difusión completa y extensa de las políticas y con el compromiso masivo de los usuarios en el cumplimiento total de las políticas.

El desarrollo de las políticas de seguridad de la información se realizó para el Departamento de Tecnología de la UISRAEL, partiendo de la información recopilada del análisis de la situación actual y basándose en los controles de la norma ISO 27002 en su versión 2013.

3.30 Políticas de seguridad

El presente dominio tiene por objetivo establecer los lineamientos iniciales para la creación de políticas de seguridad de la información, las mismas que ayudarán a preservar las tres principales características de la información como son integridad, confidencialidad y disponibilidad de la información [13]. Las políticas establecidas en el presente dominio se basan en los objetivos establecidos en el Portal de ISO, “Políticas de Seguridad”. [16]

Directrices de la dirección en seguridad de la información.

Conjunto de políticas para la seguridad de la información.

Crear un manual de roles y responsabilidades para cada uno de los funcionarios, se debe establecer como política de seguridad, el mismo que debe estar aprobado, publicado y comunicado a todos los empleados de la universidad.

Para el cumplimiento de esta política es necesario que el Departamento de Tecnología asigne un comité para la creación del manual de roles, políticas y responsabilidades para cada uno de los empleados, el mismo que debe ser documentado, revisado, verificado, y aprobado por la máxima autoridad de la Dirección y Universidad, tomando en cuenta todos los cargos concernientes a políticas de seguridad de la información. En este manual deben constar todos los cargos, que se encuentran detallados en el organigrama de la Dirección.

3.31 Revisión de las políticas para la seguridad de la información

En lo que corresponde a revisión de políticas de seguridad se debe realizar periódicamente, al igual que el manual de roles y responsabilidades asignados a los funcionarios o al realizarse un cambio dentro de la universidad.

Para el cumplimiento de esta política es necesario que el Departamento de Tecnología de la UISRAEL asigne un comité interno o externo para la revisión del manual de roles, políticas y responsabilidades asignadas a los diferentes cargos de la dirección, este manual debe detallar las responsabilidades y procedimientos necesarios para mantener segura la información.

3.32 Aspectos organizativos de la seguridad de la información

Una de las partes fundamentales de los objetivos y actividades de la universidad es la administración de la seguridad de la información [14], para ello lo primordial es la gestión,

para realizar tareas como la aprobación, implementación y asignación de procedimientos y responsabilidades de políticas de seguridad. Para un desenvolvimiento exitoso en aspectos de seguridad se debe tener un asesoramiento externo sobre seguridad de la información. Las políticas establecidas en el presente dominio se basan en los objetivos expuestos en el portal de ISO, "Aspectos organizativos de la seguridad de la información". [17]

3.33 Organización interna

3.33.1 Asignación de responsabilidades para la seguridad de la información

Se establece como política de seguridad definir y documentar las responsabilidades de los usuarios del Departamento de Tecnología, en especial las que tienen que ver con seguridad de la información. [15]

Para el cumplimiento de esta política es necesario que la persona responsable del Departamento de Tecnología de la UISRAEL asigne un responsable para elaborar el manual de políticas y procedimientos para el área de tecnologías de la información y comunicación en el que se debe plasmar los diversos roles y responsabilidades, con énfasis principal a los cargos concernientes a seguridad de la información. Las debilidades detectadas son:

- Actualmente la universidad no cuenta con personas dedicadas a la seguridad de la información.
- No poseen un manual de respaldos de la información, pero si realizan un respaldo semestral de los sistemas y bases de datos.
- No disponen de un listado de amenazas de activo de información.

- No generan manuales de configuración de los diversos sistemas, ni planes de contingencia anti desastres.

3.34 Segregación de tareas

La política de seguridad es segregar tareas y áreas de responsabilidad para cada uno de los miembros o funcionarios de la dirección para evitar modificaciones no autorizadas o no intencionadas.

Para el cumplimiento de esta política es necesario que cada funcionario o encargado del área de sistemas de cada departamento o facultad capacite a los usuarios de su área o departamento asignado a su responsabilidad, sobre el uso de los sistemas de información y bases de datos si fuera el caso, para evitar modificación no autorizada o no intencionada, o el mal uso de los activos. De ocurrir algún conflicto el responsable del departamento o área será el encargado de solucionarlo.

En caso de ocurrir incidentes relacionados con áreas seguras como perímetros de seguridad, control de acceso, protección contra amenazas externas y de medio ambiente que el encargado del departamento o facultad no pueda solucionarlo deben notificar al encargado de Seguridad de la Información.

3.34.1 Contacto con las autoridades

Mantener el contacto con las autoridades institucionales o nacionales apropiadas que rijan la Educación Superior para mantenerse actualizados ante posibles cambios en los reglamentos o leyes.

Para el cumplimiento de esta política es necesario que se mantenga contacto con autoridades de universidades de la provincia y nacionales para brindar un mejor rendimiento dentro de la institución, en caso de realizarse alguna actualización en las políticas de uso de la información.

Además, al mantener contacto con las autoridades pertinentes dentro de la universidad es importante para la aprobación y revisión de las políticas y procedimientos que se agreguen dentro de la universidad.

3.34.2 Contacto con grupos de interés especial

La política de seguridad es mantener contacto con especialistas de seguridad de la información ya sea mediante grupos o foros.

Para el cumplimiento de esta política es necesario que una persona se mantenga actualizada sobre seguridad de la información, debe estar agregada a foros o grupos de especialistas de seguridad de la información para tener información sobre cambios o actualizaciones de las políticas de seguridad de la información.

3.35 Seguridad de la información en la gestión de proyectos.

Para la seguridad de la información en la gestión de proyectos la política de seguridad es implementar procedimientos de control de la información en la gestión y desarrollo de proyectos dentro de la universidad.

Para el cumplimiento de esta política es necesario que al gestionar y desarrollar nuevos proyectos dentro de la universidad, sin importar la índole del proyecto se aplique políticas de seguridad, es necesario que todo proyecto sea comunicado a la dirección para determinar que políticas se aplican a dicho proyecto.

Se debe asignar una comisión para que realice un análisis sobre la información a utilizar en el proyecto y para determinar las políticas a utilizar.

3.36 Dispositivos para movilidad y teletrabajo

3.36.1 Política de uso de dispositivos para movilidad

La política de seguridad es adoptar medidas de seguridad para manipulación de datos mediante dispositivos de movilidad.

Para el cumplimiento de esta política es necesario que la red de datos para dispositivos móviles sea restringida por control de acceso a redes, además que se debe controlar las aplicaciones o sistemas de información que se puedan ingresar desde dispositivos móviles. Se debe tomar en cuenta el control de acceso y la virtualización de las redes.

3.36.2 Teletrabajo

La política de seguridad es proteger la información a la que accede, procesa o almacena él o los funcionarios, desde ubicaciones distintas a su puesto de trabajo.

Para el cumplimiento de esta política es necesario realizar protección lógica de los equipos, que únicamente el personal autorizado por el responsable de seguridad de la información podrá ingresar a realizar cambios o trabajo fuera de la oficina. En caso de ocurrir fallas en la red deberá ingresar mediante los puertos de configuración, los que únicamente personal autorizado debe conocer las claves de acceso. Además, proteger mediante la utilización de contraseñas de acceso tanto a acceso remoto como a los puertos de configuración de servidores.

3.37 Seguridad ligada a los recursos humanos

El presente dominio pretende educar e informar a los funcionarios y colaboradores de la universidad desde que ingresan y de forma continua sobre la prioridad de preservar la confidencialidad de la información que se maneja, las sanciones a las que se encuentra expuesto en caso de incumplimiento de alguna política de seguridad. Además de que la universidad deposita toda su confianza al entregarle el acceso a información, por ende, el funcionario debe estar cociente de la importancia y responsabilidad que tiene a su cargo. Las políticas establecidas en el presente dominio se basan en los objetivos expuestos en el Portal de ISO, "Seguridad ligada a los recursos humanos". [18]

3.37.1 Antes de la contratación

- **Investigación de antecedentes**

Para los aspirantes a cargos administrativos o docentes para la universidad, es necesario realizar una investigación previa de antecedentes e historial laboral, para descartar todo tipo de amenaza a la seguridad de la universidad y de la información.

Para cumplir con esta política se debe realizar pruebas de admisión, pedir referencias personales, laborares, record del aspirante que asegure no tener problemas de índole legal.

3.37.2 Durante la contratación

- **Responsabilidades de gestión**

La política de seguridad es incluir todos los términos y condiciones de seguridad de la información cuando se realice el contrato con empleados, contratistas y terceros para la gestión de las mismas.

Para el cumplimiento de esta política es necesario que los términos y condiciones estén incluidas en el contrato de trabajo, estableciendo las diversas responsabilidades del empleado en la seguridad de la información. Los empleados deben estar informados adecuadamente sobre los roles y responsabilidades de seguridad, además de las sanciones en caso de incumplimiento, cuando la información este bajo su responsabilidad.

3.38 Concienciación, educación y capacitación de seguridad de la información

La política es incluir capacitaciones y requerimientos de seguridad, al asignar responsabilidades a cada funcionario, al iniciar y durante las labores. El responsable de coordinar las labores de capacitación necesarias para difundir las políticas de seguridad, es el departamento de talento humano en coordinación con la Dirección de Tecnología.

Todo el personal administrativo y docente debe recibir una adecuada capacitación y actualización sobre las políticas y normas relacionadas a la seguridad institucional y de la información.

Dentro del Departamento de Tecnología, el área de seguridad de la información es la encargada de proporcionar el material necesario para la capacitación, dicho material debe ser actualizado cada seis meses o cada vez que sea necesaria a fin de que la información ahí reflejada sea precisa.

3.39 Proceso disciplinario

En cuanto al proceso disciplinario, la política es que todos los incumplimientos u omisiones según la gravedad del acto, deben ser sancionados según políticas administrativas internas vigentes en la UISRAEL.

Para el cumplimiento de esta política, cualquier proceso disciplinario debe iniciarse cuando se haya verificado que se ha producido una violación a la seguridad de la información, este proceso debe garantizar el trato justo y correcto para la universidad y los empleados.

El proceso debe pronosticar una respuesta gradual, tomando en consideración la gravedad del acto, su impacto en la universidad, si el empleado fue correctamente capacitado, la sanción debe estar basada en el acuerdo de confidencial firmado al iniciar el contrato. Dependiendo de la gravedad del acto, el proceso deberá permitir la remoción inmediata de los derechos de acceso y privilegios otorgados, o la separación inmediata del empleado de la universidad.

3.40 Cese o cambio de puesto de trabajo

La política de seguridad es incluir la comunicación de las responsabilidades a la terminación de las actividades, los términos y condiciones incluidos en el contrato y acuerdo de

confidencialidad. El funcionario administrativo o docente debe presentar su renuncia de cese de funciones con suficiente tiempo de antelación, por lo menos 15 días de anticipación.

El encargado del área donde el empleado realizó sus funciones, es el responsable de supervisar la entrega formal de los activos al nuevo funcionario a ocupar la vacante, esto incluye claves de acceso, documentación, llaves, credenciales, herramientas de trabajo, equipos de cómputo y demás activos a su cargo.

El área de seguridad de la información es la encargada de inhabilitar las claves de acceso a los diversos sistemas de información, acceso a central de datos, acceso a bases de datos y correo electrónico del empleado que deja de pertenecer a la universidad. De ser necesario cambiar las claves de acceso a todos los sistemas de información que sean vulnerables a acceso.

3.41 Gestión de activos

Este dominio tiene por objetivo que la universidad tenga conocimiento de todos los activos que posee, que son importantes para administrar los diversos procesos que se realizan dentro de esta. Incluyendo los activos informáticos que son base de datos y archivos, procedimientos, manuales, planes de contingencia y de continuidad, documentación de archivos; activos de software como aplicaciones, sistemas de información, utilitarios y herramientas; los activos físicos son equipos de administración, comunicación y de uso de estudiantes, medios magnéticos, equipos técnicos y activos en cuanto a servicios informáticos de comunicación y utilitarios. Las políticas de seguridad desarrolladas en este dominio proyectan cumplir con los objetivos de control planteados en el portal ISO, “Gestión de activos”. [19]

3.42 Responsabilidad sobre los activos

3.42.1 Inventario de Activos

Como política de seguridad del Departamento de Tecnología debe tener identificados los activos de información, en especial los más importantes y la relación con los sistemas de información que maneja la universidad, así como sus respectivos custodios y la ubicación física de cada activo.

Se verificó que la UISRAEL cuenta con el departamento de administración de bienes el que está a cargo de realizar el inventario de activos de cada departamento y dirección.

El inventario de activos debe estar actualizado permanentemente, en caso de que exista alguna modificación administrativa o de estado del activo, en caso de que sucediera un cambio en el activo y este no se notificaría al departamento de administración de bienes o de la Dirección de Tecnología dependiendo del activo, la responsabilidad recaerá sobre el custodio del activo.

3.42.2 Propiedad de los Activos

En cuanto a propiedad de activos, la política es que toda la información que pertenezca a la universidad está sujeta a revisiones periódicas por parte del área de seguridad de la información por la persona asignada para esta función.

Los activos de información pertenecen a la UISRAEL a menos que las leyes nacionales dicten lo contrario, por esta razón la facultad de otorgar acceso a la información es el Área de Seguridad, área encargada de resguardar la seguridad de los datos.

Para cumplir esta política, cada uno de los activos de la información como hardware, software, equipos de cómputo, de comunicaciones y la información deben estar custodiadas por un funcionario a cargo de actividades relacionadas con dicho activo. Con esta relación se crea una responsabilidad sobre el uso del activo.

3.42.3 Uso aceptable de los activos

La política se rige en que los activos de información de la UISRAEL son de propiedad de la misma, por tal motivo debe ser utilizada únicamente para fines laborales.

3.42.4 Devolución de activos

Durante el proceso se cesación de funciones la política de seguridad es garantizar que se cumpla con la entrega formal de los activos a cago del funcionario.

3.43 Clasificación de la información

3.43.1 Directrices de clasificación

La política de seguridad es clasificar la información de acuerdo a las tres características de seguridad: confidencialidad, integridad y disponibilidad.

Se debe clasificar la información almacenada en medios físicos, utilizando etiquetas para establecer el nivel de criticidad, y capacitar a los funcionarios que la manipula para evitar hurto de información o manipulación inadecuada o eliminación de información importante para la universidad.

3.43.2 Etiquetado y manipulado de la información

En lo que se refiere al etiquetado y manipulación la política de seguridad es etiquetar la información y los activos, para que los funcionarios sepan cómo manipularlos y evitar perdida, manipulación o hurto de información esencial.

3.43.3 Manipulación de activos

En referencia a la manipulación de activos, la política de seguridad es que todos los funcionarios que utilizan activos de información, deben tener conocimiento de los niveles de criticidad y las políticas de seguridad que debe cumplir para manipular la información.

Para el cumplimiento de esta política es necesario que al momento que ingresa un nuevo empleado a la universidad, se realizase una capacitación sobre los niveles de criticidad de la información a la que va a acceder, además de compartir las políticas de seguridad que debe aplicar, para evitar errores en la manipulación de activos de información.

Mantener constantemente capacitados a todo el personal de la universidad sobre las nuevas políticas o niveles de criticidad de la información.

3.44 Manejo de los soportes de almacenamiento

3.44.1 Gestión de soporte extraíbles

Para la gestión de soporte extraíbles la política de seguridad es que el responsable de cada área, departamento o facultad dependiendo de la criticidad de la información que ahí se procese, controlar los medios informáticos removibles que ahí se utilicen.

Para el cumplimiento de esta política es necesario que los medios informáticos removibles que existan en cada departamento, debe estar asignado para cada proceso o para almacenar determinada información, por ejemplo, se debe asignar solo un disco duro para guardar los respaldos de información, y no utilizarlo para otro fin.

3.44.2 Eliminación de soportes

En lo que se refiere a eliminación de soporte la política de seguridad es eliminar o expulsar los medios informáticos removibles de los equipos de forma segura, para evitar el plagio de información.

Para el cumplimiento de esta política es necesario que el encargado del área o dirección, realice una revisión del medio informático al que se va a eliminar el soporte para verificar que se haya obtenidos los respaldos necesarios, y que no contenga información de la Universidad.

Una vez realizada la revisión debe ser formateado para borrar toda la información que contenía.

3.44.3 Soportes físicos en tránsito

Como política de seguridad se propone proteger los medios de información contra acceso no autorizado cuando salgan del departamento o perímetro y seguridad.

Para el cumplimiento de esta política es necesario que la información que se encuentre en los medios removibles que salen fuera de la Universidad, sean protegidos por claves de acceso, o de lo contrario evitar que los medios removibles contengan información sensible o de alta criticidad para evitar el acceso no autorizado o la corrupción.

3.45 Control de acceso

Este dominio tiene por objetivo controlar el acceso a los sistemas de información, servicios de información, bases de datos e instalaciones de procesamiento de información por medio de restricciones de acceso y excepciones. Esto ayuda a mantener protegida la información, contra accesos no autorizados y manipulación inadecuada de información por personal ajeno a la Universidad. Las políticas de seguridad que se establecen en este dominio procuran cumplir con los controles establecidos en el Portal ISO, “Control de acceso”. [20]

3.46 Requisitos de negocio para el control de acceso

3.46.1 Política de control de acceso

Como política de seguridad se propone, definir claramente los controles de derechos de acceso individual y grupal.

3.46.2 Gestión de acceso de usuario

- **Gestión de altas/bajas en el registro de usuarios**

La política de seguridad es que el registro y cancelación de usuario, se debe realizar de manera independiente a cada usuario que requiera acceso a la información.

- **Gestión de los derechos de acceso asignados a usuarios**

Como política de seguridad se define implementar una herramienta o procedimientos para el control de usuarios, agregar o quitar permisos además de la gestión de las actividades realizadas por cada uno de ellos.

Es decir, utilizar una herramienta que facilite el trabajo de una auditoria sobre los derechos de acceso asignados a cada usuario. Se recomienda utilizar herramientas open source, que faciliten la realización de auditorías, además de implementar procedimientos que ayuden a controlar que los permisos otorgados a los usuarios sean los que pueda realizar dentro de los sistemas de información.

- **Gestión de los derechos de acceso con privilegios especiales**

Para la gestión de privilegios especiales, la política de seguridad es filtrar a los usuarios que requieran privilegios especiales a los sistemas de información, servidores, base de datos y servicios.

3.46.3 Revisión de los derechos de acceso de los usuarios

La política de seguridad es que el área de seguridad de la información debe realizar revisiones periódicas de los niveles de acceso otorgadas a los diferentes usuarios.

3.46.4 Retirada o adaptación de los derechos de acceso.

Cuando un funcionario finalice su contrato o decida finalizar sus funciones dentro de la universidad, la política de seguridad manifiesta que se debe retirar todos los derechos de acceso a los sistemas, bases de datos y servidores para resguardar la información.

Para que esta política se cumpla, el jefe de cada departamento es el responsable de notificar al área de seguridad de la información, del cese de funciones de los usuarios para que la persona encargada de creación y eliminación de cuentas de usuario, elimine al usuario y los privilegios asignados.

3.47 Responsabilidad del usuario

3.47.1 Uso de información confidencial para la autenticación.

La política de seguridad es que los usuarios tengan claras las buenas prácticas de seguridad de la información, para mantener segura la información de la universidad.

3.48 Control de acceso a sistemas y aplicaciones

3.48.1 Restricciones de acceso a la información

La política de seguridad es restringir el acceso a los sistemas de la información a cada usuario, tanto a externos como a usuarios del Departamento de Tecnología

3.48.2 Procedimientos seguros de inicio de sesión

En cuanto al inicio de sesión seguro, la política de seguridad se aplica a todos los sistemas desarrollados por la universidad, así como, a las aplicaciones de acceso de información, las mismas que deben tener una pantalla de acceso seguro de log-on, para asegurar que solamente personal autorizado tenga acceso.

3.48.3 Gestión de contraseñas de usuario

Para la gestión de contraseñas, la política de seguridad es que la contraseña de acceso a los sistemas de información de cada usuario, debe tener un nivel de complejidad alto que dificulte obtenerla.

Para el cumplimiento de esta política, la universidad debe establecer la complejidad de las contraseñas, por ejemplo, la contraseña debe constar de 16 caracteres entre letras, números y caracteres especiales, o usar un software administrador de contraseñas como keePass, que es un software portable que ayuda a la generación de contraseñas.

3.48.4 Uso de herramientas de administración de sistemas.

En lo que tiene que ver con el uso de herramientas de administración, la política de seguridad es que los controles dentro de las aplicaciones deben estar restringidos, únicamente para los administradores de las aplicaciones se debe crear perfiles con acceso total, para evitar el acceso y modifican de información.

Para el cumplimiento de esta política se debe crear perfiles de usuario para cada uno de los funcionarios, dependiendo del nivel de acceso asignado.

Únicamente los administradores de los sistemas de información pueden acceder a realizar modificaciones como parametrización o anulación de alguna transacción.

3.48.5 Control de acceso al código fuente de los programas.

Restringir el ingreso al código fuente de las aplicaciones a usuarios externos y no autorizados de participar en el proyecto o desarrollo, para evitar la usurpación o cambio de código fuente.

Para el cumplimiento de esta política, cuando el analista, diseñador o programador abandone su puesto de trabajo ya sea por largo o corto tiempo, su máquina debe permanecer suspendida o apagada y con clave de acceso a la misma, y la clave no debe ser la misma que el nombre de usuario.

3.48.6 Cifrado

El objetivo de este dominio es el uso de sistemas y técnicas criptográficas para la protección de la información, en base a un análisis de riesgo efectuado previamente, con el fin de asegurar una adecuada protección.

Las políticas planteadas en este dominio se basan en los controles publicados en el Portal ISO “Cifrado”. [21]

3.49 Controles criptográficos

3.49.1 Política de uso de controles criptográficos

Definir el uso de controles criptográficos para asegurar la confidencialidad de la información y el correcto uso de la misma.

3.50 La seguridad física y ambiental

El objetivo de este dominio es minimizar los riesgos de daños en la información y las operaciones de la institución, por desastres naturales o por falta de control en la seguridad física ante desastres ambientales. Además, de establecer los perímetros de seguridad de las áreas de procesamiento de información. Las políticas de seguridad planteadas en este dominio se basan en los controles establecidos y publicados en el Portal ISO "La seguridad física y ambiental". [22]

3.51 Áreas seguras

3.51.1 Perímetro de seguridad física

En lo que respecta a perímetros de seguridad, la política de seguridad debe restringir el acceso no autorizado a recursos tecnológicos que procesen información de la universidad, para preservar la confidencialidad de la información.

Para el cumplimiento de esta política los funcionarios deben cuidar los componentes tecnológicos, mantenerlos limpios, en buen estado, así como un registro de cada cambio que

se realice en la infraestructura física la misma que debe ser previamente analizada y debe enfocarse en proteger la información.

La UISRAEL cuenta con áreas de procesamiento de información, protegida por control de acceso mediante biométrico, únicamente personal autorizado puede ingresas las áreas restringidas.

Dependiendo de la criticidad de la información que se maneje dentro de cada área de procesamiento de información, se deben establecer límites o perímetros de acceso. Las puertas del edificio donde se encuentra el área de procesamiento de información deben estar protegidas, las paredes deben ser sólidas, dentro y fuera de edificio debe estar vigilada por cámaras y alarmas sonoras. Controlar el acceso a personal externo en la recepción, con una solicitud de identificación del personal externo. Las áreas que deben estar controladas son oficinas del departamento de sistemas, bodegas, oficinas de sistemas de cada carrera.

3.51.2 Controles físicos de entrada

La política de seguridad es que se deben establecer controles de acceso físico para poder acceder a las áreas de procesamiento de información.

3.51.3 Seguridad de oficinas, despachos y recursos

Mantener protegidas las oficinas, despachos y recursos donde se encuentren recursos tecnológicos y que procesen información, como prioridad las oficinas o departamentos de sistemas de cada facultad, donde se encuentran los servidores y cableado estructurado de la red de datos.

3.52 Seguridad de los equipos

3.52.1 Emplazamiento y protección de equipos

Para este control la política de seguridad es ubicar los equipos en un lugar seguro donde no estén expuestos a diversas amenazas físicas y ambientales para proteger la información.

3.52.2 Instalaciones de suministro

Para este control la política de seguridad es que las instalaciones donde se encuentran los equipos tecnológicos deberán estar protegidos y ser tolerantes a fallas eléctricas, para evitar pérdida de información, equipos tecnológicos y de comunicación.

3.52.3 Seguridad del cableado

En cuanto a seguridad de cableado, la política de seguridad es que el cableado de datos y eléctrico debe ser protegido contra daños ya sean provocados, e interrupciones para evitar desastres.

3.52.4 Mantenimiento de los equipos

Para este control la política de seguridad es brindar mantenimiento continuo a los equipos que pertenecen a la universidad en especial a los que procesen información, para asegurar la disponibilidad de los mismos.

3.52.5 Salida de activos fuera de las dependencias de la universidad

En cuanto a la salida de activos fuera de la universidad, la política de seguridad es que los equipos portátiles o tecnológicos que tengan información de la institución no salgan de su sitio de trabajo, sin previa autorización.

3.52.6 Seguridad de los equipos y activos fuera de las instalaciones

La política de seguridad es proteger la información que se encuentre en los equipos que procesen información fuera de la universidad, para asegurar la disponibilidad, confidencialidad de la información.

3.52.7 Equipo informático de usuario desatendido

La política de seguridad es que el administrador de redes y sistemas de cada dirección realice revisiones periódicas de los equipos que no están en constante uso, en especial de los equipos que procesen información.

3.52.8 Política de puesto de trabajo despejado y bloqueo de pantalla

Para puestos de trabajo despejados y bloqueos de pantalla, la política de seguridad es mantener la información protegida, cuando el funcionario se aleja de su puesto de trabajo por un corto o largo tiempo, bloquear la pantalla en un lapso de tiempo prudente de inactividad.

3.53 Seguridad en la operativa

El objetivo de este dominio es, controlar la existencia de documentación de los procedimientos de operaciones, planes de contingencia además de la mejora y mantenimiento continuo de los mismos, para el acceso no autorizado se debe definir y documentar controles, protección contra software malicioso y documentación para resguardar la seguridad de la base de datos y la restauración de copias de seguridad. Las políticas de seguridad se basan en los controles publicados en el Portal ISO "Seguridad en la operativa". [23]

3.53.1 Responsabilidades y procedimientos de operación

- **Documentación de procedimientos de operación**

Para este control, la política de seguridad es la creación y documentación de los procedimientos operativos de los diversos sistemas de información que utiliza la UISRAEL.

- **Gestión de cambios**

En cuanto a la gestión de cambios, la política de seguridad es que antes de realizar un cambio en el ambiente operativo, este debe ser evaluado y documentado por el encargado del área de seguridad de la información en conjunto con el personal del Departamento de Tecnología.

- **Gestión de capacidades**

En cuanto a la gestión de capacidades, la política de seguridad es monitorear el rendimiento de los sistemas de información para optimizar los recursos dependiendo de la capacidad de información y requerimientos a futuro.

Separación de entornos de desarrollo, prueba y producción.

Para este control la política de seguridad es crear entornos para las principales fases del ciclo de vida de un proyecto, desarrollo, pruebas y producción de preferencia deben separarse físicamente, cuando se debe trasladar un sistema o servicio entre entornos, este traslado debe ser documentado.

3.54 Protección contra código malicioso

3.54.1 Controles contra el código malicioso

La política de seguridad es construir controles técnicos o no técnicos para proteger la información e infraestructura tecnológica contra virus, malware y concienciar a los usuarios sobre la sensibilidad de la información.

3.55 Copia de seguridad

3.55.1 Copias de seguridad de la información

En cuanto a copias de seguridad, la política de seguridad es comprobar que las copias de seguridad funcionen correctamente, y que los respaldos se realicen de acuerdo a los tiempos y días acordados.

3.56 Registro de actividad y supervisión

3.56.1 Registro y gestión de eventos de actividad

Para el registro y control de eventos, la política de seguridad es crear campos de auditoria para controlar y revisar periódicamente las actividades que cada usuario realiza, además de añadir excepciones para evitar errores y fallas en los sistemas.

3.56.2 Protección de los registros de información

Para este control la política de seguridad es que cada usuario que ingrese a los sistemas de información de la universidad tenga asignado un rol dependiendo de las funciones que vaya a realizar para proteger la información de manipulaciones no permitidas.

3.56.3 Registros de actividad del administrador y operador del sistema

En cuanto a las actividades del administrado, la política de seguridad es registrar cada una de las actividades que realiza el administrador y operadores de los sistemas de información de cada una de las facultades.

3.56.4 Sincronización de relojes

Para este control la política de seguridad es sincronizar los relojes de todos los sistemas de procesamiento de información, así como los de bases de datos para tener un registro real de las transacciones realizadas.

3.57 Control del software en explotación

3.57.1 Instalación del software en sistemas en producción

La política de seguridad es que se debe planificar los cambios en los sistemas de información y realizar pruebas con el fin de asegurar el correcto funcionamiento.

3.58 Gestión de vulnerabilidades técnicas

3.58.1 Gestión de las vulnerabilidades técnicas

Mantener actualizado el inventario de los equipos físicos y de software como fecha de compra, vida útil, versión, actualizaciones o service packs instalados, para evitar daños en los equipos por software instalado o por tiempo de vida útil de los equipos.

Para el cumplimiento de esta política es necesario asignar un responsable para el monitoreo y exploración de las vulnerabilidades, el mismo que deberá realizar una planificación en línea de tiempo de las vulnerabilidades existentes.

Cuando se identifique la vulnerabilidad se debe realizar un análisis de los riesgos y acciones a realizarse para mitigar la vulnerabilidad, dependiendo de la criticidad del riesgo primero se deberá probar y evaluar antes de ser instaladas en el ambiente de producción, luego se realizarán las acciones necesarias como actualizaciones, parches o demás configuraciones técnicas.

En caso de que los fabricantes no cuenten con el parche o la actualización se debe desconectar los servicios, agregar controles de acceso, incrementar el monitoreo, mantener el registro de auditoria de todos los procedimientos, tratar primero los sistemas de mayor criticidad y la gestión de la vulnerabilidad debe ser monitoreada y evaluada.

3.58.2 Restricciones en la instalación de software

La política de seguridad es controlar las aplicaciones y software instalado en las computadoras de cada uno de los funcionarios de la universidad.

3.59 Consideraciones de auditorías de los sistemas de información

3.59.1 Controles de auditoría de los sistemas de información

Para este control la política de seguridad es realizar auditorías internas y externas periódicamente para verificar el correcto funcionamiento de los sistemas de información.

3.60 Seguridad en las telecomunicaciones

El objetivo del presente dominio es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte, la gestión de seguridades en las telecomunicaciones considera el flujo de datos, implicaciones legales internas y externas.

El intercambio de información entre instituciones y redes públicas debe ser confidencial.

Las políticas de seguridad planteadas en el presente dominio procuran cumplir con los objetivos publicados en el Portal ISO “Seguridad en las telecomunicaciones”. [24]

3.61 Gestión de la seguridad en las redes

3.61.1 Controles de red

En relación al control de red la política de seguridad es administrar y monitorear las redes continuamente, manteniendo la seguridad y garantizando que la información transmitida este seguro y libre de acceso no autorizado.

3.61.2 Mecanismos de seguridad asociados a servicios en red

En cuanto a mecanismos de seguridad asociados a servicios en red, la política de seguridad es que cada servicio que se desee implementar externo o interno, debe incluir características de seguridad que asegure la integridad de la información.

3.61.3 Segregación de redes

Para segregación de redes, la política de seguridad es dividir la red de datos en dominios lógicos y mantener los segmentos de red separados.

3.62 Intercambio de información con partes externas

3.62.1 Políticas y procedimientos de intercambio de información

Para el intercambio de información, la política de seguridad es autorizar y revisar todo tipo de información que se transfiera a organismos externos y por cualquier medio de comunicación.

3.62.2 Acuerdos de intercambio

Para acuerdos de intercambio, la política de seguridad es asegurar la información a transferir a organizaciones externas, si es necesario la información debe ser encriptado para su transmisión.

3.62.3 Mensajería electrónica

La política de seguridad, es la utilización del correo institucional para envió y recepción de información, para su protección se debe revisar periódicamente la información que se envía y se recibe en las cuentas de correo electrónico.

3.62.4 Acuerdos de confidencialidad y secreto

Para este control, la política de seguridad es identificar, revisar y documentar regularmente los acuerdos de confidencialidad de la información que la universidad tiene para evitar su divulgación.

Para el cumplimiento de esta política es necesario que el director del Departamento de Tecnología asigne la responsabilidad de revisar continuamente los acuerdos de confidencialidad a un funcionario del área de sistemas, el mismo que revisará e informara a la dirección los cambios que crea necesarios, los mismos que serán analizados y autorizados para realizar los cambios en los acuerdos.

3.63 Adquisición, desarrollo y mantenimiento de los sistemas de información

El presente dominio tiene por objetivo la adquisición, desarrollo y mantenimiento de los sistemas de información que la universidad maneja, incluir controles para la validación de datos y correcto funcionamiento durante la adquisición y desarrollo. Aplicar procedimientos de control durante todo el ciclo de vida de desarrollo de proyectos incluyendo la protección de información crítica y sensible.

Las políticas planteadas en este dominio aplican a todos los sistemas de información ya sean desarrollos propios o de terceros, estas políticas se basan en los controles publicados en el Portal ISO “Adquisición, desarrollo y mantenimiento de los sistemas de información”. [25]

3.64 Requisitos de seguridad de los sistemas de información

3.64.1 Análisis y especificación de los requisitos de seguridad

Para este control, la política de seguridad es analizar y especificar los requerimientos de seguridad de la información para las mejoras y nuevos sistemas de información.

3.64.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas

En cuanto a seguridad de las comunicaciones en servicios accesibles por redes públicas, la política de seguridad es proteger la información que pasa atreves de las aplicaciones que utilizan redes públicas para transferirla.

3.64.3 Protección de las transacciones por redes telemáticas

La política de seguridad es proteger la información de la transmisión o enrutamiento incorrecto y evitar la alteración duplicación o divulgación no autorizada.

3.65 Seguridad de los procesos de desarrollo y soporte

3.65.1 Política de desarrollo seguro de software

Para el desarrollo de software seguro, la política de seguridad es constituir y aplicar reglas para el desarrollo de sistemas para proteger la información y el código fuente de los sistemas.

3.65.2 Procedimientos de control de cambios en los sistemas

En relación a procedimientos de control de cambios en los sistemas, la política de seguridad es mitigar los riesgos por cambios sobre el software ya sean estos planificados o requeridos.

3.65.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Para este control la política de seguridad es garantizar que los cambios realizados en los sistemas de información no tengan un impacto negativo en las operaciones y seguridad de los sistemas de información.

3.66 Seguridad en entornos de desarrollo

Para los entornos de desarrollo la política de seguridad es proteger adecuadamente los entornos de desarrollo que cubre todo el ciclo de vida de desarrollo del sistema.

3.66.1 Externalización del desarrollo de software

En cuanto a externalización del desarrollo de software la política de seguridad es monitorear y supervisar cada una de las actividades del desarrollo de sistemas que se realicen fuera de la universidad.

3.66.2 Pruebas de funcionalidad durante el desarrollo de los sistemas

Para este control la política de seguridad es realizar pruebas de funcionalidad y en especial de seguridad, durante la etapa de desarrollo para evitar desperfectos en el producto final.

Para el cumplimiento de esta política es necesario elaborar una planificación de pruebas con usuarios reales, para evaluar el nivel de seguridad de los sistemas y de ser necesario cambiar los criterios o procedimientos empleados para proteger la información. Además,

documentar las pruebas realizadas, con la fecha de las pruebas y las observaciones realizadas por los usuarios que realicen las pruebas.

3.66.3 Pruebas de aceptación.

En cuanto a pruebas de aceptación, la política de seguridad es elaborar un plan de pruebas y el ambiente en el que se realizara las pruebas para la aceptación de los nuevos sistemas o actualizaciones de versiones.

3.67 Datos de prueba

3.67.1 Protección de los datos utilizados en pruebas

En cuanto a protección de los datos utilizados en pruebas, la política de seguridad es clasificar cuidadosamente los datos a utilizar para pruebas evitando que se utilicen datos sensibles.

3.67.2 Relaciones con suministradores

El presente dominio pretende implementar y mantener el nivel de seguridad de la información, mediante los acuerdos de entrega de servicios de terceros, monitorear el cumplimiento de dichos acuerdos acorde con los estándares y manejos de cambios para satisfacer los requerimientos acordados de los servicios entregados. Las políticas de seguridad planteadas en este dominio se basan en los controles publicados en el Portal ISO “Relaciones con suministradores”. [26]

3.68 Seguridad de la información en las relaciones con suministradores

3.68.1 Política de seguridad de la información para suministradores

La política de seguridad es establecer y documentar los requerimientos de seguridad de la información para mitigar los riesgos de acceso no autorizado por parte de proveedores y terceros.

3.68.2 Cadena de suministro en tecnologías de la información y comunicaciones

Para suministros en cadena, la política de seguridad es establecer y documentar los requerimientos de seguridad de la información que se adquieren en cadena de los diferentes proveedores, para mitigar el riesgo de acceso no autorizado y el cumplimiento con las políticas anteriores de este control.

3.69 Gestión de la prestación de servicios por suministradores

3.69.1 Supervisión y revisión de los servicios prestados por terceros

Para este control, la política de seguridad es auditar y monitorear permanentemente los servicios prestados por terceros para cerciorarse que los servicios cumplen con la función para la que fueron contratados.

3.69.2 Gestión de cambios en los servicios prestados por terceros

Gestionar los cambios en los servicios prestados por terceros, el mantenimiento, procedimientos y controles de seguridad tomando en cuenta la criticidad de la información que manejan.

3.69.3 Gestión de los incidentes en la seguridad de la información

El presente dominio tiene por objetivo gestionar los diversos incidentes tomando en cuenta que todos los activos de información con los que cuenta la universidad están expuestos a sufrir incidentes de seguridad, se debe garantizar la gestión de estos incidentes iniciando desde la comunicación, de forma que sean corregidos oportunamente.

Para gestionar dichos incidentes es necesario la detección, comunicación, tratamiento y colaboración en la prevención de similares incidentes, para esto se requiere la colaboración de todo el personal de la universidad. Las políticas de seguridad establecidas en este dominio se basan en los controles publicados en el portal ISO “Gestión de los incidentes en la seguridad de la información”. [27]

3.70 Gestión de incidentes de seguridad de la información y mejoras

3.70.1 Responsabilidades y procedimientos

La política de seguridad es asignar las responsabilidades y procedimientos, a cada uno de los funcionarios del área de sistemas y demás departamentos para identificar eficaz y rápidamente los incidentes de seguridad.

3.70.2 Notificación de los eventos de seguridad de la información

En cuanto a eventos de información suscitados, la política de seguridad es informar sobre los eventos de seguridad implementados o actualizados, lo antes posible mediante correos electrónicos y circulares a los encargados y empleados que utilizan los sistemas de información afectados.

3.70.3 Notificación de puntos débiles de la seguridad

En cuanto a puntos débiles, la política de seguridad es notificar cualquier tipo de evento o debilidad sospechosa que pueda afectar al funcionamiento normal de los sistemas de información.

3.70.4 Valoración de eventos de seguridad de la información y toma de decisiones

La política de seguridad es evaluar los eventos de seguridad de acuerdo al análisis realizado y tomar decisiones sobre la calificación del incidente.

3.70.5 Respuesta a los incidentes de seguridad

La política de seguridad es que se debe proporcionar una respuesta inmediata ante los incidentes de información cumpliendo los procedimientos documentados.

3.70.6 Recopilación de evidencias

La política de seguridad es, definir y aplicar procedimientos para mantener un registro de los incidentes para identificar y prevenir que vuela a suceder.

3.71 Elaboración de un plan de evaluación continua de seguridad de la información mediante responsabilidades y procedimientos

El objetivo es evaluar continuamente la seguridad de la información para mantener sus principales características.

Para el cumplimiento de este objetivo se desarrolla políticas de seguridad para asegurar la continuidad del negocio, y el cumplimiento de políticas anteriores.

3.72 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

El objetivo de este dominio es, preservar la seguridad de la información durante las fases de activación y desarrollo de procesos, procedimientos y planes; incluyendo dentro de los procesos críticos la gestión de la seguridad referente a la legislación, personal, materiales, transporte e instalación de servicios adicionales.

Las políticas establecidas en el presente dominio se basan en los controles publicados en el portal ISO “Aspectos de seguridad de la información en la gestión de la continuidad del negocio”. [28]

3.73 Continuidad de seguridad de la Información

3.73.1 Planificación de la continuidad de la seguridad de la información

Para la planificación de la continuidad de la seguridad, la política de seguridad es determinar las necesidades y requisitos para la gestión de situaciones de crisis y desastres que afecten a la seguridad de la información.

3.73.2 Implantación de la continuidad de la seguridad de la información

Para la implementación, la política de seguridad es identificar, documentar y ejecutar los procedimientos y controles para garantizar el nivel de seguridad de la información que requiera la universidad ante situaciones adversas.

3.73.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Verificar y evaluar periódicamente los controles de políticas de seguridad de continuidad del negocio, para que en caso de situaciones adveras estos controles sean eficaces y válidos.

3.74 Redundancias

3.74.1 Disponibilidad de instalaciones para el procesamiento de información

La política de seguridad es tener un área adecuada y con suficiente espacio para las instalaciones de procesamiento de información, para que la información mantenga su característica de disponibilidad.

3.75 Cumplimiento

Las políticas detalladas en este documento deben ser cumplidas por todos los funcionarios que directa o indirectamente tengan contacto o procesen información. En especial los funcionarios que mantengan contacto directo con los sistemas de información.

Todas las implementaciones de seguridad deben estar dentro de las normas legales que rigen a las entidades educativas públicas. Se basan en los controles publicados por el portal ISO "Cumplimiento". [29]

3.76 Cumplimiento de los requisitos legales y contractuales

3.76.1 Identificación de la legislación aplicable

Para este control, la política de seguridad es identificar, documentar y mantener las normas y estatutos legales que involucran e intervienen en el cumplimiento de las políticas de seguridad.

3.76.2 Derechos de propiedad intelectual (DPI)

En cuanto a derechos de propiedad intelectual, la política de seguridad es garantizar el cumplimento de los derechos de propiedad intelectual utilizando software original.

3.76.3 Protección de datos y privacidad de la información personal

La política de seguridad es garantizar que la información personal de los empleados, docentes, funcionarios y estudiantes se encuentre protegida según los reglamentos y normativas pertinentes.

3.76.4 Regulación de los controles criptográficos

La política de seguridad es, utilizar controles criptográficos para garantizar la seguridad de la información, de acuerdo con las normas, acuerdos y reglas pertinentes.

3.77 Revisiones de la seguridad de la información

3.77.1 Revisión independiente de la seguridad de la información

Para la revisión individual de la seguridad, la política de seguridad es identificar las políticas de seguridad establecidas en el presente documento que van a ser aplicadas a la universidad dependiendo de las necesidades.

CAPITULO 1V

4. Conclusiones y recomendaciones

4.1 Conclusiones

- Al realizar la presente investigación, mediante el análisis realizado a los medios lógicos y físicos se pudo determinar que el activo más importante de la institución es la información, por lo tanto, se desarrolla las políticas de protección para evitar modificaciones o accesos no autorizados.

- El personal administrativo, docentes y estudiantes realizan sus funciones acorde a la información que brindan los sistemas de la universidad, por lo tanto, es importante que la información y centros de procesamiento tengan restringido el acceso, estableciendo lineamientos de seguridad para la información en base a la norma ISO 27002, que ayuda a protegerla, puesto que las políticas de seguridad minimizan el riesgo de pérdida de información garantizando el correcto funcionamiento de los procesos.

- La tecnología cada día cambia, por esta razón la universidad debe estar constantemente actualizada en los ámbitos de tecnología, telecomunicaciones y políticas de seguridad, aplicando procedimientos, documentación y manuales para la estandarización de los procesos.

- La Dirección de Tecnología mantendrá por medio de bitácoras y documentos de respaldo (informes, solicitudes, correos), los incidentes presentados en el manejo de la información para la mejora continua.

4.2 Recomendaciones

Se recomienda:

- Realizar una campaña de capacitación a los usuarios involucrados en los procesos, para crear una cultura de colaboración y asistencia en la seguridad, así como para la implementación de futuras mejoras dentro de la universidad.

- Que La Dirección de Tecnología profundice el conocimiento de la Norma ISO 27001 y 27002, para contar con la asistencia de personal capacitado y certificado en este estándar; se debe tomar en cuenta las diversas amenazas a los activos y aplicar las políticas necesarias para mitigar el riesgo al que está expuesto funcionamiento del activo.

- Formalizar el documento de políticas de seguridad para su aprobación por el consejo universitario y la difusión de las mismas a todos los funcionarios y empleados de la institución, de modo que se cree conciencia sobre la importancia de la información y se mantenga un estricto control en los cambios de software, acceso al código fuente para evitar el plagio de información y de sistemas desarrollados dentro de la universidad.

BIBLIOGRAFÍA

[1] Norma de Seguridad Informática ISO 27001 para mejorar la confiabilidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco LTDA., [Online]. Universidad Técnica de Ambato. Disponible en: http://repo.uta.edu.ec/bitstream/handle/123456789/2361/Tesis_t715si.pdf?sequence=1.

[2] Análisis e Implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil, [Online]. Universidad Politécnica Salesiana sede Guayaquil. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf.

[3] Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la norma ISO/IEC 27002", [Online]. Escuela Politécnica del Ejército. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/6025/1/T-ESPE-034491.pdf.

[4] Purificación Aguilera, Seguridad Informática, 1ra ed. Editex, Seguridad Informática, 2010, pp. 9.

[5] Purificación Aguilera, Seguridad Informática, 1ra ed. Editex, Tipos de Seguridad, 2010, pp. 9.

[6] Carmen de Pablos, Institución y transformación de los sistemas de información en empresas, 1ra ed. Universidad Rey San Carlos, 2011, pp. 360.

[7] Directorio de la norma ISO 27000. [Online]. Disponible en: http://www.27000.org/iso-27002.htm.

[8] El portal de ISO 27001 en Español. [Online]. Disponible en: http://www.iso27000.es/iso27000.html [Accedido: Enero. 18, 2017].

[9] ISO 27002:2013 [Online]. Disponible en: http://www.iso27000.es/download/ControlesISO27002-2013.pdf [Accedido: Enero. 18, 2017].

[10] ISO 27000.es, "El portal de ISO 27001 en Español", [Online]. Disponible en: http://iso27000.es/glosario.html [Accedido: Mayo. 18, 2014].

[11] Carla Rodríguez Salas. (2002). Gestión de la Información e las Organizaciones, Bibliotecas, vol. XX (1 y 2), pp. 19-34.

[12] Galende Díaz Juan Carlos, Criptografía Historia de la escritura cifrada, 1ra ed., Editorial Complutense, 1995, pp. 15.

[13] Martínez Juan Gaspar, Planes de contingencia, 1ra ed., Editorial Díaz de Santo S.A., 2004, pp. 28.

[14] UTA, "DITIC", [Online]. Disponible en: www.uta.edu.ec.

[15] Acuerdo de Confidencialidad [Online]. Disponible en: http://www.jcyl.es/web/jcyl/binarios/982/337/Modelo%20Contrato%20de%20Confidencialidad.doc?blobheader=application/msword&blobnocache=true

[16] ISO 27000.es, "Políticas de Seguridad", [Online]. Disponible en: http://iso27000.es/iso27002_5.html.

[17] ISO 27000.es, "Aspectos organizativos de la seguridad de la información", [Online]. Disponible en: http://iso27000.es/iso27002_6.html.

[18] ISO 27000.es, "Seguridad ligada a los recursos humanos", [Online]. Disponible en: http://iso27000.es/iso27002_7.html.

[19] ISO 27000.es, "Gestión de activos", [Online]. Disponible en: http://iso27000.es/iso27002_8.html.

[20] ISO 27000.es, "Control de acceso", [Online]. Disponible en: http://iso27000.es/iso27002_9.html.

[21] ISO 27000.es, "Cifrado", [Online]. Disponible en: http://iso27000.es/iso27002_10.html.

[22] ISO 27000.es, "La seguridad física y ambiental", [Online]. Disponible en: http://iso27000.es/iso27002_11.html.

[23] ISO 27000.es, “Seguridad en la operativa”, [Online]. Disponible en: http://iso27000.es/iso27002_12.html.

[24] ISO 27000.es, “Seguridad en las telecomunicaciones”, [Online]. Disponible en: http://iso27000.es/iso27002_13.html.

[25] ISO 27000.es, “Adquisición, desarrollo y mantenimiento de los sistemas de información”, [Online]. Disponible en: http://iso27000.es/iso27002_14.html.

[26] ISO 27000.es, “Relaciones con suministradores”, [Online]. Disponible en: http://iso27000.es/iso27002_15.html.

[27] ISO 27000.es, “Gestión de los incidentes en la seguridad de la información”, [Online]. Disponible en: http://iso27000.es/iso27002_16.html.

[28] ISO 27000.es, “Aspectos de seguridad de la información en la gestión de la continuidad del negocio”, [Online]. Disponible en: http://iso27000.es/iso27002_17.html.

[29] ISO 27000.es, “Cumplimiento”, [Online]. Disponible en: http://iso27000.es/iso27002_18.html.

ANEXOS

ANEXO A

Formulario de Creación de usuario y responsabilidad de contraseñas

	FORMULARIO DE CLAVES		
	UNIVERSIDAD TECNOLOGICA ISRAEL		
	CODIGO: F-DTI--001	**Elaborado:** 03 de Marzo de 2017	**Versión: 1.0**

Estimad@ usuari@

Para descomprimir su archivo, utilice la siguiente **CONTRASEÑA**".

Le informamos que la CONTRASEÑA es personal e intransferible, por ningún motivo debe proporcionar a terceros.

Contraseña: **Diferenciar mayúsculas y minúsculas**	

Para personalizar su clave deberá componerla con caracteres que incluyan MAYÚSCULAS, minúsculas, números y caracteres especiales (como @ # * + $ % &), mínimo 8 caracteres.

En caso de existir algún inconveniente al momento del registro de datos y/o para cambiar su contraseña, por favor comunicarse al 3316-819 la extensión 303 (Help Desk).

Atentamente,

Seguridad de la Información

XXXXXXXXXXXXXXXXXXXXXX

El Art. 202.1 del Código Penal Ecuatoriano determina que cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Recibí usuario, contraseña e inducción inicial sobre Seguridad de la Información

Quito, 03 de Marzo de 2017

Nombre del Usuario:

Cedula:

Firma: _____

Fecha: _____

ANEXO B

Acta de Entrega para Equipos de Computación

	UNIVERSIDAD TECNOLOGICA ISRAEL	03 de Marzo de 2017
		Responsable
	ACTA DE ENTREGA DE EQUIPOS DE COMPUTACIÓN	Técnico Responsable
		www.uisrael.edu.ec

Hoy _dia_ del mes de ___mes__ de __año__ en las oficinas de la institución, mediante el presente documento se realiza la entrega formal de los equipos de cómputo que se indican el punto 2.- EQUIPOS DE COMPUTO ASIGNADOS para el cumplimiento de las actividades laborales de los FUNCIONARIOS RESPONSABLES, quiénes declaran la entrega de los mismos en buen estado ya que se comprometieron a cuidar de los recursos y hacer uso de ellos para los fines establecidos.

1.- FUNCIONARIO RESPONSABLE

Nombres, Apellidos	
Cédula	
Cargo	

2.- EQUIPOS COMPUTACIONALES ASIGNADOS

MODELO DEL EQUIPO	
NUMERO DE SERIE	
NUMERO DE INVENTARIO	

Descripción	Marca	Referencia	Características	Serial
Procesador				
Disco Duro				
Memoria RAM				
Teclado				
Monitor				
Unidad Óptica				
Sistema Operativo				
Mouse				
Web Cam				
Impresora				
Accesorios:				

3.- PRUEBA DE FUNCIONALIDAD

Descripción	Calificación		Descripción	Calificación	
Pruebas On/Of	OK		Prueba de Sonido	OK	
Función S.O.	OK		Función Monitor	OK	
Función Aplicaciones	OK		Función Teclado	OK	
Unidad Óptica	OK		Función Mouse	OK	

4.- TIEMPO ESTIMADO DE USO

Se establece que el FUNCIONARIO RESPONSABLE dispondrá del equipamiento por 24 meses, por lo que la fecha estimada de DEVOLUCIÓN es 24 meses.

5.- DEVOLUCIÓN

FECHA DEVOLUCIÓN:

Entregado por:	Recibido por:

ANEXO C

Formulario para el Ingreso y Salida de Activos de Información

	Formulario para el Ingreso y Salida de Activos de Información		
	UNIVERSIDAD TECNOLOGICA ISAREL		
	Código: F-DTI–001	**Elaborado: 03/03/2017**	**Versión: 1.0**

INGRESO/SALIDA DE EQUIPOS DE CÓMPUTO			
DEPENDENCIA :	LUGAR :	FECHA DE SALIDA :	FECHA DE INGRESO :
CODIGO DEL ACTIVO:	MARCA:	MODELO:	N° DE SERIE:
DESTINO :	PERSONA A QUIEN SE AUTORIZA : NOMBRE :	JEFE QUE AUTORIZA: NOMBRE :	
AUTORIZADO PARA INGRESAR/SALIR CON LO SIGUIENTE :			

MANTENIMIENTO Y/O REPARACIÓN ☐	TRANSFERENCIA ☐	OTROS /EXPLICAR ☐
PRÉSTAMO ☐	POR SER DE SU PROPIEDAD ☐	
DEVOLUCIÓN ☐	REALIZAR UN TRABAJO ☐	

FIRMAS	
SOLICITADO POR: FECHA: HORA:	AUTORIZADO POR: FECHA: HORA:
CONTROL INGRESO (Guardia): FECHA: HORA:	CONTROL SALIDA(Guardia): FECHA: HORA:

ANEXO D

Solicitud para la solicitud de aplicaciones

SOLICITUD DE APLICACIONES DE LA UTECI			
1.- DEPENDENCIA:(PARA USO DEL SOLICITANTE INTERNO/EXTERNO)			
CASA MATRIZ/GERENCIA		AGENCIA/OFICINA	
QUITO MATRIZ		MATRIZ-QUITO	
LUGAR Y FECHA DE REQUERIMIENTO:	QUITO, 27 DE MARZO DEL 2014		
2.- DATOS PERSONALES DEL USUARIO:(PARA USO DEL SOLICITANTE INTERNO/EXTERNO)			
APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES	
CEDULA CIUDADANIA	TELEFONO OFICINA	TELEFONO CELULAR	PROFESION
CARGO QUE DESEMPEÑA		AREA	DEPARTAMENTO
3.- PARA USO DEL SOLICITANTE INTERNO			
CLASE DE REQUERIMIENTO:		CUENTAS PARA ACCESO A BASES DE DATOS Y S.O	
REQUERIMEINTO ADICIONAL:		BLOQUEO DE USUARIO (CAPACITACION, VACACIONES,ETC)	
AMBIENTE:	PRODUCCION	TIPO REQUERIMIENTO:	CREACION
3.1.- PERMISOS PARA ACCEDER APLICACIONES Y MODULOS			
WEB	☐	RRHH	☐
ISOTOOLS	☐	ACTIVE DIRECTORY	☐
GESTION DOCUMENTAL	☐	CORREO ELECTRONICO	☐
INTERNET	☐	CHAT	☐
MODULOS	☐	OTROS	☐
3.2.- TIEMPO DE SOLICITUD			
TIEMPO DE EJECUCION	HORARIO	FECHA DESDE	FECHA HASTA
PERMANENTE	8:00 A 12:00	04/04/2014	04/04/2014
4.- PARA USO EXCLUSIVO DE SOLICTUD DE CUENTAS GENERICAS			
5.- PARA USO EXCLUSIVO DE SOLICTUD DE BASE DE DATOS Y SISTEMAS OPERATIVOS			
BASE DE DATOS/S.O.	NIVEL DE ACCESO	ROL ASIGNADO	DIRECCION IP
	LECT/ESCR/EJEC		192.168.101.58
6.- PARA USO EXCLUSIVO DEL USUARIO (PUBLICO/PRIVADO) EXTERNO			
NOMBRE DE LA INSTITUCION			
CLASE DE REQUERIMIENTO			
AMBIENTE			
PERMISOS PARA ACCEDER APLICACIONES Y/O MODULOS (SOLO CONSULTAS)			
PERMISOS PARA ACCEDER A ROLES (SOLO CONSULTAS)			
MOTIVO POR EL CUAL SE REALIZO EL CONVENIO DE LA EMPRESA EXTERNA CON LA COOPCCP			
NOMBRE DEL AUTORIZADOR (RESPONSABLE INTERNO DEL CONTRATO / CONVENIO)			
7.- TIEMPO DE SOLICITUD DE USUARIO EXTERNO			
TIEMPO DE EJECUCION	HORARIO	FECHA DESDE	FECHA HASTA
ACUERDO DE CONFIDENCIALIDAD E INTEGRIDAD			
ESPACIO PARA FIRMA ELECTRONICA		ESPACIO PARA LA FIRMA ELCTRONICA	
NOTA: Este requerimeinto debe ser aprobado y enviado por la Jefatura Inmediata via Email a: soporte@uisrael.edu.ec			

ANEXO E

Modelo de acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD

A los (día en letras) días del mes de (mes en letras) del año dos mil (año en letras), comparecen por una parte, (Nombre de la empresa o compañía), representada por el(a) Señor(a) (nombre del representante legal o jefe en área), portador(a) de la Cédula de Identidad Nº (en números), en calidad de (cargo de la persona), parte a la cual para los efectos del presente contrato se le llamará LA EMPRESA y, por otra parte el(a) (nombres y apellidos del empleado), portador(a) de la Cédula de Identidad Nº (en números), parte a la cual para los efectos de este contrato se le denominará EL(A) EMPLEADO(A).

PRIMERA: ANTECEDENTES. -

LA EMPRESA es una compañía (sociedad anónima, limitada, etc.) constituida bajo las leyes de la República del Ecuador, autorizada para realizar actividades de (especificar actividad principal u objeto del contrato).

EL(A) EMPLEADO(A) tiene en su campo de acción las funciones de (cargo conforme a contrato de trabajo).

SEGUNDA: CONFIDENCIALIDAD. -

LA EMPRESA declara que la información que proporciona al EMPLEADO(A) respecto de sus clientes, servicios, precios, aplicaciones, etc., será manejada dentro de la más absoluta reserva y utilizada exclusivamente para los fines relacionados con sus funciones dentro de LA EMPRESA, no podrá ser utilizada está información bajo ningún motivo para fines de otra índole, ni traspasarla, copiarla o usarla para otros propósitos.

EL(A) EMPLEADO(A) se obliga a guardar dentro de la más absoluta reserva, toda la información, cualquiera sea su índole, que por razón de sus actividades y relación con LA EMPRESA, llegase a su conocimiento, estándole por tanto prohibida la divulgación, reproducción, utilización o apropiación de cualquier información o documentación a terceros. El incumplimiento de esta obligación será causa suficiente para dar por terminado el contrato y la relación profesional que tuvieran las partes sin perjuicio de que la parte que incumpliera podrá ser demandada por el pago de indemnizaciones por los daños y perjuicios causados.

EL(A) EMPLEADO(A) se obliga a tener la más absoluta reserva con toda la información, cualquiera fuera su índole, que por su relación con LA EMPRESA llegaré a conocer sea en forma oral, visual, escrita o por cualquier otro medio que haga posible conocerla, sea este en documento escrito, archivos, cintas magnéticas, discos magnéticos, videos, películas, acuerdos verbales, entre otros medios; y en cualquier momento, sea antes o después de la fecha de suscripción de este contrato.

La información confidencial puede ser de naturaleza contable, administrativa, legal, financiera, comercial, tal como la siguiente, sin que esta enumeración pueda considerarse como taxativa. Información sobre estrategias de negocios, operaciones, producción, publicidad y mercadeo, estructuras de comercialización, clientes, productos, ventas y cualquier otra información entregada con el carácter de confidencial por alguno de los partícipes. Información financiera, contable, tributaria y cualquier otra relacionada con la gestión de los partícipes.

A fin de preservar la debida confidencialidad y reserva de la información, EL(A) EMPLEADO(A) acepta y se obliga a: tratar la información confidencial en secreto y en privado, tomando todas las medidas que resulten necesarias para preservar su confidencialidad; mantener en estricta confidencialidad todos los documentos de trabajo que elabore en forma individual o en forma conjunta; usar la información confidencial con el único y exclusivo propósito de su trabajo.

TERCERA: PLAZO.-

El plazo del presente contrato de confidencialidad es de (tiempo en letras, pueden ser meses o año) contado a partir de la fecha de su suscripción, y podrá ser extendido a voluntad de las partes. Sin embargo la obligación de reserva y confidencialidad de la información mutuamente entregada suscrita se mantendrá aun después de haber terminado las relaciones laborales y contractuales que dieron origen al presente contrato.

CUARTA: RESPONSABILIDAD.-

EL(A) EMPLEADO(A) será responsable ante LA EMPRESA por los perjuicios que sean ocasionados por el incumplimiento de las obligaciones derivadas del presente contrato y responderá por el manejo de la información.

QUINTA: JURISDICCIÓN Y COMPETENCIA. -

Las partes aceptan la vigencia y validez del presente contrato por contener estipulaciones hechas en sus mutuos beneficios e intereses y en la buena fe de que cumplieran cada una con las obligaciones asumidas. Aceptan que toda controversia o diferencia derivada de este contrato sea resuelta con la asistencia de un mediador calificado de un reconocido Centro de Arbitraje y Mediación, con asiento en la ciudad de Quito, en la República del Ecuador. En el evento que el conflicto no fuere resuelto mediante este procedimiento, las partes someten sus controversias a la resolución de un Tribunal de Arbitraje que se sujetará a lo dispuesto en la Ley aplicable sobre la materia.

Para constancia de lo acordado, las partes suscriben el presente contrato en dos originales del mismo tenor, a los (días en letras) días del mes de (mes en letras) del año dos mil (año en letras).

LA EMPRESA EL(A) EMPLEADO(A

ANEXO F

Reporte de un Incidente de Seguridad de la Información

REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la Universidad.

El reporte de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

Al presentarse un fallo o incidente de seguridad de la información, por favor complete y presente este formulario, con la mayor cantidad de información posible, dentro de las 24 horas de detectado el incidente. Se solicitan algunos datos de tipo técnico que puede omitir si usted no los conoce.

Este reporte debe entregarse personalmente al Depto. de Seguridad Informática o enviarse mediante correo electrónico a la dirección seguridad@uisrael.edu.ec
Por cualquier consulta puede comunicarse con el personal del Departamento de Tecnología.

UNIVERSIDAD ISRAEL

REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Fecha de notificación:	Hora de notificación:

DATOS DE LA PERSONA QUE NOTIFICA		
Apellido y Nombres:		
Ubicación:		Área / Dependencia:
Correo electrónico:		
Teléfono:	Interno:	Teléfono particular:

INFORMACIÓN SOBRE EL INCIDENTE			
Fecha en que observó el incidente:		Hora en que observó el incidente:	
Marque con una cruz todas las opciones que considere aplicables.			
	Uso indebido de información crítica.		Ingeniería social, fraude o phishing.
	Uso prohibido de un recurso informático o de red de la Universidad.		Modificación no autorizada de un sitio o página web de la Universidad.
	Divulgación no autorizada de información personal.		Eliminación insegura de información.
	Intrusión física.		Modificación o eliminación no autorizada de datos.
	Destrucción no autorizada de información.		Anomalía o vulnerabilidad técnica de software.
	Robo o pérdida de información.		Amenaza o acoso por medio electrónico.
	Interrupción prolongada en un sistema o servicio de red.		Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)
	Modificación, instalación o eliminación no autorizada de software.		Robo o pérdida de un recurso informático de la Universidad.
	Acceso o intento de acceso no autorizado a un sistema informático.		Otro no contemplado. Describa:

INFORMACIÓN SOBRE EL INCIDENTE
Describa el incidente:

Si el incidente:

- Se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus.
- Se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla.
- Se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de T.I. y reenvíe el mensaje como adjunto a la dirección seguridad@uisrael.edu.ec

Describa brevemente cómo detectó el incidente:
El incidente aún está en progreso: [ ] SI [ ] NO
Tiempo estimado de duración del incidente:
Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente:

INFORMACIÓN SOBRE EL RECURSO AFECTADO				
Sistema, computadora o red afectada:				
Localización física:				
Describa brevemente la información contenida en el sistema / computador:				
¿Existe copia de respaldo de los datos o software afectado?		SI		NO
¿El recurso afectado tiene conexión con la red de la Universidad?		SI		NO
¿El recurso afectado tiene conexión a Internet?		SI		NO
Sistema operativo:				

OTROS CONTACTOS
Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente:
Apellido y nombres: Datos de contacto:
Apellido y nombres: Datos de contacto:

ANEXO G

Listado de verificación de Redes

Esta herramienta permitirá identificar una serie de mecanismos mediante los cuales se probará una red informática evaluando su desempeño y seguridad, logrando una utilización más eficiente e información más segura.

Gestión administrativa de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Los objetivos de la red de cómputo.					
Las características de la red de cómputo.					
Los componentes físicos de la red de cómputo.					
La conectividad y las comunicaciones de la red de cómputo.					
Los servicios que proporciona la red de cómputo.					
Los sistemas operativos, lenguajes, programas, paqueterías, utilerías y bibliotecas de la red de cómputo.					
Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.					
Los protocolos de comunicación interna de la red.					
La administración de la red de cómputo.					
La seguridad de las redes de cómputo.					

Evaluación del análisis de la red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de la existencia y uso de metodologías, normas, estándares y políticas para el análisis y diseño de redes de cómputo.					
Análisis de la definición de la problemática y solución para instalar redes de cómputo en la empresa.					
Análisis del cumplimiento de los objetivos fundamentales de la institución para instalar una red de cómputo, evaluando en cada caso:					
La forma de compartir los recursos informáticos de la institución, especialmente la información y los activos.					
La cobertura de los servicios informáticos para la captura, el procesamiento y la emisión de información en la institución.					
La cobertura de los servicios de comunicación.					
La frecuencia con que los usuarios recurren a los recursos de la red.					
La confiabilidad y seguridad en el uso de la información institucional.					
La centralización, administración, operación, asignación y el control de los recursos informáticos de la institución.					
La distribución equitativa de los costos de adquisición y operación de los recursos informáticos de la institución.					
La escalabilidad y migración de los recursos computacionales de la institución.					
La satisfacción de las necesidades de poder computacional de la institución, sea con redes, cliente/servidor o mainframe.					
La solución a los problemas de comunicación de información y datos en las áreas de la institución.					

Análisis de la delimitación de los proyectos de red, a fin de evaluar la manera en que se cumplen:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
La delimitación temporal, por el tiempo en que se instalará la red.					
La delimitación espacial, por las dimensiones físicas y lógicas del proyecto de red.					
La delimitación conceptual, por el análisis específico de las necesidades que se deben satisfacer con la red de cómputo.					
La delimitación tecnológica, por los requerimientos y conocimientos informáticos específicos en sistemas de red.					

Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
El estudio de factibilidad tecnológica.					
El estudio de factibilidad económica.					
El estudio de factibilidad administrativa.					
El estudio de factibilidad operativa.					
Otros estudios de factibilidad que repercuten en el diseño e instalación de la red en la institución.					

Análisis de la escalabilidad y el aprovechamiento de los recursos informáticos de la empresa para instalar una red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de la tolerancia de las posibles fallas de la red.					
Análisis de la transparencia del trabajo para los usuarios de la red.					

Evaluación del diseño e implementación de la red según el ámbito de cobertura

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de las redes de multicomputadoras.					
Evaluar el funcionamiento de la cobertura de punto a punto.					
Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas.					
Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes.					

Análisis de la red de área local (LAN)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 10 metros a 10 kilómetros					
Evaluar el uso adecuado y confiable de la tecnología utilizada internamente para la transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas, en todas las computadoras conectadas a la LAN.					
Evaluar la restricción adoptada para establecer el tamaño de la red.					
Evaluar el tiempo promedio de transmisión de la red (entre el peor caso y el mejor caso de transmisiones conocidas de datos).					
Evaluar que las velocidades utilizadas normalmente en su transmisión estén en el rango de 10 a 100 Mbps.					

Análisis de la red de área amplia (WAN)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 100 a 1,000 kilómetros.					
Evaluar el funcionamiento de la composición, consistente en la colección de hosts (computadoras interconectadas) o LANs de hosts conectados por medio de subredes.					
Evaluar la forma de enviar los paquetes de un enrutador a otro, según las características de envío de la red.					
Evaluar el uso adecuado y confiable de la tecnología (interna y externa) de transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas, en todas las máquinas conectadas a las LANs y a la WAN.					
Evaluar la conveniencia del tiempo promedio de transmisión de la red entre LANs y entre subredes.					
Evaluar que las velocidades utilizadas normalmente en la transmisión cumplan con los rangos establecidos para este tipo de redes.					

Análisis de las redes públicas (también conocidas como Internet)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 10,000 a 100,00 kilómetros.					
Evaluar la composición de esta red, consistente en la integración de la red Internet a la vinculación con puertas de enlace (gateways), computadoras que pueden traducir entre formatos incompatibles.					
Evaluar el uso adecuado y confiable de la tecnología y sistemas de interconexión utilizados (interna y externamente) en la transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas.					
Evaluar las velocidades utilizadas normalmente en la transmisión.					

Análisis de las redes inalámbricas

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar el uso adecuado de este tipo de red según sus características.					
Evaluar el uso adecuado y confiable del radio, microondas, satélites, infrarrojo o cualquier otro mecanismo de comunicación sin cable.					
Evaluar la posibilidad de combinar las redes inalámbricas con otras computadoras móviles y/u otras redes.					
Evaluar las posibilidades de integrar Internet o su vinculación con puertas de enlace u otros sistemas de computadoras que pueden traducir entre formatos incompatibles.					

Evaluación del diseño e instalación de la red según su configuración básica

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Red(es) establecida(s) en la empresa:					
Análisis del diseño e implementación del tipo de red basada en el concepto de servidor único.					
Análisis del diseño e implementación del tipo de red basada en el concepto cliente/servidor.					
Análisis del diseño e implementación del tipo de red de punto a punto (uno a uno).					
Análisis del diseño e implementación del tipo de redes de multipunto (uno a muchos, muchos a muchos).					
Análisis del diseño e implementación del tipo de red lógica basada en el concepto de conexión entre terminales sin cables.					
Análisis del diseño e implementación del tipo de red virtual basada en el concepto de tecnología y comunicación vía Internet.					

Análisis del diseño e implementación de la topología de cobertura de la red, en cuanto a:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Estudio de las necesidades de cobertura con la topología física de la red.					
Estudio de las necesidades de cobertura con la topología lógica de la red.					

Análisis del diseño de los modelos de comunicación ISO de la red de la empresa, en cuanto al funcionamiento de las siguientes capas:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Capas físicas.					
Capas de enlace.					
Capas de red.					
Capas de transporte.					
Capa de sesión.					
Capa de presentación.					
Capa de aplicación.					

Análisis de los estándares adoptados para el funcionamiento de las redes

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
EtherNet (norma IEEE 802.3).					
Token ring (norma IEEE 802-5).					
ARCnet (Attached Resource Computer Network).					
IPX (Internetwork Packet Exchange).					

Evaluación del diseño e implementación de las características de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de la confiabilidad en el funcionamiento de los medios de transmisión y del medio físico que utiliza la red para la comunicación entre las computadoras que la integran.					
Cableado.					
Transmisión por radio, microondas, satelital, infrarrojo y cualquier otro tipo de comunicación sin cable.					
Combinación de los medios de transmisión.					

Análisis de las técnicas de transmisión que determinan cómo se utilizan los medios físicos para la comunicación entre las computadoras de la red, estudiando el funcionamiento de:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
La transmisión síncrona.					
La transmisión asíncrona.					
La transmisión analógica.					
La transmisión digital.					
La codificación de datos en señales analógicas.					
La transmisión en paralelo.					
La transmisión en serie.					
Los códigos de comunicación de datos.					

Análisis del funcionamiento y la confiabilidad de los dispositivos para conectar las redes

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Repetidores. Sirven para amplificar o regenerar las señales, con lo cual pueden utilizarse cables más largos.					
Puentes. Son los dispositivos para guardar y reenviar los datos en la red; operan en el nivel de enlace y pueden cambiar los campos de las tramas.					
Enrutadores de protocolos múltiples. Son como los puentes que funcionan en el nivel de red y que permiten la conexión de redes con distintos protocolos.					
Puertas de enlace de transporte. Conectan las redes en nivel de transporte.					
Puertas de enlace de aplicación. Conectan dos partes de una aplicación, aunque éstas utilicen formatos distintos.					

Análisis del funcionamiento de las técnicas de transferencia de datos

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Simplex. Solamente en un sentido.					
Semidúplex. En ambos sentidos, pero uno a la vez.					
Dúplex total. En ambos sentidos a la vez.					

Análisis de los tipos de topologías utilizados en el diseño de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Topología de bus.					
Topología de estrella.					
Topología de anillo.					
Topología de malla.					
Topología de doble anillo.					
Análisis de los métodos de acceso al medio y de la manera en que se conectan los dispositivos de la red para utilizar la transmisión por el medio físico.					
Evaluación del diseño e implementación de los componentes de la red de cómputo.					
Análisis del diseño e implementación del tipo de servidor principal establecido para la red.					
Análisis del diseño e implementación de los servidores dedicados.					
Análisis del diseño e implementación de los servidores no dedicados.					
Análisis del diseño e implementación de los servidores de apoyo.					
Servidores de archivos (distribuidos, dedicados y no dedicados).					
Servidores de discos (dedicados y no dedicados).					
Análisis del diseño e implementación de los servidores de impresión.					
Análisis del diseño e implementación de los servidores de comunicación.					
Análisis del diseño e implementación de los concentradores.					
Análisis del diseño e implementación de los otros tipos de servidores.					

Análisis del diseño e implementación de las estaciones de trabajo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Características y componentes de la terminal o estación de trabajo.					
Número de terminales o estaciones de trabajo.					
Aplicaciones de la terminal o estación de trabajo.					
Privilegios, información y uso de la terminal o estación de trabajo.					

Análisis del funcionamiento y la confiabilidad de los elementos de enlace físico de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del diseño e implementación de los nodos de la red.					
Análisis del uso de las tarjetas de la red.					
Tarjetas de interfaz de red.					
Adaptador de 2Mbps (este adaptador soporta longitudes de hasta 500 metros de cable de par trenzado sin blindaje o UTP.					
Adaptador EtherNet AE-1/t de bajo costo y número limitado por número de puertos hub, y velocidad de transferencia de 10Mbps.					
Adaptador EtherNet AE-2; es un adaptador inteligente con autoconfiguración de selección de parámetros óptimos de funcionamiento.					
Adaptador EtherNet AE-2/t para conexiones de cables UTP y coaxial.					
Adaptador EtherNet AE-3 para soportar tres tipos de cable: UTP, coaxial grueso y coaxial delgado.					
Cable de par trenzado de amplio rango, sin blindaje y UTP.					
Cable coaxial.					
Cable de banda base para un solo canal con un solo mensaje a la vez y velocidades de 10 a 80 Mbps.					
Cable de banda ancha; este cable maneja varias bandas a la vez y en diferentes frecuencias de manera simultánea, con sistema dual de cable o un solo cable y amplificadores bidireccionales.					
Cable de fibra óptica.					

Análisis de la confiabilidad y el funcionamiento correcto de los elementos establecidos para la expansión de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Repetidores, para recibir y retransmitir datos, compensando las pérdidas de señal.					
Puentes y dispositivos para la capa de enlace OSI, para manejar datos de origen y destino.					
Puentes/enrutadores y dispositivo de interconexión de la red.					
Enrutadores relacionados directamente con los protocolos de comunicación.					
Puertas de enlace, dispositivos para la conexión de minicomputadoras y mainframes.					
Evaluación del diseño e implementación de los protocolos de comunicación de la red.					

Análisis de la adopción de jerarquías de protocolos en la red de la empresa

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
El software para controlar las redes y las estructuras para manejar la complejidad.					
La institución en la mayoría de las redes en una pila de niveles.					
Los niveles que ofrecen ciertos servicios a los niveles superiores y la implementación de estos servicios en el nivel inferior siguiente para implementar sus servicios.					
El nivel de comunicación “n” de una computadora con el nivel “n” de otra computadora.					
Las reglas y convenciones que controlan la conversación entre las computadoras, según el nivel “n” de los protocolos.					
Las entidades en niveles correspondientes de comunicación entre computadoras distintas.					
La transferencia de los datos directamente del nivel “n” de otro nivel, a fin de pasar la información hacia abajo de un nivel a otro hasta que llegue al nivel del medio físico.					
Los niveles donde están las interfaces permiten cambios en la implementación de un nivel sin afectar el nivel superior.					

Análisis del funcionamiento del modelo OSI para la red, estudiando el comportamiento de los siguientes niveles:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Nivel físico. Para las relaciones de los voltajes, la duración de un bit, el establecimiento de una conexión, el número de polos de enchufe y demás aspectos técnicos de este nivel.					
Nivel de enlace. Para convertir el medio de transmisión crudo en uno que esté libre de errores de transmisión en cuanto al remitente de los datos de entrada, el procesamiento de los de acuse y el manejo de las tramas perdidas, dañadas, o duplicadas, y en cuanto a la regulación de la velocidad del tráfico.					
Nivel de red. Para determinar el enrutamiento de los paquetes desde sus fuentes hasta sus destinos, manejando la congestión a la vez y su incorporación a la función de contabilidad.					
Nivel de transporte. Es el primer nivel de comunicación directa de su par en el destino (los anteriores niveles son de computadora a computadora). Este nivel suministra varios tipos de servicio, como abrir conexiones múltiples de red para proveer capacidad alta. Se puede utilizar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples que entran en una máquina y abastecer el control de flujo entre los hosts.					
Nivel de sesión. Parecido al nivel de transporte, pero provee servicios adicionales, ya que puede manejar token (objetos abstractos y únicos) para controlar las acciones de los participantes, o puede hacer checkpoints (puntos de inspección) en las transferencias de datos.					
Nivel de presentación. Provee funciones comunes a muchas aplicaciones, como traducciones entre juegos de caracteres, códigos de números, etc.					
Nivel de aplicación. Define los protocolos usados por las aplicaciones individuales de la red. Entre estas aplicaciones tenemos el correo electrónico y Telnet, entre otros.					

Análisis del funcionamiento adecuado de los protocolos X.25 para la red, estudiando el comportamiento de las siguientes capas:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Capa física.					
Capa de bloque.					
Capa de paquetes.					

Análisis del funcionamiento adecuado de los protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar el cumplimiento de los objetivos, la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida.					
Evaluar la aplicación de red packet- switched, basada en un nivel de Internet sin conexiones.					
Evaluar la aplicación y el funcionamiento de los niveles físico y de enlace (nivel de hosts a red) y su definición (si la hay) en esta arquitectura.					
Evaluar el funcionamiento del nivel de Internet, en el que los hosts introducen paquetes en la red, los cuales viajan independientemente del destino, pero sin garantías de entrega ni de orden.					
Evaluar la definición que provee el enrutamiento y control de congestión en el nivel del IP.					
Evaluar el funcionamiento del nivel de transporte. Esto permite que los pares en los hosts de fuente y destino puedan conversar en sus dos protocolos: TCP (Protocolo de Control de Transmisión),el cual permite que dos computadoras conectadas a Internet establezcan una conexión confiable para la entrega sin errores de un flujo de bytes; también maneja el control de flujo. Y el UDP (Protocolo de Datagrama de Usuario).					
Este protocolo es menos confiable que el TCP y no intenta establecer una conexión con una computadora remota para la entrega de mensajes discretos					

Análisis del funcionamiento de los protocolos kernel

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
IP.					
ICPM (Protocolo de Mensajes de Control en Internet).					
TCP.					
UDP.					
FTP.					
SMTP.					
SNMP.					
DNS (Servicio de Nombres de Dominio).					
Telnet.					
Análisis de otros protocolos de transmisión de una red.					

Evaluación de la instalación física de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del diseño arquitectónico de las instalaciones de la red.					
Análisis de los elementos de enlace y cableado de la red.					
Análisis del mantenimiento físico, correctivo y preventivo de los foros donde están las instalaciones de la red.					
Análisis de la instalación, el funcionamiento y mantenimiento de las tarjetas que configuran la red.					
Análisis de la instalación, el funcionamiento y mantenimiento de los servidores y terminales de la red de la empresa.					

Evaluación de los elementos de expansión de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de los aspectos técnicos de la red de cómputo.					
Análisis de los estándares de redes locales, según la referencia y formatos que se utilicen para el funcionamiento de la red de la empresa.					
Modelo de Referencia OSI.					
Norma IEEE 802.					
Métodos de acceso CSMA/CD.					
IPX.					
SPX (Secuenced Packet Exchange)					
Análisis del funcionamiento técnico de los sistemas operativos de la red.					

Evaluación de la administración y el control de la red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del acceso a la información institucional por áreas, privilegios y niveles de operación de los datos.					
Análisis de los sistemas y software.					
Análisis del cambio periódico de niveles, privilegios y contraseñas de acceso al sistema.					
Análisis de los reportes de incidencias, contingencias y circunstancias que afecten el funcionamiento de la red, de su información o software.					
Análisis de la atención y rapidez de respuesta para satisfacer las necesidades informáticas de los usuarios del sistema.					
Análisis de la existencia, acatamiento y actualización de las políticas y reglamentos de uso de los sistemas computacionales de la red.					
Análisis del cumplimiento de la actividad informática de los servidores, terminales, sistemas y programas de cómputo utilizados para satisfacer las necesidades de los usuarios del sistema.					

Análisis de la atención y solución de algunas diferencias en la operación entre redes

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
La clase de servicio. Evaluando su orientación permanente a la conexión y/o no conexión de las terminales de servicio, de acuerdo con las políticas del área de sistemas.					
El funcionamiento adecuado de los protocolos de la red.					
El funcionamiento correcto de direcciones, ya sean por un nivel o jerárquicas.					
El manejo de los tamaños de paquetes que se manejan en la red, según su máximo.					
El control de errores para la entrega confiable y en orden o sin orden de la información que se transmite en la red.					
Control del flujo y de velocidad de transmisión de los datos de la red.					
Control de la congestión del manejo de la información, transmisión y					
Protocolos de la red.					
Administración y control de la problemática de seguridad de la red, la información, los usuarios, los sistemas computacionales y de las instalaciones físicas.					
Contabilidad de los tiempos de uso del sistema, ya sea por conexión de las terminales, por paquete, por byte, por proceso o por cualquier otra actividad que se realice en los sistemas de la red.					
Evaluación de la seguridad y protección de la red y de los activos informáticos de la empresa.					
Análisis del funcionamiento de los mecanismos de control de acceso a las instalaciones, información y software institucionales.					
Análisis de la prevención de accesos múltiples, sin permisos, dolosos y de todas aquellas acciones para ingresar al sistema sin la autorización correspondiente.					
Análisis del procesamiento de información en los sistemas de red.					
Análisis de la administración y el control de la asignación de los niveles de acceso, privilegios y contraseñas para los usuarios para ingresar al sistema y tener acceso a la información.					
Análisis del monitoreo de las actividades de los usuarios.					
Análisis de las medidas correctivas y preventivas para evitar la piratería de información, software, activos informáticos y consumibles del área de sistemas.					
Análisis de la realización, actualización y custodia de los respaldos de					
Sistemas e información que se procesan en la red.					
Análisis de las auditorías periódicas del funcionamiento de la red.					
Análisis de las medidas preventivas y correctivas para erradicar los virus informáticos de la red.					
Análisis del establecimiento de las barreras físicas y lógicas para proteger los accesos de intrusos, piratas y hackers informáticos y cualquier otra intromisión, accidental o fraudulento.					

Evaluación del uso y funcionamiento adecuado del software de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de los sistemas operativos para el funcionamiento de la red.					
Análisis de los lenguajes y programas de desarrollo de la red.					
Análisis de los programas y paquetes de aplicación de la red.					
Análisis a las utilerías y bibliotecas de la red.					
Análisis de la disponibilidad de licencias y permisos de instalación del software de la red.					
Análisis de la actualización informática y de los proveedores de sistemas de la red.					
Análisis del diseño de nuevos proyectos informáticos para el funcionamiento de la red.					

ANEXO H

Lista de verificación para el hardware de la computadora

Tarjeta madre del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricante, tipo, versión del BIOS, configuración y componentes.					
Arquitectura, componentes y características de la tarjeta madre.					
Conjunto de chips.					
Ranuras de expansión para bus.					
Ranuras de expansión tipo PCI.					
Ranuras de expansión tipo ISA.					
Capacidad máxima en RAM.					
Ranuras de expansión de memoria (SIMM y DIMM).					
Puertos paralelos, seriales y para ratón.					
Socket para multiprocesadores.					
Bahías para unidades accesibles en parte frontal e interna.					
Capacidad del voltaje de la fuente de energía.					
Capacidad máxima en ROM, EROM y EPROM.					
Conexiones periféricas.					

Procesador

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricante, marca, tipo, configuración y características.					
Velocidad de procesamiento en MHz.					
Máxima memoria en RAM del sistema.					
Memoria caché y RAM externa.					
Coprocesador matemático.					
Conjunto de chips (fabricante, modelo, capacidad y características).					
Administrador de memoria.					

Unidades adicionales, características, interfaz y capacidad

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Unidades de discos flexibles.					
Discos duros (fabricante, capacidad, características y número).					
Unidades de CD-ROM, DVD, CD-R (modelo y velocidad).					
Unidades de cinta.					
Dispositivos multimedia: sonido, tarjetas, bocinas, tarjeta multimedia y sintetizador, bocinas, micrófono y vídeo.					
Fax-módem (marca, modelo, velocidad en Kbps).					
Soporte para gráficos (fabricante, capacidad en RAM e interfaz).					
Monitor (fabricante, modelo, tamaño y características).					
Teclado, ratón, joystick.					

Tarjetas adicionales al sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Tarjeta aceleradora de gráficos.					
Tarjetas para red.					
Tarjeta para multimedia.					
Tarjeta para fax-módem.					
Tarjetas para vídeo.					
Otras tarjetas a través de extensiones del sistema.					

Periféricos externos asociados al sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Impresoras (fabricante, modelo, tamaño y características).					
Sistemas de videoconferencia (fabricante, modelo, alcance, nitidez y características).					
Escáner y dictador de textos.					

Aprovechamiento y utilidad de cada uno de los componentes internos y periféricos del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Monitor, teclado, ratón y unidad de disco flexible.					
CD-ROM, CD-RW, DVD y disco duro.					
Conexiones de periféricos, de conectividad y de comunicación.					

Aprovechamiento y utilidad del sistema computacional

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Capacidad para el crecimiento del sistema.					
Calidad de los componentes del sistema (fabricante, marca y características).					
Obsolescencia y durabilidad del equipo (sistema y componentes).					
Garantía y soporte del fabricante.					

Mantenimiento básico para los sistemas

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Mantenimiento preventivo y correctivo (frecuencia y resultados).					
Sistemas reguladores de corriente y no-breaks.					
Instalaciones y conexiones eléctricas y de tierra.					
Protección del medio ambiente contra humedad, polvo y estática.					

ANEXO I

Lista de verificación para las características del software

Evaluación al sistema operativo

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricante, características y operabilidad.					
Plataforma y ambientes de aplicación.					
Licencias y permisos.					
Versión, actualizaciones, cambios e innovaciones.					
Manuales e instructivos técnicos, de operación, de programación y demás documentación relacionada con el funcionamiento del lenguaje.					
Facilidad para la administración del sistema operativo.					
Sistemas, rutinas y programas para la seguridad y protección de los datos y del sistema operativo.					
Tecnología de aprovechamiento.					
Compatibilidad y escalabilidad con otros sistemas operativos.					
Ventajas y desventajas.					

Evaluación de los lenguajes de desarrollo

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricantes, características y operabilidad del lenguaje.					
Plataforma y ambientes de aplicación y desarrollo.					
Versión, actualización y utilidad para el sistema.					
Facilidad de compilación y traducción al lenguaje de máquina.					
Uso y generación de códigos y programas fuente, seudocódigos, programas objeto y programas ejecutables.					
Bibliotecas, herramientas y utilerías para programación.					
Facilidad de programación y desarrollo.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento del programa.					
Administración del lenguaje.					
Sistemas para la seguridad y protección de los datos y del propio lenguaje.					
Facilidad de programación, compatibilidad, escalabilidad y desarrollo con otras plataformas y lenguajes.					
Ventajas y desventajas.					
Requerimientos de capacitación y especialización.					

Evaluación de los programas de desarrollo

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricantes, características y operabilidad.					
Plataforma y ambientes de aplicación y explotación.					
Versión, actualización y utilidad para el sistema.					
Licencias y permisos.					
Facilidad de traducción, comunicación y compilación con lenguaje de máquina.					
Bibliotecas, herramientas y utilerías para programación.					
Programas para bases de datos.					
Facilidad de programación (visual y decodificación).					
Uso y generación de programas fuente, programas objeto, programas gráficos y programas ejecutables.					
Compatibilidad, exportabilidad y escalabilidad con otros lenguajes y programas.					
Sistemas para la seguridad y protección de los datos y del propio programa.					
Administración del programa de aplicación.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento y uso del programa.					
Requerimientos de capacitación y especialización.					
Facilidad de programación, compatibilidad, escalabilidad y desarrollo con otros sistemas, plataformas, lenguajes y programas.					
Ventajas y desventajas.					

Evaluación de los programas y paquetería de aplicación y explotación

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricantes, características y operabilidad de programa.					
Ambiente de aplicación y uso.					
Versión, actualización y utilidad para el usuario.					
Licencias y permisos.					
Bibliotecas y utilerías de apoyo.					
Compatibilidad, ex portabilidad y escalabilidad con otros programas y paqueterías de aplicación, de desarrollo o con el sistema operativo.					
Requerimientos de capacitación y especialización.					
Paqueterías y programas desarrollados internamente.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento del programa.					
Ventajas y desventajas de los programas y paqueterías de aplicación.					

Evaluación de la administración del software para aplicaciones

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Paqueterías y programas integrados (Office y					
SmartSuite, por ejemplo).					
Programas y paqueterías para aplicaciones de escritorio (hojas de cálculo, bases de datos, procesadores de texto, agendas y presentaciones).					
Programas y paqueterías para gráficos, diseño, presentaciones, publicaciones, autoedición y multimedia.					
Programas y paqueterías de negocios y productividad.					
Programas y paqueterías para comunicación y red.					
Aplicaciones y utilerías para Internet.					
Aplicaciones para la administración de redes, cliente/servidor y sistemas mayores.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento y uso del programa.					
Otro software para aplicaciones y productividad.					

ANEXO J

Lista de verificación para la administración de accesos

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Evaluación de los estándares e instrucciones de operación y manipulación para el procesamiento de datos, de acuerdo con el propio sistema y su software.					
Evaluación de la estandarización del uso de sistemas operativos, lenguajes, programas y paqueterías para el procesamiento de información en el sistema.					
Evaluación de los procesos lógicos y físicos para el procesamiento de datos.					
Evaluación de los procesos en línea, en lote, multiprocesamiento y procesos compartidos en el sistema.					
Evaluación de la administración y control de la frecuencia, volumen, repetitividad e incidencias en los procesamientos de datos y operaciones lógico-matemáticas de las actividades que se realizan en el sistema.					
Evaluación de la administración centralizada y descentralizada de sistemas para el procesamiento de información.					
Lista de verificación para la administración y los controles de almacenamiento.					
Evaluación del diseño de archivos, bases de datos y medios establecidos para el almacenamiento de información de la empresa.					
Evaluación de la administración y control de archivos de información del área de sistemas y de la empresa.					
Evaluación de los planes y programas de prevención de contingencias relacionadas con el manejo de la información en el área de sistemas.					
Evaluación de la administración y control de respaldos de información y de datos del sistema, así como de los programas institucionales para el manejo de los archivos del centro de cómputo.					
Evaluación de la administración y control de la seguridad y protección de respaldos de información y de datos.					
Evaluación de las normas, políticas y procedimientos para el almacenamiento, custodia, protección y seguridad de la información del área de sistemas y de las áreas de la empresa que cuenten con sistemas computacionales.					

Lista de verificación para la administración de los controles de seguridad del sistema computacional

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Evaluación de los métodos, rutinas de programación, procedimientos y medidas de seguridad y protección de los sistemas operativos, lenguajes, programas, paquetes, utilerías y demás software del sistema computacional.					
Evaluación de los métodos, rutinas de programación, procedimientos y medidas de seguridad y protección de los componentes físicos (internos y externos) del sistema computacional, como son los periféricos, dispositivos asociados y demás componentes físicos.					
Evaluación de las rutinas de programación, procedimientos y medidas de seguridad y protección de la información que se procesa en el sistema computacional.					

ANEXO K

ENCUESTA A USUARIOS

1. ***¿En la Universidad Tecnológica Israel se tiene implementadas políticas de seguridad de la información?***

   Sí ____ *No ____*

2. ***¿Cuál sería el beneficio que tendría la institución al contar con políticas de Seguridad de la Información?***

   a. Mayor seguridad en los medios de almacenamiento de información
   b. Aumenta la productividad a través de consultas confiables
   c. Calidad en el servicio para los alumnos, docentes y terceros
   d. Otros*:* _____

3. ***¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la Información?***

   a. Desarrollo de políticas de seguridad
   b. Clasificación del acceso de la información
   c. Capacitación de usuarios
   d. Monitoreo y reportes de las actividades en la red
   e. La continuidad del negocio después de incidentes
   f. Otros

4. ***¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?***

   a. Omitir la seguridad como un aspecto fundamental de configuración del Servidor
   b. Transmisión en pleno texto de contraseñas
   c. Uso inadecuado de herramientas de seguridad, o no uso alguno
   d. Obtener y mantener programas y aplicaciones (software) que son vulnerables
   e. Otros

5. ***¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?***

   a. Fenómenos Naturales (Terremotos, Inundaciones)
   b. Fallas mecánicas (Cortes de fluido eléctrico, incendios)
   c. Divulgación ilícita de la información por el personal
   d. Destrucción o modificación de la información
   e. Intrusos al sistema de la red
   f. Virus informáticos, gusanos, spam
   g. Otros

6. ***¿Sus equipos de cómputo en su oficina tienen fuente de poder interrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?***

   Sí ____ *No____*

7. ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

a. Incidencias que se dan con más frecuencia
b. Saturación de la red por programas indebidos (música, video)
c. Olvido de contraseña
d. No realizar copias de respaldo
e. Otros: No organizar la información para mayor seguridad

8. ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

a. Aproximadamente 3 meses
b. Aproximadamente 6 meses
c. Aproximadamente 1 año
d. Nunca

9. ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

a. Muy interesado
b. Poco interesado
c. Nada interesado

10. ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad? ¿Por qué?

Sí_____ No_____

11. ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?

a. Muy beneficioso
b. Poco beneficioso
c. Nada beneficioso

ANEXO L

CARTA DE ACEPTACIÓN

Quito, 20 de julio del 2017

Dirección de Recursos Tecnológicos de la Universidad Israel

Ing. Edwin Lagos
Coordinador de la Dirección de Tecnología
PRESENTE

Por medio de la presente manifiesto y pongo en constancia que el Sr. Edison Rolando Reinoso Diaz con C.I. No. 171279062-3, ha realizado la presentación del resultado final del Proyecto de Titulación: **"Propuesta de sistema de gestión de seguridad de la información con la norma ISO/IEC 27001 – 27002 ver.2013, para el Departamento de Sistemas y Recursos Tecnológicos de la Universidad Israel"**, la cual se ha revisado las políticas, normas y formatos establecidos de acuerdo a las necesidades que presenta la institución, quedando satisfechos con el trabajo de investigación realizado por el postulante.

Ing. Edwin Lagos
Coordinador de la Dirección de Tecnología