Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR EL CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Evelyn Lucia Oliva Salguero
Asesorada por el Ing. Marlon Antonio Pérez Türk

Guatemala, mayo de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR CENTRO DE CÁLCULO E INVESTIGACION EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

Evelyn Lucia Oliva Salguero
ASESORADA POR MARLON ANTONIO PEREZ TÜRK

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, MAYO DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Vladimir Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Miguel Ángel Cancinos Rendón
EXAMINADOR	Ing. Marlon Francisco Orellana López,
EXAMINADOR	Ing. Oscar Alejandro Paz Campos,
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR EL CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 9 de septiembre del 2015.

Evelyn Lucia Oliva Salguero

Guatemala, 14/septiembre/2020

Ingeniero Carlos Azurdia
Coordinador Trabajos de Tesis
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería, USAC
Presente

Estimado Ing. Azurdia:

Por este medio informo que he revisado y aprobado el Trabajo de Tesis titulado: "ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA", de la estudiante Evelyn Lucia Oliva Salguero (Carnet número 200915554), quien se identifica con DPI número 2334 24148 0101.

Con base en la evaluación realizada hago constar que he evaluado la calidad, validez, pertinencia y coherencia de los resultados obtenidos en el trabajo presentado, por lo cual el trabajo evaluado cuenta con mi aprobación.

Agradeciendo su atención y deseándole éxitos en sus actividades profesionales me suscribo.

Atentamente,

"Id y Enseñad a Todos"

MARLON ANTONIO PEREZ TURK
INGENIERO EN CIENCIAS Y SISTEMAS
COLEGIADO No. 4492

MA. Ing. Marlon Antonio Pérez Türk
Asesor
Colegiado No. 4492

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 5 de noviembre de 2020

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **EVELYN LUCIA OLIVA SALGUERO** con carné **200915554** y CUI **2334 24148 0101** titulado **"ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR EL CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA ",*** *realizado por la estudiante, EVELYN LUCIA OLIVA SALGUERO aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Msc. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 03 de mayo de 2021

Decanato
Facultad de Ingeniería
24189101 - 24189102

DTG.200.2021

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **ANÁLISIS DEL ESTÁNDAR ISO/IEC 27001 PARA GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES PUBLICADAS POR EL CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por la estudiante universitaria: **Evelyn Lucia Oliva Salguero,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, mayo de 2021

/gdech

ACTO QUE DEDICO A:

Dios	Por ser la principal guía en mi vida, por darme sabiduría, y siempre bendecirme en cada propósito.
Virgen María	Por su intercesión y bendición.
Mis padres	Lorena Salguero y Álvaro Oliva, por su apoyo incondicional, sus consejos, sabiduría, comprensión y amor. Esta dedicatoria queda muy corta para demostrarle mi agradecimiento y amor. Es de ustedes este triunfo.
Mi hermana	Susana Oliva, por su cariño, apoyo, por siempre inspirarme a ser una mejor persona y ser un buen ejemplo.
Mi novio	Fredy Eduardo Mendoza por siempre creer en mí, por su apoyo incondicional, por siempre motivarme a confiar en mí. Eres una persona importante en mi vida.

Mi familia	Por su cariño, apoyo y motivación.
Mis amigos	Por su valiosa amistad, palabras de apoyo y por los momentos compartidos de alegría y superación.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudio que me permitió obtener mi formación universitaria y obtener este logro académico.
Facultad de Ingeniería	Por ser el centro de estudio que me otorgo las enseñanzas necesarias para concluir mis estudios profesionales.
Mis amigos de la Facultad	Por su amistad y apoyo incondicional.
Ing. Marlon Antonio Pérez Türk	Por los consejos y asesoría en el desarrollo de este trabajo de graduación.
Centro de Cálculo e Investigación Educativa de la Facultad de Ingeniería	Por aceptar este trabajo de graduación y compartir la información necesaria para el desarrollo del tema.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
R#	Número de riesgo
%	Porcentaje

GLOSARIO

Activo	Bienes, derecho y recursos que posee una empresa. Puede ser económico o dependiendo de la naturaleza del negocio.
Amenaza	Es una acción que aprovecha una debilidad y podría generar un efecto negativo en un sistema y provocar daños potenciales.
Aplicaciones web	Herramienta informática accesible por medio de internet o red local (Intranet) utilizando un navegador.
CCIE	Centro de Cálculo e Investigación Educativa.
DBA	Administrador de base de datos.
Fuga de información	Suceso que permite a personas o servicios ajenos a la organización tener conocimiento de información privada o sensible.
Gestión de riesgo	Cultura donde se realizan procesos de identificación, análisis y evaluación de la probabilidad de riesgos e impacto de los mismos.
IEC	Comisión Electrotécnica Internacional.

Información	Agrupación de datos que, al ser procesados, transmiten un mensaje.
Ingeniería social	Conjunto de técnicas que son utilizadas para manipular a usuarios y obtener información personal y confidencial.
ISO 27001	Norma internacional perteneciente a la familia ISO 27000, permite la creación de sistemas de gestión de seguridad la información, donde la principal preocupación es garantizar la confiabilidad, integridad y disponibilidad de la información.
ISO	Organización Internacional de normalización.
OWASP	Proyecto abierto de seguridad de aplicaciones web.
Partes interesadas	Grupos o personas que son beneficiadas y tienen interés en el éxito de los procesos de una organización.
Políticas	Agrupación de directrices, reglas, procesos y comportamientos que deben seguir las personas que pertenecen a una organización o son afines a un grupo.
Riesgo	La probabilidad de que un evento ocurra y que este genere un impacto en los procesos y objetivos.

SANS	Instituto de Auditoría, Redes y Seguridad de SysAdmin.
Seguridad informática	Técnicas utilizadas para prevenir que la información crítica, valiosa y sensible sea divulgada o destruida por entes externos o no autorizados.
SGSI	Sistema de Gestión de Seguridad de la Información.
Sistemas informáticos	Conjunto de elementos conocidos como hardware y software que permiten el almacenamiento y proceso de información.
Software	Parte lógica de un sistema informático. Está formado por programas, instrucciones que procesan tareas.
TI	Tecnología de la información.
Vulnerabilidad	Debilidad o fragilidad de un sistema, que puede ser utilizado para causar daño al sistema.

RESUMEN

El presente trabajo consiste en el análisis de la norma ISO/IEC 27001, la cual busca determinar las reglas o pasos necesarios para crear un buen sistema de gestión de seguridad, o bien que avale el sistema de seguridad que posee la organización o institución, en este caso el Centro de Cálculo de la Facultad de Ingeniería.

El primer capítulo está formado por la explicación detallada de cada uno de los términos relacionados con la norma ISO/IEC 27001, para que de esta manera sea fácil para el lector comprender los términos y los consejos que más adelante serán desarrollados. Se expondrá cuáles son los parámetros requeridos en forma general, y se explicará el concepto en forma individual.

En el segundo capítulo se analiza el Centro de Cálculo, se describe su misión, visión, objetivos, función principal, procesos y servicios que realiza, para crear un concepto general sobre las medidas más adecuadas de seguridad para el mismo.

En el tercer capítulo se unen los conceptos de ISO 27001/IEC y Centro de Cálculo. Se desarrolla los requisitos mínimos y opcionales indicados por la norma ISO/IEC 27001 para crear un sistema de gestión de seguridad de la información que incluya las necesidades y expectativas de Centro de Cálculo.

El cuarto capítulo describe los objetivos de un sistema de gestión de seguridad de la información, y se desarrollan las políticas de seguridad acordes a los objetivos de Centro de Cálculo.

Las políticas de seguridad se encuentran clasificadas dependiendo del área que podría ser afectada y más vulnerable a amenazas en el proceso. Cada política está formada por una breve explicación que incluye introducción, objetivos y las reglas que deben ser seguidas para cumplir con la política.

En el quinto capítulo se realiza un análisis de riesgo del procedimiento para desarrollo de nuevos sistemas informáticos que pertenece a Centro de Cálculo de la Facultad de Ingeniería. Este procedimiento se divide en etapas y en cada una se analiza dónde se determina el evento, causas, consecuencias, tratamiento y respuesta al riesgo.

Al encontrar los posibles riesgos, se establece el tratamiento de cada uno de estos. Cada tratamiento es son detallado de forma simple para que sea fácil para el lector comprender el origen de los posibles riesgos.

OBJETIVOS

General

Proporcionar una guía que establece los lineamientos y estándares por seguir para definir una guía de seguridad de la información basada en el estándar ISO 27001 y que pueda ser aplicada en Centro de Cálculo de la Facultad de Ingeniería.

Específicos

1. Dar a conocer los conceptos y definiciones para entender el estándar ISO 27001.

2. Dar a conocer cuáles son los riesgos de no tener implementada una normativa como la propuesta con la certificación ISO 27001 en Centro de Cálculo de la Facultad de Ingeniería.

3. Establecer los requerimientos y recursos de Centro de Cálculo de la Facultad de Ingeniería para crear un sistema de gestión de la seguridad de la información basada en el estándar ISO 27001.

4. Establecer una metodología factible para que Centro de Cálculo de la Facultad de Ingeniería pueda crear un sistema de gestión de seguridad de la información.

INTRODUCCIÓN

El presente trabajo contiene información sobre seguridad de la información y los pasos necesarios para optar por una certificación ISO 27001.

Para los ingenieros en ciencias y sistemas, la seguridad de la información es un recurso muy importante que se debe proteger porque gracias al mismo es posible obtener resultados y procesar los análisis necesarios.

Existen diferentes problemas que pueden causar una fuga de información. Estos pueden ser externos e internos. La ISO 27001 determina una guía necesaria que cualquier entidad no especializada debe contener para asegurar en su mayor porcentaje el resguardo de este recurso.

La ingeniería social está muy latente en todas partes, debido a lo desconocido del tema, por lo que aplicar la norma ISO 27001 es muy importante ya que establece los lineamientos sobre cómo evitar este tipo de fuga.

La ingeniería social se refiera al engaño que realizan personas para obtener información. Por ejemplo, personas son muy persuasivas se entrenan para engañar a otras al hacerse pasar por trabajadores de una compañía importante y solicitan información. Puede tratarse de una persona individual o un empleado. A este último es muy importante educarlo y entregarle técnicas, reglas que pueda seguir para identificar quiénes realizan estos engaños, porque la información es el recurso más importante.

Usualmente, los términos de seguridad informática y seguridad de la información suelen confundirse, debido a que la informática trabaja con datos que en su conjunto agrupan y se transforman en información.

1. ANÁLISIS TEÓRICO SOBRE ISO 27001 Y SEGURIDAD DE LA INFORMACIÓN

1.1. Introducción

En este capítulo se describe la estructura de la ISO 27001, la cual es comúnmente utilizada para crear una gestión de la seguridad de la información.

Se detallará las desventajas de no contar con un plan de acción contra las amenazas presentes en cualquier departamento administrativo o tecnológico, en este caso en Centro de Cálculo, y cuáles son las ventajas de aplicar esta norma en la creación de una gestión de la seguridad de la información que une el recurso humano, tecnológico y administrativo.

1.2. Definición de seguridad de la información

La información es un activo muy importante en cualquier empresa y organización; por tanto, debe ser protegida al igual que otros recursos. Esta protección minimiza las amenazas o daños que la organización puede presentar.

Todo sistema de información está formado por datos que necesitan ser protegidos. Para lograrlo es necesario crear una gestión de riesgo que considere diferentes factores para controlar adecuadamente los riesgos que puedan existir.

Para una gestión de riesgo, es importante identificar la diferencia entre protección de datos y seguridad de la información, para clasificar los elementos y seleccionar a cuáles se debe prestar mayor atención.

El resultado de un sistema de información se utiliza para tomar decisiones en una organización. El sistema está formado por diferentes procesos o elementos que ayudan a producir los resultados. Entre los procesos de mayor importancia están:

- Adquisición de información: es la fuente de donde se obtuvo la información.

- Transformación de datos en producto final: consiste en seleccionar correctamente los datos que una organización o entidad necesita para realizar el proceso de seguridad y obtener un buen resultado.

Para comprender mejor el tema de fuente de información y la selección de datos, podemos crear el siguiente escenario:

En una entidad bancaria se realizan una gran cantidad de procesos internos y externos en los cuales se maneja información importante, tanto para el banco como para las personas que hacen uso de la entidad.

En este escenario, la fuente de información puede ser una persona que otorgue los datos a la entidad bancaria, datos que necesitan protección por ser confidenciales.

El otro punto de vista es la entidad bancaria que procesa la información otorgada por la persona y selecciona lo que es de interés para el negocio. Esta información no necesariamente debe contener todos los datos proporcionados por el usuario, porque no todo lo que da la persona le sirve al banco para realizar los procesos internos y externos.

Esto demuestra que en los dos puntos de vista se manejan datos muy importantes que son vitales para el negocio y también para la persona que otorga la información. Por tanto, es necesario crear una gestión de seguridad para manejar de forma responsable los datos facilitados por las fuentes que conforman el sistema.

Es muy común confundir seguridad de la información con seguridad informática, por lo cual es necesario definir las diferencias entre ambas.

Tabla I. **Diferencia entre seguridad de la información y seguridad informática**

Tema	Definición
Seguridad de la información	• La seguridad de la información ayuda a cumplir las metas y objetivos planteados por la organización. • Diseña un sistema seguro que involucra todas las áreas que forman parte de los procesos establecidos por la organización. • Involucra los riesgos que se puedan encontrar en el área administrativa, tecnológica, personal, incluyendo a los clientes. • Como, por ejemplo, analizar la seguridad de la información en un departamento de recursos humanos La seguridad de la información involucra a todas las personas que se encuentren adentro del departamento, no importa si son trabajadores o no. También toma en cuenta

Continuación tabla I.

	a personas externas que solo realizan consultas sobre determinados procesos. A la vez, la seguridad de la información involucra todos los procesos, y sistemas que realiza dicho departamento, como el proceso de llegada del personal, proceso de salida contratación de personal, despido de personal, el proceso de reclutamiento, y equipos electrónicos dentro del departamento.
Seguridad informática	• Seguridad informática se enfoca en analizar y crear un sistema para el manejo correcto de la información que se utilizan en el área tecnológica (software y hardware) que posee el departamento, • Ejemplo; crear políticas especiales para los servidores que pueda poseer el departamento.

Fuente: SGSI. *Confidencialidad, integridad y disponibilidad*. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/. Consulta: 2 de julio 2019.

1.2.1. Pilares de la seguridad de la Información

Existen tres pilares de la seguridad de la información:

Tabla II. **Pilares de la seguridad de la información**

Categoría	Definición
Integridad	Consiste en la necesidad de mantener la información exacta y completa.
Disponibilidad	Mantener la información con un acceso continuo y oportuno
Confidencialidad	Privatizar la información dependiendo de los niveles de acceso.

Fuente: SGSI. *Confidencialidad, integridad y disponibilidad*. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/. Consulta: 2 de julio 2019.

La información puede ser dividida dependiendo de la categoría en la que se encuentra:

Tabla III. **Clasificación de la información según la integridad**

Categoría	Definición
Modificación altamente restringida	Se requiere autorización por el dueño de la información para realizar cualquier manipulación sobre la misma.
Modificación restringida	Información a la cual se le puede realizar ciertos cambios
Modificación controlada	Recursos de información que se le pueden dar a cualquier usuario para efectuar modificaciones Bajo circunstancias debidamente controlada.

Fuente: GOMEZ FERNANDEZ, Sheila Etty. *Seguridad de la información*. http://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf. Consulta: 2 de julio 2019.

Tabla IV. **Clasificación de la información según la disponibilidad**

Categoría	Definición
Muy crítica	Información que debe estar disponible todo el tiempo, si no se encuentra la información puede causar consecuencias graves.
Crítica	Información necesaria para la continuidad de operaciones. Si no está disponible en el término de uno a dos días o durante los períodos de cierre, puede causar consecuencias sobre el negocio.
Importante	La falta de disponibilidad de esta información permite operar por algunos días sin esos recursos de información en particular o puede encontrar modos de procesamiento alternos.

Fuente: GOMEZ FERNANDEZ, Sheila Etty. *Seguridad de la información*. http://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf. Consulta: 3 de julio 2019.

Tabla V. **Clasificación de la información según la confidencialidad**

Categoría	Definición
Restringida	Información de la más alta confidencialidad. Se autoriza el acceso a personas que tengan una necesidad específica de conocerla o usarla para cumplir con sus funciones; no debe ser compartida a menos que exista aprobación de la Alta Gerencia.
Confidencial	Información de uso selectivo. Su acceso se basa en la necesidad de conocerla o usarla para cumplir con su función. Esta información es compartida solamente bajo condiciones predefinidas.
Uso interno	Este valor se asigna a la información que se debe mantener interna. Información dirigida al uso dentro de la organización y normalmente no compartida con personas que no son empleados.
General	Información dirigida al público. Tiene muy poco o ningún impacto para la organización si es divulgada, o utilizada de una manera inapropiada.

Fuente: GOMEZ FERNANDEZ, Sheila Etty. *Seguridad de la información*. http://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf. Consulta: 4 de julio 2019.

1.3. Riesgos y peligros por falta de seguridad de la información

En la actualidad, todas las organizaciones están formadas por procesos tecnológicos y no tecnológicos que ayudan a cumplir los objetivos deseados e involucran a las diferentes áreas, como el área humana y tecnológica.

Cada una está formada por diferentes activos que deben ser protegidos por que agregan valor a la organización. Por ejemplo, si nos enfocamos en la tecnología nos daremos cuenta que esta tiene un cambio contaste y rápido; si no se le presta una atención adecuada puede quedar obsoleta y dar espacio a que ocurran errores y/o amenazas en la organización.

Una amenaza es considerada como cualquier evento que puede afectar los activos de información[1]

Tabla VI. **Clasificación de amenazas**

Clasificación	Definición
Interrupción	Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.
Intercepción	Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad.
Modificación	Una entidad no autorizada consigue acceder a un recurso, y es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplo modificar una aplicación para que no funcione en la forma correcta.

[1] ISO Tools. *Seguridad de la información*. https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/. Consulta: 8 de julio de 2020.

Continuación tabla VI.

Fabricación	Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

Fuente: GOMEZ FERNANDEZ, Sheila Etty. *Seguridad de la información*. http://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf. Consulta: 29 de julio 2019.

Tabla VII. **Clasificación de riesgos**

Riesgos
Riesgos naturales
Riesgo país
Riesgo social
Riesgo económico
Riesgo político
Riesgo estratégico
Riesgo operativo
Riesgo financiero
Riesgo legal
Riesgos laborales
Riesgos físicos
Riesgos tecnológicos

Fuente: GOMEZ FERNANDEZ, Sheilla Etty. *Seguridad de la información.* http://cybertesis.uni.edu.pe/bitstream/uni/9764/1/gomez_fs.pdf. Consulta: 29 de julio 2019.

En este trabajo se analizará el riesgo tecnológico, el cual involucra la estructura tecnológica de cualquier organización que puede ser afectada por fallas en los sistemas, procesos o cualquier software o hardware que sea utilizado y pueda perjudicar en la interrupción de las operaciones y provocar pérdidas financieras, entre otras.

Existen riesgos de origen humano que se pueden clasificar en intencionales y no intencionales. Entre los primeros se puede citar el robo de información y los segundos, errores por falta de información, malentendidos.

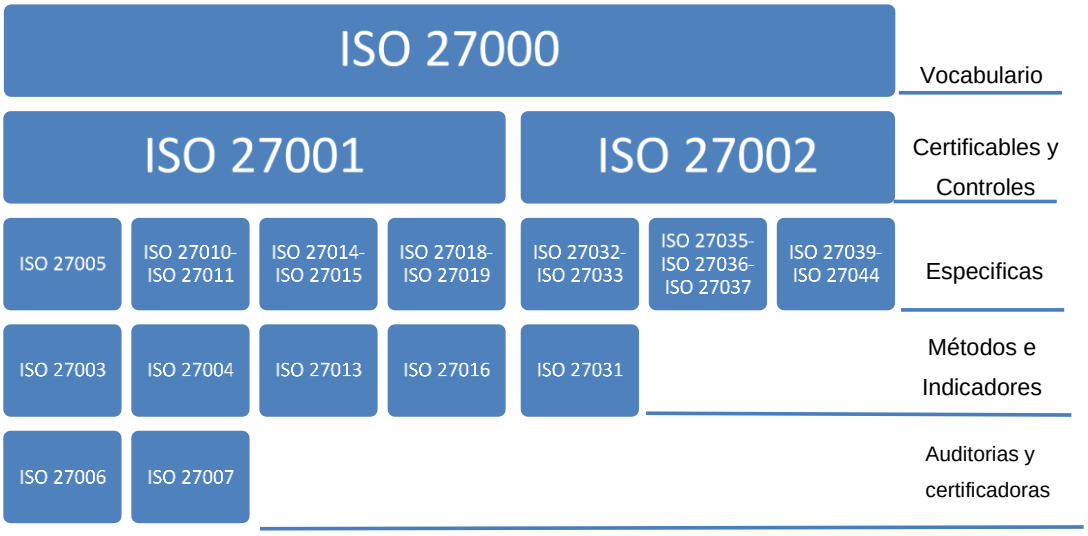
1.4. Norma ISO/IEC 27001

La familia ISO/IEC 27 000 consiste en una agrupación de estándares que determinan las diferentes métricas, directrices y terminologías necesarias para crear una gestión de seguridad de la información aplicable en diferentes tipos de organizaciones.

La ISO 27 000 proporciona un análisis global de las normas que apoyan a la ISO 27001. Brinda una descripción general sobre la gestión de seguridad de la información, proporciona términos básicos que son implementados en las diferentes normas de la familia ISO 27 000.

En la figura 1 se puede observar las diferentes normas que pertenecen a la familia 27 000, clasificadas en el grupo al que pertenecen.

Figura 1. **Familia ISO 27 000**



Fuente: BACKTRACK ACADEMY. *Método para implementar un SGSI según el ISO/IEC 27001:2013*. https://backtrackacademy.com/articulo/metodo-para-implementar-un-sgsi-segun-el-iso-iec-27001-2013. Consulta: 21 de julio 2019.

La norma ISO 27 001 fue emitida por la Organización Internacional de Normalización (ISO). La primera publicación de esta norma se realizó en el 2005, pero se establecieron todas las reglas en el 2013.

ISO 27 001 es una norma internacional que se encarga de administrar la seguridad de la información en las organizaciones sin importar el campo de trabajo en el cual se desempeñe. Su metodología crear una gestión de seguridad de la información. Toma como eje central la confidencialidad, integridad y disponibilidad de la información.

Un paso importante en ISO 27 001 consiste en evaluar los riesgos y debilidades que existen en la organización, lo cual permite gestionar un sistema

de seguridad de la información para contrarrestar las debilidades y riesgos que la organización posee. La ISO 27 001 determina políticas, documentos legales y procesos necesarios que la organización necesita cumplir y de esta forma garantizar una mayor seguridad en los procesos ejecutados.

1.4.1. Ventajas de la certificación ISO/IEC 27 001

Al obtener una certificación o poseer un sistema de gestión de riesgos de seguridad de la información, la organización demuestra que está comprometida en generar un ambiente agradable y seguro para proteger la información que utilice. Logra así obtener los siguientes beneficios:

Tabla VIII. **Beneficios de un SGSI o certificación**

Identificar los principales riesgos en materia de seguridad informática
Clasificar los riesgos en función de su gravedad y posibilidades reales de que se lleguen a producir.
Adaptar y alinear los controles a todas las áreas de la empresa.
Crear confianza en los clientes y partes interesadas
Cumplimiento de las leyes y reglamentos
Ahorrar costes por la reducción de incidentes.
Proteger la reputación de la empresa.
Fortalecer la organización interna y los procesos de mejora continua.

Fuente: ISO Tools. *Beneficios de aplicar la norma ISO 27001*. https://www.isotools.org/2015/09/08/beneficios-de-aplicar-la-norma-iso-27001/. Consulta: 21 de julio 2019.

1.4.2. Metodología para implementación de un sistema de gestión de seguridad de la Información

A continuación, se describirá las etapas para crear un sistema de seguridad de la información para optar a una certificación en ISO 27 001.

Figura 2. **Fases para un sistema de gestión de seguridad de la información**

Fuente: ISO27000.ES. *Metodología SGSI*. https://www.iso27000.es/sgsi.html. Consulta: 22 de julio 2019.

2. ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN EN CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA, FACULTAD DE INGENIERÍA

2.1. Introducción

En el presente capítulo se analizará el Centro de Cálculo. Por su importancia en la Facultad de Ingeniería es necesario comprender su función y el propósito por el cual fue creado. Centro de Cálculo administra eficientemente la información de cada persona dentro de la Facultad de Ingeniería, como los catedráticos, estudiantes y personal administrativo. Desarrolla distintos servicios tecnológicos, los cuales fueron clasificados en diferentes áreas dependiendo del origen del servicio; por ejemplo, el área de desarrollo de investigación, coordinación, entre otros, los cuales están formados por diferentes procesos.

El Centro de Cálculo de la Facultad de Ingeniería fue fundado en 1965[2]. Desarrolla un papel importante, el cual consiste en gestionar en una forma adecuada la información de las diferentes carreras que posee la Facultad de Ingeniería.

Es necesario conocer y analizar su estructura para comprender los diferentes procesos que desarrolla y determinar una guía en seguridad de la información, basada en los procesos que se presentan más adelante en este capítulo.

[2] Centro de Calculo e investigación educativa. *Historia*. http://ccie.ingenieria.usac.edu.gt/index.php/historia.

La Facultad de Ingeniería “actualmente cuenta con 12 carreras, las cuales se encuentran divididas en seis escuelas facultativas que la coloca como una de las facultades más grandes de la Universidad con un aproximado de 14 000 estudiantes.”[3] Con base en la información anterior y teniendo en cuenta el número aproximado de estudiantes, se puede tener un panorama amplio sobre la cantidad de información que debe administrar el Centro de Cálculo de la Facultad de Ingeniería.

2.2. Contexto de la organización

La misión de Centro de Cálculo e Investigación Educativa es:

> Crear las mejores soluciones informáticas para el manejo de la información académica y administrativa generada en la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, tomando en cuenta las necesidades de los usuarios, tanto estudiantes como personal administrativo y docente, aprovechando al máximo los recursos asignados por medio de la utilización de herramientas adecuadas para su desarrollo.[4]

La visión es la siguiente:

> Administrar toda la información de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala de manera eficiente, segura y accesible a todas las personas que la soliciten, cumpliendo con los reglamentos y normas establecidas, mejorar día a día las aplicaciones desarrolladas, además de mantener el equipo de cómputo de la Facultad en las mejores condiciones posibles.[5]

El objetivo es:

[3] *Centro de Calculo e investigación educativa*. Misión y Visión. http://ccie.ingenieria.usac.edu.gt/docs/Manual_de_Normas_y_procedimientos.pdf.
[4] Ibid.
[5] Ibid.

“Una administración eficiente de la información académica y administrativa de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala” [6].

2.2.1. Análisis y recopilación de procesos y servicios realizados por Centro de Cálculo e Investigación Educativa, Facultad de Ingeniería

Centro de Cálculo brinda diferentes servicios a la Facultad de Ingeniería, los cuales fueron diseñados para satisfacer las necesidades que posee dicha Facultad en temas administrativos y tecnológicos, además de la información proporcionada por cada estudiante.

A continuación, se presenta la tabla IX donde se clasifican los servicios que presta el Centro de Cálculo.

Tabla IX. **Servicios prestados por Centro de Cálculo e Investigación Educativa**

Servicios brindados vía Internet	Consulta de información, tanto a estudiantes como a docentes de la Facultad de Ingeniería
	Asignación de cursos en línea.
	Ingreso de notas de cursos en línea.
	Procesamiento de propuestas de contratación de personal docente.
	Consulta de información general, servicio utilizado exclusivamente por la administración.
Servicios adicionales:	Atención a estudiantes con el área de informática, a entidades que la solicitan (internas y externas a la facultad).
	Atención a estudiantes con problemas de indoles estudiantil.
	Soporte técnico, en el área de informática
	Docencia en el laboratorio de la india.

Fuente: Centro de Cálculo e Investigación Educativa. *Servicios.* http://ccie.ingenieria.usac.edu.gt/index.php/servicios. Consulta: 8 de mayo del 2019.

[6] *Centro de Calculo e investigación educativa*. Misión y Visión. http://ccie.ingenieria.usac.edu.gt/docs/Manual_de_Normas_y_procedimientos.pdf.

Centro de Cálculo se organiza en tres áreas de trabajo, que permiten distribuir los procesos con funciones específicas para ofrecer los diferentes servicios. En la tabla X se presentan las áreas y sus funciones.

Tabla X. **Áreas y funciones de Centro de Cálculo e Investigación Educativa**

Área	Función
Desarrollo de sistemas	Es la encargada del análisis, desarrollo e implantación de sistemas en general, además de brindar soporte a los usuarios finales de las soluciones creadas. También se encarga de la administración de los servidores de Internet y de bases de datos de las distintas soluciones Web creadas por el Centro de Cálculo.
Redes	Se encarga de la administración de la red de cómputo principal de la Facultad de Ingeniería. Brinda servicio de soporte técnico a las distintas dependencias de la facultad, adicionalmente, se encarga del procesamiento de datos tal como horarios, notas de cursos, entre otros. Y de la administración de los servidores y soluciones en sus versiones anteriores.
Investigación educativa	Principalmente, es la encargada de la generación de informes y estadísticas solicitadas al Centro de Cálculo por cualquier entidad, tanto de la Facultad de Ingeniería, así como de entidades externas a ésta. Cada área de trabajo tiene diferentes procesos que ayudan a cumplir los objetivos determinados por Centro de Cálculo.

Fuente: Centro de Cálculo e Investigación Educativa. *Desarrollo de Sistemas*. http://ccie.ingenieria.usac.edu.gt/index.php/2014-10-16-21-17-01/desarrollo-de-sistemas. Consulta: 11 de mayo del 2019.

A continuación, se presentan los procesos desarrollados por Centro de Cálculo, clasificados en función del área a la cual pertenecen. La información de cada proceso que se detalla fue obtenida del Manual de Normas y procedimientos desarrollado por Centro de Cálculo, revisado por la División de Desarrollo Organizacional, y aprobado por la Junta Directiva de la Facultad de Ingeniería.

2.2.2. Procesos de Centro de Cálculo e Investigación Educativa definidos en el Manual de Normas y Procedimientos

En esta sección se muestra una tabla en donde se definen los procesos que son ejecutados por Centro de Cálculo, los cuales son clasificados con base en el área en la cual son desarrollados.

Tabla XI. **Procesos de Centro de Cálculo e Investigación Educativa**

Área	Procedimiento
Coordinación	Procedimiento de elaboración de plan operativo anual.
	Procedimiento reclutamiento de nuevos trabajadores.
	Procedimiento para solicitar cambios en un sistema.
	Procedimiento para solicitar un nuevo sitio web.
Redes, operación y soporte técnico	*Procedimiento Manejo y control de actas.*
	Procedimiento Emisión de certificaciones de cursos aprobados.
	Procedimiento de creación de calendarios de exámenes finales y de retrasada.
	Procedimiento nuevas instalaciones de red.
	Procedimiento para solicitar elaboración de padrón electoral.
	Procedimiento recepción y mantenimiento de equipo de cómputo.
	Procedimiento para alojar sitio web en servidores del Centro de Cálculo.
	Procedimiento para solicitar informe técnico para dar de baja un equipo.
	Procedimiento para recepción de equipo de computación nuevo.

Continuación de la tabla XI.

Desarrollo de Sistemas	Procedimiento asignación de cursos a estudiantes de primer ingreso.
Desarrollo de Sistemas	Procedimiento para habilitación de procesos de asignación.
	Procedimiento para habilitación de procesos de asignación de curso de vacaciones.
	Procedimiento de carga de acuerdos de Junta Directiva.
	Procedimiento habilitación de asignación de exámenes de suficiencias.
	Procedimiento asignación de laboratorios y diplomados.
	Gestión y carga de nueva base de datos de inscritos.
	Procedimiento para solicitar cambios en un sitio.
	Desarrollo de sistemas
	Implementación de sistemas.
	Prueba para nuevos sistemas.
	Capacitación de sistemas desarrollados por CCIE
	Elaboración de manuales de usuario para herramientas desarrolladas por el CCIE.
	Manejo de inscripción de la carrera de industrias agropecuarias y forestales.
	Procedimiento ingreso de notas de actividades.
	Asignación de pruebas específicas.
Investigación educativa	Procedimiento para solicitar datos estadísticos

Fuente: Centro de Cálculo e Investigación Educativa. *Manual de Normas y procedimientos*. http://ccie.ingenieria.usac.edu.gt/docs/Manual_de_Normas_y_procedimientos.pdf. Consulta: 22 de mayo 2019.

2.2.3. Análisis para identificar procedimientos críticos para la seguridad de la información

En la sección anterior se clasificaron los diferentes procesos que Centro de Cálculo desarrolla; cada uno comprende tareas que son desarrolladas por un representante, quien es el encargado de ejecutar cada una con los requisitos necesarios.

Centro de Cálculo está dividido en diferentes áreas formadas por los procesos enlistados en la sección anterior. Para el análisis y la creación de un sistema de gestión de seguridad de la información se evaluará el área de desarrollo de sistemas.

Para realizar la evaluación se creó una matriz de priorización de procesos, donde se determinan criterios, se les asigna un porcentaje y, al final, el proceso con mayor calificación es el proceso crítico y es el que se elegirá para la creación de un SGSI (Sistema de Gestión de Seguridad de la Información).

Los criterios son evaluados tomando en cuenta el nivel de afectación que el proceso tiene sobre el criterio.

Tabla XII. **Criterios matrices de priorización de procesos**

Aplicación de Nuevas soluciones	Análisis y planificación de procesos
Procesamiento de datos	La información relacionada se conoce dentro del área de TI
Administración de Hardware	La información relacionada se conoce dentro del área de la organización
Personas ajenas a la entidad	La información relacionada se conoce públicamente.

Fuente: elaboración propia, empleando Word 2019.

En la siguiente tabla se desarrolla la distribución en los porcentajes que pueden ser elegidos al calificar un proceso con el nivel de afectación en el criterio.

Tabla XIII. **Evaluación cualitativa**

Evaluación cualitativa		
1	5 %	Afectación muy baja sobre el criterio
2	10 %	Afectación baja sobre el criterio
3	15 %	Afectación moderada sobre el criterio
4	20 %	Afectación importante sobre el criterio
5	25 %	Afectación muy importante sobre el criterio

Fuente: elaboración propia, empleando Word 2019.

La metodología de la matriz de priorización de procesos consiste en elegir el proceso, evaluar el nivel de afectación colocar un número entre el rango de 1 a 5. Cada número posee un valor en porcentaje. Al final se suma el que el proceso obtuvo en cada criterio, y el que tiene mayor puntuación será el crítico.

Por ejemplo, si el proceso tiene una afectación baja en el criterio de evaluación, se coloca el número 2, lo cual indica que representa el 10 %; si tiene una afectación importante sobre el criterio, se coloca el número 4, lo cual indica que representa el 20 % sobre el proceso y así hasta evaluar cada uno de los procesos con los criterios.

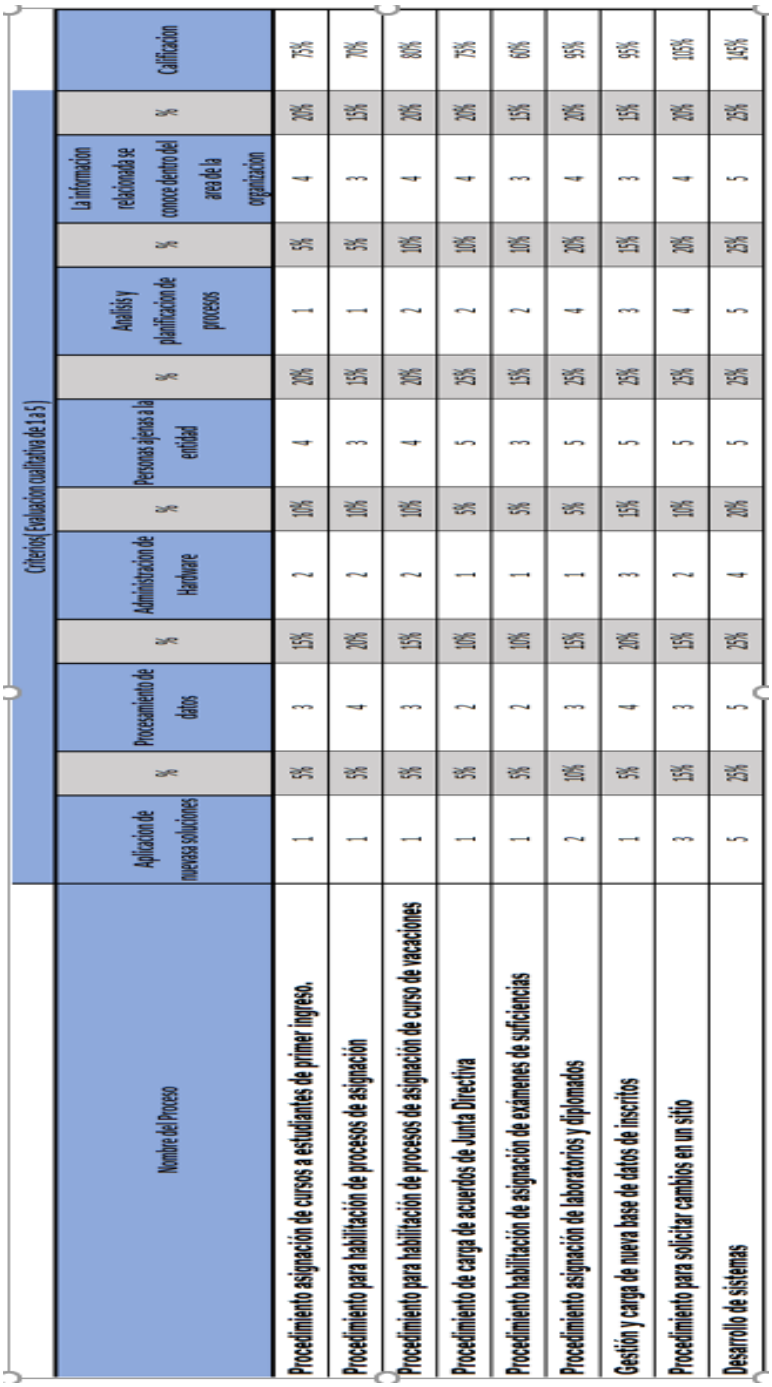
A continuación, se mostrarán los procesos del área de desarrollo que serán evaluados en la matriz de priorización.

Tabla XIV. **Procesos por evaluar**

Procedimiento asignación de cursos a estudiantes de primer ingreso
Procedimiento para habilitación de procesos de asignación
Procedimiento para habilitación de procesos de asignación de curso de vacaciones
Procedimiento de carga de acuerdos de Junta Directiva
Procedimiento habilitación de asignación de exámenes de suficiencias
Procedimiento asignación de laboratorios y diplomados
Gestión y carga de nueva base de datos de inscritos
Procedimiento para solicitar cambios en un sitio
Desarrollo de sistemas

Fuente: Centro de Cálculo e Investigación Educativa. *Manual de Normas y procedimientos*. http://ccie.ingenieria.usac.edu.gt/docs/Manual_de_Normas_y_procedimientos.pdf. Consulta: 16 de mayo del 2019.

Figura 3. **Criterios de evaluación para selección de proceso**



	Criterios(Evaluación cualitativa de 1 a 5)																					
Nombre del Proceso	Aplicacion de nuevass soluciones	%	Procesamiento de datos	%	Administracion de Hardware	%	Personas ajenas a la entidad	%	Analisis y planificacion de procesos	%	La información relacionada se conoce dentro del area de la organizacion	%	Calificacion
Procedimiento asignación de cursos a estudiantes de primer ingreso.	1	5%	3	15%	2	10%	4	20%	1	5%	4	20%	75%
Procedimiento para habilitación de procesos de asignacion	1	5%	4	20%	2	10%	3	15%	1	5%	3	15%	70%
Procedimiento para habilitación de procesos de asignación de curso de vacaciones	1	5%	3	15%	2	10%	4	20%	2	10%	4	20%	80%
Procedimiento de carga de acuerdos de Junta Directiva	1	5%	2	10%	1	5%	5	25%	2	10%	4	20%	75%
Procedimiento habilitación de asignación de exámenes de suficiencias	1	5%	2	10%	1	5%	3	15%	2	10%	3	15%	60%
Procedimiento asignación de laboratorios y diplomados	2	10%	3	15%	1	5%	5	25%	4	20%	4	20%	95%
Gestión y carga de nueva base de datos de inscritos	1	5%	4	20%	3	15%	5	25%	3	15%	3	15%	95%
Procedimiento para solicitar cambios en un sitio	3	15%	3	15%	2	10%	5	25%	4	20%	4	20%	105%
Desarrollo de sistemas	5	25%	5	25%	4	20%	5	25%	5	25%	5	25%	145%

Fuente: elaboración propia, empleando Excel 2019.

La siguiente tabla muestra las actividades necesarias para el desarrollo de nuevos sistemas informáticos y los responsables de su ejecución.

Tabla XV. **Procedimiento para desarrollo de nuevo sistemas informáticos**

Descripción del procedimiento		
Responsable	Paso No.	Actividad
Interesado	1	Determina la necesidad de un nuevo sistema informático
	2	Solicita a la coordinación del CCIE la creación de un nuevo sistema detallando el procedimiento que se desea automatizar
Coordinador	3	Recibe la solicitud y la traslada al jefe del área de desarrollo
Jefe de Desarrollo	4	Recibe y asigna personal para realizar el análisis de factibilidad del proyecto.
Programador de computadoras	5	Realiza la propuesta de solución.
Jefe de Desarrollo	6	Verifica la solución junto al programador de computadoras
	7	Si es aprobada la solución, realiza la planificación para el desarrollo del sistema informático, de lo contrario devuelve al programador de computadoras para preparar nueva propuesta.
Jefe de Desarrollo	8	Carga la planificación al sistema de gestión de proyectos.
	9	Asigna permisos a los recursos asignados para desarrollar el sistema informático.
	10	Provee plan, propuesta y contactos al recurso asignado para el desarrollo del sistema.
Programador de Computadoras	11	Entrevista a los usuarios para desarrollar las funcionalidades del sistema.
	12	Elabora un documento con los requerimientos funcionales y no funcionales.
	13	Elabora un documento de diseño técnico que incluye:

Continuación de la tabla XV.

Programador de Computadoras		• Requerimientos técnicos • Diseño de pantallas (Prototipo) • Diseño tecnológico
	14	Presenta documentos a involucrados, jefe de Desarrollo y a la dependencia solicitante, si es necesario al jefe del área de Redes.
	15	Si son aprobados los documentos, se cargan y autorizan en el sistema de gestión de proyectos, de lo contrario realiza de nuevo el análisis y regresa al paso # 11.
Jefe de Desarrollo	16	Autoriza el inicio del desarrollo.
Programador de computadoras	17	Inicia el desarrollo de cada una de las fases.
	18	Programa el requerimiento indicado en la planificación.
	19	Realiza las pruebas en conjunto con el Jefe de Desarrollo para verificar el funcionamiento del requerimiento.
	20	Si se cumple con el requerimiento se actualiza el documento de diseño técnico, de lo contrario debe regresar al paso # 17
	21	Actualiza los avances del proyecto en el sistema de gestión de proyectos.
	22	Si aún existen requerimientos por desarrollar continua con el paso 18, si los requerimientos fueron completados continúa con el paso 23.
	23	Realiza las pruebas para verificar el funcionamiento del sistema informático. Ver procedimiento de Prueba para nuevos sistemas.
	24	Si el proceso de pruebas es satisfactorio y se autoriza por involucrados, continua en el paso 28, de lo contrario siga al paso 25.
	25	Si se encontraron inconsistencias en la aplicación regresa al desarrollo paso 11. Si se encuentran en el proceso regresa hasta el análisis paso 5.
	26	Elabora el plan de implementación.
Programador de computadoras Si es necesario Jefes del área de desarrollo y redes	27	Realiza la implementación del sistema, ver procedimiento para implementación de un nuevo sistema.

Continuación de la tabla XV.

Jefe de desarrollo	28	Realiza pruebas al sistema ya implementado
	29	Si la implementación es satisfactoria notifica a los involucrados y al Coordinador del CCIE e informa los días en que se realizara la capacitación, de lo contrario continúa con el paso 31.
	30	Realiza un RollBack del sistema y regresa al plan de implementación paso 28.
Jefe de Desarrollo & Programador de computadoras	31	Genera documento para la entrega del nuevo sistema y Genera manuales de usuario. Ver procedimiento Elaboración de manuales.
Jefe de Desarrollo	32	Notifica a los involucrados y al Coordinador del CCIE.
	33	Se informa e Indica a los interesados los días en que se realizara la capacitación.
Programador de computadoras	34	Capacita a los usuarios del sistema.

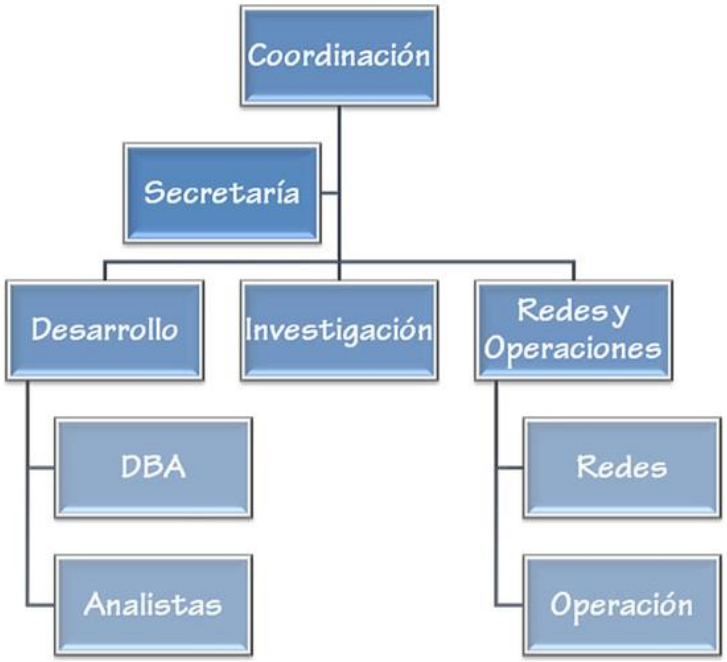
Fuente: Centro de Cálculo e Investigación Educativa. *Manual de Normas y procedimientos*. http://ccie.ingenieria.usac.edu.gt/docs/Manual_de_Normas_y_procedimientos.pdf. Consulta: 16 de mayo del 2019.

2.3. Organización interna de Centro de Cálculo e Investigación Educativa

En la sección anterior se mencionó que el Centro de Cálculo de la Facultad de Ingeniería está formado por tres áreas, las cuales desempeñan diferentes procesos o servicios. Para una buena administración en cada área es necesario crear una estructura organizacional y definir roles, asignar a cada uno tareas para completar los procesos deseados.

En la figura 4 se presenta el organigrama que define los procedimientos y responsabilidades de cada rol dentro de los distintos procesos.

Figura 4. **Organigrama Centro de Cálculo e Investigación Educativa**



Fuente: Centro de Cálculo e Investigación Educativa. Organigrama Centro de Cálculo e Investigación Educativa. http://ccie.ingenieria.usac.edu.gt/index.php/2014-10-16-21-13-42/organigrama. Consulta: 18 de mayo del 2019.

2.4. Estrategia de aseguramiento de la información enfocada en el recurso humano

El recurso humano es de gran importancia en cualquier departamento; por lo tanto, debe poseer las habilidades técnicas necesarias para desarrollar el cargo por el cual fue contratado.

Debe ser evaluado y capacitado para que siga en constante aprendizaje y pueda aplicar los conocimientos necesarios en el departamento y así garantizar una mejor ejecución en las actividades.

A las capacitaciones técnicas deben sumarse otras en distintos temas relacionadas los objetivos del departamento, como seguridad de la información, cuyo objetivo es crear conciencia en el personal sobre la importancia de cumplir las normas de seguridad.

De esta forma de evitará riesgos y amenazas en el manejo de información que cada posición dentro de la organización represente.

Cada persona que se desee incorporar a Centro de Cálculo debe pasar por un proceso de selección que depende del rol que va a desempeñar.

El proceso de selección consta de evaluaciones y entrevistas en donde las personas encargadas de ejecutar este proceso tienen comunicación directa con los aspirantes de para conocerlos mejor y transmitir los requisitos solicitados. Este proceso se considera como el primer filtro de seguridad, debido a que el resultado permite seleccionar al personal adecuado. Luego de ser contratados se realizará una inducción donde se les dará a conocer los proyectos y servicios que se encuentran en desarrollo, así como consejos sobre la seguridad y confidencialidad que deben manejar con la información de Centro de Cálculo.

2.4.1. Estrategia de aseguramiento de la información enfocada a asesoría externa

Centro de Cálculo es una dependencia al servicio de la Facultad de Ingeniería, pero a la vez ofrece asesorías externas. Estas son aprobadas por Secretaría Académica, que define los lineamientos a seguir y las actividades por cumplir. La Coordinación de Centro de Cálculo debe definir los lineamientos necesarios sobre los proyectos y/o servicios por desarrollar. Al

tener los requisitos indicados por la parte interesada, en Centro de Cálculo se realizan reuniones internas con los jefes de área, jefe de proyecto, coordinador y personas interesadas, para definir qué procesos serán ejecutados por determinados roles, indicar los objetivos, políticas y restricciones.

Una vez comprendido el propósito del proyecto, el jefe de área transmite la información al jefe de proyecto y este al equipo de trabajo, que puede estar conformado por diferentes roles, como por ejemplo DBA, analista, jefe de proyecto, jefe de área y coordinador.

El jefe de proyecto presenta al equipo la propuesta, indica a cada rol cuáles serán los procesos que les corresponda ejecutar, lineamientos a seguir, y cuál será la información que manejarán.

A la vez indica algunos estándares de desarrollo, por ejemplo, la estructura de las tablas en una base de datos, cuáles son los posibles nombres para clases, variables, entre otros. Todos estos estándares son transmitidos de forma verbal al equipo por el jefe de proyecto.

Todo el trabajo desarrollado por el personal de Centro de Cálculo es elaborado dentro de la instalación del departamento. Se recomienda al personal no realizar trabajos relacionados con algún proyecto de Centro de Cálculo en lugares ajenos y únicamente utilizar el equipo físico proporcionado por el departamento, para evitar que la información manejada sea mal utilizada.

El personal tiene obligación de leer el Manual de normas y procedimientos, para conocer los procesos que se manejan en Centro de Cálculo y actuar correctamente dentro y fuera de las instalaciones.

Este manual especifica detalladamente cada proceso; sin embargo, no se refiere claramente a las políticas y reglamentos de seguridad de la información que el personal debe cumplir. Tampoco define el personal que debe realizar auditorías internas con respecto a políticas de seguridad de la información.

Actualmente, el equipo de Centro de Cálculo es personal de confianza que maneja de forma eficiente y segura los documentos, equipo e información necesaria para el desarrollo de los proyectos, lo que ha propiciado un ambiente de trabajo sin problema o riesgo de seguridad de la información.

3. ANÁLISIS Y CREACIÓN DE ESTRUCTURA DE UN SGSI EN CENTRO DE CÁLCULO E INVESTIGACIÓN EDUCATIVA DE LA FACULTAD DE INGENIERÍA

3.1. Introducción

En el presente capítulo se realizará un análisis de los requisitos obligatorios y opcionales que son necesarios para la creación de un Sistema de Gestión de Seguridad de la Información.

Los requisitos que se analizan en este capítulo son los establecidos por ISO 27001. Es necesario documentar los requisitos para que se cree un registro de políticas, reglas y procesos dentro de la organización.

ISO 27001 establece que el sistema de gestión de seguridad de la información debe estar formado por documentos obligatorios, los cuales ayudan a entender el negocio de la organización y, a la vez, determina que algunos documentos son opcionales porque no todas las organizaciones tienen el mismo campo de negocio; por lo tanto, pueden o no aplicar los mismos procesos, políticas y reglas.

Los temas que se desarrollarán en este capítulo serán basados en las actividades de Centro de Cálculo de la Facultad de Ingeniería.

3.2. Alcance del Sistema de Gestión de Seguridad de la Información

En esta sección se definirá cuáles son los límites del SGSI tomando en cuenta:

- Asuntos internos y externos de la organización
- Necesidades y expectativas de partes interesadas
- Interferencia y dependencia entre organización interna y externa.[7]

3.2.1. Factores internos y externos de Centro de Cálculo e Investigación Educativa de la Facultad de Ingeniería

Las organizaciones se encuentran limitadas por los aspectos internos y externos que los rodean. Debido a que cambian continuamente, si no se toman en cuenta los cambios y se monitorean regularmente, pueden afectar al objetivo de la organización.

Se debe analizar los asuntos externos e internos en forma individual, para que se considere cada aspecto en el área correspondiente.

Al hacerlo se consideran aspectos sociales y culturales, económicos, legales y tecnológicos.

La descripción de los aspectos externos que influyen en los objetivos de Centro de Cálculo se muestra en la tabla XVI.

[7] Norma Chilena. *Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información -Requisitos NCh-ISO 27001:2013.* p. 22.

Tabla XVI. **Aspectos externos**

Factores	Descripción
Económicos	Centro de Cálculo es un departamento que pertenece a la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala. La Universidad de San Carlos de Guatemala por ser una universidad pública y autónoma le corresponde recibir un porcentaje no menor al cinco por ciento del Presupuesto General de Ingresos Ordinarios del Estado[8], dicho presupuesto debe ser administrado en todas las entidades pertenecientes a la Universidad de San Carlos de Guatemala, ya sea en la sede central, como en las sedes departamentales. Por lo tanto el factor económico de Centro de Cálculo de la Facultad de Ingeniería se encuentra dentro del porcentaje correspondiente para la Facultad de Ingeniería, lo cual crea un margen sobre las decisiones que puede ejecutar e implementar incluyendo que todos los gastos de Centro de Cálculo deben ser aprobados por el Decano y por la Junta directiva, lo cual indica que los proyectos a realizar toman un tiempo debido a que primero se debe presupuestar y luego de la aprobación se ejecuta el proyecto.
Social cultural	El factor social-cultural que afecta a Centro de Cálculo de la Facultad de Ingeniería está formado por entes que posean una conexión directa con los procesos de Centro de Cálculo, en este caso corresponde a los estudiantes de la Facultad de Ingeniería que son los que otorgan la información necesaria a ser procesada, los trabajadores de la Facultad de Ingeniería y entidades externas que requieren de servicios prestados por Centro de Cálculo.
Legales	El factor legal que rodea a Centro de Cálculo incluye las leyes determinadas en Guatemala, leyes que incluyen en sus artículos temas sobre delitos informáticos e iniciativas sobre la protección de datos públicos y/o privados, tales como el Código Penal de Guatemala Decreto no. 17-73 capítulo VII de los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos y la iniciativa 4090-2009, Ley de protección de datos personales

[8] Constitución Política de la Republica de Guatemala. *Sección Quinta*\ *Universidades*\ *Articulo 83*. https://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-const.pdf.

Continuación de la tabla XVI.

Tecnológicos	El factor tecnológico es un factor muy importante, debido a que este factor sufre contantes cambios en corto tiempo, la tecnología que afecta a Centro de Cálculo envuelve cada uno de los procesos que este ejecuta, para el desarrollo de este trabajo se tomará en cuenta el proceso de desarrollo de sistemas informáticos.

Fuente: elaboración propia, empleando Word 2019.

Al analizar los asuntos internos que afectan a Centro de Cálculo se debe tomar en cuenta cada elemento, ya sea tangible o intangible. El análisis de aspectos internos permite a las organizaciones conocer cuáles son las fortalezas y debilidades que posee para tomar el control, realizar planes de acción y así prevenir posibles riesgos, o saber cómo actuar sobre los aspectos externos que pueden afectar a la organización.

Los aspectos internos se pueden clasificar como fortalezas o debilidades, dependiendo del punto de estudio y análisis que se le dé a cada aspecto. En la tabla XVII se presentan las posibles fortalezas y debilidades de los aspectos internos.

Tabla XVII. **Aspectos internos**

Aspecto	Descripción
Ambiente laboral	Es considerado un factor importante en cualquier organización debido a que influye en el crecimiento y productividad de esta, este crecimiento depende del punto de vista que el empleado perciba de la organización.
Estructura organizacional	Es el orden jerárquico creado en cada organización, que establece un orden definiendo a las personas y el orden correcto en los procesos para alcanzar los objetivos.

Continuación de la tabla XVII.

Manual de procesos	Un manual de procesos es un instrumento que ayuda a crear un orden en las tareas diarias de las organizaciones, en el manual de procesos se definen las secuencias de las tareas y actividades que se deben realizar para llevar a cabo el proceso y a la vez, se determina quién es la persona encargada de realizar cada actividad, el tiempo estimado, y las herramientas o equipo a utilizar para desarrollarlo.
Manual de riesgos	Un manual de riesgos indica cuáles son los derechos y obligaciones de cada trabajador relacionados a temas de riesgos, en este manual se expresa cuáles son los objetivos de las organizaciones respecto a la prevención de riesgos e indica a los trabajadores normas de seguridad, indicando cuales son los accidentes que se pueden evitar si se respetan las normas.
Presupuesto	Un presupuesto consiste en crear un listado con los recursos que posee la organización en forma monetaria para poder alcanzar los objetivos deseados, y así distribuir de forma eficiente los recursos monetarios previendo sobre lo que se podrá gastar.
Recursos	Los recursos son todos los elementos que una organización necesita para completar los objetivos deseados, existen diferentes tipos de recursos: • Técnico • Financiero • Humano

Continuación de la tabla XVII.

Roles de trabajo	Un rol de trabajo consiste en las características especiales de cada puesto de trabajo, sin importar que persona ocupe la posición de trabajo, el rol de trabajo determina los atributos y comportamientos que son necesario para ejecutar en buena manera las propiedades de la posición.

Fuente: elaboración propia, empleando Word 2019.

3.2.2. Comprender las necesidades y expectativas de las partes interesadas

En esta sección analizará las partes involucradas en los procesos que realiza Centro de Cálculo, tomando en cuenta tanto los procesos administrativos como tecnológicos.

Centro de Cálculo se encarga de diferentes procesos tanto con cada escuela de la Facultad de Ingeniería, como con entidades externas a la misma, pero pertenecientes a la Universidad de San Carlos de Guatemala.

Cada proceso inicia con la atención al cliente, a cargo de las secretarias o el personal de recursos humanos; luego, sigue el análisis, creación y/o desarrollo de los proyectos solicitados, tomando en cuenta las decisiones de Secretaría Académica.

Cada entidad descrita debe participar y comprometerse a respetar y seguir los lineamientos para proteger la información que se comparte en cada proyecto o transacción de información.

Por ejemplo, las decisiones tomadas por Secretaría Académica deben ser notificadas y conocidas únicamente por el personal correspondiente, y no ser divulgadas al personal o entidades que no se encuentran involucradas en esta parte del proceso o no aparezcan en las actas firmadas en las sesiones realizadas.

A la vez, la información compartida por entidades externas a la Facultad de Ingeniería, al solicitar algún servicio a Centro de Cálculo debe ser conocida únicamente por el personal determinado, y luego transmitir la información necesaria al personal que desarrolla el servicio solicitado. Siempre se debe respetar los documentos que establecen los procesos para desarrollar el servicio.

Otro ejemplo incluye al personal encargado de desarrollar alguna aplicación solicitada a Centro de Cálculo, que únicamente conoce los requisitos para cumplir con el proyecto. Cada persona involucrada debe ser responsable de la información que le fue otorgada y no divulgarla con entidades que no forman parte del proyecto. También debe ser responsable de las herramientas para el desarrollo del proyecto, usarlas con responsabilidad y cuidado, evitar el daño de las mismas y no utilizar las en otros procesos fuera de lo establecido por Centro de Cálculo.

Al realizar un análisis de los ejemplos expuestos, se concluye que en cada proceso hay involucradas diferentes entidades, las cuales tienen interés en ejecutar los procesos, pero comparten diferente información que para ellos es importante. Por tanto, esperan que esta información sea protegida y únicamente utilizada para el propósito establecido.

Se debe garantizar la seguridad de los datos compartidos por cada entidad, respetar los acuerdos y utilizar de manera responsable las herramientas o equipo involucrado.

La tabla XVIII presenta las partes interesadas en la seguridad de la información de Centro de Cálculo.

Tabla XVIII. **Partes Interesadas**

• Junta Directiva de la Facultad de Ingeniería
• Coordinación
• Secretaria
• Equipo de desarrollo
• Facultad y/o escuelas externas a la Facultad de Ingeniería.

Fuente: elaboración propia, empleando Word 2019.

4. POLÍTICAS Y OBJETIVOS DE SGSI

En esta sección se presenta el análisis de los elementos necesarios para desarrollar un documento de políticas de seguridad de la información. Este debe ser desarrollado por Centro de Cálculo para establecer un Sistema de Gestión de Seguridad de la Información.

El documento mencionado debe estar acorde a los objetivos de Centro de Cálculo y respetar los objetivos de un SGSI. Es necesario incluir las acciones permitidas y prohibidas para que se puedan minimizar las vulnerabilidades que puedan existir. Funciona como una prevención de riesgos, donde se incluye las medidas necesarias para prevenir las fallas o pérdidas en los procesos.

Para elaborar un documento de políticas de seguridad, se mencionó que se debe cumplir con los objetivos de Centro de Cálculo, pero a la vez considerar los objetivos de un SGSI. Ambos objetivos deben considerarse para crear políticas seguras y acordes a la ISO 27001.

En la tabla XIX se describen los objetivos más comunes de un SGSI:

Tabla XIX. **Objetivos de SGSI**

Establecer políticas medibles para su posterior análisis.
Crear un sistema de gestión de seguridad de la información, que respete y cumpla los tres pilares de la seguridad de la información (Integridad, confiabilidad, disponibilidad)
Crear un sistema de seguridad que mitigue y/o elimine los riesgos detectados.
Crear un sistema seguro, donde la información sea el activo más importante para proteger.

Fuente: elaboración propia.

Existen requisitos que deben ser tomados en cuenta al plantear el trayecto para cumplir los objetivos de un SGSI, los cuales se encuentran descritos en la tabla XX.

Tabla XX. **Requisitos de objetivos de un SGSI**

Debe estar disponible y debe ser comunicado dentro de la organización.
Debe tener un compromiso con la mejora continua.
Establecer la persona que será responsable de velar por el cumplimiento de los objetivos
Indicar cuándo se terminará la planificación de los objetivos y la inspección del plan.
Establecer un mecanismo para evaluación de resultados.[9]

Fuente: elaboración propia.

[9] Norma Chilena. *Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de la seguridad de la información -Requisitos NCh-ISO 27001:2013.* p. 32.

El objetivo principal de Centro de Cálculo, que se detalló en el primer capítulo, consiste en lo siguiente: “Una administración eficiente de la información académica y administrativa de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala.”[10]

Como propósito de este capítulo se hará énfasis en la parte de administración eficiente de la información, que se puede cumplir al establecer políticas que obedezcan los objetivos de un SGSI.

A continuación, se describe las políticas de seguridad de la información recomendadas por ISO 27001 y las plantillas recomendadas por SANS *(information security training),* que se adecuan al procedimiento que se analizará en este trabajo de graduación: el procedimiento para el desarrollo de nuevos sistemas informáticos**,** realizado por Centro de Cálculo. Este procedimiento es de vital importancia para atender la crisis provocada por la pandemia de Covid-19.

Las políticas serán clasificadas tomando como guía las creadas por SANS, desarrolladas por expertos en el tema de seguridad de la información[11].

En la tabla XXI se muestran las categorías que serán utilizadas para crear las políticas adecuadas al procedimiento en estudio.

[10] Centro de Cálculo e investigación Educativa. *Misión y Visión.* http://ccie.ingenieria.usac.edu.gt/index.php/2014-10-16-21-13-42/mision-y-vision.
[11] SANS. *Security Policy*. https://www.sans.org/information-security-policy/?category=general.

Tabla XXI. **Categorías de políticas de seguridad de la Información**

Categorías	Objetivos
1. Políticas del equipo de cómputo	Define los lineamientos a seguir, indicando qué está permitido y qué no está permitido para el uso del hardware y equipo físico
2. Políticas del control de acceso	Define el proceso y comportamiento adecuado para acceder al equipo de cómputo, a los servicios de red y acceso remoto.
3. Políticas del Software	Define los requisitos que se deben seguir para la administración, implementación y actualización del software.
4. Políticas sobre la instalación del software y propiedad de la institución	Define el proceso y requisitos a seguir al instalar software propio y software externo (Software de terceros)
5. Políticas de escritorio limpio	Definir las condiciones para mantener un escritorio limpio; Proteger la información sensible y que no sea visible por personas no autorizadas.
6. Políticas de correo electrónico	Define las instrucciones y requisitos del uso correcto del correo electrónico en la organización, haciendo conciencia a los usuarios sobre los peligros del mal uso de éste.
7. Pautas para la construcción de contraseña	Indica las instrucciones para la creación de una contraseña segura.

Continuación de la tabla XXI.

8. Políticas para la protección de contraseña	Define la forma correcta para la protección de contraseñas, la constancia de su uso, cambio y repetición.
9. Política de seguridad de aplicaciones web	Define los parámetros para la evaluación de una página web, para que la creación y uso de ésta sea segura.
10. Políticas para un desarrollo seguro de software	Define las pautas a seguir por el equipo de desarrollo para que el software minimice su vulnerabilidad.

Fuente: SANS. *Security Policy Templates.* https://www.sans.org/information-security-policy/?category=general. Consulta: 2 de octubre 2019.

La descripción de cada política y sus subcategorías se desarrollará al definir la descripción y el objetivo.

4.1. Políticas

Las políticas descritas a continuación indican el comportamiento que los miembros del departamento deben seguir.

La lista de políticas descrita puede ser modificada por Centro de Cálculo si así lo considera necesario.

4.1.1. Política del equipo

Descripción de políticas sobre el uso adecuado del equipo utilizado por los miembros de Centro de Cálculo.

4.1.1.1. Introducción

El equipo de cómputo es un activo importante en cada organización, por lo tanto, es importante protegerlo. Este equipo maneja y almacena información valiosa, que debe ser gestionada con mucha precaución y responsabilidad por parte de personas internas y externas, quienes deben seguir los lineamientos que se indican en este documento.

4.1.1.2. Objetivo

El objetivo de esta política es definir los lineamientos a seguir, indicar qué está permitido y qué no está permitido para el uso del hardware y equipo físico.

4.1.1.3. Instalación del equipo de computo

La administración de Centro de Cálculo deberá registrar los equipos que posee en sus instalaciones y son utilizados para el desarrollo de los procesos y proyectos, para llevar un control adecuado de cada uno clasificado en áreas específicas.

Cualquier nuevo equipo que desee ser instalado y deba hacer uso de la red deberá ser autorizado por las personas encargadas.

Cada equipo de cómputo deberá ser ubicado en un área correspondiente, identificar los accesos y quienés serán las personas encargadas de su mantenimiento y limpieza; si es necesaria alguna reparación o traslado del equipo. Esta acción deberá ser notificada al encargado de mantenimiento de cada equipo o de forma general.

4.1.1.4. Del mantenimiento de equipo de cómputo

El departamento encargado de los equipos de cómputo deberá autorizar cada mantenimiento, administrar los mantenimientos de prevención y corrección, indicar quién deberá realizarlo y si se encuentra en capacidad de hacerlo. También deberá asegurarse de que se realice con las herramientas indicadas y respetando los procesos.

4.1.1.5. De la actualización del equipo

El equipo de cómputo debe seguir el proceso necesario para ser actualizado. La actualización debe ser acorde al equipo en cuestión y siguiendo el estándar de las versiones que se encuentren disponibles. Se debe determinar un periodo para evaluar si el equipo se encuentra actualizado o desactualizado.

4.1.2. Política de control de acceso

Descripción de políticas sobre el control de acceso adecuado en Centro de Cálculo.

4.1.2.1. Introducción

Administrar el acceso a los equipos, programas o recursos que pertenecen a las organizaciones es muy importante en la seguridad de la información. Esto permite controlar qué persona realiza determinada acción y quién tiene acceso a información sensible.

4.1.2.2. Objetivo

El objetivo de esta política es definir el proceso y comportamiento adecuado para acceder al equipo de cómputo, a los servicios de red y acceso remoto, protegiendo los pilares de la información.

4.1.2.3. Del control de acceso al equipo de cómputo

Centro de Cálculo tiene el derecho de vigilar cada software y sistema operativo utilizado dentro del departamento.

El equipo asignado al personal de forma individual es responsabilidad de cada usuario. El personal deberá cuidar el equipo siguiendo los lineamientos indicados.

Centro de Cálculo deberá indicar qué personal puede acceder a las distintas áreas restringidas.

4.1.2.4. Del control de acceso remoto y acceso a la red local

Centro de Cálculo debe proporcionar el acceso a los usuarios e indicar cuál es el uso correcto de la red local. Debe, además, observar y cuidar el acceso a equipo crítico conectado a la red local.

Cada equipo externo de que se conecte a la red local debe respetar los lineamientos indicados, para minimizar riesgos de pérdida de información o daño al equipo de trabajo.

Al poseer servicios o equipo de cómputo que puedan ser accedidos de forma remota, debe indicar las limitaciones que poseen y cuándo es posible acceder a ellos.

Acerca de las herramientas de acceso remoto, se deberá usar únicamente el software y herramientas para acceder de a los servicios y/o equipo.

4.1.3. Política del software

Descripción de políticas sobre el uso adecuado del software en Centro de Cálculo.

4.1.3.1. Introducción

El software es una de las herramientas principales que las organizaciones dedicadas a TI utilizan. Debe protegerse y actualizarse para que se encuentre en óptimas condiciones y sea capaz de procesar la información en una forma segura.

4.1.3.2. Objetivo

El objetivo de esta política es definir los requisitos para la administración, implementación y actualización del software, y el proceso que se debe seguir para instalar software propio y externo (de terceros).

4.1.3.3. Del software

Se debe hacer un listado del software de cada equipo de cómputo de uso diario o crítico, e instalar actualizaciones para contar con la última versión

proporcionada por la empresa creadora del software y así minimizar los riesgos de infección o fallas al equipo. Estas actualizaciones deben ser calendarizadas y autorizadas por el encargado del equipo de cómputo.

Centro de Cálculo también debe velar porque el software instalado posea licencias válidas.

Si usa software libre, se debe respetar las reglas establecidas por los creadores del mismo y las propiedades intelectuales establecidas originalmente.

La adquisición de licencias y software original debe ser contemplado en el presupuesto otorgado al departamento.

4.1.3.4. De la instalación del software y software propiedad de la instalación

El equipo de cómputo de uso diario laboral asignado al personal de debe ser cuidado por cada usuario, quien debe velar por el software que posee el equipo, respetando las reglas dictadas por Centro de Cálculo. Si el personal desea instalar algún software debe ser autorizado por Centro de Cálculo y seguir los lineamientos.

Cada equipo debe poseer software de seguridad instalado, como antivirus, así como otro software, con licencias originales, propiedad de Centro de Cálculo.

El software, base de datos y aplicaciones desarrolladas por Centro de Cálculo, son consideradas como propiedad del departamento.

Cada software e información manejada debe poseer un respaldo. Esta acción debe ser calendarizada para evitar la pérdida de datos al existir un daño en el software. El respaldo debe ser almacenado en una forma segura y solo tiene acceso personal autorizado.

Si es necesario que una entidad externa al departamento de Centro de Cálculo haga uso del software creado por el mismo, se debe pedir a la entidad externa que respete la propiedad intelectual del software.

4.1.4. Política del escritorio

Descripción de políticas a seguir para mantener el escritorio de trabajo en óptimas condiciones.

4.1.4.1. Introducción

Uno de los principales métodos para incrementar la conciencia en los trabajadores sobre la importancia de la seguridad de la información, consiste en crear lineamientos a seguir para mantener segura la información, y que el trabajador esté atento sobre no tener visible en su escritorio información confidencial, sensible y que esté disponible a personas no autorizadas.

4.1.4.2. Objetivo

Definir las condiciones para mantener un escritorio limpio; proteger la información sensible y que no sea visible a personas no autorizadas.

4.1.4.3. Escritorio limpio

El cuidado del área de trabajo dependerá de cada empleado, quien debe evitar mantener a la vista cualquier elemento o información personal o crítica que pertenezca a Centro de Cálculo.

El personal debe procurar que la información almacenada en forma electrónica esté segura y a la vista de cualquier persona que pueda acercarse al área de trabajo. Este cuidado debe ser llevado a cabo siempre que la persona deje el área, ya sea al finalizar el horario laboral o si la se ausentará por mucho tiempo.

Si en el área de trabajo hay gabinetes con información crítica, estos deben permanecer cerrados cuando no son utilizados. Cuando la persona que está utilizando la computadora deja el área de trabajo, debe asegurarse de bloquear el equipo y no dejar información sensible a la vista.

Al finalizar el horario laboral, las computadoras deben ser apagadas en su totalidad para evitar daños y posibles riesgos de visibilidad de datos críticos. Si las computadoras usadas son laptops, deben ser aseguradas con cable al área de trabajo, o almacenadas en un lugar seguro.

Las contraseñas que se usen para acceder al equipo no deben ser escritas en papel y ser dejadas en áreas visibles, como debajo de la computadora o en una gaveta sin llave, entre otros.

Documentos que ya no sean necesarios y posean información crítica deben ser triturados o ser desechados en el contendor autorizado. Los documentos impresos con información sensible no deben permanecer mucho

tiempo en la impresora y deben ser retirados lo más pronto posible. Si se hace uso de pizarrón o tablero, no se debe dejar con información sensible sino ser borrada. [12]

4.1.5. Políticas de correo electrónico

Descripción de políticas a seguir para el envió de correo electrónico.

4.1.5.1. Introducción

El uso del correo electrónico representa una de las principales formas de comunicación electrónica que las organizaciones utilizan; por lo tanto, es importante crear políticas que regulen e indiquen el uso correcto del mismo, que indiquen qué se puede o no compartir por correo electrónico.

4.1.5.2. Objetivo

El objetivo de esta política consiste en definir las instrucciones y requisitos del uso correcto del correo electrónico en la organización, para hacer conciencia a los usuarios sobre los peligros del mal uso de este.

4.1.5.3. Uso de correo electrónico

El uso de correo electrónico dentro de Centro de Cálculo debe respetar las políticas y estándares establecidos.

[12] SANS. *Security Policy.* https://www.sans.org/information-security-policy/?category=general.

Las cuentas de correo electrónico deben ser usadas correctamente para propósitos de negocio. No puede ser usado para situaciones personales o ajenas a los objetivos la institución.

Al enviar un correo electrónico perteneciente a Centro de Cálculo, la información contenida debe respetar los estándares definidos sobre qué tipo de información puede ser enviada por este medio, o qué tipo de archivos pueden ser adjuntados al correo.

Deben también respetar un formato de envío. No se debe abrir ni dar respuesta a los correos sospechosos, desconocidos autorizados.

Los correos enviados y pertenecientes a Centro de Cálculo no deben ser reenviados a personas no autorizadas ni utilizarse para participar en ningún evento político, no debe ser utilizado para promover violencia, racismo, o cualquier comportamiento no adecuado. [13]

4.1.6. Políticas para protección de contraseña

Descripción de políticas a seguir para la protección y creación de contraseñas.

4.1.6.1. Introducción

La implementación de buenas políticas para la creación de contraseñas puede evitar acceso no autorizados a información sensible.

[13] SANS. *Security Policy*. https://www.sans.org/information-security-policy/?category=general.

La implementación de un estándar en la creación de una contraseña protege a los diferentes usuarios que hacen uso de un sistema, ya sean usuarios internos o externos a la organización.

4.1.6.2. Objetivo

El objetivo de esta política consiste en definir la forma correcta para la protección de contraseñas, la constancia de su uso, cambio y repetición, e indicar las instrucciones para la creación de una contraseña segura.

4.1.6.3. Pautas para la construcción de una contraseña

El tipo de contraseñas que deben ser incluidas en esta guía son todas las utilizadas en Centro de Cálculo. Incluye de computadoras personales, de equipo sensible como servidores, routers, disco duro, correo electrónico, aplicaciones web, entre otros.

Cada miembro de Centro de Cálculo debe poseer diferentes contraseñas, de acuerdo con los diferentes estándares.

No pueden estar formadas de los siguientes elementos:

- Patrones como aaabbb, qwerty, zyxwvuts o 123321.

- Con información personal como fechas de nacimiento, números de teléfono o nombres de familiares, mascotas, personajes de fantasía.

- Con ocho caracteres o menos [14]

4.1.6.4. Protección de contraseña

Todo el personal de Centro de Cálculo deberá seguir las pautas de construcción de contraseña, indicadas en el punto anterior. Si existen entidades externas que tienen acceso en algún sistema o equipo electrónico de Centro de Cálculo, también deberán poseer una contraseña.

Los usuarios no pueden usar contraseñas relacionadas con el trabajo para sus propias cuentas personales. Las contraseñas deben cambiarse solo cuando existan motivos para creer que se ha utilizado una contraseña comprometida. No deben compartirse con nadie, incluidos supervisores y compañeros de trabajo. Todas deben tratarse como información confidencial. Tampoco deben insertarse en mensajes de correo electrónico u otras formas de comunicación electrónica, ni revelada por teléfono a nadie.

No se debe utilizar la función "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web). Para crearla es altamente recomendable la autenticación multi-factor y debe usarse siempre que sea posible. [15]

4.1.7. Política para la seguridad de aplicaciones web

Descripción de políticas a seguir para mantener la seguridad de aplicaciones web.

[14] SANS. *Security Policy*. https://www.sans.org/information-security-policy/?category=general.
[15] Ibid.

4.1.7.1. Introducción

En la actualidad las aplicaciones web son uno de los elementos más vulnerables y atacados, por lo cual es importante la creación de políticas que minimicen o eliminen las vulnerabilidades y se tenga preparado un plan para rescatar las aplicaciones por si alguno de estos ataques sucede.

4.1.7.2. Objetivo

El objetivo de esta política consiste en definir los parámetros para la evaluación de una página web, para que la creación y uso de esta misma sea seguro.

4.1.7.3. Seguridad de aplicaciones web

El nuevo lanzamiento de aplicaciones web estará sujeto a una evaluación completa antes de la aprobación de la documentación de control de cambios o lanzamiento al entorno en vivo.

Las aplicaciones web externas a deberán respetar las políticas sobre seguridad establecidas. Se realizará evaluaciones en esta etapa para observar si existe algún problema o complicación en el cambio de la arquitectura de la aplicación.

Sin embargo, se permitirá liberaciones de emergencia siempre y cuando el responsable del proyecto o seguridad de la aplicación lo autorice. Una de las condiciones para esta liberación es indicar la fecha de evaluación de la liberación permitida.

Todos los problemas de seguridad que se descubran durante las evaluaciones deben mitigarse en función de los niveles de riesgo. Estos se basan en la calificación de riesgo de la metodología OWASP. Se requerirá pruebas de validación de corrección para validar el arreglo o estrategias de mitigación para cualquier problema descubierto de nivel de riesgo medio o mayor.

- Alto: cualquier problema de alto riesgo debe solucionarse de inmediato o se debe implementar otras estrategias de mitigación para limitar el efecto antes del despliegue. Aplicaciones con alto riesgo están sujetas a ser desconectadas.

- Medio: se debe revisar los problemas de riesgo medio para determinar qué se requiere para mitigar y programar en consecuencia. Las aplicaciones con problemas de riesgo medio pueden ser fuera de línea o denegada su liberación al entorno en vivo en función del número de problemas. V arios problemas aumentan el riesgo a un nivel inaceptable. Los problemas deberían corregirse en un parche / lanzamiento de punto a menos que otras estrategias de mitigación limiten la exposición.
- Bajo: el problema debe revisarse para determinar qué se requiere para corregir el problema y programarlo[16]

4.1.8. Políticas para un desarrollo de software seguro

Descripción de políticas para el desarrollo seguro de software.

[16] SANS. *Security Policy*. https://www.sans.org/security-resources/policies/application-security#web-application-security-policy.

4.1.8.1. Introducción

El proceso principal al desarrollar aplicaciones consiste en transformar los datos en información, y transmitirla a los usuarios. El resultado es el valor que se le otorga a la aplicación.

La información manipulada en las aplicaciones debe ser protegida, no únicamente cuando la aplicación esté terminada. Los datos deben ser protegidos desde la recolección hasta el resultado final. En todas las etapas de desarrollo se debe proteger la información, lo cual demuestra que la creación de políticas es un factor importante en el desarrollo de aplicaciones.

4.1.8.2. Objetivos

El objetivo de esta política consiste en definir las pautas a seguir por el equipo de desarrollo para que el software minimice su vulnerabilidad.

4.1.8.3. Desarrollo de software seguro

Para un desarrollo seguro de software se recomienda incluir buenas prácticas que incluyen diferentes tipos de seguridad en todas las etapas, como, por ejemplo, en la autenticación del software:

- Las aplicaciones deben admitir la autenticación de usuarios individuales, no de grupos.
- Las aplicaciones no deben almacenar contraseñas en texto en cualquier forma.
- Las aplicaciones no deben transmitir contraseñas en texto a través de la red.

- Las aplicaciones deben proporcionar algún tipo de gestión de roles, de modo que un usuario no pueda actuar sobre las funciones de otro sin tener que saber la contraseña del otro.
- Autenticación multifactorial.

Cada rol que participe en el desarrollo de software debe ser responsable por la seguridad del proyecto. Esto incluye no divulgar información a terceros o personas no autorizadas en el manejo del software.

El acceso a la documentación utilizada e implementada para el desarrollo no debe estar al alcance de cualquier persona que no pertenezca al equipo de trabajo. La modificación del proyecto debe ser autorizada por el líder del mismo.

Cada participante en el desarrollo de software debe respetar las políticas establecidas por Centro de Cálculo.

5. EVALUACIÓN DE RIESGOS

En esta sección se realizará el análisis de riesgo del procedimiento para desarrollo de nuevos sistemas informáticos que pertenece a Centro de Cálculo, el procedimiento fue descrito en la sección 2 de este trabajo de graduación.

En la actualidad, los riesgos que pueden afectar a las diferentes organizaciones han aumentado, sin importar el giro de negocio al que se dediquen o la clasificación a la cual pertenezca el riesgo. Por lo tanto, es importante el análisis para determinar el apetito de riesgo que la organización está dispuesta a tolerar y para determinar la respuesta a los diferentes riesgos que puedan ser detectados. Requiere identificar a los encargados, al responsable y los controles por utilizar para minimizar el impacto.

Centro de Cálculo tiene como objetivo el desarrollo de soluciones informáticas, que satisfagan las necesidades de los usuarios que pertenezcan a la Facultad de Ingeniería, ya sea, estudiantes, personal administrativo o docente. Administrar la información utilizada en una forma segura, eficiente y transparente, aprovecha al máximo los recursos disponibles y utiliza herramientas adecuadas para el desarrollo.

Uno de los aspectos que destaca Centro de Cálculo e Investigación Educativa es el deseo de administrar la información en forma segura, eficiente y transparente. Estas características se pueden lograr al aplicar un sistema de gestión de seguridad de la información, que vele por el cumplimiento, tome en cuenta las amenazas y cree soluciones para la eliminación o mitigación de estas.

Para crear un sistema de gestión se deben detectar los riegos identificar las partes interesadas en la creación de un sistema de gestión de seguridad de la información. Las partes interesadas pueden ser grupos o personas que poseen presencia en los procesos de las organizaciones y que pueden afectar o ser afectados por las decisiones de las organizaciones, en este caso, por Centro de Cálculo de la Facultad de Ingeniería.

En la tabla XXII se enlistan las partes interesadas en un sistema de gestión de seguridad de la información en el proceso indicado al inicio de esta sección.

Tabla XXII. **Partes interesadas**

Partes Interesadas
Junta directica de Facultad de Ingeniería
Coordinación
Secretaria
Equipo de desarrollo
Facultad y/o escuelas externas a la Facultad de Ingeniería.

Fuente: elaboración propia, empleando Word 2019.

5.1. Identificar el nivel de riesgo

Al realizar un análisis e identificar los riesgos de los procesos o eventos que están en observación, es necesario definir cuál es el nivel de riesgo permitido. Cada organización tiene diferente nivel de riesgo que está dispuesto a aceptar, por lo tanto, estos niveles no pueden ser genéricos sino definidos especialmente para entidad bajo observación.

5.1.1. Variables de riesgo: apetito y tolerancia

Los niveles de riesgos están comprendidos por el apetito de riesgo y tolerancia de riesgo. Estos términos usualmente son confundidos y se piensa que son sinónimos, pero la diferencia consiste en el rango de aceptación.

El apetito de riesgo es considerado como el riesgo que la organización está dispuesto a aceptar, con el fin de lograr los objetivos.

La tolerancia de riesgo se considera como la desviación máxima del riesgo con respecto al apetito que las organizaciones desean o están dispuestas a aceptar, siempre teniendo como meta el cumplimiento de los objetivos.

Por ejemplo, una empresa encargada de construir una casa, al comenzar el proyecto le notifica que los días disponibles para construir la serían 130. La empresa estimó que la casa debería estar terminada en 90 días, pero considerando las condiciones meteorológicas decidieron agregar 20 días para un total de 110 días y así tener los 20 días extras para afinar detalles.

Lo que se observa en este ejemplo, es que el apetito de riesgo consta de 90 días, pero tienen una tolerancia al riesgo de 110 días.

Para determinar el apetito de riesgo es importante primero determinar el impacto y la probabilidad aceptada para los riesgos identificados en el proceso bajo análisis. La probabilidad determina la frecuencia con la cual pueden suceder los riesgos o eventos identificados en la organización. El impacto determina la gravedad o tipo de pérdida que el riesgo representa para la organización.

En la tabla XXIII se muestra la probabilidad de ocurrencia de riesgos identificados en el proceso bajo análisis.

Tabla XXIII. **Probabilidad**

Probabilidad		
5	Frecuente	Una vez por semana
4	Moderado	Una vez por mes
3	Ocasional	Una vez por semestre
2	Remoto	Una vez por año
1	Improbable	Cada 2 años

Fuente: elaboración propia, empleando Word 2019.

En la tabla XXIV se muestra el impacto de los riesgos para el proceso

Tabla XXIV. **Impacto**

Impacto		
5	Catastrófico	Pérdidas graves
4	Mayor	Pérdidas sustanciales
3	Moderado	Pérdidas significativas
2	Menor	Pérdidas menores
1	Insignificante	Pérdidas mínimas

Fuente: elaboración propia, empleando Word 2019.

Al tener definido el impacto y probabilidad, se pueden definir los criterios de aceptación, (apetito de riesgo y tolerancia de riesgo).

En la tabla XXV se definen los criterios de aceptación específicos para el proceso bajo análisis.

Tabla XXV. **Criterios de aceptación**

Criterios		
1 a 4	Acepta	Aceptar las consecuencias del riesgo sin reducir y controlar.
5 a 9	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
10 a 14	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
15 o mas	Transferir	Designar a terceros la responsabilidad del tratamiento del riesgo

Fuente: elaboración propia, empleando Word 2019.

5.2. Mapa y matriz de riesgo

El mapa de riesgo y la matriz de riesgo son herramientas útiles y necesarias para el análisis de riesgo.

5.2.1. Mapa de riesgo

Es una herramienta que permite clasificar el agravio que el riesgo podría causar. Los rangos que el mapa de riesgo utiliza están comprendidos en alto, medio y bajo. También involucra la ocurrencia.

5.2.2. Matriz de riesgo

La matriz de riesgo es una herramienta muy útil para la evaluación de riesgos. Permite determinar cuáles son los riesgos que necesitan atención y son relevantes en los procesos. Esto se logra tomando como base las dos dimensiones primordiales de esta matriz, que son el: riesgo el impacto.

Así mismo, esta matriz es útil para implementar un estudio en todas las fases necesarias para la determinación de riesgos, las cuales son: identificación, análisis, evaluación y tratamiento.

En este trabajo de graduación se utilizará la matriz de riesgo como herramienta para el análisis de riesgo del proceso bajo análisis.

Los riesgos descritos puede que hayan o no ocurrido en Centro de Cálculo de la Facultad de Ingeniería; algunos riesgos descritos son comunes que se pueden presentar en el proceso y fueron identificados para crear controles de prevención y evitar su ocurrencia.

A continuación, se presenta los riesgos detectados en el proceso de desarrollo de nuevos sistemas de Centro de Cálculo. El análisis de riesgos se dividió en las fases correspondientes las cuales son descritas en la tabla XXVI.

Tabla XXVI. **Fases del análisis de riesgo**

Fase	Descripción
Identificación de riesgo	Se determina que el riesgo que puede ocurrir, como las causas, y las razones de su ocurrencia.
Análisis y evaluación de riesgo	**Se determina la frecuencia de ocurrencia del riesgo, como el impacto que este puede efectuar, y a la vez, se asignan prioridades a los diferentes riesgos para ser comparados con el apetito y tolerancia de riesgo.**
Tratamiento de riesgo	Asignación de métodos a seguir para el manejo de los riesgos.

Fuente: School Of Management, ESI. *Glosario de términos de gestión de riesgos*. p. 23.

A continuación, en la tabla XXVII, se desglosará cada una de las fases del análisis de riesgo descritas en la tabla XXVI. En este análisis se estudiará el procedimiento para desarrollo de nuevos sistemas informáticos que pertenece a Centro de Cálculo.

Cada etapa se desglosa en subetapas por las cuales debe pasar el proceso para ser estudiado.

Por ejemplo, la etapa de identificaciones de riesgo está formada por**:**

- Número de riesgo (Identificador de riesgo)
- Etapas del proceso
- Evento
- Causa

La etapa de análisis y evaluación del riesgo está formada por:

- Consecuencias (que el evento puede provocar en el proceso)
- Probabilidad (de que el evento suceda)
- Impacto (que el evento pueda provocar en el proceso)
- Indicador de riesgo (es la multiplicación de la probabilidad y el impacto. Se utiliza para clasificar el riesgo en el mapa de riesgo).

La etapa de tratamiento de riesgo está formada por:

- Respuesta al riesgo (consiste en los criterios de aceptación descritos en la tabla XXV)
- Riesgo residual (acciones que aún se puedan presentar a causa del riesgo inicial)
- Existe control (existe medida para monitorear evento)
- Estatus de control (estado vigente del control)
- Acciones para implementar (al ocurrir el evento)
- Unidades responsables (quiénes son los responsables sobre las acciones para monitorear el riesgo, sus consecuencias y acciones).

Tabla XXVII. **Identificación, análisis, evaluación y tratamiento de riesgo**

Procedimiento para desarrollo de nuevos sistemas informáticos

Identificación del Riesgo				Análisis y Evaluación del Riesgo				Tratamiento de Riesgos					
No.	Etapas	Evento	Causas	Consecuencias	Probabilidad	Impacto	Indicador de Riesgo	Respuesta al Riesgo	Riesgo Residual	Existe Control	Estatus del Control	Acciones a implementar	Unidades Responsables
R1	Determina la necesidad de un nuevo sistema informático	Información incompleta sobre la funcionalidad	Posible rechazo de solicitud por información.	Atraso en la aceptación e inicio del proyecto.	4	2	8	Evita	Observación	Si	Ajustado	Creación de guía donde indique los pasos necesarios para solicitar nuevo sistema.	Interesado (Cliente)
R2	Recibe y asigna personal para realizar el análisis de factibilidad del proyecto	Contrato de confidencialidad	Protección del bienestar del proyecto e información confidencial con personal y personas externas.	Filtración de información antes del inicio del proyecto, uso indebido de la información.	2	3	6	Evita	Observación	Si	Ajustado	Implementar un contrato de confidencialidad donde se indique las condiciones aceptables e inaceptables.	Coordinador
R3	Realiza la propuesta de solución.	Imprecisión en la planificación de excepciones pertinentes al proyecto	El manejo de las excepciones pertinentes al proyecto no fueron consideradas al realizar la propuesta de solución.	Fallas en el sistema al presentar las soluciones, cliente no acepte la solución inicial.	3	4	12	Reducir	Controlado	Si	En revisión	Creación de guía con pasos a seguir para la realización de propuestas de cambios en sistemas o desarrollo de nuevos sistemas.	Programador de Computadoras
R4	Realiza la planificación para el desarrollo del sistema informático	Planificación de proyecto sobrepaso alcance y costo	Al realizar la planificación del proyecto no se consideraron ciertas actividades por lo cual se sobrepaso el costo y el alcance no fue definido correctamente.	Al proyecto no será realizado en forma exitosa debido al problema de costo y los objetivos no fueron definidos oportunamente.	3	4	12	Reducir	Controlado	Si	En revisión	Crear un modelo de doble aprobación, donde la planificación será revisado y aprobado por dos personas, para crear dos estaciones de supervisión y aceptación de planificación.	Programador de Computadoras y Jefe de desarrollo
R5	Asigna permisos a los recursos asignados para desarrollar el sistema informático	Protección de datos contenidos en los recursos para el desarrollo del proyecto	Lineamientos escasos que indican el correcto uso de la información correspondiente al proyecto.	Información confidencial o privada es de acceso publico.	3	5	15	Transferir	Observación	Si	En revisión	Asignar a una persona o grupo responsable para la protección de la información.	Jefe de desarrollo

Continuación de la tabla XVII.

Procedimiento para desarrollo de nuevos sistemas informáticos

Identificación del Riesgo				Análisis y Evaluación del Riesgo				Tratamiento de Riesgos					
No.	Etapas	Evento	Causas	Consecuencias	Probabilidad	Impacto	Indicador de Riesgo	Respuesta al Riesgo	Riesgo Residual	Existe Control	Estatus del Control	Acciones a implementar	Unidades Responsables
R6	Entrevista a los usuarios para desarrollar las funcionalidades del sistema.	Requerimientos o elementos no identificados en la entrevista a los usuarios.	El usuario no esta consciente de los detalles esenciales del proyecto solicitado. El entrevistador no realiza las preguntas necesarias para obtener la	Retraso en planeación y desarrollo del proyecto, produce situaciones inesperadas.	3	3	9	Evita	Controlado	Si	Ajustado	Creación de guía con preguntas generales, y necesarias para la entrevista y toma de requerimientos.	Programador de Computadoras
R7	Elabora un documento con los requerimientos funcionales y no funcionales.	Bitácora de eventos y tareas.	Ausencia o historial incompleto que registre los eventos y tareas realizadas y por realizar	Por ausencia de historial, se dificulta el estudio de sucesos que afectan al proyecto.	3	1	3	Acepta	Controlado	Si	Optimo	Creación de bitácora o designar un periodo para la actualización.	
R8		Desorganización en la elaboración del documento, fuentes no	Se localiza diversas fuentes de información para obtener requerimientos funcionales y no funcionales, sin poder	Mal entendidos en la comunicación entre los participantes del proyecto, errores al identificar requerimientos funcionales y no funcionales.	4	1	4	Acepta	Controlado	Si	Optimo	Crear lineamientos y protocolos para identificar el orden de las fuentes de información.	
R9	Programa el requerimiento indicado en la planificación.	Funcionamiento incorrecto del software.	El equipo utilizado para programar los requerimientos es se encuentran dañados.	Demora en el sistema en fase de desarrollo, posible perdida de continuidad de servicio, interrupción de fase de desarrollo.	5	3	15	Transferir	Observación	Si	En revisión	Determinar ciclos de revisión y mantenimiento para el equipo y software utilizado para el desarrollo.	Jefe de desarrollo, programador de computadoras
R10		Acceso de usuario	Posible confusión de permisos a perfiles no correspondientes.	Acceso indebido de terceros a información o sistemas no autorizados.	1	5	5	Evita	Observación	Si	Optimo	Creación de perfiles y asignar permisos específicos.	Programador de Computadoras
R11		Poca comunicación en el equipo de desarrollo.	No existe comunican entre los miembros del equipo de desarrollo sobre el manejo y	Poca interacción entre los miembros del equipo de desarrollo, coordinación en cambios de requerimiento descuidada.	4	2	8	Evita	Controlado	Si	Ajustado	Crear rutinas sociales, para incrementar la comunicación entre el equipo de desarrollo.	
R12		Perdida de Información	Seguridad de información débil, mínima cantidad de políticas.	Demora en la realización de tareas y eventos en el fase de desarrollo.	2	5	10	Reducir	Observación	Si	Ajustado	Implementación de políticas para la seguridad de información. Capacitar al equipo de desarrollo, sobre buenas practicas en seguridad de la información.	
R13		No realizar copias de seguridad en un tiempo establecido.	Al no tener un sistema de copias se seguridad, puede existir perdida de información en el tiempo que no se realizaron las copias	Perdida de información útil para el desarrollo y funcionalidad del sistema y posible atraso en el desarrollo del sistema.	3	5	15	Transferir	Observación	Si	En revisión	Crear políticas para realizar copias de seguridad, determinar a un grupo responsable por el cumplimiento de esta acción.	

Continuación de la tabla XVII.

Procedimiento para desarrollo de nuevos sistemas informáticos

Identificación del Riesgo				Análisis y Evaluación del Riesgo				Tratamiento de Riesgos					
No.	Etapas	Evento	Causas	Consecuencias	Probabilidad	Impacto	Indicador de Riesgo	Respuesta al Riesgo	Riesgo Residual	Existe Control	Estatus del Control	Acciones a implementar	Unidades Responsables
R20	Genera documento para la entrega del nuevo sistema y Genera manuales de usuario. Ver procedimiento	Documentos desgastados o perdidos.	Mantenimiento y almacenamiento inadecuado de documentación.	Pérdida de información, y documentación.	3	2	6	Evita	Controlado	Si	Optimo	Determinar un área para el almacenamiento de documentación, como la creación de una guía para generar nuevos documentos.	Jefe de desarrollo y programador de computadoras
R21		Proyectos sin documentación.	Poco control de la administración del proyecto y miembros del grupo.	Atraso en la definición y creación de documentos que registren información para el uso del proyecto.	3	2	6	Evita	Controlado	Si	Optimo	El jefe de desarrollo debe solicitar al equipo de desarrollo documentación periódica sobre el avance, y/o eventos correspondientes al proyecto.	
R22	Capacita a los usuarios del sistema	Conclusión del proyecto no realizado según las guías establecidas.	La conclusión del proyecto no se realizo como se esperaba, se siguieron los lineamientos establecidos. La capacitación a los usuarios no se	Existen desacuerdos en los miembros del proyecto, ya sean internos o externos; esto permite que existan inconvenientes en la entrega del proyecto, y la capacitación del usuario no funcione como se esperaba.	2	3	6	Evita	Controlado	Si	Optimo	Instruir al equipo de desarrollo para que realice buenas capacitaciones de usuario y a la vez proporcione la información necesaria al interesado para que pueda utilizar el sistema desarrollado.	Programador de Computadoras

Continuación de la tabla XVII.

Procedimiento para desarrollo de nuevos sistemas informáticos

Identificación del Riesgo				Análisis y Evaluación del Riesgo				Tratamiento de Riesgos						
No.	Etapas	Evento	Causas	Consecuencias	Probabilidad	Impacto	Indicador de Riesgo	Respuesta al Riesgo	Riesgo Residual	Existe Control	Estatus del Control	Acciones a implementar	Unidades Responsables
RI4	Realiza las pruebas en conjunto con el Jefe de Desarrollo para verificar el funcionamiento del requerimiento.	Pruebas de aceptación incompletas.	Inconsistencia en las pruebas realizadas, no existe fuente confiable para comprobar resultados.	Atraso en la realización de tareas para complementar el desarrollo del proyecto.	4	3	12	Reducir	Controlado	Si	En revisión	Crear un paquete de pruebas básicas a seguir y solicitar al interesado los resultados deseados, para posible comparación de los mismo.	Programador de Computadoras, Jefe de desarrollo, si es necesario Jefe del área de redes.
RI5	Realiza la implementación del sistema, ver procedimiento para implementación de un nuevo sistema.	Desempeño del proyecto no es el	Requerimientos y tareas no programadas según lo esperado.	Usuario insatisfecho por el desempeño del sistema.	3	3	9	Evita	Controlado	Si	Ajustado	Jefe desarrollo debe implementar métodos para evaluar el progreso y cumplimiento de tareas creadas por el equipo de desarrollo que fueron solicitadas por	
RI6		Inexistencia de copias de seguridad	Extravió de información útil y de respaldo para el sistema.	Extravió de información útil para el sistema.	2	5	10	Reducir	Observación	No	En revisión	Crear políticas para realizar copias de respaldo ya sea por cada cambio realizado o por tiempo determinado.	
RI7		Inconveniente al realizar la migración de datos en la implementación del proyecto.	Existe incongruencia en la definición de los conceptos de información.	Información transferida no es útil en el nuevo sistema.	3	4	12	Reducir	Observación	Si	En revisión	Crear un plan estándar para realizar migración de datos, capacitar al equipo de desarrollo con políticas y guías a seguir para realizar una buena migración.	
RI8	Realiza pruebas al sistema ya implementado	Pruebas de aceptación incorrectas.	Guía incompleta sobre pasos a seguir para realizar pruebas de	Resultados incongruentes en el desempeño del proyecto.	2	2	4	Acepta	Controlado	Si	Optimo	Crear política para pruebas de aceptación.	Jefe de desarrollo
RI9		El resultado de las pruebas no son aceptadas por el usuario.	El usuario no tuvo mucha participación desde el inicio del desarrollo del proyecto, decidió	La puesta en producción del sistema presenta retrasos que afectan las expectativas del sistema y el cierre del mismo.	5	3	15	Transferir	Controlado	Si	En revisión	El jefe de desarrollo debe crear métodos para que el cliente este mas interesado, aunque este no muestre interés, pero debe solicitar su participación para el avance del desarrollo.	

Fuente: elaboración propia, empleando Excel 2019.

El desglose de las etapas de riesgo es una herramienta ampliamente utilizada para la evaluacion de riesgos. Presenta los detalles necesarios para entender el comportamiento y origen del riesgo, para así clasificar los, encontrar el tratamiento y acciones por implementar.

La columna Indicador de riesgo es calculada al multiplicar la probabilidad y el impacto. El resultado está representado por un color que identifica los diferentes criterios de aceptación que puede tener el riesgo.

En la tabla XXV se detalla el rango y el tipo de criterio; a cada rango se le asigna un color para que visualmente sea fácil clasificar los riesgos e identificar qué tipo de criterio de aceptación debe ser aplicado.

En la tabla XXVII se representa el rango del criterio con el color designado.

Tabla XXVIII. **Criterios de aceptación por color**

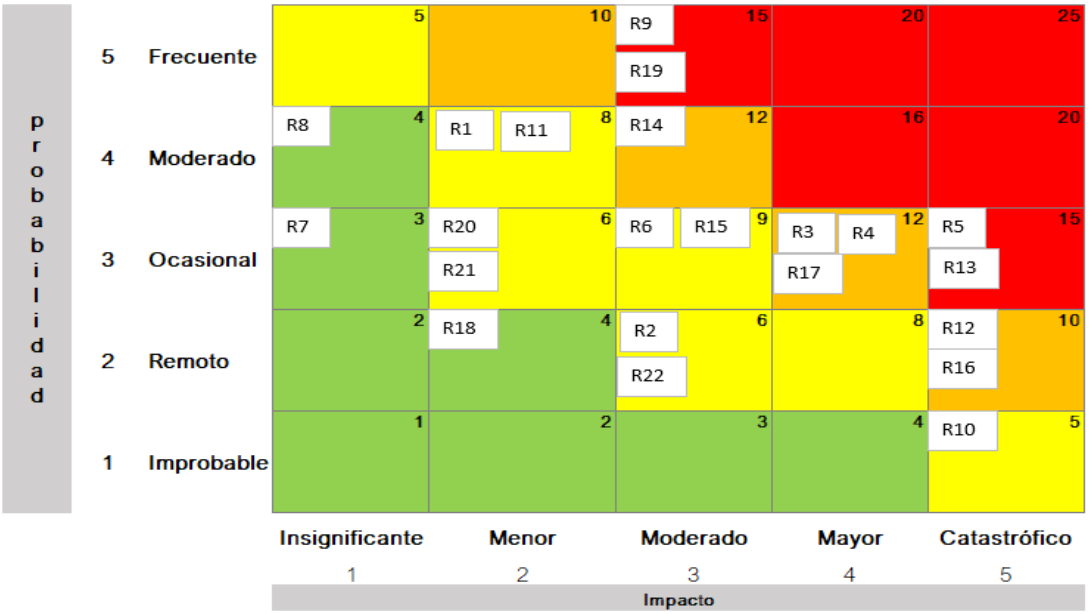
Apetito de riesgo	
1 a 4	Acepta
5 a 9	Evita
10 a 14	Reducirlo
15 a mas	Transferirlo

Fuente: elaboración propia, empleando Word 2019.

La matriz de riesgo es una herramienta que permite observar cuales son los riegos más trascendentales en el procedimiento y que pueden afectar bruscamente las acciones que lo forman. La matriz de riesgo es una herramienta visual que permite relacionar el identificador del riesgo (no el riesgo) con los colores designados a los criterios de aceptación, se considera la

clasificación como un tipo semáforo debido a que cada color representa una acción a seguir.

Figura 5. **Matriz de riesgo**



Fuente: elaboración propia, empleando Excel 2019.

5.3. Respuesta al riesgo

En el presente capítulo se ha realizado el desglose de los riesgos detectados en el procedimiento para desarrollar nuevos sistemas informáticos. Se ha identificado, analizado y asignado un tipo de respuesta a cada riesgo.

Este análisis ha cuantificado cada riesgo y dependiendo del valor, este será clasificado por el tipo de respuesta o criterio de aceptación.

La tabla XXVIII muestra un resumen sobre el riesgo y el tipo de respuesta que fue asignado. Esta información fue obtenida de la matriz de riesgo donde el número de riesgo fue clasificado por color, y se determinó que cada color corresponde a un rango de tipo de respuesta al riesgo.

Tabla XXIX. **Resumen matriz de riesgo**

Número de riesgo	Respuesta al riesgo
R1	Evita
R2	Evita
R3	Reducir
R4	Reducir
R5	Transferir
R6	Evita
R7	Acepta
R8	Acepta
R9	Transferir
R10	Evita
R11	Evita
R12	Reducir
R13	Transferir
R14	Reducir
R15	Evita
R16	Reducir
R17	Reducir
R18	Acepta
R19	Transferir
R20	Evita

Continuación tabla XXIX.

R21	**Evita**
R22	Evita

Fuente: elaboración propia, empleando Word 2019.

5.4. Análisis de resultados

En la tabla XXIX se describe la relación entre el identificador de riesgo, la respuesta al mismo y por qué se le asignó esa respuesta.

Con base en la matriz de riesgo se puede visualizar que dependiendo de los parámetros de probabilidad e impacto, un riesgo puede tener una probabilidad alta, pero poco impacto. Por lo tanto, dependiendo de este juego de parámetros así es la respuesta al riesgo.

Tabla XXX. **Descripción de respuesta al riesgo**

Número de riesgo	Nombre	Respuesta al riesgo	
R1	Información incompleta sobre la funcionalidad del sistema	Evita	Se considera que este riesgo debe ser evitado porque la organización no desea verse involucrada en el riesgo, por lo tanto, se deben realizar tareas para que este riesgo no se pueda presentar.
R2	Contrato de confidencialidad	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
R3	Imprecisión en la planificación de excepciones pertinentes al proyecto	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
R4	Planificación de proyecto sobrepasó alcance y costo	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
R5	Protección de datos contenidos en los recursos para el desarrollo del proyecto	Transferir	Designar a terceros la responsabilidad del tratamiento del riesgo
R6	Requerimientos o elementos no identificados en la entrevista a los usuarios.	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
R7	Bitácora de eventos y tareas.	Acepta	Aceptar las consecuencias del riesgo sin reducir y controlar.
R8	Desorganización en la elaboración del documento, fuentes no identificadas correctamente.	Acepta	Aceptar las consecuencias del riesgo sin reducir y controlar.

Continuación de la tabla XXX.

R9	Funcionamiento incorrecto del software.	Transferir	Designar a terceros la responsabilidad del tratamiento del riesgo.
R10	Acceso de usuario	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
R11	Poca comunicación en el equipo de desarrollo.	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
R12	Pérdida de Información	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
R13	No realizar copias de seguridad en un tiempo establecido.	Transferir	Designar a terceros la responsabilidad del tratamiento del riesgo.
R14	Pruebas de aceptación incompletas.	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
R15	Desempeño del proyecto no es el óptimo.	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
R16	Inexistencia de copias de seguridad	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
R17	Inconveniente al realizar la migración de datos en la implementación del proyecto.	Reducir	Aplicar reglas o herramientas para minimizar la probabilidad del riesgo y las consecuencias.
R18	Pruebas de aceptación incorrectas.	Acepta	Aceptar las consecuencias del riesgo sin reducir y controlar.
R19	El resultado de las pruebas no es aceptado por el usuario.	Transferir	Designar a terceros la responsabilidad del tratamiento del riesgo
R20	Documentos desgastados o perdidos.	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.

Continuación de la tabla XXX.

R21	Proyectos sin documentación.	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.
R22	Conclusión del proyecto no realizado según las guías establecidas.	Evita	Elección de no verse implicado en la situación de riesgo, por lo tanto, evitar la realización de tareas que impliquen el riesgo.

Fuente: elaboración propia, empleando Word 2019.

Al finalizar el análisis, Centro de Cálculo puede decidir qué acciones tomar para enfrentar los posibles riesgos y minimizar el impacto de los mismos.

Los riegos detectados en este análisis no son los únicos que se puedan presentar en este proceso, y no significa que sean riesgos que Centro de Cálculo no haya previsto.

CONCLUSIONES

1. El estándar ISO27001 proporciona directrices a seguir para la creación y administración de un sistema de seguridad de la información. Además, otorga lineamientos necesarios para determinar cuáles son los pasos para seguir, dependiendo del área en que se desarrolla la organización. La guía proporcionada para Centro de Cálculo e Investigación Educativa se describe en cada uno de los capítulos desarrollados, en especial el 4, donde se presentan políticas útiles para prevenir la fuga de información. A la vez, proporciona lineamientos de seguridad por seguir en el procedimiento para desarrollo de nuevos sistemas informáticos. La guía incluye el desarrollo del concepto de ISO 27001, seguridad de la información, el análisis del procedimiento para desarrollo de nuevos sistemas informáticos, requisitos obligatorios y opcionales para la creación del sistema de gestión de seguridad, el desarrollo de políticas a seguir y el análisis de posibles riesgos.

2. El estándar ISO 27000 consiste en una agrupación de estándares que establecen los lineamientos para la creación de un sistema de seguridad de la información. A esta agrupación pertenece el estándar ISO 27001, el cual describe una metodología para crear un sistema de seguridad de la información considerando la integridad, confidencialidad y disponibilidad de la información. Se encarga de realizar el análisis de riesgo y de definir la documentación mínima necesaria que debe tener la organización que desea obtener la certificación, o los requisitos mínimos para crear un sistema de gestión de seguridad de la información. El concepto ISO 27001 fue desarrollado en el capítulo 2 de este trabajo de

graduación; en este se presentan las ventajas de seguir las directrices de dicho estándar y se presenta el concepto de ISO 27001.

3. Los riesgos de no tener implementada una normativa como la propuesta con la certificación ISO 27001 son inherentes a cada organización, dependiendo del campo en el que se desarrollan. El capítulo 1 presenta los riesgos y peligros por falta de seguridad de la información. El capítulo 5 presenta el análisis de riesgos con un enfoque en el procedimiento de desarrollo de nuevos sistemas informáticos en Centro de Cálculo e Investigación Educativa.

4. Los requerimientos y recursos necesarios para crear un sistema de gestión de seguridad de la información se expresan en documentos y políticas que debe definir Centro de Cálculo e Investigación Educativa para crear una cultura de seguridad de la información en el departamento. El capítulo 1 presenta las fases para construir un sistema de gestión de seguridad de la información, mientras que en el capítulo 3 se desarrolla la estructura de un SGSI, en el cual se determina los factores internos y externos que pueden afectar a Centro de Cálculo e Investigación Educativa.

5. Este trabajo de graduación presenta una metodología que permite a Centro de Cálculo e Investigación Educativa crear un sistema de gestión de seguridad de la información. El capítulo 4 presenta las políticas que se ajustan a las necesidades de Centro de Cálculo e Investigación Educativa para el desarrollo de nuevos sistemas informáticos. Finalmente, el capítulo 5 presenta los pasos para realizar un análisis de riesgo si se desea analizar otro procedimiento fundamental.

RECOMENDACIONES

1. Desarrollar un estudio para aplicar el estándar ISO 27001 y construir un SGSI en los departamentos de informática de la Facultad de ingeniería de la Universidad de San Carlos de Guatemala.

2. Adoptar un plan de estudio sobre el estándar ISO 27001 y la familia ISO 27000 para comprender la función de cada estándar perteneciente a la familia y cómo puede ser combinada con diferentes estándares para ser implementadas en otras áreas.

3. Diseñar un sistema de evaluación que será útil para identificar los riesgos informáticos que pueda tener el departamento. Se sugiere realizar un análisis de riesgos periódicamente para establecer una respuesta que cumpla con los lineamientos del estándar ISO 27001.

4. Evaluar herramientas de software y tecnologías que aseguren la seguridad de la información considerando los factores internos y externos de la organización.

5. Investigar cómo la gestión por procesos puede apoyar y fortalecer la creación de un sistema de gestión de seguridad de la información y la forma en que esta metodología puede favorecer a la creación de políticas y la disminución de riesgos de seguridad en las organizaciones.

BIBLIOGRAFÍA

1. AREITIO BERTOLIN, Javier. *Seguridad de la información.* [en línea]. <https://books.google.com.gt/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=PP1&dq=seguridad+de+la+informaci%C3%B3n&ots=wrlltJFWVk&sig=WbKYeW2R8CFr6u3IOpE0tYKFrEo#v=onepage&q=seguridad%20de%20la%20informaci%C3%B3n&f=false>. [Consulta: 6 de noviembre 2019].

2. Facultad de Ingeniería, USAC. *Centro de Cálculo e investigación Educativa*. [en línea]. <http://ccie.ingenieria.usac.edu.gt/>. [Consulta: 15 de noviembre 2019].

3. 360 Factors. *Five Steps of the Risk Management Process*. [en línea]. <https://www.360factors.com/blog/five-steps-of-risk-management-process/>. [Consulta: 5 de junio 2020].

4. Instituto Nacional de Normalización Tecnologías de la información. *Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información*. 2da ed. Chile: INN, 2013. 104 p.

5. ISO Tools. *¿En qué consiste una matriz de riesgos?* [en línea]. <https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/>. [Consulta: 10 de julio 2020].

6. ISO 27000. *SGSI.* [en línea]. <https://www.iso27000.es/sgsi.html>. [Consulta: 11 de noviembre 2019].

7. ISO 27001 Academy. *¿Qué es norma ISO 27001?* [en línea]. <https://advisera.com/27001academy/es/que-es-iso-27001/>. [Consulta: 15 de noviembre 2019].

8. ISO 27001. *Seguridad de la información*. [en línea]. <https://www.normas-iso.com/iso-27001/>. [Consulta: 8 de noviembre 2019].

9. Qualiex. *¿Qué es una Matriz de Riesgo?* [en línea]. <https://blogdelacalidad.com/que-es-una-matriz-de-riesgo/#:~:text=La%20matriz%20de%20riesgo%2C%20tambi%C3%A9n,y%20participar%20en%20el%20proceso?>. [Consulta: 12 de julio 2020].

10. SECCOND. *Ciberseguridad, seguridad informática y seguridad de la información*. [en línea]. <https://www.seccond.es/ciberseguridad-seguridad-informatica-y-seguridad-de-la-informacion/>. [Consulta 3 de junio 2020].

11. TechTarget. *Risk management*. [en línea]. <https://searchcompliance.techtarget.com/definition/risk-management#:~:text=Risk%20management%20is%20the%20process,errors%2C%20accidents%20and%20natural%20disasters>. [Consulta: 11 de junio 2020].

12. Tecon. *La seguridad de la información*. [en línea]. <https://www.tecon.es/la-seguridad-de-la-informacion/>. [Consulta: 23 de noviembre 2019].

13. Web y Empresas. *Matriz de selección*. [en línea]. <https://www.webyempresas.com/matriz-de-seleccion-de-procesos-criticos/>. [Consulta: 2 de diciembre 2019].