# Gap de Seguridad de la Información UCompensar

Adriana Mercedes Moya Aguirre

Heriberto Miranda Vaca

Fundación Universitaria Compensar

Proyecto fin de grado

Docente tutor

Carlos Alberto Cañón

18 de noviembre de 2022

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

# GAP Seguridad de la Información para la UCompensar

Adriana Mercedes Moya Aguirre

Heriberto Miranda Vaca

Trabajo de grado presentado como requisito parcial para optar al título de:
Especialista de Seguridad Informática

Director: Ingeniero Carlos Alberto Cañón

Codirector: Ingeniero Jairo Cesar Gómez Acero

Línea de Investigación:
Seguridad de la Información

Fundación Universitaria Compensar
Facultad de Ingeniería, Especialización en Seguridad Informática
Bogotá, Colombia
2022

## Resumen

La presente propuesta va enfocada a prestar un servicio de diagnóstico respecto a Seguridad de la Información, basada en el modelo de madurez internacional NIST-CSEAT (*National Institute of Standards and Technology-Computer Security Expert Assist Team*), que permite a la Fundación Universitaria Compensar, identificar el estado actual de los cinco (5) niveles: Políticas, Procedimientos, Implementación, Pruebas e Integración. Todo lo anterior, alineado a los objetivos estratégicos y de Seguridad de la Información.

Se realizarán entrevistas y reuniones con los líderes de las áreas para identificar el estado actual. Como resultado, se obtendrá el nivel de madurez, como una medida cuantificable (porcentual) del nivel de implementación, que nos indica el grado de desarrollo y fortalezas de las medidas de Seguridad de la Información de la Fundación Universitaria Compensar, así como un portafolio de iniciativas, programas y proyectos para ejecutar el Plan de Optimización.

Con esta consultoría, se logra conocer el estado actual y planear hacia donde se desea cumplir en términos de Seguridad de la Información, con el fin de aumentar el nivel de credibilidad y competitividad de la Fundación Universitaria Compensar tanto internamente como en su entorno.

**Palabras clave:**

**Seguridad de la información,** conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad en los activos de la información.

**Activos de la información,** son los recursos necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

**Datos personales,** cualquier información relativa a una persona física viva identificada o identificable.

**SOC (Security Operation Center),** centro de operaciones de seguridad que previene, monitorea y controla la Ciberseguridad.

**NIST-CSEAT (***National Institute of Standards and Technology-Computer Security Expert Assist Team***)** El marco para la mejora de la seguridad cibernética en infraestructuras críticas, fue emitida inicialmente en los Estados Unidos en febrero de 2.014. La orientación del marco es ayudar a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporcionando un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

# Contenido

**PÁG.**

**RESUMEN** ..... III

**INTRODUCCIÓN** ..... 2

ANTECEDENTES Y JUSTIFICACIÓN ..... 3
FORMULACIÓN DEL PROBLEMA ..... 4
OBJETIVO GENERAL ..... 5
*Objetivos Específicos* ..... *5*
ALCANCES Y LIMITACIONES ..... 6

**1. MARCO TEÓRICO** ..... 9

1.1 MARCO LEGAL Y REGULATORIO ..... 10
1.2 GESTIÓN DEL RIESGO ..... 11
1.3 NORMA ISO/IEC 27001 ..... 11
1.4 NORMA NIST-CSEAT ..... 12

**2. DISEÑO METODOLÓGICO** ..... 13

**3. RESULTADOS** ..... 14

**4.** ..... 24

**5. DISCUSIÓN** ..... 24

**6. CONCLUSIONES Y RECOMENDACIONES** ..... 25

6.1 CONCLUSIONES ..... 25
6.2 RECOMENDACIONES ..... 27

**BIBLIOGRAFÍA** ..... 28

# Introducción

En la actualidad, las preocupaciones de las Universidades, no solo se basan en dictar cátedra y mantener la calidad de la educación, también es importante cumplir con normas legales, que día a día se hacen más estrictas y conllevan a unas altas sanciones al momento de no ser cumplidas, fuera de esto, la globalización obliga a las empresas a cumplir con normas para poder ofrecer una educación competitiva.

Por todo lo anterior, más que un requerimiento, es una obligación conocer el estado actual de sus procesos desde diferentes puntos de vista, tales como efectividad de controles, calidad de la infraestructura tecnológica, protección de datos personales, plan de continuidad de negocio, etc. Y proteger lo que hoy en día se considera lo más importante para una organización: su INFORMACIÓN.

Reconociendo las necesidades que tiene la Fundación Universidad Compensar de evaluar sus procesos y garantizar la seguridad de la información con miras a la Certificación, se propone determinar el estado de madurez, soportado en las mejores prácticas internacionales como es la NIST-CSEAT, siguiendo la metodología de listas de chequeo a través de entrevistas y reuniones con las personas encargadas de la ejecución de tareas por parte de la Universidad, esto permitirá identificar la evolución de los procesos de TI, la evaluación e identificación de riesgos, la implementación de controles, entre otros factores que se deben tener en cuenta al realizar la valoración del estado actual de la Seguridad de la Información y lograr ofrecerle a la Fundación Universitaria Compensar herramientas que cubran sus necesidades frente a la evaluación de la Seguridad de la Información.

## Antecedentes y Justificación

La Fundación Universitaria Compensar es una institución educativa de nivel superior, con gran reconocimiento. La Institución nació el 26 de octubre de 1978 al recibir de la división de carreras intermedias del M.E.N. el permiso de fundación. En su primera etapa, se llamó Instituto de Enseñanza Profesional – INESPRO, su carácter académico era Técnico Profesional y abrió sus puertas al público con tres programas de formación. En 1992 se logró el cambio de carácter a institución Tecnológica, de modo que recibió el nombre de Tecnológico INESPRO – Investigaciones Estudios y Proyectos. Durante esta etapa se perfilaron las facultades y programas académicos actuales y gracias a la gran experiencia en educación, se obtuvo un código especial del ICFES para ofrecer las Licenciaturas en Preescolar, Básica Primaria y Básica Secundaria en convenio con la Universidad de San Buenaventura y también se logró en 1998 la acreditación de la Licenciatura en Educación Preescolar, reconocimiento importante de por sí, pero particularmente valioso pues fue obtenido siendo una institución tecnológica. Finalmente, en septiembre 2002 y después de muchos esfuerzos, se logró la transformación a Institución Universitaria y así también, se modificó la razón social a Fundación Universitaria Panamericana o Fundación Universitaria Compensar. Desde entonces, el crecimiento de la Institución ha sido sostenido y en aumento.

El propósito de este estudio es establecer el nivel de madurez de la Fundación Universitaria Compensar y  nivel de cumplimiento, esto con el fin de proponer un alcance para la implementación de un SGSI(Sistema de Gestión de Seguridad de la información) según lo establece la NTC ISO/IEC 27001:2013. De manera que la universidad crezca en sus estándares de gestión de la seguridad de la información y de la privacidad.

## Formulación del Problema

¿Qué tan importante es la seguridad de la información para la Institución?

El análisis se debe dar desde tres grandes grupos, los equipos, los procesos y las personas, siendo las personas el grupo más importante y a su vez el más vulnerable ya que son los que ejecutan los procesos y administran los equipos, es de suma importancia generar un cambio cultural enfocado a la seguridad de la información, no solo la data de las instituciones está en juego, todos estamos expuestos a ser vulnerados por algún ciberdelincuente y ver comprometida nuestra información, en ese orden de ideas no deberíamos ver a las personas como el eslabón más débil en la cadena de la ciberseguridad sino como el más fuerte ya que son la primera línea de defensa, esto se podrá dar a medida que se den capacitaciones, charlas de sensibilización y haya un acompañamiento continuo, ya teniendo su atención podremos darles herramientas que ayuden a la gestión de la seguridad de la información. Esta propuesta va enfocada a bridar un apoyo para que se dé un cambio organizacional, se puedan tener procedimientos, lineamiento y herramientas tecnológicas que lleven a la institución a mantener la confidencialidad, integridad y disponibilidad de sus activos de la información y por ende mantener la continuidad del negocio en dado caso que se presente un evento de seguridad.

## Objetivo General

Encontrar brechas de seguridad o riesgos en los procesos y establecer estrategias para cerrarlas, un análisis de la situación actual nos llevara a saber dónde estamos y hacia dónde queremos estar con respecto a la seguridad de la información, si bien en el mercado encontraremos muchos lineamientos y herramientas, en esta propuesta tejeremos un ecosistema que se adapte a las necesidades de la UCompensar.,

## Objetivos Específicos

- Presentar una clasificación por niveles, donde se permita ubicar el estado en que se encuentra la Universidad.
- Revisar con que infraestructura tecnológica cuenta la institución.
- Analizar las capacidades y conocimientos del personal con respecto a la seguridad de la información
- Evidenciar las falencias que se obtuvieron posterior a la evaluación para facilitar sus acciones correctivas.
- Generar recomendaciones que lleven a la UCompensar a tener una infraestructura segura.

## Alcances y Limitaciones

La evaluación del nivel de madurez en Seguridad de la Información para la UCompensar, permite medir “done estoy hoy”, definir a donde quiero llegar y basados en ese GAP, planear y finalmente gestionar el crecimiento y evolución.

Para este estudio se utilizará como guía metodológica la norma NIST-CSEAT, aplicada a la Fundación Universitaria Compensar, mediante entrevistas y reuniones con los colaboradores líderes de los procesos.

**Entregables**

1. Resultado del estado actual de la empresa y su nivel de madurez
2. Plan de trabajo de acuerdo a los resultados obtenidos, clasificados en iniciativas, planes y proyectos.
3. Recomendaciones para temas propios del negocio y el proceso de seguridad.
4. Recomendaciones y ajustes a las políticas de protección de datos
5. Recomendaciones y ajustes a las políticas de seguridad.
6. Cronograma de trabajo para temas de Seguridad y Protección de datos personales.

## Equipo de trabajo

Ingeniera Adriana Mercedes Moya Aguirre

Ingeniera de sistemas, Especialista en telecomunicaciones, con amplios conocimientos de Ethical Hacking. Análisis de Vulnerabilidades.

Ingeniero Heriberto Miranda Vaca

Ingeniero Electrónico, Especialista de proyectos de infraestructura, con experiencia en temas de Seguridad de la Información Ethical Hacking y Análisis de vulnerabilidades.

## INVERSIÓN DE LA CONSULTORIA

**Tabla 1**

*Inversión consultoría en diagnóstico de seguridad de la Información*

| Actividad | Tiempo | Valor Pesos Col. |
|---|---|---|
| Consultoría en Seguridad y Privacidad. | 2.5 días semanales durante 3 meses = 240 horas | $ 22.560.000 +IVA |
| Formación capacitaciones. | 48 horas | $4.512.000 + IVA |
| SUBTOTAL | | $27.072.000 +IVA |

**Tabla 2**

*Inversión implementación de brechas de seguridad de la Información*

| Actividad | Tiempo | Valor Pesos Col. |
|---|---|---|
| Implementación de un SGSI. | 400 horas | $37.600.000 + IVA |
| Acompañamiento en la escogencia de una herramienta de SOC. | 30 horas | $2.820.000 + IVA |
| SUBTOTAL | | $27.072.000 +IVA |

El servicio consiste en la Consultoría en Seguridad y Privacidad de la Información, en la ciudad de Bogotá, Cundinamarca – Colombia, durante tres (3) meses, con el apoyo de medios tecnológicos parcialmente remota

- El costo ha sido estimado con base en la experiencia de los consultores a cargo del mismo.
- Todos los valores están expresados en pesos colombianos. Mensualmente se realizarán entregas que respaldarán las facturas. Las facturas se expedirán con un vencimiento de treinta (30) días calendario.
- Es necesario incluir en el proyecto un Documentador, un Líder de proyecto y un Líder de Tecnología con conocimiento en la plataforma tecnológica de la Fundación Universitaria Compensar.
- El agendamiento de la bolsa de horas depende exclusivamente de la Fundación Universitaria Compensar.

## Marco teórico

Hablar de Seguridad de la Información y ciberseguridad es sin duda hablar acerca de realizar una evaluación consciente sobre la protección de componentes de tecnología, hardware, software, datos, aplicaciones, etc. Sin embargo, aún se suele pasar por alto o de manera tangencial la base que hace posible la existencia de los anteriores elementos. Esta base es la información. Por lo tanto, es necesario que las organizaciones sin importar el tipo establezcan directrices y parámetros que permitan la gestión, monitoreo y evaluación de todos los aspectos relacionados con la información que procesan, almacenan o transmiten teniendo en cuenta el conocimiento de la misma y la identificación adecuada de cada uno de sus componentes, con el fin de identificar aspectos como:

- ¿La información está almacenada y procesada en sistemas de cómputo?
- ¿Puede ser confidencial para algunas personas o a escala institucional?
- ¿Puede ser mal utilizada o divulgada?
- ¿puede estar sujeta a robos, sabotaje o fraudes?
- ¿Son las personas un elemento clave en su gestión y protección?
- ¿Existen elementos que pongan en riesgo la confidencialidad, integridad, confiabilidad y disponibilidad?
- ¿Existen mecanismos alternos que garanticen la continuidad en las operaciones?

Los anteriores son entre otros, aspectos relacionados con la gestión de seguridad de la información y ciberseguridad que no dependen única y exclusivamente de un área específica, sino que aún mas, deberán estar alineados con los objetivos y razón de ser de la organización, de lo contrario la gestión de seguridad de la información pasara a ser un proceso más, que no generará ningún tipo de valor a la empresa y por consiguiente podría ser percibido como un obstáculo y no como un cimiento clave que genera valor y compromiso para la organización. Por esto, la gestión de Seguridad de la Información es un proceso constante y de crecimiento directamente proporcional a la organización, dentro del cual deberán interactuar de forma explícita todos los componentes del sistema incluyendo el más importante, "El Recurso Humano", con el fin de establecer un sistema de gestión robusto y que apoye los demás procesos de la organización y disminuya el riesgo frente a las amenazas que cada día van en aumento.

**Marco legal y regulatorio**

**Ley 1273 del 5 de enero de 2009,** por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicacionesMarco Teórico-conceptual que debe estar orientado sobre el tema central que se va a desarrollar, debe contener el sustento teórico que fundamenta los procesos, técnicas o metodologías a desarrollar o implementar.

**Conpes 3995 del 2020**, Política Nacional de Confianza y Seguridad Digital, tiene por objetivo establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

## Gestión del riesgo

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información. Previo a este ejercicio, es importante conocer la situación actual de la institución y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información. Para el proyecto se tienen los siguientes riesgos,

**Tabla 3**

*Mapa de identificación de riesgos de seguridad de la información*

compensar | fundación universitaria

| | Riesgo | Causa | Impacto | Área impactada | Prob. | Imp. |
|---|---|---|---|---|---|---|
| 2. | **Alcance de a solución insuficiente para cubrir las necesidades y expectativas de la Universidad** | Acotamiento del alcance insuficiente | Insatisfacción, retrasos y sobrecostos por controles de cambio | Toda la Institución | Bajo | Medio |
| 3. | **Inadecuada adopción de la solución por las personas que hacen parte de la Universidad** | Inadecuado, tardío o insuficiente proceso de gestión del cambio organizacional y/o diseño y divulgación de nuevos procesos operativos | Rechazo y resistencia al cambio en la implementación de la nueva solución | Toda la Institución | Medio | Medio |
| 4. | **No disponibilidad temporal o definitiva de algunos de los integrantes del proyecto** | Necesidad de continuar atendiendo el día a día o traslados/retiros de las personas | Retrasos en el proyecto o dificultades en la transferencia de conocimiento al interior del proyecto | Todo el proyecto | alto | Medio |

## Norma ISO/IEC 27001

Es un estándar para la seguridad de la información aprobado y publicado como un estándar internacional en octubre de 2005 por la International Organization for Standardization y por la International Electrotechnical Commission.

**Norma NIST-CSEAT**

Los Niveles de Implementación de NIST proporcionan un mecanismo para que las organizaciones puedan ver y comprender las características de su enfoque para gestionar el riesgo de seguridad cibernética, lo que ayudará a priorizar y alcanzar los objetivos de la seguridad cibernética. El marco considera 4 niveles desde el más débil hasta el más robusto: Parcial, Riesgo informado, Repetible y Adaptativo. El nivel es determinado con base en 3 atributos (Proceso de gestión de riesgos, integración de la gestión de riesgos, y Participación externa)

## Diseño Metodológico

Como parte de la metodología de diagnóstico implementada se encuentra un análisis DOFA que busca en primera medida identificar la situación actual de la Fundación Universitaria Compensar, facilitar la identificación de Fortalezas que le permitan a la Organización apalancar su desarrollo, la identificación de debilidades que permitan construir un plan de acción para mejorar sus procesos basándose en la identificación de Amenazas que puedan llegar a ser contrarrestadas, una vez identificadas las oportunidades.

Los siguientes documentos fueron entregados para revisar y establecer la forma y estructura de documentación:

- Mapa de Procesos de la Institución
- Políticas del proceso de tecnología
- Política de Seguridad de la Información
- Procedimiento TI
- Matriz de Riesgos TI
- Mapa de red de la institución

## Resultados

En el presente trabajo se describen los conceptos e importancia de la gestión del riesgo presentes en la seguridad de la información la cual se administra a través de los diversos equipos, servicios y colaboradores del área de TI; además se utilizó la metodología NIST para evaluar el nivel de madurez actual que facilitan y posibilitan conocer el estado actual y hacia donde se quiere llegar en la UCompensarEsta metodología, nos permitió ingresar las valoraciones para realizar evaluaciones en referencia a los activos, amenazas y controles para finalmente obtener los niveles de riesgo permitiendo identificar de manera más clara la necesidad de implementar procedimientos y normas cuya finalidad sea la protección de los activos y recursos de la información

La consultoría de diagnóstico se basó en la realización de entrevistas con los líderes de los procesos de la UCompensar:

5 Siempre 4 Casi siempre 3 Algunas veces 2 Casi nunca 1 Nunca

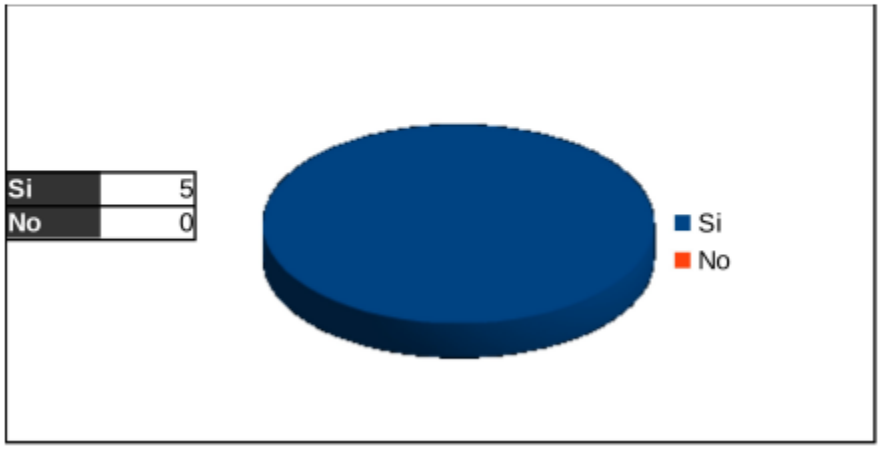
| | NIVEL DE INICIO | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | ¿Se realizan chequeos de Seguridad de la Información de Manera periódica? | | | | | |
| 2 | ¿Los incidentes asociados a la Seguridad de la Información conducen a impacto de consideración con que frecuencia? | | | | | |

| | NIVEL DE RECONOCIMIENTO | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | ¿Se revisa de manera cotidiana el tema de la Seguridad de la Información, en las diversas áreas? | | | | | |
| 2 | ¿Con que frecuencia el impacto de los incidentes de seguridad tienen consecuencias de máximo impacto? | | | | | |
| 3 | ¿Con que frecuencia se definen las responsabilidades en materia de seguridad de la información | | | | | |
| 4 | ¿Con que frecuencia se pierden los esfuerzos en materia de seguridad de la información, que son implementados en la plataforma institucional? | | | | | |

| | NIVEL DE DEFINICIÓN | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | ¿La plataforma tecnológica de la institución se actualiza de manera periódica? | | | | | |

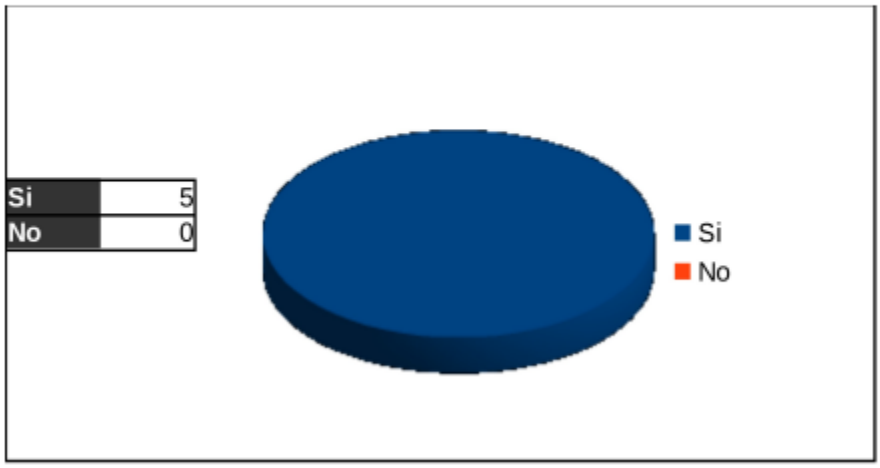
**Resultados del cuestionario exploratorio Nivel Inicio**

1) ¿Existe un departamento encargado de la Seguridad Informática en la Institución?

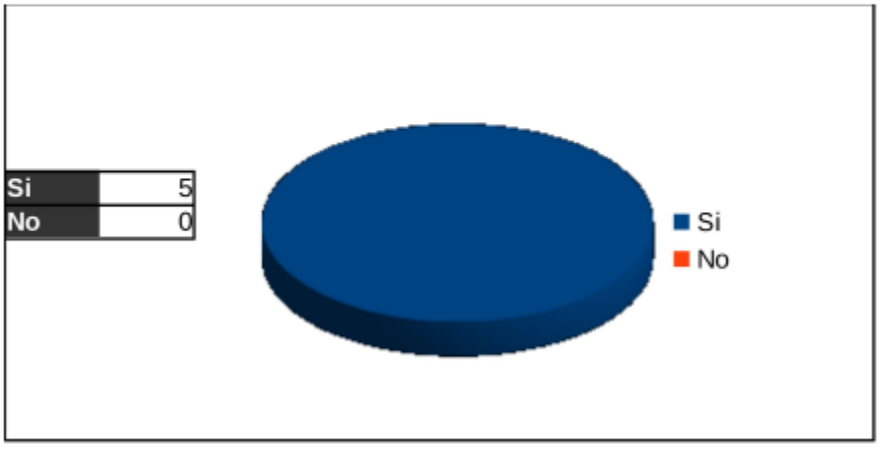


**Nivel de reconocimiento**

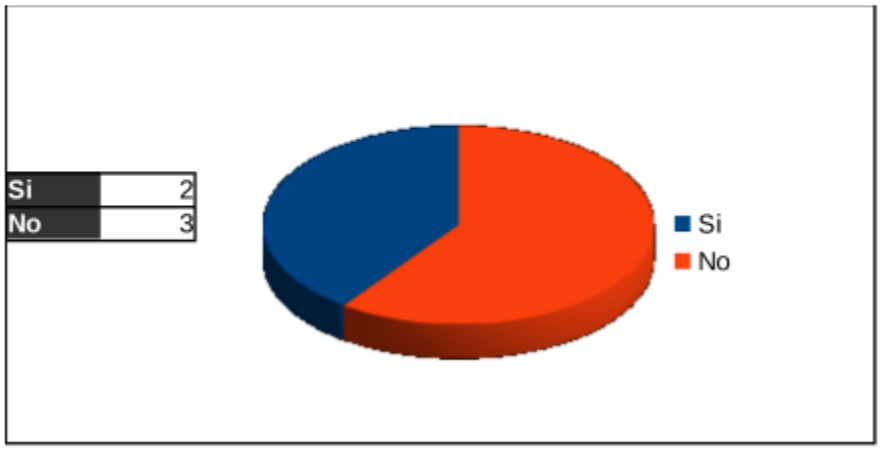
1)¿Existe una persona encargada de la Seguridad de la Información?



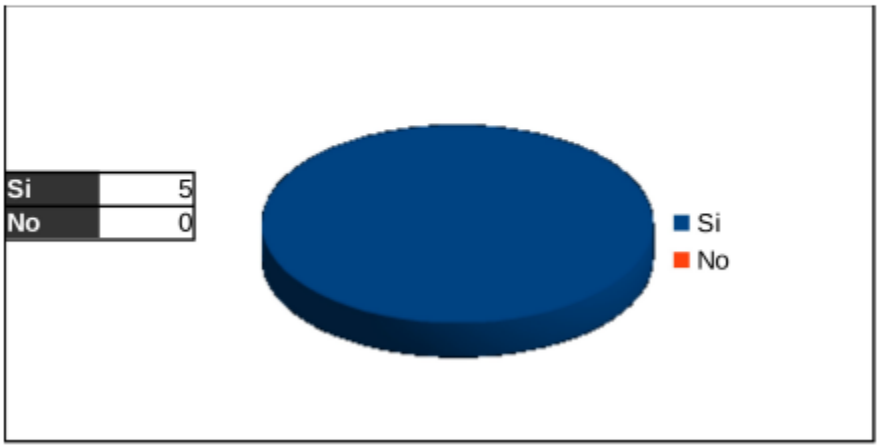

2)¿Las personas que conforman el departamento encargado de la Seguridad Informática son del área Informática?



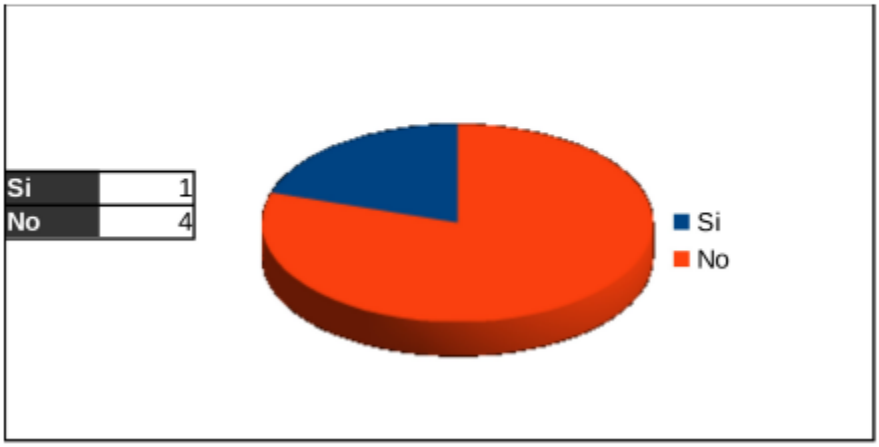
3)¿Las personas que laboran en el departamento tienen experiencia en el área?



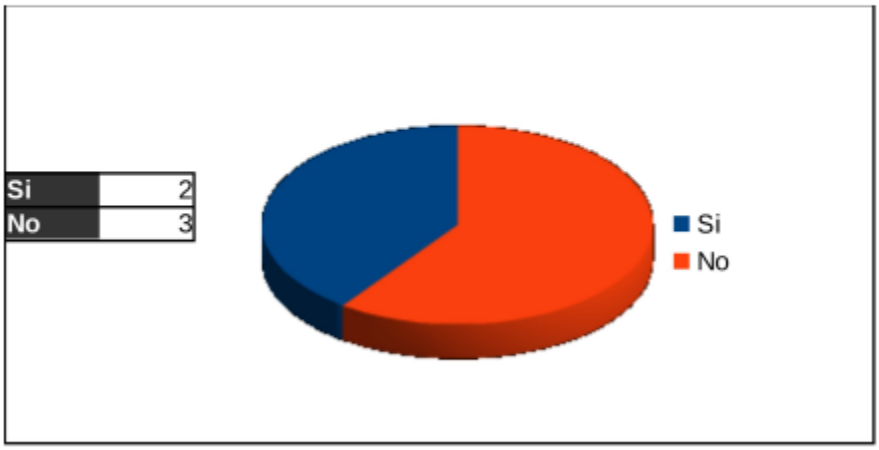

4)¿Hay herramientas de seguridad como antivirus en la plataforma institucional?



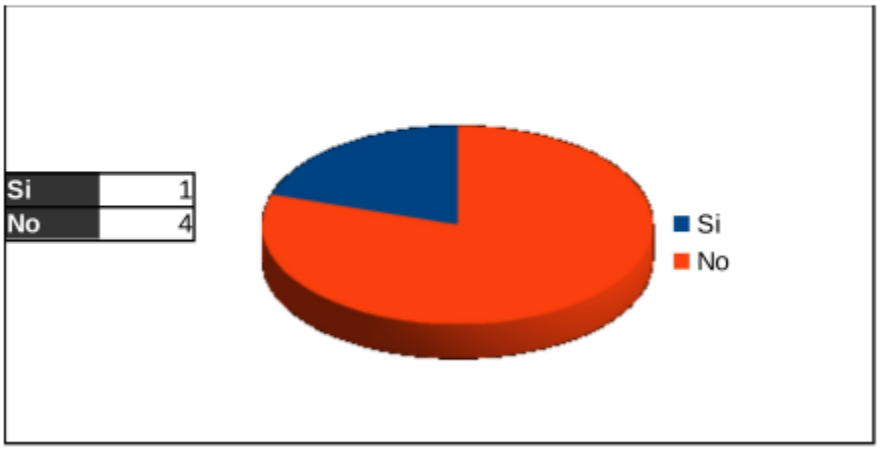
5)¿Hay herramientas de seguridad como detector de intrusos en la plataforma institucional?



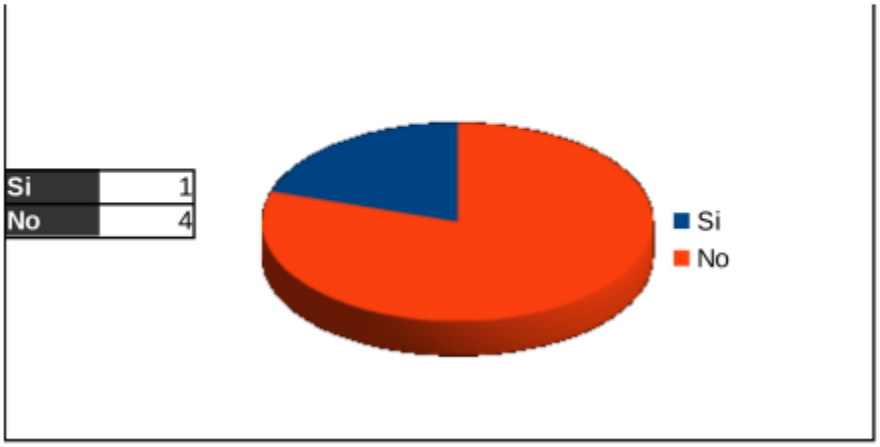

7)¿Tiene la plataforma institucional herramientas como firewall de sotfware?



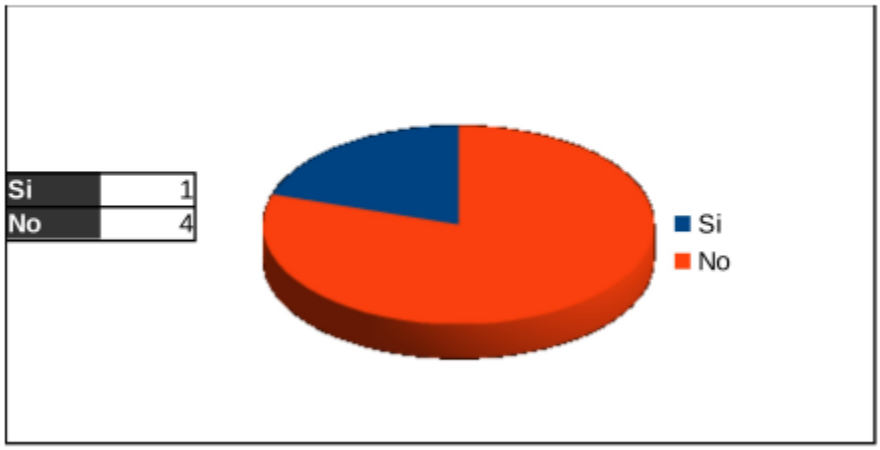
9)¿Tiene instalada en la plataforma institucional alguna herramienta de software antiespias?



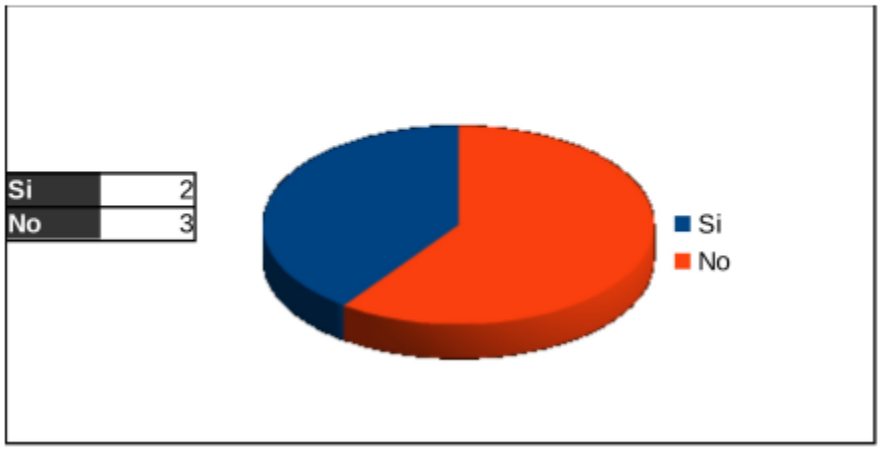

23)¿Hay estrategias tendientes a mejorar las falencias en materia de seguridad de la información que permitan trazar un camino a seguir en esta materia?



¿Se realiza auditoría interna sobre la Seguridad de la Información?




8)¿Se lleva un control de acceso físico para determinados sitios de la institución, de acuerdo a las funciones del empleado?



**Resultados del cuestionario para la elaboración del Modelo de Madurez**

Instrucciones: Lea las siguientes interrogantes y conteste de acuerdo a la frecuencia con la que ocurre el evento, tomando en consideración los siguientes valores:

5 Siempre 4 Casi siempre 3 Algunas veces 2 Casi nunca 1 Nunca

| | NIVEL DE INICIO | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | ¿Se realizan chequeos de Seguridad de la Información de Manera periódica? | | | 3 | 2 | |
| 2 | ¿Los incidentes asociados a la Seguridad de la Información conducen a impacto de consideración con que frecuencia? | | | 3 | 2 | |

| | NIVEL DE RECONOCIMIENTO | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | ¿Se revisa de manera cotidiana el tema de la Seguridad de la Información, en las diversas áreas? | | | 3 | 1 | 1 |
| 2 | ¿Con que frecuencia el impacto de los incidentes de seguridad tienen consecuencias de máximo impacto? | | | | 4 | 1 |
| 3 | ¿Con que frecuencia se definen las responsabilidades en materia de seguridad de la información | | | | 5 | |
| 4 | ¿Con que frecuencia se pierden los esfuerzos en materia de seguridad de la información, que son implementados en la plataforma institucional? | | | 2 | 3 | |

| | NIVEL DE GESTIÓN | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | ¿La institución tiene un registro detallado de los incidentes de seguridad? | | 1 | 3 | 1 | |
| 2 | ¿Tiene la institución registro automatizado de los eventos que puedan comprometer la seguridad informática de la plataforma? | | | | 4 | 1 |
| 3 | ¿Hay difusión masiva de los planes en materia de seguridad informática? | | | | | 5 |
| 4 | ¿El trabajo en materia de seguridad informática se maneja al mas alto nivel en la institución? | | | 1 | 3 | 1 |
| 5 | ¿Están definidos los valores éticos de la Seguridad de la Información? | | 2 | 3 | | |
| 6 | ¿Hay difusión masiva de los valores éticos de la Seguridad de la Información? | | | | 4 | 1 |
| 7 | ¿Se ofrecen al personal directivo charlas, cursos, seminarios, con la finalidad de crear cultura organizacional en materia de seguridad de la información? | | | | | 5 |
| 8 | Se ofrecen al personal no directivo charlas, | | | | | 5 |

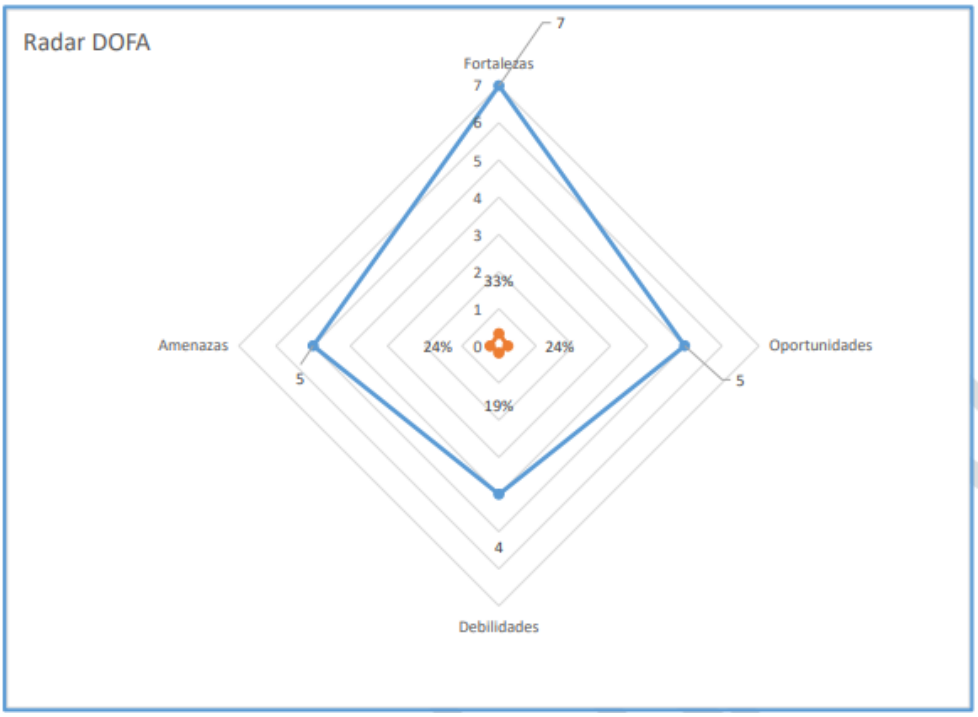
Luego de realizada la investigación se puede llegar a la conclusión de que aun cuando a nivel tecnológico hay soluciones implementadas para procurar minimizar las vulnerabilidades presentes en la plataforma, la gestión de la seguridad informática tiene debilidades.

*Matriz DOFA para la UCompensar*

| | ORIGEN INTERNO (Atributos de la empresa) | ORIGEN EXTERNO (Atributos del Entorno) |
|---|---|---|
| POSITIVOS (Para alcanzar el objetivo) | **F**<br>Respaldo del equipo de TI<br><br>Aseguramiento de infraestructura de nube<br><br>Herramientas de protección anti malware<br>Herramientas de seguirdad perimetral<br><br>Seguridad física<br>Existencia de comité de transformación digital que se reune cada semana<br>Existencia de un equipo jurídico que aporte en el desarrollo de lineamientos en privacidad y normativos | **O**<br>Desarrollo de planes de capacitación y sensibilización en seguridad<br>**Vincular a la comunidad académica en el desarrollo de medidas de aseguramiento para la universidad (Hackaton)**<br>incluir dentro de los retos de la semana de la innovación temas de ciberseguridad<br>Creación de un SGSI apuntando a certificación ISO 27001<br>Establecer mayores controles en la gestión de la infraestructura de aplicaciones |
| NEGATIVOS (Para alcanzar el objetivo) | **D**<br>No se aplican las buenas prácticas de documentación según ISO9000<br><br>Falta de documentación de Políticas de Seguridad<br>Falta de conocimiento en la gestión de seguridad<br>Falta de definición de roles organizacionales | **A**<br>Falta de cultura en la seguridad de la infomación<br><br>Capacidad de la comunidad académinca de generar incidentes de seguridad<br>Uso inseguro de credenciales de acceso<br>Uso de software irregular por parte de la comunidad académica<br>Falta de conocimiento de la normatividad aplicable en el sector educativo |

**Figura 1**

*Identificación DOFA – diagrama QRADAR*




*Nota*. El gráfico permite conocer más a fondo el estado actual de la UCompensar

## Discusión

Para obtener el máximo beneficio del modelo aquí propuesto, es necesario conocer e indagar, ante de comenzar a aplicar las evaluaciones, acerca de la organización, su estructura, entorno y sector al que pertenece, haciendo especial énfasis en el área de TI, ya que con esto se contextualiza y se puede definir qué aspectos del modelo aplicarían.

Debido a que la Universidad UCompensar se encuentra actualmente en una etapa en la que planea obtener la certificación ISO27001:2013, la participación de la consultoría permite identificar áreas de oportunidad de mejora que deberían ser analizadas y corregidas durante el proceso de pre-certificación.

El proceso de mejora en seguridad de la información en la UCompensar también crea una visión de conjunto de la credibilidad y la transparencia, lo que implica un enfoque sistemático para lograr los niveles de seguridad más altos para mantener los datos de los estudiantes y del cuerpo docente protegido.

# Conclusiones y recomendaciones

## Conclusiones

El modelo de madurez en seguridad de la información como conjunto estructurado de elementos que muestran la evolución de la seguridad de la información en los procesos de la Organización, no solo se clasifica desde los dominios de la 27001, NIST, COBIT, sino también desde los siguientes aspectos, Autoanálisis, Estrategia. DOFA. Capacidad, Oportunidades e Indicadores.

El nivel de madurez debe estar alineado a la evolución del negocio. Y debe tener en cuenta el ciclo constante de cambio de la seguridad de la información. El nivel de madurez determina el grado de evolución de una aérea, proceso o ciclo de una organización. El nivel de madurez también se soporta en las siguientes actividades

- Identificar: Desarrollar la comprensión organizativa necesaria para gestionar los riesgos de ciberseguridad sobre los sistemas, activos, datos y capacidades
- Proteger: Desarrollar e implantar las salvaguardas apropiadas para asegurar la entrega de los servicios críticos.
- Detectar: Desarrollar e implementar las actividades adecuadas para identificar la ocurrencia de eventos de ciberseguridad.
- Responder: Desarrollar e implantar las actividades apropiadas para adoptar acciones en relación a los eventos de ciberseguridad detectados.
- Recuperar: Desarrollar e implementar las actividades adecuadas para mantener planes orientados a la resiliencia y para recuperar las capacidades o servicios afectados por los eventos de ciberseguridad

A continuación, los tipos de niveles de madurez y donde está ubicada la UCompensar,

- Ninguno
- **Inicial- Estado actual de la Fundación Universitaria Compensar**.
- Gestionado
- Definido
- Optimizado

Se evidencia la necesidad de implementar un SGSI (Sistema de Seguridad de la Información) en la UCompensar, dicho sistema debe estar sincronizado con el sistema de Gestión de Calidad ya que es en tema transversal a la Institucional, por otra parte, se debe definir un gobierno que se encargue de hacerle seguimiento a los controles, funcionamiento de la infraestructura y Gestión del cambio.

Por otra parte, para apoyar la Ciberdefensa de la institución se debería contar con un servicio que monitoree, correlacione y le de manejo a los eventos de seguridad que se dan en la UCompensar, dicho servicio apoyara el trabajo y agrupará los incidentes que actualmente son mitigados por el actual Firewall y antivirus. Se recomienda un servicio de SOC (centro de operaciones de seguridad).

## Recomendaciones

- En primer lugar, se recomienda establecer un plan estratégico para la UCompensar, basado en acciones para las vigencias: 2023, 2024, 2025.
- Documentación de procesos de Fundación Universitaria Compensar, con narrativa, responsables basados en temas de gestión de calidad. La documentación debe tener narrativa del proceso, explicación, responsable, flujos de información y una descripción de actividades.
- Creación de un SGSI, protegiendo un proceso de baja complejidad en una primera fase, y extendiéndolo a los distintos procesos de la Institución.
- Identificar y documentar los riesgos de la seguridad de la información durante el 2022.
- Definición de las capacidades del equipo responsable de la gestión del sistema de calidad y de seguridad de la información.
- Sensibilización y capacitación a la alta dirección con el fin de crear el compromiso que se requiere para la implementación de un SGSI. Se recomienda generar una cultura de Seguridad de la información, en empleados, contratistas, proveedores, profesores y la comunidad estudiantil.
- Se propone utilizar las facultades de Ingeniería de Sistemas, con el fin de generar hackatones, o actividades para mejorar la seguridad de la información, invitar a docentes y alumnos a identificar riesgos de seguridad y generar espacios de investigación.
- Se recomienda realizar pruebas de Ethical Hacking de forma continua a los sistemas de la información, como mínimo cada 3 meses. Ya que son un indicador de la realidad actual.
- Capacitarse en gestión de riesgos y en identificar que riesgos puede tener cada producto o servicio.
- Se deben identificar los riesgos en seguridad asociados a las plataformas, infraestructura, aplicaciones, páginas web, entre otros.
- Determinar la metodología para preservar el conocimiento de la organización y prevenir fugas de información.

- Establecer controles en seguridad a las aplicaciones, a los desarrollos internos y a la infraestructura en la nube.
- Determinar el método para que los conocimientos puedan ser compartidos a todos los operativos, para evitar la dependencia en caso de ausencia de alguno.
- Establecer la independencia de funciones para la persona que se vaya a hacer cargo de la gestión de la Seguridad de la Información y de seguridad informática
- Crear un mecanismo para la detección de oportunidades de mejora que incluya el análisis del entorno y la gestión de riesgos no solo de la plataforma de la UCompensar, sino de todos los procesos empresariales.
- Establecer por temas de riesgos controles en seguridad de la información en la UCompensar, es el caso de uso de firmas digitales, firmas electrónicas, cifrado de la información, etc.
- Contar con información documentada del proceso de desarrollo y mantener un control documental estableciendo un procedimiento y elaborando una nemotecnia.
- Se debe contar con indicadores de gestión revisados semanalmente para la toma de decisiones.
- Adquirir una herramienta que correlacione los eventos de Ciberseguridad que se presentan en los diferentes servidores, firewalls y equipos de la institución, esto con el fin de hacer un análisis y tomar decisiones frente a los casos.

## Referencias

Imagine Easy Solutions. (09 de 2016). *Normas APA*. Obtenido de http://normasapa.net

/ https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Mendeley. (09 de 2016). *Mendeley*. Obtenido de https://www.mendeley.com/

Roy Rosenzweig Center for History and New Media. (09 de 2016). *Zotero*. Obtenido de https://www.zotero.org

Sáenz, J. (09 de 09 de 2016). *Wiki Sistemas Digitales*. Obtenido de http://sistdig.wikidot.com

Suárez, R. (2015). Energías renovables, Impacto y Efectividad. *Revista Científica Ingeniería y Desarrollo en Energía*, 48-53.

Thomson Reuters. (09 de 2016). *EndNote*. Obtenido de http://endnote.com/