UNIVERSIDAD NACIONAL DE TUCUMÁN

FACULTAD DE CIENCIAS ECONÓMICAS

MBA maestría en administración

TESIS

Para optar el Grado Académico Superior de:
Magister en Administración

"Conocimientos en Seguridad de la Información requeridos por Profesionales en Ciencias Económicas para la Gestión Estratégica de Negocios"

Marcelo Adrián García

- 2021 -

CARRERA DE POSGRADO
MAESTRÍA EN ADMINISTRACIÓN
Acreditada según Resolución N° 702/10 - CONEAU

DIRECTOR
Prof. Dr. Julio M. Soria

TRABAJO FINAL PARA LA OBTENCIÓN DEL GRADO ACADÉMICO SUPERIOR DE MAGISTER EN ADMINISTRACIÓN
TITULADO:

Conocimientos en Seguridad de la Información requeridos por Profesionales en Ciencias Económicas para la Gestión Estratégica de Negocios

TESISTA
Marcelo Adrián García
Contador Público Nacional

DIRECTORA
Prof. María Alejandra Masclef

COMISIÓN DE SUPERVISIÓN
Prof. María Alejandra Masclef
Prof. Teresa Carolina Ferreyra
Prof. Eduardo Juárez
(194-HCD-20)

Resumen

El propósito de este trabajo es analizar el estado actual, describir el proceso realizado y plantear una propuesta didáctica y de contenido respecto a “Seguridad y Control de Sistemas Informáticos” necesarios para la administración estratégica de negocios, considerando los requerimientos procedimentales y técnicos que demandan las organizaciones y las normativas vigentes. Lo planteado conlleva a la propuesta de una asignatura optativa para ser incorporada en las carreras de Contador Público y Licenciatura en Administración de la Facultad de Ciencias Económicas (FACE) de la Universidad Nacional de Tucumán (UNT).

Se analiza la formación actual de los alumnos de la FACE respecto a Tecnologías y Sistemas de Información en general, y en particular sobre Seguridad y Control de Sistemas Informáticos, considerando otras ofertas académicas brindadas por diferentes instituciones educativas de nivel superior y los requerimientos del mercado. Se destaca que esta investigación se enriquece a partir del intercambio con la Asociación de Docentes Universitarios en Sistemas y Tecnologías de la Información de Facultades de Ciencias Económicas de Universidades Nacionales (DUTI). Asimismo, presenta un desarrollo sobre los principales postulados del área disciplinar, dentro del ámbito de las ciencias de la Administración.

En este proyecto se elabora una propuesta formativa que efectuaría una importante contribución a la oferta académica brindada por la FACE de la U.N.T., en un área de vacancia disciplinar de trascendental importancia para el desempeño de profesionales en ciencias económicas en el contexto actual y futuro.

"Gracias a la vida, que me ha dado tanto

me ha dado el sonido del abecedario

con él las palabras que pienso y declaro…

Gracias a la vida, que me ha dado tanto

me dio el corazón, que agita su marco

cuando miro el fruto, del cerebro humano

cuando miro el bueno tan lejos del malo…"

(Violeta Parra)

Índice

Prólogo……...9

Prefacio……..…….……12

Capítulo N° 1: Marco Teórico ……...……...……14

1.1 Introducción a la Seguridad y al Control de la Información……...14

1.1.1 Notas preliminares……..……14

1.1.2 Las organizaciones en entornos informatizados…….……14

1.1.3 Definición y alcance de la Seguridad de la Información……17

1.1.4 Propiedades de la Información que deben asegurarse……18

1.1.5 Definiciones básicas……20

1.1.6 Aspectos estratégicos y tácticos……..23

1.1.7 Tipos de riesgos en Seguridad Informática…….24

1.1.8 El valor de los sistemas de información. Activo de información……...25

1.1.9 Cultura de Seguridad de la Información…….26

1.1.10 El proceso administrativo de la Seguridad Informática……..27

1.1.11 Sistema de Gestión de Seguridad de la Información……..28

1.1.12 Plan Director de Seguridad…….30

1.1.13 Implementación de un Programa de Seguridad……..32

1.1.14 Diseño de una estrategia de Seguridad de la Información……..33

1.1.15 Comité de Seguridad……...34

1.1.16 Riesgo…….……34

1.1.17 Vulnerabilidad……..…36

1.1.18 Amenaza…….36

1.1.19 Ataque…….38

1.2 Relación entre la Seguridad de la Información y la Ciencia de la Administración……38

1.3 La Propuesta de Cátedra.....…….…….……39

1.3.1 Justificación del abordaje de esta temática…….39

1.3.2 Estructura de los Proyectos de Cátedra……...……39

Capítulo N° 2: Estado de Seguridad de la Información: Informes especializados……..…46

2.1 Introducción……46

2.2 Tendencias - Academia ESET Latinoamérica …….……...…….…...46

2.3 Reporte de Seguridad "ESET Latinoamérica" ……....54

2.4 Las empresas y los nuevos desafíos de seguridad……58

2.5 Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción a las TIC..59

2.6 La Seguridad Informática, factor clave en la transformación de todos los sectores empresariales……..62

2.7 Cuarta Revolución Industrial en Latinoamérica: ¿cómo lo llevan los gobiernos?.....63

Capítulo N°3: Contenidos de Seguridad Informática impartidos por Instituciones Educativas de Nivel Superior…….....……..…64

3.1 Introducción…….....64

3.2 Situación Externa: Encuesta a Integrantes de DUTI……65

3.3 Situación: Facultad de Ciencias Económicas de la UNT…….……...77

3.4 Acreditación de la Carrera de Contador Público en todas las Universidades del país…….....85

3.5 Aprobación del Nuevo Plan de Estudios de la Carrera de CP en la UNT…….90

3.6 Próxima acreditación de la Carrera de Licenciatura en Administración…….94

3.7 Planes de estudios analizados para el desarrollo del programa de asignatura……94

Capítulo N° 4: Propuesta de Asignatura sobre "Seguridad y Control de Sistemas Informáticos" ……...……..96

4.1 Introducción……96

4.2 Marco Referencial……...96

4.3 Objetivos de la Asignatura…….101

4.4 Contenidos y Habilidades……..104

4.5 Bibliografía Propuesta……...107

4.6 Estrategias Didácticas ……..……109

4.7 Recursos Didácticos……...…111

4.8 Condiciones para aprobar y obtener la promocionalidad …….…….111

Capítulo N°5: Resultados y Conclusiones……...…….114

5.1 Resultados de la Tesis de Maestría……...…..…114

5.2 Reflexiones finales sobre el ámbito de la Seguridad Informática…….117

5.3 Conclusión Final ….……..118

5.4 Divulgación de Resultados……....119

Anexos……121

Anexo A: Encuesta a integrantes de DUTI – Año 2018…...……..……122

Anexo B: Entrevista semi estructurada FACE…….…….127

Anexo C: Presentación del Programa de Asignatura……....133

Anexo D: Aprobación del Programa Analítico “Seguridad y Control de Sistemas Informáticos”….. 134

Anexo E: Encuesta a integrantes de DUTI – Año 2019……....135

Anexo F: Encuesta a Expertos de la Seguridad de la Información – Año 2020 ……...140

Apéndice ……...……..…….…148

Abreviaturas…….….150

Bibliografía……151

Gráficos y Tablas

Gráficos

1. Amenazas, riesgos, vulnerabilidades y tolerancia de ellas……..…..…….28

2. Incidentes de Seguridad por países ……...…….56

Tablas

A. Materias optativas y obligatorias de TI por Institución educativa y carreras…….…..…67

B. Asignaturas exclusivas de Seguridad y Control de Sistemas Informáticos por Institución…68

C. Contenidos de seguridad informática impartidos en otras unidades académicas……...…68

D. Contenidos sobre TI impartidos en otras carreras de grado……69

E. Programas de posgrado en donde se imparten conceptos de seguridad informática……..69

F. Acciones realizadas para dar cumplimiento a la Resolución 3400/17 ……71

G. Modificaciones realizadas para incluir la temática ……72

H. Ponderación otorgada a la formación en SyTI para la carrera de CP ……. 72

I. Ponderación otorgada a la formación en SyTI para la carrera de LA …… 73

J. Ponderación otorgada a la formación en SyCTI en CP …….. 73

K. Ponderación otorgada a la formación en SyCTI en LA …….. 74

L. Profesionales capacitados en Argentina en Seguridad Informática ……..... 74

M. Formación del CP en aspectos de SyCSI para Auditoría ……... 75

N. Incumbencia profesional del CP con la formación en SyCSI ……. 75

O. Perfil diferencial del graduado en Ciencias Económicas …… 76

P. Accionar de la cátedra tras el requerimiento de la Resolución 3400/17…….89

Q. Contenidos conceptuales de la asignatura Seguridad y Control de SI……104

Prólogo

El colega Marcelo Adrián García, bajo la dirección de la Prof. María Alejandra Masclef, aborda en esta Tesis, un tema prioritario para la formación del Profesional en Ciencias Económicas.

Por su trascendencia, la Seguridad de la Información y el Control Informático, son contenidos esenciales en la currícula de Contadores Públicos y Licenciados en Administración.

Con el desarrollo, generalización y agresivo crecimiento, tanto en lo tecnológico, como en el campo de opciones de generación, vinculación y disponibilidad de datos e información, estamos frente a un universo que poco tiene que ver con el modo de instrumentar los procedimientos tradicionales y los mecanismos de asistencia a la toma de decisiones.

Generalización de Internet, como vínculo de alcance universal, el desarrollo de las comunicaciones, uso de tecnologías combinadas: mainframes, redes locales, movilidad (equipos portables y *Smartphone*); perfeccionamiento y divulgación del uso de sistemas integrados de procesamiento y almacenamiento de datos e información, las pujantes opciones para resguardarlos fuera de la organización (nube), las variantes de tercerización de medios y procesos, son algunos de los hitos que marcan una profunda transformación que trasciende el campo registral para potenciar y multiplicar las formas de explotación de datos e información.

Estos avances, sinceramente revolucionarios, no pensados apenas un par de décadas anteriores, deslumbran y precipitan cambios irreversibles.

En este marco de análisis global, se ha detectado una necesidad creciente, imprescindible, de privilegiar los controles y la seguridad de la información, como requisito necesario para proveer integridad, confiabilidad, confidencialidad y disponibilidad a los datos e información.

El ser humano no se caracteriza por aplicar visiones planificadas ni sistemáticas en la incorporación de cambios. Por ello, mientras las nuevas tecnologías irrumpen en las

organizaciones, se deteriora, subestima o ignora la importancia de instrumentar controles y políticas de seguridad de la información. La extrema preeminencia de la digitalización crea una muy alta dependencia para la organización. Cualquier falla, omisión, pérdida de datos e información, repercuten, multiplican las consecuencias negativas y pueden afectar seriamente al negocio.

Ante semejantes riesgos y pérdidas potenciales, la necesidad impulsa la búsqueda y aplicación de medidas que procuran mitigarlas.

El mercado soporta una verdadera avalancha de medios y mecanismos que procuran enfrentar los riesgos que generan los nuevos modos de trabajar (constante desafío) y los problemas de calidad de controles y seguridad.

Las currículas de las profesiones de Ciencias Económicas no han dado respuesta satisfactoria, en la mayoría de las universidades, a la necesidad de incorporar conocimientos específicos para la formación profesional que prepare a los futuros graduados para comprender estos fenómenos, evaluar el impacto potencial y administrar los controles y la seguridad asumiéndolos como aquello que son: “procesos”.

No se pretende formar un especialista en las técnicas. Se necesita que el profesional pueda intervenir activa y proactivamente en el abordaje de esta problemática con un sentido global, integrador, que permita visualizar el tema con criterios sistémicos, que convenza a las organizaciones que se está frente a procesos específicos: controles y seguridad, que, como tales, deben armonizarse y coordinarse con los demás procesos vigentes.

La visión global, integradora, no exige un especialista técnico, sino esa concepción general, identificación de requerimientos adecuados a la organización y capacidad de administrar en forma equilibrada estos procesos.

Por todo aquello que reflexionamos en los párrafos que anteceden, esta Tesis encara contenidos que deben ser incluidos en la currícula de formación profesional sin más demora.

La propuesta de una asignatura de carácter optativo satisface un primer paso y crea las condiciones para ser incorporada como obligatoria en una próxima reforma curricular.

La considero como un gran aporte para adecuar la formación profesional a necesidades que tienen ya hoy las organizaciones en este campo del conocimiento. Propicia una suerte de "atajo académico" que sin duda permitirá reducir en buena parte una brecha entre "el ser" y el "deber ser".

Felicito a Marcelo por encarar esta iniciativa innovadora sobre control y seguridad de la información en el campo académico, que, como bien destaca, ha sido reiteradamente discutido en las DUTI y provocado consenso sobre la urgencia de materializar acciones para incorporar, de algún modo, el tema en el ámbito educativo.

Cordialmente,

Dr. Ricardo O. Rivas

Presidente honorario de DUTI
Subdirector de la Especialización en Seguridad Informática de la UBA
Prof. Titular de Posgrado - Facultad de CEyN, FI y FCE
Universidad de Buenos Aires, Argentina

Prefacio

"Las organizaciones gastan millones de dólares en cortafuegos y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón mas débil de la cadena de seguridad: la gente que usa y administra las computadoras.

Kevin Mitnick[1]

Los sistemas de información de una organización constituyen uno sus activos más valiosos, pero a la vez presentan vulnerabilidades que deben ser tenidas en cuenta. Un ataque informático puede provocar su destrucción total o parcial y afectar su disponibilidad, causando retrasos y provocando un alto costo económico y de reputación para la compañía.

Debido a esta situación, la gestión de los riesgos informáticos es considerada una necesidad inevitable para cualquier ente que quiera administrar y utilizar su información de manera confiable, segura y funcional para el logro de su misión.

Pese a esta situación, el capital humano instruido en materia de seguridad informática en nuestro país es insuficiente y las carreras de grado relacionadas a las ciencias económicas y la administración de negocios, en general, no contemplan en sus planes de estudio un enfoque integral para solucionar las crecientes necesidades del área.

El propósito de esta tesis de maestría es analizar el estado actual, describir el proceso realizado y plantear las unidades de estudio y habilidades respecto a "Seguridad y Control de Sistemas Informáticos" necesarios para la administración estratégica de negocios y evidenciar el paradigma vigente en esta disciplina. A partir de ello y teniendo en cuenta los requerimientos procedimentales y técnicos existentes en las organizaciones, se plantearán los contenidos y habilidades para generar un programa de asignatura sobre "Seguridad y Control de Sistemas

[1] *Hackers, crackers* y *phreakers* estadounidense más famoso de la historia. Su apodo fue "Cóndor". Actualmente se dedica a la consultoría desde la óptica particular de la ingeniería social; considera que más allá de las técnicas de *hardware* y *software* que se pueden implementar en las redes, el factor determinante de la seguridad de las mismas es la capacidad de los usuarios de interpretar correctamente las políticas de seguridad y hacerlas cumplir.

Informáticos", el cual será propuesto como materia optativa para las carreras de Contador Público y Licenciatura en Administración de la FACE de la UNT.

El objetivo principal de esta propuesta innovadora, implica la formación de los alumnos de las carreras vinculadas a las Ciencias Económicas, centrándose en la importancia del conocimiento en la disciplina, a fin de proporcionar al futuro egresado competencias en lo referido a seguridad informática y control interno. Estas últimas habilidades son sumamente requeridas para actuar en el ambiente de los negocios altamente informatizados, permitiéndoles reconocer riesgos, vulnerabilidades y amenazas. Además, esta formación brindaría competencias que permitirían diseñar e implementar un Sistema de Gestión de Seguridad de la Información y herramientas conceptuales para tomar decisiones en el caso que el profesional participe en un comité de seguridad informática u ocupe cargos de alta dirección.

En conclusión, se proponen contenidos para formar profesionales con una visión integral y multidisciplinaria sobre la problemática de la seguridad de la información en las organizaciones actuales.

Para finalizar esta introducción, cabe destacar que los actuales y futuros administradores de negocios deberán poseer estas competencias, las cuales son necesarias para dirigir organizaciones bajo el ámbito de la seguridad informática, permitiendo su gestión en contextos ubicuos, tecnológicos e informatizados.

Marcelo Adrián García
Contador Público Nacional

Capítulo Nº 1: Marco Teórico

1.1 Introducción a la Seguridad y al Control de la Información

1.1.1 Notas preliminares.

El objetivo de este capítulo es definir y entender en toda su dimensión teórica, el concepto de gestión estratégica de la seguridad de la información, identificando su relevancia en el campo de la ciencia de la Administración.

Tras el relevamiento de bibliografía y el análisis de diversos informes relacionados a la temática, a continuación, se desarrolla un cuerpo teórico que versa sobre los principales postulados y problemáticas que plantea esta disciplina. Posteriormente se lo relaciona con la Ciencia de la Administración y se determina la importancia de incorporar dicha temática en las carreras de Ciencias Económicas, actualmente considerada un área de vacancia disciplinar.

Para concluir el capítulo, teniendo en cuenta el enfoque que se expone en esta Tesis de Maestría, se desarrolla un ensayo respecto al diseño de programas de estudios en la educación superior, con el objetivo de, dar cumplimiento al objetivo principal planteado de generar una propuesta de asignatura optativa para ser incorporada en las carreras de grado de nuestra facultad.

1.1.2 Las organizaciones en entornos informatizados.

Para comenzar, se plantea que las organizaciones cualquiera sea su tamaño y sector de desempeño, dependen cada vez más de las Tecnologías de la Información y la Comunicación (TIC), las cuales han sido clave para su innovación, productividad y crecimiento. No obstante los innumerables beneficios y oportunidades ofrecidas por ellas, surgen retos para los cuales las compañías deben estar preparadas. El tener una infraestructura de TIC insuficiente, no saber cómo abordar adecuadamente las complejas amenazas de seguridad informática o subestimar

la importancia de la protección de los datos personales, son ejemplos de los desafíos actuales para las Pymes[2].

Las organizaciones necesitan apoyarse en la tecnología para el desarrollo de su misión corporativa, dada las posibilidades que esta ofrece. Por lo que es fundamental que los profesionales en ciencias económicas cuenten con las competencias necesarias que le permitan comprender y desarrollar procedimientos para resguardar la información que generan.

La seguridad de la información es uno de los desafíos más importantes a los que se enfrentan las compañías en la actualidad. Cuando nos referimos a seguridad informática, no solo nos enfocamos en las empresas, sino a todo tipo de organizaciones, incluyendo a los gobiernos de los Estados del mundo.

En la actualidad los países están muy preocupados por esta problemática, situación agravada con la aparición del cibercrimen y las ciberguerras. Un claro ejemplo de esta situación, surge en el discurso del presidente argentino Mauricio Macri, del 23 de julio de 2018, en donde expresa: *"Como parte de las nuevas misiones será fundamental la participación de las Fuerzas Armadas en la protección de objetivos estratégicos. A esto se agrega el desafío del ciberespacio. Tenemos que garantizar la seguridad de los activos e infraestructura informática críticas del sistema de Defensa Nacional*[3]". Otro ejemplo que evidencia la importancia de la temática se evidenció en la cumbre del "G20" realizada en nuestro país en el año 2018, en donde uno de los temas de interés se refirió a los nuevos desafíos del trabajo ante la brecha digital y la ciberseguridad[4].

---

[2] OEA y AWS (2018). Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción a las TIC. *White paper series,* 3° edición. Publicado el 28 de agosto de 2018. Chile.

[3] El plan para reconvertir el aparato militar (23 de julio de 2018). Diario Clarín: Clarin.com. Buenos Aires, Argentina.

[4] Herrera J. (29 de noviembre de 2018). Mercados rezan porque surjan señales de paz comercial. Diario Ámbito Financiero: ámbito.com. Buenos Aires, Argentina.

Enfocándonos nuevamente a la aplicación de este trabajo, la seguridad no debe entenderse valiosa solo para lograr el normal desenvolvimiento de las actividades de un negocio, sino también para aumentar la confianza, elemento fundamental para el desarrollo económico de una comunidad de intereses. Una compañía que mantiene a salvo su información sensible cuenta con una buena reputación sobre los competidores, por este motivo es importante la seguridad de la información[5].

La infraestructura tecnológica se ha tornado fundamental en todas las organizaciones, cualquiera sea su objeto y envergadura, para lograr el correcto desempeño de sus procesos de negocio. Por esta razón, es necesario que todos los miembros de ella conozcan y entiendan los riesgos que implica la utilización de estas tecnologías.

Los peligros o amenazas más comunes en los entornos actuales, pueden estar inducidos por: descuidos o errores, desconocimiento de la problemática, ataques maliciosos internos o externos al ente, causas naturales o de origen industrial, entre otros. Además, estos pueden desencadenar en daños reputacionales y/o producir el detenimiento de la continuidad del negocio, originando pérdidas económicas significativas y comprometiendo los resultados presentes y futuros.

Los ataques son cada vez más complejos y sofisticados, ya que se aprovechan de las vulnerabilidades tecnológicas y no tecnológicas de las organizaciones, para que sea más dificultoso detectarlos.

Dada esta situación, cobra protagonismo la seguridad informática, que protege la información almacenada en los servidores de la compañía, en los dispositivos móviles de sus miembros, enviada y recibida desde internet u otras aplicaciones, proveniente de programas, páginas web, la nube y de cualquier otro origen en general.

---

[5] ¿Cómo asegurar la seguridad de la información en las organizaciones? (s.f). En SGSI: Blog especializado en sistemas de gestión de seguridad de la información

Como se puede deducir, esta disciplina abarca a los negocios en general, en mayor o menor grado según de su dependencia tecnológica, lo que permitirá analizar los riesgos a la que están expuestas las organizaciones.

1.1.3 Definición y alcance de la Seguridad de la Información.

El Instituto Nacional de Seguridad Informática del gobierno de España (2020), define a la Seguridad de la Información como: "*el conjunto de medidas aplicadas para la protección de los activos de la información*". Esta es una enunciación que resume sencillamente lo que implica este concepto; cuando hace referencia a los activos de información, se debe tener en cuenta que son los válidos y necesarios para el normal desenvolvimiento del negocio.

La seguridad de la información es un concepto más amplio que el de la seguridad de los recursos informáticos, pues tiene como objetivo proteger la información de los diversos riesgos que pueden afectarla, en sus diferentes formas y estados.

Otra definición al respecto, nos la ofrece Baca Urbina (2016) y en la cual establece que "*la seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la organización, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta*" (p. 12).

Según lo enuncia la norma ISO/IEC 27001:2015[6], la Seguridad de la Información involucra todo lo referido a la *"preservación de la confidencialidad, integridad y disponibilidad de la información; además pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad"*.

[6] IRAM (2015). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad en Tecnología de la Información.

Por otra parte, Laudon & Laudon (2016) define a la seguridad como: *"las políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso sin autorización, la alteración, el robo o el daño físico, a los sistemas de información*"(p 306).

El concepto de Seguridad Informática aporta elementos que se están volviendo indispensables en la gestión empresarial y obliga a permanecer alerta ante la presencia de un entorno inseguro si no se toman las precauciones necesarias. Según manifiesta Lardent (2001) "*las nuevas herramientas de comunicación crean nuevas soluciones, pero también generan nuevos problemas que son necesarios preverlos, detectarlos y solucionarlos*" (p 227).

Actualmente, las organizaciones deben asegurar su información, la cual en su mayoría no se encuentra físicamente, sino que está almacenada en formato digital, alojada en medios tecnológicos, pudiéndose encontrar dentro o fuera de las instalaciones de la compañía y en muchos casos, desconociéndose la ubicación exacta de la ella, pues se encuentran en la nube. A todo esto, se le suman las amenazas cibernéticas que evolucionan diariamente y a una mayor velocidad que las salvaguardas para mitigarlas.

Es por ello que el profesional en ciencias económicas necesita conocer cuáles son las buenas prácticas y las medidas de seguridad que deben adoptarse en una organización, para poder asegurar la integridad, confidencialidad y disponibilidad de la información, lo que es vital para la supervivencia de un negocio.

1.1.4 Propiedades de la Información que deben asegurarse.

La doctrina actual de la disciplina está de acuerdo en que la seguridad de la información se basa en articular y asegurar tres propiedades:

a) **Disponibilidad**: se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran[7]. Esta característica de la información es la única que se relaciona con el factor tiempo.

b) **Integridad**: es la propiedad por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software, hardware o por condiciones medioambientales[8]. Es decir que asegura que los datos no hayan sido manipulados o modificados sin la correspondiente autorización.

c) **Confidencialidad**: garantiza que la información estará accesible únicamente al personal autorizado a acceder a ella[9]. Esta característica no debe ser confundida con la "privacidad", relacionada con la protección de la asociación de la identidad de los usuarios y sus actividades[10].

Si la información de una organización carece de alguna de las características mencionadas anteriormente, se considera que no se ha mantenido con toda la seguridad requerida y como consecuencia deberá determinar la causa de esta situación.

No obstante, a estas características principales pueden considerarse otras, que también están vinculadas con la seguridad de la información:

a) **Apego a estándares:** Se refiere a que en el procesamiento de información se deberán respetar estándares, leyes y normas internas a los cuales está sujeto el proceso de negocios.

b) **Autenticidad:** propiedad de una entidad para demostrar ser quien dice ser.

c) **Efectividad:** lograr que la información sea la necesaria para desarrollar una tarea, teniendo en cuenta el modelo de negocios.

---

[7] Glosario de términos de ciberseguridad: una guía de aproximación para el empresario (s.f). INCIBE.

[8] Ibidem

[9] Ibidem

[10] Recomendación UIT-T X. 805, emitida por la *International Telecommunication Union*

d) **Eficiencia:** conseguir que la información sea generada y utilizada de manera óptima según los recursos disponibles con los que la organización cuenta para tal fin.

e) **Fiabilidad:** propiedad de mantener la consistencia ente un comportamiento previsto y sus resultados[11].

f) **No repudio:** capacidad para probar la ocurrencia de un evento o acción realizada por una entidad de origen.

g) **Responsabilidad:** rendición de cuentas por parte de una organización o persona por sus actos y decisiones.

Conforme lo descripto, podemos afirmar que el objetivo de la seguridad informática no consiste solamente en asegurar las características de la información señaladas, sino también el prevenir los posibles ataques internos, externos, físicos y lógicos sobre ella y contar con planes de recuperación en caso de haberse verificado daños.

1.1.5 Definiciones básicas.[12]

1.1.5.1 ***Seguridad.***

Según el diccionario de la Real Academia Española, seguridad se define como "libre o exento de todo peligro, daño o riesgo". No obstante, esta definición se refiere a una condición ideal, ya que en la realidad es materialmente imposible tener certeza absoluta de que se pueden evitar los peligros en su totalidad.

Es por ello que el propósito de la seguridad, en todas sus esferas de aplicación es reducir los riesgos hasta un nivel que sea aceptado por la dirección de la organización, quienes también están interesados en mitigar las amenazas.

En un sentido más general, por seguridad también se entiende a todas aquellas acciones realizadas con la finalidad de protegerse de algún tipo de peligro.

---

[11] Mendoza M. A. (2015). Conceptos básicos de Seguridad de la Información. Academia ESET Latinoamérica.

[12] Ibidem

1.1.5.2 ***Información.***

Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe lo recibe[13].

La información dentro de una organización es un activo y como tal debe ser protegido, ya que este es imprescindible para la toma de decisiones, el logro de los objetivos y el cumplimiento de la misión corporativa.

Los activos de información pueden encontrarse en distintos formatos: digital (medios electrónicos u ópticos), en forma física (escrita o impresa en papel) o de manera no representada (ideas o conocimiento de personas). Por lo expresado, podría definirse a los activos de información como todo conocimiento o dato que tiene valor para la organización[14].

En este aspecto adquieren importancia los activos en donde se aloja la información, llamados contenedores o activos de soporte. Estos son clasificados como técnicos (*hardware*, *software*, servidores, redes, etc.), físicos (armarios o archivadores) y humanos (personas que tienen acceso a ella).

1.1.5.3 ***Informática.***

Según Baca Urbina (2016) es la "*ciencia que estudia la transmisión (recepción y envío), el almacenamiento y el análisis de datos, que al ser procesados se convierten en información, realizando estos procesos con la ayuda de un dispositivo automático*" (p.11).

1.1.5.4 ***Evento de Seguridad.***

Se refiere a la ocurrencia identificada en un sistema, servicio o estado de la red, que indica una posible violación de las políticas de seguridad, la falla de los controles o una situación previamente desconocida que puede estar relacionada con la seguridad.

---

[13] Información (s.f.). En Wikipedia. Recuperado el 30 de enero de 2019.

[14] Mendoza M. Á. (2015). *Conceptos básicos de Seguridad de la Información.* Academia ESET Latinoamérica. Argentina.

1.1.5.5 ***Incidente de Seguridad.***

Evento o conjunto de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.

1.1.5.6 ***Objetivo de control.***

Manifestación que describe lo que se desea alcanzar como resultado de la implementación de controles.

1.1.5.7 ***Control.***

La palabra control proviene del término francés *contrôle* y significa comprobación, inspección, fiscalización o intervención[15]. Es una medida que modifica el riesgo. En este sentido, una de las referencias más utilizadas para la selección de controles de seguridad es el estándar de la norma ISO 27001[16], que en su anexo "A" describe una lista de 114 controles de seguridad agrupados en 35 objetivos de control, que a su vez están considerados en 14 dominios.

1.1.5.8 ***Mejor Práctica.***

Conjunto de acciones, metodologías, herramientas y técnicas que han sido aplicadas y probadas en un contexto determinado y que han producido resultados considerados como buenos, respecto a los objetivos establecidos. Por estas razones son recomendables y se espera que en situaciones similares puedan generar resultados aceptables.

1.1.5.9 ***Estándar.***

Es un documento que provee requisitos, especificaciones, guías o características que pueden ser utilizados de manera consistente, para asegurar que materiales, productos, procesos y

---

[15] Control (s.f.). En definion.es. Recuperado el 22 de febrero de 2019.

[16] IRAM, Instituto Argentino de Normalización (2015). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad en Tecnología de la Información.

servicios son adecuados para su propósito. Estos surgen a partir de las mejores prácticas y son utilizados como herramientas estratégicas para intentar reducir costos, minimizar errores o aumentar la productividad. Asimismo, las organizaciones pueden acceder a nuevos mercados y demostrar competencias adquiridas durante su proceso de madurez.

El estándar más conocido mundialmente referido a la gestión de la seguridad de la información es la norma ISO 27001[17].

1.1.6 Aspectos estratégicos y tácticos.

En esta recopilación bibliográfica se hará mención al término "seguridad informática" y "seguridad de la información" como si estos fueran sinónimos. Sin embargo, la doctrina hace la siguiente distinción:

La disciplina de la "Seguridad de la Información" se encarga de los activos de la información, vulnerabilidades, amenazas y riesgos. Asimismo, observa las buenas prácticas y los marcos normativos aplicables. Por lo tanto, ella se encuentra en un nivel estratégico y es propia de la dirección del negocio, reflejado en la estrategia que se va a seguir para proteger la información de la organización.

Por otro lado, la seguridad informática, es una parte específica de lo anteriormente explicado y se encarga de las medidas, controles y demás implementaciones técnicas para la protección de la información. Ejemplo de ello es la implementación de antivirus, detección de intrusos, gestión de usuarios y contraseñas, entre otros. Estas funciones son llevadas a cabo por el departamento de Tecnologías de la Información (sección seguridad) y se encuentra en un nivel táctico.

Ambas distinciones tienen un mismo objetivo, el cual implica asegurar la disponibilidad, integridad y confidencialidad de la información.

---

[17] Ibidem.

Así también cabe destacar que dada la importancia que han tomado las tecnologías a nivel mundial en la actualidad, se está popularizando el término “ciberseguridad”, que implica la intersección entre la seguridad de las aplicaciones, de las redes, de Internet y de las infraestructuras críticas, es decir, la seguridad en el ciberespacio[18].

1.1.7 Tipos de riesgos en Seguridad Informática.

Toda organización se enfrenta a dos tipos de riesgos: el “electrónico” (seguridad lógica), provenientes de internet y de todos los sistemas lógicos de funcionamiento de las computadoras y el “físico”, que a la vez es clasificado en interno o externo.

La seguridad física externa, se refiere a impedir la entrada de personal no autorizado a áreas restringidas, en donde se encuentra con mayor facilidad o acceso la información valiosa.

La seguridad física interna se encarga del personal que tiene la intención de robar, dañar o destruir información importante, ya sea por insatisfacción, venganza o para cederla o venderla a otra compañía o sujeto interesado. Por lo tanto será necesario tomar todas las medidas necesarias para que esto no suceda, pues si bien se podrá denunciar legalmente al empleado que produzca algún perjuicio, será difícil recuperar la información que se ha fugado, dañado o borrado.

Por otra parte, se encuentran los controles ambientales: el aire acondicionado, el drenaje, la supresión de incendios y otras medidas tomadas para garantizar que las instalaciones en las cuales se almacenan los sistemas, están diseñadas con las limitaciones físicas de la operación del sistema informático como requerimiento.

---

[18] IRAM, Instituto Argentino de Normalización (2012). Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad".

Actualmente, hay tantos tipos de seguridad informática como fuentes de amenaza existen para esa seguridad y dentro de los agentes externos e internos, el factor humano juega un papel muy importante como amenaza[19].

1.1.8 El valor de los sistemas de información. Activo de información.

Según la RT 16 de la FACPCE[20] *"Un ente tiene un activo cuando, debido a un hecho ya ocurrido, controla los beneficios económicos que produce un bien (un objeto material o inmaterial con valor de cambio o de uso para el ente). Se considera que algo tiene valor para un ente cuando representa fondos o equivalentes de fondos o tiene aptitud para generar (por sí o en combinación con otros bienes) un flujo positivo de fondos o equivalentes de fondos".*

Si definimos el término activo, como todo aquello que tiene valor para una organización por su capacidad para generar futuros flujos de fondos, podríamos decir que el concepto de "activo de información" hace referencia a la información necesaria para el giro normal del negocio y toda aquella infraestructura que la contiene. En otras palabras, es cualquier información o sistema relacionado con su tratamiento que tenga valor para la organización: pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Dado el valor que se le atribuye, la información es susceptible de ser atacada deliberada o accidentalmente con consecuencias para la organización[21].

La valuación de estos activos de información depende de las particularidades del negocio y de sus necesidades concretas. Esta valoración determinará los controles y las pruebas sustantivas necesarias para garantizar su seguridad.

---

[19] Baca Urbina G. (2016). Introducción a la Seguridad Informática. 1ra edición *ebook*. México. Grupo Editorial Patria. Pág. 18

[20] Federación Argentina de Consejos Profesionales en Ciencias Económicas, CECYT (2008). Resolución Técnica N° 16: Marco Conceptual de las Normas Contables Profesionales. Argentina

[21] Glosario de términos de Ciberseguridad: una guía de aproximación para el empresario (s.f). INCIBE

Es por esto que resulta importante clasificarla e identificar aquella que es más relevante para llevar a cabo la misión organizacional. De esta manera los responsables de la gestión del ente, tendrán presente cuales son los activos que deben proteger.

Como se mencionó anteriormente, cuando nos referimos a información no solo señalamos a aquella que se encuentra en formato papel o electrónico, sino también a otras formas como ser fotografías, cintas de audio, etc. Es decir que la protección de la información es independiente al soporte de su formato. Dicha defensa se realizará a través de controles físicos y lógicos, los cuales fueron explicados anteriormente.

A modo de ejemplo se transcribe el copete de una nota sobre la temática, escrita en la revista *Info Technology*: *"En el último tiempo la industria sanitaria se ha convertido en una de las más vulnerables frente a los ataques cibernéticos ¿Qué tiene el sector que la convierte en el objetivo preferido de los atacantes? La respuesta es contundente: el valor de la información que manejan es alto y su precio, pagado en el mercado negro*[22]".

1.1.9 Cultura de Seguridad de la Información.

Comprender el comportamiento de las personas frente a los temas de seguridad es un tema de percepción y de valoración personal, de acuerdo con múltiples variables que cada uno de ellos conoce.

La psicología de la seguridad de la información pasa por un reconocimiento del riesgo y una percepción del mismo, que mantiene o no alerta a la persona frente a situaciones que pueden vulnerar su espacio individual o comunitario, cuando de manejo de información u otra situación se trate.

Por lo tanto, comprender los riesgos, actuar conforme a ese entendimiento y hacer visible una acción en los procesos de negocios, debe ser un quehacer diario en la dirección de una

[22] Bravo R. (2018). Doble Virus. *Update trending*. Revista *Info Tecnology*. Año 22, N° 252, septiembre 2018, pág. 20.

organización. Si no se valora la información como lo que ella es: un activo de la organización y no se reconocen en los procesos de negocios la importancia de ella, se está advirtiendo una dinámica organizacional dispersa y animada por una informalidad en la administración de los riesgos de la información.

Cuando las expectativas del nivel directivo establecen que la información es un bien crítico y sensible para la permanencia de la organización, cada uno de los colaboradores activa un programa de prevención y control de los riesgos de seguridad. Si en cambio este no muestra interés legítimo con sus actuaciones respecto de la protección de los recursos de información, la organización sabrá que la pérdida de información, la inconsistencia de archivos y su eliminación son eventos que debe asumir solo el área de tecnología y no cada uno por su lado.

Una cultura de seguridad de la información fuerte y consistente no implica una compañía sin incidentes de seguridad ni fraudes, sino de una que destruye sus propias auto restricciones para conocer y atender nuevas formas de equivocarse, aprendiendo de ellas[23].

1.1.10 El proceso administrativo de la Seguridad Informática.

El primer paso del proceso administrativo para una implementación exitosa de un sistema de seguridad de la información, es elaborar un proyecto. Este comienza a partir de una necesidad, en este caso la de proteger la información, teniendo en cuenta que la organización ya ha realizado una planeación estratégica y ha declarado su misión, visión y objetivos.

Dentro de los objetivos, se debe considerar el logro de un alto estándar de calidad en la seguridad informática, pues la compañía debe ser consciente de la importancia que tiene la información histórica y la que se genera diariamente. A partir de esto se deberá asegurar que el proyecto de seguridad de la información está alineado con el planeamiento estratégico organizacional.

---

[23] Cano M. J. J. (2013). Inseguridad de la información: Una visión estratégica. Bogotá. Alfaomega. Pág. 21 a 23

La segunda etapa es la dirección: en ella se debe determinar el tipo de amenazas, los riesgos y las vulnerabilidades del sistema de información. Será necesario determinar umbrales de tolerancia, clasificar la infraestructura tecnológica y la información existente.

La siguiente etapa es la organización. Esto se logra mediante la confección de una política de seguridad y la definición de manuales de procedimientos de cumplimiento obligatorio por parte del personal de la compañía.

La última etapa se refiere al control. Generalmente se utilizan métricas y se elaboran reportes periódicos del comportamiento del área, calificando el desempeño de cada parámetro de control, señalando éxitos, fracasos y responsables.

Gráfico N°1: Tabla de amenazas, riesgos, vulnerabilidades y tolerancia de ellas.

ACTIVO	PRIORIDAD	AMENAZA		TIPO DE RIESGO	VULNERABILIDAD		TOLERANCIA	
		FÍSICA	LÓGICA		HUMANA	LÓGICA	MÁXIMA	MÍNIMA
Servidores								
Terminales								
Otros								

Fuente: Baca Urbina G. (2016*).* Introducción a la Seguridad Informática. Primera Edición digital. México. Grupo Editorial Patria. Pág. 46.

1.1.11 Sistema de Gestión de Seguridad de la Información (SGSI).

1.1.11.1 ***Definición****.*

Un SGSI está compuesto por un conjunto de políticas, procedimientos, directrices, recursos y actividades asociadas, colectivamente gestionadas por una organización, con el propósito de proteger sus activos de información. El mismo parte de una evaluación de riesgos relacionados con la información y los niveles de aceptación de dichos riesgos. Incluye un análisis de los requisitos y la aplicación de controles adecuados para proteger los activos de información, a través de un ciclo de mejora continua[24].

[24] Mendoza M. Á. (2015). Conceptos básicos de Seguridad de la Información. Academia ESET Latinoamérica. Argentina.

1.1.11.2 ***Objetivos de seguridad.***

Es difícil que un administrador se enfrente a una situación en la cual no exista ninguna actividad relacionada a la seguridad de la información. Es por ello que se debe realizar un "análisis de brechas", entre las medidas implementadas y aquello que se considera necesario para alcanzar un nivel de seguridad acorde al riesgo definido como tolerable por la dirección.

El punto de partida será determinar las necesidades de seguridad, lo cual ayudará a clarificar los objetivos del programa a desarrollarse y proporcionará la base para el diseño de las métricas correspondientes. Para ello se deberán identificar los controles necesarios, implementarlos y desarrollar los indicadores correspondientes, lo que servirá de base de apoyo para monitorear el cumplimiento de los objetivos propuestos.

Esta definición de objetivos también se la conoce como definición de la estrategia de seguridad de la información, la cuál debe ser congruente a la estrategia corporativa y considerar las cuestiones relativas a la administración de riesgos planteadas por la dirección ejecutiva.

1.1.11.3 ***El estado deseado.***

La meta de un plan de seguridad consiste en contar con indicadores que tengan sus objetivos correspondientes y estén asociados a una actividad de control que se ejecuta y se puede medir. No es solo importante identificar y medir el alcance de los objetivos, sino el desempeño del programa de seguridad, en relación con las tecnologías aplicadas y los procesos llevados a cabo en la organización.

1.1.11.4 ***Buenas prácticas para los controles de la Seguridad de la Información[25].***

Las organizaciones de todo tipo y tamaño, recopilan, procesan, almacenan y transmiten información en muchas formas, incluyendo electrónica, física y verbal.

---

[25] IRAM, Instituto Argentino de Normalización (2019). Norma ISO/IEC 27002: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de la seguridad de la información. Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad

En un mundo interconectado, la información y los procesos, son valiosos para el negocio de la organización y por lo tanto merecen o precisan protección contra distintos peligros.

Los activos son sujeto tanto de amenazas intencionales como accidentales, mientras que los procesos, sistemas, redes y personas tienen vulnerabilidades inherentes. Por lo tanto, dada la variedad de formas en las cuales las amenazas pueden aprovechar las vulnerabilidades para perjudicar a la organización, siempre están presentes los riesgos respecto de la seguridad de la información. Una seguridad de la información eficaz reduce estos riesgos y, en consecuencia, disminuye los impactos sobre sus activos.

Esta se alcanza implementando un conjunto adecuado de controles, que incluyen políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Es necesario que estos controles se establezcan, implementen, monitoreen, revisen y mejoren, si corresponde, para garantizar que se cumplan los objetivos de negocio y los específicos a la seguridad de la organización.

La seguridad que se puede lograr por medios técnicos es limitada y se recomienda que esté respaldada por una gestión y procedimientos apropiados.

1.1.12 Plan Director de Seguridad (PDS).

Un Plan Director de Seguridad consiste en determinar y priorizar un conjunto de proyectos en materia de seguridad de la información, con el objetivo de reducir hasta un nivel aceptable los riesgos a los que está expuesta la organización, partiendo de un análisis de la situación inicial. Es fundamental que este plan esté alineado a los objetivos estratégicos de la empresa, incluya una definición de su alcance y especifique las obligaciones y buenas prácticas de seguridad que tienen que cumplir los empleados y los terceros que interactúan con la organización. [26]

[26] Plan Director de Seguridad. Colección: Protege tu empresa (s.f.). INCIBE

Basándose en la mejora continua, el PDS, se compone de los siguientes pasos:

a) Conocer la situación actual de la organización: en esta fase es muy importante el apoyo de la dirección, para garantizar la disposición de recursos y la alineación con la filosofía y estrategia corporativa. En esta etapa se debe definir el alcance del plan, las responsabilidades sobre los activos, el responsable de seguridad, de la información y del ámbito.

b) Realizar una valoración preliminar de la situación actual respecto a la seguridad de la información, tomando como base algún marco de referencia y estableciendo los controles correspondientes.

c) Elaborar un documento con las medidas de seguridad que se aplican y su grado de madurez, es decir, si están implantados y su estado de cumplimiento.

d) Establecer los objetivos a cumplir respecto a la seguridad de la información, lo que evidenciará ámbitos a mejorar e identificará los aspectos en donde se deberán enfocar los esfuerzos.

e) Debido a que se trata de un trabajo especializado, es habitual que la organización opte por externalizar el análisis técnico de la seguridad. En estos casos se debe prestar especial atención a la coordinación del equipo externo con el personal propio de la organización, para establecer el tipo de pruebas a realizar y el método de trabajo que se utilizará. Sin embargo, se recomienda llevar a cabo auditorías técnicas externas e internas, para tener el enfoque de atacante interno, como ser un empleado mal intencionado y un atacante externo, como ser un hacker.

f) Conocer la estrategia de la organización: esta etapa permite implementar medidas de seguridad acordes a la naturaleza de la organización. Asimismo permite alinear la estrategia de seguridad, con la de TI y con la corporativa.

g) Definir proyectos e iniciativas: **a** partir de la información recopilada en las etapas anteriores, se deben definir las acciones, iniciativas y proyectos necesarios para alcanzar el

nivel de seguridad requerida. Estos deben consistir en mejorar los métodos de trabajos actuales, controles técnicos y físicos, gestión del riesgo, etc. Si es posible, se debe estimar el costo temporal y económico para llevarlos a cabo, contemplando los recursos materiales y humanos necesarios para ello.

h) Clasificar y priorizar los proyectos a realizar: se recomienda organizar los proyectos teniendo en cuenta el esfuerzo que requieren y su costo temporal, para establecer planes de corto, medio y largo plazo.

i) Aprobar el Plan Director de Seguridad: cuando se tenga la versión final aprobada del PDS por la dirección, es recomendable que se interiorice a todos los integrantes de la organización y se haga hincapié en la importancia del compromiso de todos los miembros para la implementación del mismo.

j) Puesta en marcha: cada compañía puede utilizar la metodología de gestión de proyectos que considere más oportuno para llevarlo a cabo.

1.1.13 Implementación de un Programa de Seguridad.

1.1.13.1 ***Aspectos a considerar.***

Para implementar un programa de seguridad se debe considerar los siguientes elementos:

a) Contar con los recursos necesarios que se requieren para formar los componentes básicos del mismo

b) Se hayan definido los controles de TI y los operativos

c) Que las revisiones de seguridad y las auditorías se encuentran disponibles para indicar si existen deficiencias y brechas en el programa.

d) Que el órgano de dirección de la organización respalda las actividades del programa de seguridad

Una clave para el cumplimiento de la política es la existencia de una persona encargada para cada uno de los sistemas de información utilizados. En la mayoría de los ambientes

tecnológicos, las plataformas cambian continuamente y la responsabilidad por su seguridad también lo deberá hacer con frecuencia.

Asimismo, en el contexto del programa de seguridad de la información, se requiere de la capacidad de la alta dirección para determinar si el programa está funcionando. El gerente de seguridad de la información debe identificar métricas, su recopilación y difusión. Los informes permiten a la gerencia determinar si se están cumpliendo determinados objetivos de control.

1.1.13.2 ***Infraestructura de la Información.***

Se refiere a la base o fundamento subyacente sobre la cual se utilizan los sistemas de información. Cuando la infraestructura se diseña e implementa de manera consistente con las políticas y las normas, se dice que es esta segura.

1.1.13.3 ***Integración del programa de Seguridad con los procesos organizacionales.***

La alta dirección, respaldando el programa de seguridad de la información, debe asignar responsabilidades del trabajo de seguridad a personal ajeno al departamento de TI, lo cual permitirá achicar brechas de seguridad, las cuales serían materialmente imposible controlar, si estarían a cargo de un solo individuo.

1.1.14 Diseño de una estrategia de Seguridad de la Información.

Como se ha hecho referencia anteriormente, el plan estratégico del área de Informática, debe estar alineado con el plan estratégico corporativo. Este consta de tres sub planes:

- Plan de Prevención: Tiene como objetivo identificar y medir el tipo de riesgo al que está expuesta la organización, en especial en el área de informática. En este, se identifican los equipos informáticos que están más expuestos con la finalidad de determinar el personal, el equipamiento y el software necesario para protegerlos de cualquier amenaza física y lógica. Finalmente se deberá seleccionar la mejor alternativa de costo-protección de acuerdo con el valor que la empresa otorga a su información.

- Plan de Predicción: muestra los riesgos a los que está expuesta el ente, con su correspondiente probabilidad de ocurrencia (depreciable, baja, media y alta). Para realizarlo es necesario contar con datos históricos, de la propia organización y si es posible, de otras externas.
- Plan de Continuidad de Negocio: conjunto formado por planes de actuación, de emergencia, financieros, de comunicación y de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía[27]. Es decir que es un conjunto de acciones que posibilitan la recuperación, tras un incidente grave, en un plazo de tiempo determinado.

1.1.15 Comité de Seguridad.

La seguridad de la información es una responsabilidad de la empresa compartida por todos los miembros del equipo gerencial. Por consiguiente, debe tenerse en cuenta la creación de un foro gerencial para garantizar que existe una clara dirección y un apoyo manifiesto de la gerencia a las iniciativas de seguridad. Debe promover la seguridad dentro de la organización mediante un adecuado compromiso y una apropiada reasignación de recursos.

Este foro podría ser parte de un cuerpo gerencial existente o en una gran organización, podría ser necesaria la creación de un foro ínter funcional que comprenda representantes gerenciales de sectores relevantes de la organización para coordinar la implementación de controles de seguridad de la información[28].

1.1.16 Riesgo.

Según el diccionario de la Real Academia Española, "riesgo" es una contingencia o proximidad de un daño[29]. Además, nos informa que dicha palabra proviene del árabe "*rizq*",

---

[27] Glosario de términos de ciberseguridad: una guía de aproximación para el empresario (s.f.). INCIBE.

[28] Masclef, M. A. (2016). Infraestructura de Seguridad de la Información. Cátedra de Sistemas de Información I. Facultad de Ciencias Económicas UNT, Tucumán, Argentina.

[29] Riesgo (s.f.). En Real Academia Española. Diccionario de la lengua española.

que significa “lo que depara la providencia”. Según Corominas (1961), este término tiene la misma etimología que risco (peñasco alto y escarpado de difícil tránsito), por el peligro que se sufre al andar por él[30].

Para el ámbito de la seguridad de la información, podríamos decir que son todos aquellos eventos que pueden poner en peligro la información, comprometiendo de este modo las actividades habituales del negocio. También podría ser definido como la posibilidad que no se obtengan los resultados deseados. Por ello es importante poder cuantificar el impacto que puede generar en la compañía, para determinar cuáles de ellos son más importantes.

El riesgo es la combinación entre la probabilidad que se produzca un evento (desastres naturales, fortuitos o intencionados) y sus consecuencias negativas.

La norma ISO 27005[31] define este concepto como la posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Debido a que cada organización tiene activos de información, características y necesidades específicas, la evaluación del riesgo en un proceso particular para cada una de ellas. La probabilidad puede calcularse mediante determinaciones empíricas basadas en sucesos del pasado o medios subjetivos, como por ejemplo la opinión de peritos o expertos en la materia.

Dada esta situación, es sumamente importante la aplicación de contramedidas para mitigar la existencia de los riesgos en las organizaciones. En la esfera de la seguridad informática, los estándares internacionales definen “contramedidas” como las políticas, procedimientos,

[30] Coraminas, J. (1961). Breve diccionario epistemológico de la lengua castellana. 3° ed. Madrid, España. Editorial Gredos.

[31]IRAM, Instituto Argentino de Normalización (2012). Norma ISO/IEC 27005: Tecnología de la información. Gestión del riesgo de seguridad de la información. Subcomité de Seguridad en Tecnología de la Información.

prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo tolerable por la dirección[32].

Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización. Otros a los que se enfrenta pueden ser: riesgos estratégicos, ambientales, de mercado, de crédito, operativos y de cumplimiento.

1.1.17 Vulnerabilidad.

La palabra vulnerable tiene su origen latín y proviene del vocablo "*vulnus*" que significa herida y el sufijo "*abilis*" que expresa posibilidad.

Llevado este término al ámbito de la seguridad de la información, podríamos afirmar que vulnerabilidad es una debilidad que puede poner en peligro la información del negocio y el buen funcionamiento de su actividad. Constituye un hecho o una actividad que permite concretar una amenaza. Ella se hace presente en los activos de la información, dada la escasez o la falta de medidas que los resguarden. Esto posibilita a un atacante transgredir la confidencialidad, integridad y disponibilidad de la información.

El ente siempre está amenazado de sufrir algún daño en su sistema de información, estas amenazas son mayores cuando los sistemas informáticos presentan puntos débiles o "vulnerabilidades". De este modo se tiene mayor o menor riesgo dependiendo de la cantidad y número de vulnerabilidades presentes. De esta manera al disminuir las vulnerabilidades, también disminuirá el riesgo de sufrir daños, no sólo en el aspecto informático, sino en toda la organización.

1.1.18 Amenaza.

La amenaza es todo elemento que aprovecha una vulnerabilidad para atentar contra la seguridad de un activo de información. Si la amenaza impacta sobre la vulnerabilidad se

---

[32] IRAM, Instituto Argentino de Normalización (2007). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad en Tecnología de la Información.

produce un incidente de seguridad, comprometiéndose la seguridad de la información. Se trata de una condición del entorno de los sistemas, áreas o dispositivos que contienen información valiosa que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando parte de la información y de la infraestructura tecnológica de la organización.

Algunos de los objetivos de la seguridad informática es identificar las amenazas a las cuales está expuesta la información, minimizar los riesgos de esa exposición, gestionar la adecuada utilización de las TIC que tiene la organización, garantizar que en caso de un desastre informático se tenga una recuperación del negocio inmediata e integral, y cumplir con el marco legal que se exige por el manejo de datos personales y empresariales de los clientes y socios de la empresa[33].

La normativa internacional ISO 27001[34], también lo define como la causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema u organización.

Algunos problemas respecto a amenazas en materia de seguridad informática que se observan a nivel mundial están asociadas a cuatro sucesos: ataques de denegación de servicios; acceso no autorizado a la información de una base de datos; fuga de información; robo de credenciales de acceso.

Cuando la información o cualquier otro activo es víctima de una amenaza se deben evaluar dos aspectos:

a) Degradación: implica cuan perjudicado resultó el activo y su costo de reposición o reparación.

b) Frecuencia: se refiere a cada cuanto se puede materializar la amenaza.

---

[33] Baca Urbina G. (2016*).* Introducción a la Seguridad Informática. 1ra edición *ebook*. México. Grupo Editorial Patria. Pág. 45.

[34]IRAM, Instituto Argentino de Normalización (2007). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad en Tecnología de la Información.

1.1.19 Ataque.

Un ataque es el intento de destruir, exponer, alterar, inutilizar, robar, obtener acceso no autorizado o hacer uso indebido de los activos[35]. Estos ataques se clasifican en cuatro grandes categorías: intercepción, que afecta a la confidencialidad; modificación que distorsiona la integridad; interrupción que dificulta la disponibilidad y suplantación que busca atentar contra la autenticidad. Estos pueden ser intencionados o no intencionados.

1.2 Relación entre la Seguridad de la Información y la Ciencia de la Administración

De manera genérica, podríamos definir qué Administración es la ciencia social que tiene por objeto el estudio de las organizaciones y la técnica encargada de la planificación, organización, dirección y control de sus recursos, con el fin de obtener el máximo beneficio posible, pudiendo este ser social o económico, dependiendo de los fines perseguidos por el ente[36]. Es decir que esta disciplina, hace énfasis en las organizaciones y en los recursos que la componen, entre estos, como ya se ha plasmado anteriormente, la información.

Como cualquier otro activo, la información otorga valor a la compañía, por lo tanto debe ser resguardada de las amenazas que pudiera sufrir.

En este sentido, cobra significativa importancia el concepto de "Seguridad de la Información", la cual se encarga de proteger la integridad, disponibilidad y privacidad de la información, contra cualquier tipo de amenaza, minimizando los riesgos a los que estuviera expuesta. Esto posibilita, por lo tanto, el normal desenvolvimiento de las actividades del negocio y el cumplimiento de su misión corporativa.

El objetivo de la seguridad informática no solo consiste en prevenir los potenciales ataques internos, externos, físicos y lógicos, sino también se encarga del diseño e implementación de los planes de recuperación en caso de haberse concretado daños. Este método se relaciona

---

[35] Mendoza M. Á. (2015). Conceptos básicos de Seguridad de la Información. Academia ESET Latinoamérica.

[36] Administración (s.f.). En Wikipedia. Recuperado el 30 de enero de 2019.

estrechamente con la continuidad del negocio, aspecto estrictamente necesario para la labor profesional de la administración.

Teniendo en cuenta lo descripto, podemos observar que la Ciencia de la Administración no está percibiendo esta realidad y por ende no está considerando en la formación de sus profesionales aspectos relacionados al ámbito de la seguridad informática, de vital importancia.

Por lo anteriormente expuesto, se refuerza el postulado principal de este trabajo, el cual considera a la Seguridad Informática como un área de vacancia disciplinar, en las carreras de Ciencias Económicas, lo que tratará de ser corroborado en el trabajo de campo desarrollado.

1.3 La propuesta de Cátedra

1.3.1 Justificación del abordaje de esta temática.

Debido a que este trabajo tiene como finalidad generar un programa de asignatura sobre "Seguridad y Control de Sistemas Informáticos", para ser propuesto como materia optativa para las carreras de Contador Público y Licenciatura en Administración de la FACE de la UNT, a continuación se presentan los principales conceptos recabados sobre metodología de armado de proyectos de Cátedra. Se decidió utilizar como base de estudio a Steiman[37], dadas sus explicaciones simples y por considerarse el más apropiado para el contexto universitario.

1.3.2 Estructura de los Proyectos de Cátedra.

1.3.2.1 ***El valor pedagógico de los Proyectos de Cátedra.***

El autor consultado como referencia, define proyecto de cátedra como una propuesta académica en la educación superior en la que se explicitan ciertas previsiones, decisiones y condiciones para la práctica didáctica en el aula y que intenta hacer explícito ciertos acuerdos que conforman aquello que puede objetivarse del contrato didáctico que se establece con los

[37] Steiman, J. (2007). Más Didáctica en la educación superior. Cap. 1: Los proyectos de cátedra. Miño y Dávila-UNSAM. Argentina.

alumnos y con la institución. Por lo tanto, se puede decir que se trata de una herramienta que supera, por su valor pedagógico los diseños de “programa de asignatura”.

Para su formulación se tendrán en cuenta tres componentes:

- El docente
- El alumno
- La institución

1.3.2.2 ***El equipo docente.***

Este proyecto puede ser de gran utilidad para el equipo docente, considerando los siguientes aspectos:

- Organizar mejor el trabajo de cátedra, permitiendo realizar las previsiones necesarias para el dictado de la asignatura
- Evitar incoherencias e improvisaciones debido a un trabajo no planificado previamente
- Contribuir al intercambio académico al constituirse como un instrumento de comunicación referido a la propuesta de enseñanza de cada docente
- Es un documento que contiene un conjunto de previsiones, por lo que mejora el intercambio académico con los alumnos
- Facilita el análisis y la reflexión sobre la práctica, ya que su lectura permite replantear la propuesta
- Permite realizar un balance entre lo propuesto y lo realmente efectuado y determinar las desviaciones y sus causas correspondientes

1.3.2.3 ***Los alumnos.***

Para los alumnos también es importante el proyecto de cátedra. A continuación se expresan los aspectos más relevantes:

- Especifica los contenidos a aprender y la bibliografía obligatoria, lo cual ayuda a al alumno a organizar su estudio

- Contribuye a la distribución de su propio tiempo, al poder consultar las fechas de exámenes y los plazos para la presentación de trabajos prácticos
- Conocer la orientación que la cátedra concede a cada unidad curricular, los objetivos de enseñanza y la concepción de aprendizaje que subyace a la propuesta
- Informarse sobre las condiciones de aprobación de cada unidad de estudio en cuanto a parciales y finales y criterios que tomará en cuenta el equipo docente para decidir la aprobación
- Encontrar bibliografía complementaria para la profundización de ciertas temáticas
- El documento le garantiza interiorizarse de sus obligaciones académicas con cierta anterioridad

1.3.2.4 ***La Institución.***

Al contrario de los que muchos piensan, el proyecto de cátedra no debe ser visto como un elemento burocrático administrativo o de control, sino como un documento de utilidad para:

- Coordinar acuerdos referidos a ausencia o superposición de contenidos, enfoques epistemológicos, propuesta metodológica y criterios de acreditación propios de un área
- Establecer la relación entre los proyectos de la institución y los de la cátedra
- Es un elemento para la evaluación de la calidad académica
- Verificar el cumplimiento de los contenidos mínimos planteados en los planes de estudio
- Contar con un documento que permita decidir sobre equivalencias u otorgamiento de pases a otras unidades académicas

1.3.2.5 ***Sugerencias para su desarrollo.***

a) Encabezamiento: deben estar consignados mínimamente los datos institucionales y curriculares mínimos. Entre ellos: nombre de la universidad, facultad, carrera, unidad curricular; asimismo indicar cuatrimestre y año, cantidad de horas semanales y equipo de cátedra.

b) Actividad académica de la cátedra: una cátedra por el solo hecho de serlo, hace docencia. Pero ella necesita también hacer investigación y si puede, es recomendable que haga extensión. El proyecto de cátedra puede al respecto, comunicar la actividad académica que realice en función a estas tres funciones.

- La **investigación** es una actividad inherente a la vida universitaria. Hacer docencia e investigación en la universidad son actividades interdependientes y complementarias, por lo que se desprende que, no puede pensarse la actividad de una cátedra al margen de algún proyecto de investigación.
- La **extensión** abarca aquellas acciones que se lleven a cabo con relación a otros sujetos que no sean los alumnos/as (como empresas, otras instituciones, egresado/as, docentes, etc.).
- La función **docente** resulta ser la actividad de una cátedra más directamente relacionada con la comunicación del conocimiento.

c) Marco referencial: Cualquier propuesta de cátedra debe fundamentarse implícitamente en una serie de supuestos que le den sostén. Este debe referirse específicamente a la actividad de la docencia y ser una primera aproximación global del proyecto de trabajos con los alumnos en torno al conocimiento. En ella debe tenerse en cuenta los siguientes elementos:

- **Marco curricular:** La propuesta tendrá mayor coherencia con el plan de estudios si se contempla el sentido de su totalidad ya que, la sola experiencia del equipo docente, no puede ser un elemento suficiente para interpretar la direccionalidad que se le puede dar a una cátedra. El análisis que el equipo docente realiza del plan de estudios y la primera interpretación que hace acerca del sentido de la cátedra en un determinado trayecto de formación, debería ser comunicado. En este espacio pueden incluirse tres aspectos centrales: descripción de la ubicación de la asignatura en el plan de estudios y su relación con el ciclo en el cual se encuentra; así también identificar los aportes específicos a la incumbencia profesional del

egresado y expresar la relación de la unidad curricular de la propia cátedra con otras de años anteriores y posteriores.

- **Marco epistemológico:** Tiene que ver con la "lectura" y el "posicionamiento" que la cátedra realiza en relación con la disciplina como objeto científico y como producción de conocimiento social a partir de lo cual se desprende su "núcleo duro" como contenido de enseñanza.

- **Marco didáctico:** se vincula con el referente teórico por el que opta la cátedra con relación a los procesos de enseñar y aprender una disciplina en particular. Cada disciplina tiene, por la especificidad de su contenido y sus métodos de investigación, una forma que le es propia de ser aprehendido y comunicado.

- **Marco institucional:** ciertas particularidades coyunturales del contexto socio histórico, de la propia institución o del grupo de alumnos pueden llegar a incidir fuertemente sobre el desarrollo de las clases y, en consecuencia, condicionar alguna de las decisiones que el equipo docente debe tomar al realizar las previsiones para la puesta en marcha de su proyecto de cátedra.

d) Propósitos

- **El planteo de objetivos:** los objetivos tratan de enunciar qué aprendizajes, en relación con los contenidos, se espera que realicen los alumnos en el transcurso de la cursada de una unidad curricular.

- **El planteo de propósitos:** Se refiere a todo lo que el equipo docente se propone enseñar, es decir la expectativa que se tiene al respecto. Estos deben evidenciar la dirección que se le intenta dar al proceso áulico respecto a las prácticas que sucederán en el aula. Los propósitos deben ser formulados iniciando con un verbo, que indique la acción del docente respecto a su hacer propio y específico.

e) Contenidos: representan el eje central de todo proyecto didáctico y responden a la pregunta ¿qué enseñar?

La primera limitación que presenta el trabajo respecto a los contenidos, está representada por la presencia de los contenidos mínimos presentes en el plan de estudios. Estos posibilitan una coherencia en un trayecto de formación articulando los núcleos centrales de cada disciplina. Sin embargo, la libertad de cátedra de la educación superior otorga una necesaria y sana libertad que no puede ni debe desaprovecharse. Asimismo, se pueden incorporar contendidos por las siguientes razones: por resultar significativos, por su vinculación con los intereses ideológicos de la cátedra, por el resultado de las últimas investigaciones científicas que figuran en textos de reciente aparición, por su demanda profesional, ente otros.

Así también se debe tomar una decisión respecto al tipo de "organización epistemológica" o "didáctica" de los contenidos. La forma más habitual de esta última es a través de unidades de estudio. Dentro del proyecto de cátedra, junto a cada unidad o en un apartado final, se puede especificar la bibliografía obligatoria, para orientar a los alumnos en su proceso de estudio.

Junto al proceso de organización, se debe definir sobre la secuenciación de los contenidos, es decir el ordenamiento que se les dará a cada uno de los temas, en los que intervienen cuestiones de tiempo e importancia. Finalmente se debe realizar una presentación de los contenidos.

f) **Marco metodológico:** Se refiere a aquello que rodea la situación didáctica de la enseñanza y el aprendizaje. Explica la secuencia por la que se organiza la clase.

g) **Cronograma:** Debe hacer referencia a la distribución en el tiempo de los contenidos previstos en las unidades didácticas, así como una aproximación predecible al tiempo en que se efectuarán las evaluaciones parciales y/o la entrega de trabajos prácticos si los hubiera.

h) **Evaluación**: El concepto de evaluación es mucho más abarcativo que los parciales, finales y notas, ya que la enseñanza es objeto de evaluación. En este punto se deben especificar

los métodos en los cuales se evaluará (exámenes, trabajos prácticos o prácticas de campo, los cuales deben ser acordes a la metodología utilizada en clases).

i) **Bibliografía:** Se debe diferenciar la bibliografía obligatoria de la de consulta. La primera se refiere a la que los alumnos tendrán que leer indefectiblemente porque sostiene conceptualmente el desarrollo de la unidad curricular y se la considera indispensable a los efectos del aprender. La segunda es aquella que orienta la lectura optativa de alguna temática y la permite profundizar o leer desde otro marco teórico e ideológico.

Capítulo Nº 2: Estado de Seguridad de la Información: Informes especializados

2.1 Introducción

Con la finalidad de reconocer el estado de la seguridad de la información en las organizaciones de la región, se realizó un análisis de reportes especializados en la temática. A continuación, se reseñan algunos de ellos, referidos a las principales problemáticas observadas en Latinoamérica.

2.2 Tendencias - Academia ESET Latinoamérica

2.2.1 Notas preliminares.

Los especialistas de la academia ESET[38] de todo el mundo, anualmente participan del documento de "Tendencias" en el que se repasan los principales acontecimientos en materia de seguridad y se plantean cuáles pueden ser los escenarios futuros sobre ataques y las medidas para contrarrestarlos.

A pesar de las novedades tecnológicas que surgen con el correr del tiempo el foco de la seguridad de la información se trata en resguardar la privacidad, integridad y confidencialidad de los datos de los usuarios y empresas frente a los embates de los ciber criminales que intentan acceder a ellos, manipularlos y/o robarlos.

Los incidentes de seguridad amenazan a las grandes industrias y abre un interrogante sobre cuál es el impacto para otros negocios de menor envergadura que no puedan o no saben proteger apropiadamente la privacidad de sus usuarios. Esto nos indica que los problemas de fondo, en definitiva giran en torno a la protección de los datos y la privacidad. Las secciones de este informe muestran la importancia que tienen los datos, tanto para las empresas, los usuarios,

[38] ESET es una compañía de seguridad informática establecida en Bratislava, Eslovaquia. Fue fundada en 1992 como resultado de la fusión de dos compañías privadas, dando desarrollo a su producto más famoso, ESET NOD32, el potencial software antivirus.

para quienes se encargan de brindar protección y también para los cibercriminales. A continuación se desarrollan los principales conceptos descriptos por este informe especializado.

2.2.2 **Mantenerse Seguros en tiempo de Incertidumbre.**[39]

La pandemia del COVID-19 fue un cimbronazo mundial y simbolizó un cambio de paradigma y hábitos, que sin dudas tendrá consecuencias muy profundas y que todavía no podemos advertir.

Se considera que el mayor cambio que tuvo el año 2020 está relacionado con la expansión del trabajo remoto, el cuál sucedió de manera abrupta, precipitadamente e interfiriendo en la vida cotidiana. A esta situación se le sumó un contexto social muy convulsionado.

Así las cosas, los cibercriminales se adaptaron rápidamente a esta situación y buscaron empezar a explotar las oportunidades que la improvisada implementación del teletrabajo le presentaba: empresas poco preparadas a nivel técnico y de conocimiento en esta disciplina, empleados no concientizados en un uso seguro y correcto de las herramientas a disposición, entre otros.

Se destaca que el año 2020 nos demostró que la gran mayoría de los procesos y prácticas humanas tienen alguna conexión con el ámbito tecnológico.

Por otra parte, el *ransomware* viene pisando fuerte en este último tiempo. A su funcionamiento "tradicional", que implicaba el secuestro de información y el pedido de un rescate para restaurar el acceso a la misma, ahora se le suman mecanismos extorsivos y la amenaza de difundir la información secuestrada, para persuadir a las víctimas de realizar el pago correspondiente.

La pandemia forzó la aceleración de los procesos de transformación digital y visibilizó la necesidad de que la seguridad esté en el centro de las decisiones corporativas. La actividad

---

[39] *Welivesecurity* (2020). Tendencias en Ciberseguridad para el 2021: mantenerse seguros en tiempos de incertidumbre.

maliciosa tuvo un importante crecimiento durante el año 2020 con actores malintencionados, pretendiendo aprovecharse de un escenario que presentaba un mayor vector de ataque, con más usuarios conectados, por más tiempo, y dispuestos a adoptar el uso de tecnologías y servicios online que no tenían tanta demanda previamente.

2.2.3 **El futuro del trabajo: abrazando una nueva realidad.**[40]

Desde la implementación del aislamiento social preventivo, que los gobiernos de todo el mundo debieron efectuar a raíz de la pandemia de COVID-19, la cultura del trabajo ha cambiado drásticamente en formas que la mayoría de las personas nunca hubiera pensado.

La pandemia demostró que es posible trabajar desde casa y las organizaciones son capaces de crear políticas y hacerlas cumplir rápidamente. Además ha quedado claro que el trabajo remoto llegó para quedarse en el largo plazo, pero para operar de manera eficiente se requiere contar con una excelente gestión corporativa y con políticas de seguridad perfectamente integradas. Las corporaciones deben darles la misma importancia a las prácticas de gestión y a las de seguridad, lo que a su vez protege al personal y a la empresa. La capacitación puede resultar muy útil para proteger al capital humano y funciona mejor cuando se imparte con frecuencia y en pequeñas dosis.

El teletrabajo aportó flexibilidad, alteró drásticamente los procesos y sistemas empresariales para atender a una fuerza de trabajo geográficamente dispersa. Por lo tanto, es necesario entender que el elemento humano en la seguridad de la información es tan importante como el técnico.

---

[40] Jake Moore (2020). El futuro del trabajo: abrazando una nueva realidad. Welivesecurity de ESET Latinoamérica. Tendencias en Ciberseguridad para el 2021: mantenerse seguros en tiempos de incertidumbre.

2.2.4 **Transformación digital y seguridad de la información: el reto para las empresas.**[41]

La dinámica del mercado ha llevado a que la transformación digital se vuelva un aspecto fundamental que deben abordar todas las áreas de una organización, involucrando tecnologías que brinden mayor valor a sus clientes. Estas incorporaciones, suponen un cambio cultural a nivel organizacional que representan un gran desafío, por lo que la seguridad de la información debe considerarse como parte importante de los objetivos.

Como esta transformación suele tener implícita una restructuración de los procesos y las estrategias corporativas, se abren nuevos perfiles de riesgo que no pueden perderse de vista. Ello, tiene un impacto directo en la seguridad que obliga a reducir las posibilidades de ser víctima de un ataque informático. En este aspecto debe entenderse que no es solo una la tecnología que permite garantizar la seguridad de los datos y la continuidad del negocio.

Por lo anteriormente descripto, es significativo que las organizaciones no sigan considerando a la seguridad de manera clásica, sino que comiencen a plantear modelos adaptativos que puedan responder a los cambios. Además es preciso que habiliten sus procesos para responder ante posibles incidentes y volver a la operación, aplicando las medidas de corrección adecuadas

Seguidamente, en este informe se realizan cinco consideraciones necesarias para llevar adelante esta transformación digital de manera segura:

1) Buscar un equilibrio entre la implementación de tecnologías y la seguridad informática.

2) Desarrollar proyectos que faciliten la visibilidad y el control de las tecnologías. Este rumbo no debe estar centrado solamente en la prevención de incidentes, sino también en la detección y la respuesta ante ellos.

---

41 Gutiérrez C. (2020). Transformación digital y seguridad de la información: el reto para las empresas. Academia ESET Latinoamérica. Tendencias 2020: La tecnología se está volviendo cada vez más inteligente ¿Y nosotros?

3) El enfoque de la seguridad no puede estar únicamente sobre los dispositivos.

4) Debe propiciarse una mayor colaboración entre las personas y los procesos, de tal manera que estén alineados y que la toma de decisiones esté basada en datos comunes.

5) No puede descuidarse el componente humano y se debe trabajar para evitar que la información de la empresa pueda ser vulnerada por ataques de ingeniería social.

Finalmente el reporte hace referencia a que las personas deben estar preparadas, tanto desde lo tecnológico como de lo educativo, para tener herramientas suficientes que les permitan afrontar ataques que vulneren la seguridad y privacidad de su información y de las organizaciones de las que forman parte.

2.2.5 ***Coinminers*: el nuevo chico del barrio.**[42]

Las criptomonedas o monedas virtuales, las cuales se popularizaron con los ataques tipo *ramsomware*, son utilizadas como método de pago por criminales, pues estas transacciones no son fáciles de asociar con entidades del mundo real, especialmente si existe un proceso de conversión a otras criptomonedas antes de finalmente ser cambiadas por efectivo o valores en el mercado.

La minería de monedas virtuales es un proceso costoso y apenas rentable para cualquiera, salvo para quienes lo realizan a gran escala, ya que demanda demasiado poder de procesamiento como para ser realizado por computadoras individuales y dispositivos.

Debido a esta práctica, se origina el "*criptojacking*", que se produce cuando parte del poder de procesamiento utilizado para la minería de monedas virtuales proviene de un sistema "secuestrado" por un malware (comúnmente referido como un *coinminer*) o mediante secuencias de comandos en un sitio web.

---

[42] Harley, D. (2019). *Coinminers*: el nuevo chico del barrio. Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

El evidente y alto uso de ciclos de CPU y GPU podría evidenciar la presencia de este tipo malware. Otro posible síntoma incluye el sobrecalentamiento, congelamientos inesperados, reinicios y volúmenes inexplicablemente altos de tráfico de red.

El malware de minería de criptomonedas es descrito como "el nuevo *ransomware*", a pesar de haber atraído mucho menos la atención de los medios. "La criptominería incrementó en un 956% en el último año y el número de organizaciones afectadas se duplicaron en la primera mitad de 2018, lo que permitió a los cibercriminales ganar aproximadamente 2.500 millones de dólares durante esos meses."

2.2.6 **Las Máquinas aprenden, los humanos no tanto.**[43]

La base de cualquier buen sistema de "*machine learning"*[44] es contar con una vasta cantidad de datos útiles. Sin información de la cual aprender, las máquinas no tienen los insumos necesarios para generar reglas efectivas y poder tomar decisiones.

Los productos de seguridad vienen utilizando la automatización y el aprendizaje automático desde hace tiempo, para determinar qué archivos y comportamientos se consideran sospechosos y cuales intentos benignos.

En contraste a ello, a medida que se amplía el mercado del ciber crimen y más Estados se suman a la lucha, es probable que los criminales se vean impulsados a utilizar la automatización en mayor medida para hacer sus creaciones más eficientes. Los ciberdelincuentes ya utilizan búsquedas automáticas para asistir en el hallazgo de máquinas vulnerables y cuentas en línea, y así reunir grandes cantidades de datos dispersos para el subsecuente reconocimiento dirigido a objetivos y así obtener un mayor entendimiento del valor de cada target.

---

[43] Myers, L. (2019). Las Máquinas aprenden, los Humanos no tanto. Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

[44] Es el sub campo de las ciencias de la computación y una rama de la inteligencia artificial, cuyo objetivo es desarrollar técnicas que permitan que las computadoras aprendan. De forma más concreta, se trata de crear programas capaces de generalizar comportamientos a partir de una información suministrada en forma de ejemplos.

Cabe destacar que el cibercrimen es sumamente lucrativo para la mayoría de sus integrantes sin la necesidad de desarrollar nuevas herramientas, aunque deberíamos prepararnos como si estuvieran por lanzar sus armas más sofisticadas. Y la seguridad para la defensa es tan compleja que no solo los humanos necesitarán de las computadoras para poder identificar archivos y comportamientos sospechosos, sino que las computadoras siempre necesitarán de los humanos para identificar nuevos tipos de armas.

2.2.7 **Reglamento General de Protección de Datos (GDPR): ¿El primer paso hacia una ley de privacidad global?**[45]

La legislación ya está teniendo un gran impacto en la privacidad digital, no solo dentro de la Unión Europea, sino también en Estados Unidos, así como en otros países; una tendencia que afectará el panorama de la ciberseguridad desde 2019 en adelante.

Un objetivo clave en la ciberseguridad es controlar el acceso a la información para evitar que sea expuesta sin autorización. Un objetivo de la regulación de la privacidad es influir la manera en que se define la "exposición desautorizada" en lo que respecta a información personal, y luego explicitar las consecuencias que pueden tener las organizaciones si permiten que ocurra dicha exposición.

En consecuencia, una brecha de datos podría hacer más que dañar la confianza que la gente deposita en las organizaciones, ya que podría también resultar costoso si la brecha, y/o el manejo de la misma, viola las regulaciones de privacidad.

Es por ello que compañías de todo el mundo se están planteado una alineación de sus estrategias corporativas en lo que concierne a datos con esta regulación ya que es inevitable algún tipo de equivalente al GDPR donde sea que hagan negocios.

---

[45] Cobb, S. (2019). GDPR: ¿El primer paso hacia una ley de privacidad global? Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

2.2.8 **Privacidad recargada: ¿Será ella quién decida que negocios sigan en pie?** [46]

El número de personas cuya privacidad digital estuvo en riesgo durante 2018 por algún problema en relación a la seguridad de los datos, probablemente haya superado los 2.000 mil millones antes de que finalizara el tercer trimestre del año.

Lo que podremos ver convertirse en tendencia hacia 2019 es un aumento en el número de gente buscando alternativas a las plataformas que dominan actualmente el panorama en línea, en un esfuerzo por diversificar su propio mundo digital, para reducir el riesgo y simplificar la recuperación ante problemas que surjan.

2.2.9 **Asistentes de voz para el hogar: cuando tus dispositivos nunca se apagan.**[47]

El Reuter se ha convertido en el dispositivo electrónico más importante del hogar. Esto es así porque además de darles acceso a Internet a los usuarios, por este conector pasa toda la información sensible de los usuarios, y en caso de no estar correctamente actualizado puede ser aprovechado por un cibercriminal para comprometer todos los dispositivos conectados. Por lo tanto, un Reuter vulnerado puede convertirse en una plataforma de ataque que sirva como puente para acceder a otros dispositivos en la misma red.

Pero en el último tiempo también empezaron a popularizarse los asistentes de voz; que además de estar comunicados con varios dispositivos tienen la capacidad de controlarlos, como es el caso de luces inteligentes, sensores, cámaras e incluso electrodomésticos. Y de la mano de este incremento en la variedad de dispositivos interconectados también crece la superficie de ataque.

Si bien la usabilidad y facilidad que los dispositivos inteligentes ofrecen al usuario están muy bien valoradas, también pueden representar una puerta abierta para el ingreso de amenazas.

---

[46] Myers L., Cobb, S. (2019). Privacidad recargada: ¿Será ella quién decida que negocios sigan en pie? Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

[47] Gutiérrez Amaya, C. (2019). Asistentes de voz para el hogar: cuando tus dispositivos nunca se apagan. Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

La realidad es que a medida que se avanza hacia una mayor adopción en el uso de dispositivos IoT (por su traducción del Inglés, se refiere a Internet de las cosas) agrupados bajo un asistente doméstico, los riesgos para la seguridad y privacidad aumentan. No se puede perder de vista que con la evolución de la tecnología también evoluciona la forma en que piensan y actúan los cibercriminales.

Así que es necesario considerar desde el lugar físico en los que se ubiquen estos dispositivos hasta pensar en adquirir aquellos que ofrezcan mejores características de cifrado o con una autenticación robusta.

Finalmente, ser consciente de que existen riesgos, es la mejor manera de estar preparado para mantener seguros los dispositivos y la información que se maneja a través de ellos.

2.3 Reporte de Seguridad "ESET Latinoamérica"

2.3.1 **Introducción.**

Conocer el estado de la seguridad de la información en las organizaciones de la región, permite acceder a un panorama general para comprender qué prácticas están llevando a cabo, cuáles son sus preocupaciones y cómo trabajan para proteger sus infraestructuras y activos.

Para ello se realizó un análisis de la información plasmada en el **"**ESET Security Report 2018" [48], el cual es un informe que presenta el estado actual de la seguridad de la información en las empresas en Latinoamérica. Para llevarlo a cabo esta corporación recopiló datos aportados por más de 4.500 ejecutivos y gerentes de más de 2.500 empresas de 15 países de la región, lo que otorgó un panorama general de la problemática. Este informe está compuesto por tres partes: la primera dedicada a entender las preocupaciones de las empresas en materia de seguridad. Luego, se analizan los tipos de incidentes reconocidos y finalmente se centra en

[48] Academia ESET Latinoamérica (2018). ESET *Security Report* 2018.

los controles que se implementan a fin de proteger las redes corporativas, y cómo estos datos se relacionan con las preocupaciones que los profesionales de tecnología dicen tener.

2.3.2 **Preocupaciones.**

- En el año 2018, la mayor preocupación manifestada por los ejecutivos de empresas latinoamericanas fue el "*Ransonware*" con el 57% de las respuestas. Este tipo de código malicioso, ha evolucionado y se ha instalado en la realidad actual gracias a la rentabilidad que otorga a los atacantes, con el agravante de contar con la ayuda de las criptomonedas que permiten cerrar el procedimiento delictivo sin mayores riesgos.

Aprovechando este punto, se hace referencia a que gracias a la explosión global del virus "*Wannacry*" en 2017, todo el mundo comenzó a preocuparse por la seguridad informática. Este ataque golpeó más de 200.000 computadoras en 150 países, teniendo negocios fuera de línea, lo que alteró sus ventas y operaciones

- La explotación de vulnerabilidades ocupa el segundo lugar respecto a las preocupaciones manifestadas, con un 55% de las respuestas. En 2017 se reportaron más de 14.700 vulnerabilidades, contra las 6.447 de 2016. En consecuencia, las organizaciones deberán estar preparadas para determinar las principales fallas que podrían ocasionarse en sus activos de información y prevenir incidentes de seguridad.

- El *malware* (otras variantes a la indicada en primer término) aparece en tercer lugar con el 53% de las respuestas. Este concentra a gran parte de las amenazas que podrían comprometer la seguridad en una organización, aprovechando el amplio espectro de plataformas que comprenden los activos de la información en la compañía.

- En cuarto lugar, hallamos como preocupación de la mitad de los encuestados, al robo de información, el cual se destaca, teniendo en cuenta la vasta variedad de acciones que pueden emplearse para llevar a cabo esta actividad.

2.3.3 **Incidentes.**

El 60% de las empresas encuestadas sufrieron en el último año al menos un incidente de seguridad. La mitad de ellos fueron infectados por alguna variante de *ransonware*, por lo cual fueron víctimas de robo y encriptamiento de información.

Como se observa en el gráfico N° 2[49], en nuestro país el 18% de las empresas manifiestan haber sido víctimas de ataques de alguna variante de *malware*. Se destaca que Argentina se encuentra en el tercer lugar respecto a la cantidad de detecciones de códigos maliciosos de la familia *FileCoder*[50]

Además, se observa un fuerte crecimiento en detecciones de softwares maliciosos con capacidad de minar criptomonedas, utilizando la capacidad de cómputo de las máquinas infectadas. Esto atenta contra la reputación de las organizaciones, debido a que si los usuarios advierten que los servidores de una compañía han sido comprometidos, su confianza en ella también se verá afectada.

Gráfico N° 2: Incidentes de Seguridad por países

Este informe destaca que los ataques de malware se observan en organizaciones de todo tipo y tamaño. Pero no todos los incidentes de seguridad manifestados por empresas de la región están vinculados a ataques de software malicioso. Otras respuestas también estuvieron relacionadas a la denegación de servicios, acceso indebido a bases de datos y aplicaciones. En la mayoría de los casos utilizando prácticas de ingeniería social, suplantando empresas y marcas reconocidas.

---

[49] Academia ESET Latinoamérica (2018). ESET *Security Report* 2018. Gráfico N°1, página N° 6

[50] Categoría de *ransomware* que bloquea el sistema de cómputo cifrando los archivos y exige un pago para recuperar el acceso.

2.3.4 **Implementación de controles.**

Una cuarta parte de las empresas consultadas no cuenta con una política de seguridad implementada, sin embargo, todas son conscientes respecto a que la problemática requiere contar con alguna solución de seguridad o tecnológica. Esto se evidencia al corroborarse que el 99% de las encuestadas cuentan con alguna medida de seguridad.

Además, se observa que las empresas más pequeñas cuentan con una menor cantidad de medidas de protección tecnológica, respecto a las de mayor envergadura. Esto se explica gracias a la cantidad de dinero disponible en ellas, para ser destinado a la inversión en seguridad de la información. Cabe destacar que el punto más débil se evidencia en los dispositivos móviles, ya que solo el 11% de las respuestas afirman tener alguna solución de seguridad para este tipo de dispositivos.

Otro tema importante de distinguir es la baja adopción de tecnologías que permiten gestionar parches de seguridad y actualizaciones de software. Esto agravado por el aumento de dispositivos conectados a través del “internet de las cosas”.

Una preocupación generalizada que también se observa en la región, es la “fuga de información”. Sin embargo, solo el 10% de las encuestadas cuentan con alguna medida para la mitigación de este riesgo.

Una implementación exitosa de una política de seguridad implica un desafío multifactorial y complejo, por lo que no son suficientes las soluciones tecnológicas, sino que requiere un enfoque holístico. No solo debe ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino a su vez, como una función esencial de la administración por parte de toda la organización. Por lo tanto, los principales cambios no deben efectuarse en los controles tecnológicos, sino en la implementación de políticas, planes de gestión, adopción de estándares o mejores prácticas y la realización de auditorías sobre el estado de seguridad.

2.3.5 **Panorama de seguridad en Latinoamérica.**

Dado el estado de seguridad informática de la región, es de esperar que menos del 10% de las compañías encuestadas cuentan con un área específica para la gestionarla. A pesar de esta situación, la mitad de las consultadas administra su seguridad a través de su departamento de TI, lo cual representa una alternativa que no es acorde con lo que sugieren las buenas prácticas. Sin embargo, se observa en los últimos años un incremento de la tasa de independencia del área de seguridad. Los ejecutivos de las compañías explican la situación alegando la falta de presupuesto disponible para el área.

Finalmente, el informe realiza una interesante reflexión respecto al tema de la capacitación de los usuarios en materia de seguridad de la información, debido a que ellos cumplen un rol fundamental y son un factor diferencial para garantizar el cumplimiento de los objetivos propuestos en el área. Una óptima seguridad se logra a través de una buena gestión de recursos tecnológicos y de sus interrelaciones, función que solo puede ser llevada a cabo por personas capacitadas para ello.

2.4 Las empresas y los nuevos desafíos de seguridad[51]

Tiempo atrás, las organizaciones medían su seguridad teniendo en cuenta el número de personas que custodiaban los inmuebles o a las cajas, entre otros. Actualmente en un mundo digitalizado, en su economía y sus relaciones, cada vez más compañías están incorporando políticas y estrategias de seguridad de la información.

En este reporte se destacan los siguientes puntos:

[51] Encuesta de Seguridad Informática: Las empresas y los nuevos desafíos en Seguridad. Publicación, 15 de agosto de 2018. Binder Dijker Otte y Taquión. Argentina.

- Según especialistas en seguridad de 500 empresas de Argentina y Latinoamérica en el año 2018 cuatro de cada diez empresas, fueron víctimas de algún tipo de incidente que vulneró su seguridad.

- El 45% de las encuestadas considera que su nivel de seguridad informática es débil o inexistente.

- Se observa un aumento de concientización por parte de la alta gerencia de las organizaciones. El 44% de ellas incrementaron su presupuesto en relación a temas de ciberseguridad, un 55% lo mantuvo y solo el 4% lo disminuyó.

- Solo un cuarto de las encuestadas ha manifestado haber realizado pruebas en relación a estafas de Ingeniería Social, las cuales han tomado relevancia en el último tiempo por la cantidad de ataques que se realizan a través de estas técnicas.

- El 63% de las compañías manifiesta tener un área de seguridad de la información, lo cual se valora como altamente positivo y evidencia la importancia que le están otorgando a la temática las organizaciones en general.

- El 82% de las respuestas manifiestan que dentro de la estrategia corporativa, se encuentran temas relacionados con ciberseguridad.

- El 60% de las compañías encuestadas capacitó a su personal respecto a temas de seguridad informática.

2.5 Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción a las TIC".[52]

2.5.1 **Introducción.**

La Secretaría General de la Organización de los Estados Americanos (OEA) y Amazon *Web Services* (AWS) publicaron un reporte que incorpora aspectos clave para la gestión de la

[52] OEA y AWS (2018). Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción a las TIC. *White paper series*, 3° edición. Publicado el 28 de agosto de 2018 en Chile.

ciberseguridad en las Pymes de la región latinoamericana, la privacidad de los datos, la sensibilización sobre la seguridad de la información en el entorno de las pymes, el rol del gobierno para la creación de un contexto de ciberseguridad saludable. A continuación, se sintetizan los conceptos más relevantes tratados en el mismo:

2.5.2 **Oportunidades y desafíos para las Pyme en el contexto de una mayor adopción de las tic´s.**

Las Pymes y *Startups* son el motor productivo de crecimiento económico en América Latina y cumplen un papel muy importante en la creación de empleo y la reducción de la pobreza. Este mayor papel depende en gran medida de su dependencia a Internet y a las Tics, que les permite acceder a una economía global para comerciar y fortalecer sus procesos, eficiencia e innovación.

A pesar de esto, se observa que en los últimos años, han sido muy frecuentes los ataques informáticos a las Pymes, las cuales enfrentan pérdidas, con mayores costos per cápita, comparándolas con empresas más grandes. Esta situación se agrava debido a que muchas de ellas no están preparadas para abordar estas problemáticas.

De acuerdo con PwC[53] (2018), la mayor preocupación de los directores generales en Estados Unidos es enfrentar las amenazas informáticas, destacándose entre ellas el *spear phishing* y *ransomware*, introduciendo mecanismos de limpieza para cubrir las huellas de los atacantes.

Asimismo, se destaca que actualmente, la comprensión de la seguridad informática no solo incluye las actividades y violaciones puramente técnicas, sino también diversos tipos de aprovechamientos y usos de datos no autorizados, como por ejemplo: datos personales y privacidad.

[53] PwC (abreviatura de Price Waterhouse Coopers) es reconocida como una de las firmas de consultoría de las *Big Four*, junto con Deloitte, KPMG y EY. Es la segunda firma de servicios profesionales más grande del mundo prestando servicios de auditoría, consultoría y asesoramiento legal y fiscal a las principales compañías, instituciones y gobiernos a nivel global.

2.5.3 **Las Pymes, la protección de los datos personales y la privacidad de los datos.**

Desde hace unos cuantos años y debido al probado espionaje internacional entre los gobiernos, los países de la región comenzaron a analizar y confeccionar marcos normativos destinados a proteger los datos personales y la privacidad de las personas. Es por ello que las Pymes deben comprender los procedimientos de recopilación, almacenamientos, extracción, utilización y protección de datos. Al contar con un nivel sólido de protección, ellas crean ventajas competitivas y fortalecen la confianza con sus clientes. Según CISCO[54] (2018), el ciclo de ventas de las empresas puede verse profundamente afectado por las inquietudes sobre la privacidad de los datos del consumidor.

Es preciso destacar que la Argentina, junto a México y Uruguay, son las únicas Naciones consignatarias del "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", lo que pone en evidencia el compromiso que tiene nuestro país respecto a la temática.

2.5.4 **Sensibilización de la seguridad cibernética y las Pyme.**

El nivel de concientización y formación respecto a la seguridad informática y la privacidad de los datos varían ampliamente según la Pyme. Una parte de esta problemática se debe a la falta de "cultura de seguridad", por lo que se observa una comprensión limitada de la temática. Las compañías tienden a efectuar medidas de seguridad físicas y lógicas, pero subestiman el componente humano.

Según estudios a nivel mundial dos tercios de los empleados no informan sobre sus errores a sus superiores. A esta situación se le suma la ausencia de políticas de seguridad informática internas y las bajas inversiones financieras, lo cual ubica en una posición vulnerable a las pequeñas y medianas empresas.

---

[54] Cisco *Systems* es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

Finalmente, se destaca la tendencia actual de las grandes empresas, a la contratación de ejecutivos cuyo principal deber es ser responsable de la supervisión de la privacidad y la seguridad en la empresa (CIO), lo cual debería ser evaluado por las Pymes, en la medida que se vayan familiarizando con los desafíos y oportunidades que llegan con las nuevas tecnologías.

2.5.5 El papel del gobierno en la promoción de un ecosistema de seguridad cibernética saludable para las Pyme.

El sector privado actúa como un laboratorio para identificar, desarrollar e implementar las mejores prácticas de seguridad, sin embargo las pymes, en la mayoría de los casos, no cuentan con los recursos suficientes para adoptar, implementar y utilizar estas políticas de seguridad. Es por esto que los gobiernos deben crear un contexto de seguridad para este tipo de empresas.

Actualmente el reto de los gobiernos no es solo fomentar la creación y adopción de tecnologías, sino también de apoyar un ecosistema saludable que priorice las necesidades de seguridad informática.

Si bien las pymes deben esforzarse por cumplir con los estándares de seguridad informática, los gobiernos deberían apoyarlos para que tomen las medidas correctas. Asimismo debieran realizar esfuerzos para contribuir al desarrollo de contenido y conocimiento respecto a la temática, mediante cursos y programas de capacitación.

2.6 La Seguridad Informática, factor clave en la transformación de todos los sectores empresariales[55]

La introducción de este informe establece que el sector de la Ciber seguridad tendrá un crecimiento anual en la Unión Europea del 10.3% y en América Latina del 11,5% hasta el año 2020. Asimismo establece que las empresas invierten un promedio de 16,5% del total del presupuesto de TI en la protección de su infraestructura, sistemas y datos, debido a que están

[55] Presentación del Master en Seguridad de la Información y Continuidad de Negocios (Ciberseguridad) (s.f.). EADIC y Universidad Católica San Antonio de Murcia, Cohorte 2019/2020.

cada vez más conscientes del exponencial aumento de casos de ciber delito que se registran a diario. Este sector se encuentra en pleno crecimiento, una gran opción a tener en cuenta a la hora de encaminar una carrera profesional.

2.7 Cuarta Revolución Industrial en Latinoamérica: ¿cómo lo llevan los gobiernos?[56]

La automatización, la digitalización, así como las nuevas y novedosas tecnologías constituyen los principios básicos que caracterizan la Cuarta Revolución Industrial, que está cambiando la forma de hacer las cosas. Es por ello que las organizaciones que quieran seguir teniendo presencia en estos mercados cambiantes y fuertemente competitivos, deberán ajironarse y tomar las decisiones que sean necesarias para poder estar a la altura de las circunstancias.

Dada esta situación, los gobiernos latinoamericanos, con objeto de mantenerse en alza y no perder el camino, están incluyendo como puntos prioritarios en sus agendas, el desarrollo de la industria para estar preparados para esta Cuarta Revolución Industrial. Entre los aspectos que se destacan de ella se observa: *big data*, *blockchain*, internet de las cosas, realidad virtual e inteligencia artificial.

Por lo tanto, la puesta a punto en tecnologías de la Cuarta Revolución Industrial, debe ser un esfuerzo de todos los gobiernos de la región, para no quedarse atrás. En definitiva, tienen la obligación de reconocer que la vida digital es la vida real y realizar todas las acciones necesarias para procurar la seguridad de la información que genera esta explosión digital y tecnológica.

---

[56] Cuarta Revolución Industrial en Latinoamérica: ¿cómo lo llevan los gobiernos? (s.f.) ISOTools, plataforma tecnológica para la gestión de la excelencia.

Capítulo Nº 3: Contenidos de Seguridad Informática impartidos por Instituciones Educativas de Nivel Superior

3.1 Introducción

Cano (2013) afirma que "*la inseguridad de la información nos ha demostrado que existen elementos tanto en las personas como en los procesos y en la tecnología donde actuar y renovar el entendimiento de la protección de la información*" (p.98). Y continúa exponiendo que "*desarrollar una disciplina de protección de la información exige, un encuentro entre las disciplinas sociales y del comportamiento humano, con la protección de los activos, como fuente del entendimiento de la complejidad propia de las relaciones entre la tecnología y los procesos de la organización, donde los individuos son la parte activa frente a las vulnerabilidades y fallas propias de los artefactos tecnológicos*" (p.100).

En el mismo sentido, la academia ESET Latinoamérica (2019) en su informe de predicciones asevera que "*a medida que se desarrollan los avances tecnológicos, la superficie de ataques se amplía cada vez más y por eso el desafío pasa por llevar adelante la educación en varios planos y públicos*" (p.28). Las organizaciones, empresas y fabricantes deberán hacer su parte si no quieren verse afectadas por usuarios que perdieron la confianza como consecuencia de haberse visto perjudicados a raíz de un incidente de seguridad. [57]

En este capítulo se describe el proceso realizado para la determinación de los conocimientos sobre "Seguridad y Control de Sistemas Informáticos" que se consideran necesarios para el profesional que realiza la labor de la administración estratégica de negocios. Para ello se realizó un análisis de la formación actual del alumno de la FACE respecto a Tecnologías de la Información en general, y en particular sobre Seguridad y Control de Sistemas Informáticos, en comparación con los requerimientos exigidos por la CONEAU para las carreras de Ciencias

[57] Tendencias 2019: privacidad e intrusión en la aldea global (s.f). Academia ESET Latinoamérica

Económicas. Asimismo, se examinaron programas y ofertas académicas brindadas por otras instituciones educativas de nivel superior.

Se destaca que este estudio fue enriquecido a través del intercambio de información con integrantes de la Asociación de Docentes Universitarios en Sistemas y Tecnologías de la Información de Facultades de Ciencias Económicas de Universidades Nacionales[58] (DUTI), lo que posibilitó obtener precisiones de la situación actual respecto a la temática abordada, en otras casas de estudio del país.

Para facilitar la lectura de esta investigación, en primer lugar, se procederá a describir la situación actual en otras unidades académicas, a partir de los datos recabados a través de una encuesta realizada a docentes de DUTI. Posteriormente se realizará un análisis minucioso del estado académico existente en la FACE UNT respecto a la disciplina en cuestión.

Finalmente, cotejando cada una de las situaciones, se presentarán conclusiones preliminares, que serán utilizadas como punto de partida para la elaboración del objetivo principal de este trabajo de campo, el cual generará una propuesta de asignatura optativa para ser incorporada en las carreras de grado de nuestra facultad.

3.2 Situación Externa: encuesta a integrantes de DUTI

3.2.1 **Análisis de la Primera Encuesta. Año 2018.**

En el contexto de las "*XIII Jornadas de Docentes Universitarios en Sistemas y Tecnologías de la Información*" y las "*IX Jornadas Académicas Anuales de Docentes en Sistemas de la UBA*" realizadas del 13 al 15 de septiembre de 2018, en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires (UBA), se instrumentó una encuesta[59] a profesores de las principales Facultades de Ciencias Económicas del país. El objetivo de la misma, fue relevar

[58] Asociación de Docentes Universitarios en Sistemas y Tecnologías de la Información de Facultades de Ciencias Económicas. Puede verse mayor información en el sitio web oficial de la organización: http://www.duti.org.ar

[59] Véase Anexo "A"

información acerca de los contenidos relacionados a "Seguridad y Control de Sistemas Informáticos" impartidos en diferentes Universidades Nacionales.

Se encuestaron integrantes de quince unidades académicas enumeradas a continuación:

1. Universidad Nacional de Buenos Aires
2. Universidad Nacional de Catamarca
3. Universidad Nacional de Córdoba
4. Universidad Nacional de Cuyo
5. Universidad Nacional de Jujuy
6. Universidad Nacional de la Patagonia
7. Universidad Nacional de La Plata
8. Universidad Nacional de Rosario
9. Universidad Nacional de Salta
10. Universidad Nacional de Santiago del Estero
11. Universidad Nacional de Tucumán
12. Universidad Nacional del Centro de la Provincia de Buenos Aires (UNICEN)
13. Universidad Nacional del Comahue
14. Universidad Nacional del Litoral
15. Universidad Nacional del Sur

De las respuestas obtenidas se evidencia que las tres cuartas partes pertenecen a estamentos docentes superiores, la mayoría “a cargo de la asignatura”.

Partiendo de lo general a lo particular, en primer lugar se consultó respecto a las asignaturas referidas a "Sistemas y Tecnologías de la Información", obligatorias y optativas, dictadas para la carrera de Contador Público (CP) y Licenciatura en Administración (LA). Se observa que el 100% de las unidades académicas en la carrera de CP cuentan con una o más materias obligatorias referidas a la disciplina evaluada y el 93% para la carrera de LA. Asimismo, el

45% de los encuestados indica ofrecer una o más materias optativas relacionadas a la temática, para ambas carreras.

A continuación se muestra un cuadro comparativo por Institución educativa y carreras con las respuestas obtenidas:

Tabla A: Materias optativas y obligatorias de TI por Institución educativa y carreras

INSTITUCIÓN	Contador Público		Licenciatura en Administración	
	Obligatorias	Electivas/ Optativas	Obligatorias	Electivas/ Optativas
Univ. de Buenos Aires	1	2	1	2
Univ. Nac. de Catamarca	1	Ninguna	1	Ninguna
Univ. Nac. de Córdoba	1	3	2	2
Univ. Nac. de Cuyo	3	Ninguna	2	2
Univ. Nac. de Jujuy	1	Ninguna	1	Ninguna
Univ. Nac. Patagonia	2	Ninguna	2	Ninguna
Univ. Nac. de La Plata	1	Ninguna	2	Ninguna
Univ. Nac. de Rosario	1	1	2	1
Univ. Nac. de Salta	1	2	3	Ninguna
Univ. Nac de Sgo del Estero	1	Ninguna	2	Ninguna
Univ. Nac. de Tucumán	1	1	1	2
UNICEN	2	Ninguna	2	Ninguna
Univ. Nac. del Comahue	1	Ninguna	Ninguna	Ninguna
Univ. Nac. del Litoral	1	3	2	2
Univ. Nac. del Sur	2	Ninguna	2	1

Fuente: elaboración propia

En la tabla “A” se observa como la temática en la mayoría de los casos, es incluida en los planes de estudios de las carreras analizadas. Asimismo, se corrobora una disminución de la oferta de materias optativas.

Seguidamente se realizó un enfoque particular en el plan de estudios de la carrera de CP, consultando si incluye alguna asignatura exclusivamente relacionada a "Seguridad y Control

de Sistemas informáticos" o similar. Solo dos unidades académicas respondieron afirmativamente, siendo las siguientes:

Tabla B: Asignaturas de Seguridad y Control de Sistemas Informáticos por Institución

Nombre de la Universidad	Nombre de la Asignatura
Universidad de Buenos Aires	Auditoría y Control de Sistemas de Información
Univ. Nacional de Córdoba	Auditoria de Sistemas Computarizados

Fuente: elaboración propia

A continuación, se indagó respecto al plan de estudios de la carrera de Licenciado en Administración, preguntando si contiene alguna asignatura exclusivamente relacionada a "Seguridad y Control de Sistemas informáticos" o similar. Ninguna unidad académica respondió afirmativamente, por lo se podría inferir que estas materias se están enfocando a la auditoría contable u operativa y no a la gestión de sistemas informáticos y tecnología.

Se destaca que, del total de las unidades académicas, el 85% manifestaron que la asignatura principal y obligatoria relacionada a "Sistemas y Tecnologías de la Información" contempla solamente una unidad de estudio específica referida a “Seguridad y Control de Sistemas”. Las temáticas desarrolladas en dicha unidad de estudio son las siguientes:

Tabla C: Contenidos de seguridad informática impartidos en otras unidades académicas

Temática sobre Seguridad de la Información	Cantidad de Respuestas
Introducción a la seguridad y el Control Interno	15
Incidentes de seguridad y plan de contingencias	12
Seguridad en los principales recursos tecnológicos de la organización	11
Control interno y auditoría de sistemas	11
Gestión de la seguridad de la Información y buenas prácticas	11
Requerimientos legales y regulaciones de seguridad de la información	9
Desarrollo de una estructura para la seguridad y el control	8
Metodologías de evaluación y gestión del riesgo	8
Tecnologías y herramientas para la seguridad informática	8
Seguridad de la información con colaboradores, proveedores y clientes	4
Política de Seguridad	1

Fuente: elaboración propia

Posteriormente se consultó si existía en cada unidad académica, alguna otra oferta de carreras (exceptuando CP y LA) en donde se impartan asignaturas relacionadas a "Seguridad y Control de Sistemas Informáticos". Se obtuvo como resultado la siguiente información, sobre aquellas que respondieron afirmativamente (25% de las respuestas):

Tabla D: Contenidos sobre TI impartidos en otras carreras de grado

Nombre de la Universidad	Carrera de Grado
Universidad de Buenos Aires	Lic. en Sistemas de Información de las Org.
Universidad Nacional de Salta	Licenciatura en Economía
UNICEN	Licenciatura en Gestión Tecnológica
Universidad Nacional del Comahue	Licenciatura en Sistemas de Información

Fuente: elaboración propia

En relación a si la oferta académica de posgrado cuenta con cursos relacionados a "Seguridad y Control de Sistemas Informáticos, es importante destacar, que el 30% de los docentes encuestados responde desconocer al respecto. El 40% responde afirmativamente y se obtuvo la siguiente información:

Tabla E: Programas de posgrado en donde se imparten conceptos de seguridad informática.

Nombre de la Universidad	Programa de Posgrado
Universidad de Buenos Aires	Maestría / Esp. en Seguridad Informática Maestría / Esp. en Gestión TIC Maestría en Ciberdefensa y Ciberseguridad
Universidad Nacional de Catamarca	Maestría en Contabilidad Superior y Auditoría
Universidad Nacional de Córdoba	Esp. en Contabilidad Superior y Auditoria
Universidad Nacional de Rosario	Esp. en Gestión Estratégica de la TI
Universidad Nacional de Salta	Especialización en Fiscalía Penal Acusatoria
UNICEN	Especialización en Contabilidad y Auditoría

Fuente: elaboración propia

3.2.2 **Análisis de la Segunda Encuesta. Año 2019.**

En el marco de las “XIV Jornadas de Docentes Universitarios en Sistemas y Tecnologías de la Información” realizadas en octubre de 2019, en la Facultad de Ciencias Económicas de la Universidad Nacional de La Plata, se instrumentó una segunda encuesta[60].

El objetivo de la misma, fue relevar la situación actual de las diferentes unidades académicas, respecto a los planes de estudios vigentes y su relación con la formación del alumno sobre “Sistemas y Tecnologías de la Información” en general y, "Seguridad y Control de Sistemas Informáticos" en particular, luego de transcurrida la primera etapa del proceso de acreditación de la Carrera de Contador Público por parte de la CONEAU.

Para ello, se encuestaron representantes de dieciocho Universidades:

1. Universidad de Buenos Aires
2. Universidad Nacional de Catamarca
3. Universidad Nacional de Córdoba
4. Universidad Nacional de Cuyo
5. Universidad Nacional de Jujuy
6. Universidad Nacional de Patagonia “San Juan Bosco”
7. Universidad Nacional de La Plata
8. Universidad Nacional de Lomas de Zamora
9. Universidad Nacional de Rosario
10. Universidad Nacional de Salta
11. Universidad Nacional de San Martín
12. Santiago del Estero
13. Universidad Nacional del Sur

[60] Véase Anexo “E”

14. Universidad Nacional de Tucumán
15. Universidad Nacional del Centro de la Provincia de Buenos Aires
16. Universidad Nacional del Comahue
17. Universidad Nacional del Litoral
18. Universidad Nacional del Nordeste

A continuación, se exponen las principales conclusiones obtenidas:

De las respuestas obtenidas la mayoría pertenecen a estamentos docentes superiores “a cargo de la asignatura”.

Tal como se realizó en la primera encuesta, se consultó si consideran importante el dictado de temas relacionados con "Seguridad y Control de Sistemas Informáticos" en las carreras de CP y LA, para la gestión estratégica de los negocios. En este caso se reafirmó el resultado, contestando la totalidad de manera afirmativa.

Se constató que para dar cumplimiento a la Resolución 3400/17, en lo relativo al área temática "Administración y Tecnologías de la Información" que incluye como contenido mínimo obligatorio el tema “Seguridad en los Sistemas de Información”, se llevaron a cabo las siguientes acciones:

Tabla F: Acciones realizadas para dar cumplimiento a la Resolución 3400/17

Acción realizada	**%**
El tema ya se encontraba incluido en alguna de las asignaturas	70%
No sabe / No Conoce	17%
Se realizaron modificaciones para incluir el tema	13%
Total general	100%

Fuente: elaboración propia

En la Tabla “F” se evidencia que la amplia mayoría sigue manifestando que la temática en cuestión ya se encontraba incluida en alguna asignatura del plan de estudios de la carrera de

CP. Esto nos permite inferir que el tema ya era percibido como un requerimiento para el perfil profesional, antes que surgiera la exigencia de la normativa.

Respecto de unidades académicas que realizaron modificaciones para incluir el tema (13%), se corrobora que las acciones realizadas fueron:

Tabla G: Modificaciones realizadas para incluir la temática

Acciones realizadas	%
El tema fue incluido dentro de la materia principal de TI / SI	50%
El tema fue incorporado en otra asignatura, no relacionada con la disciplina TI / SI.	25%
Se modificó la condición de optativa a obligatoria de una materia de la carrera CP	25%

Fuente: elaboración propia

En la tabla "G" se puede observar que en su mayoría, las Cátedras del área "Administración y Tecnologías de la Información" incluyeron el dictado de la temática.

Partiendo de lo general a lo particular, se consultó sobre la ponderación otorgada a la formación, respecto a "Sistemas y Tecnologías de la Información", considerando el plan de estudio vigente, posterior al proceso de acreditación para la carrera de CP. Las respuestas fueron las siguientes:

Tabla H: Ponderación otorgada a la formación en S y TI para la carrera de CP

Respuesta	%
Insuficiente	50%
Suficiente	47%
No Sabe / No Conoce	3%
Total general	100%

Fuente: elaboración propia

La tabla "H" nos muestra que la mitad de los encuestados considera que la formación en Sistemas y Tecnologías de la Información es insuficiente.

Los resultados de la misma consulta, pero en relación a la carrera de LA, son los siguientes:

Tabla I: Ponderación otorgada a la formación en S y TI para la carrera de LA

Respuesta	%
Insuficiente	33%
Suficiente	53%
No Sabe / No Conoce	13%
Total general	100%

Fuente: elaboración propia

En la tabla "I" se observan que la respuesta "insuficiente" se reduce a un tercio de los encuestados.

Se indagó sobre como evalúan la formación en "Seguridad y Control de Sistemas Informáticos" en la carrera de CP, teniendo en cuenta que esta temática forma parte de los contenidos curriculares mínimos obligatorios indicados por la Resolución 3400/17. Las respuestas fueron las siguientes:

Tabla J: Ponderación otorgada a la formación en S y C TI en CP

Respuesta	%
Insuficiente	53%
Suficiente	37%
No Sabe / No Conoce	10%
Total general	100%

Fuente: elaboración propia

Más de la mitad de los encuestados manifiesta que la formación en la temática considerada como contenido curricular mínimo obligatorio en la carrera, es insuficiente. Cabe destacar que un 10% de las respuestas indican un desconocimiento del tema.

La misma pregunta, pero respecto a la carrera de Licenciatura en Administración, brinda las siguientes respuestas:

Tabla K: Ponderación otorgada a la formación en S y C TI en LA

Respuesta	%
Insuficiente	50%
Suficiente	27%
No Sabe / No Conoce	23%
Total general	100%

Fuente: elaboración propia

La situación observada en la tabla "J" se repite en el caso de LA.

En su amplia mayoría, los docentes encuestados consideran que para ambas carreras, la formación actual respecto a "Seguridad y Control de Sistemas informáticos" es insuficiente. Este aspecto debería ser considerado, dado el ámbito altamente informatizado donde se desenvuelven los futuros egresados.

Respecto de la solicitud de su nivel de acuerdo respecto a la siguiente frase: "en la Argentina, no hay suficientes profesionales capacitados en aspectos sobre seguridad informática para la Dirección y Gestión de las Organizaciones". Las respuestas fueron las siguientes:

Tabla L: Profesionales capacitados en Argentina en Seguridad Informática

Respuesta	%
Muy de acuerdo	27%
De acuerdo	40%
Poco de acuerdo	27%
Nada de acuerdo	7%
Total general	100%

Fuente: elaboración propia

Las dos terceras partes de los encuestados están de acuerdo con la frase indicada precedentemente.

Respecto a la pregunta: "consideran que el alumno de CP debería necesariamente recibir formación en su carrera de grado sobre "S y C SI para efectuar tareas de auditoria", se obtuvieron las siguientes respuestas:

Tabla M: Formación del CP en aspectos de S y C SI para Auditoría

Respuesta	%
Muy de acuerdo	40%
De acuerdo	50%
Poco de acuerdo	7%
Nada de acuerdo	3%
Total general	100%

Fuente: elaboración propia

El 90% de las respuestas indican un nivel de acuerdo respecto a la necesidad de formación en aspectos de seguridad informática para la realización de labores profesionales de auditoría.

Respecto de considerar que la formación sobre "Seguridad y Control en Sistemas Informáticos" permitiría al graduado en Ciencias Económicas ampliar su ámbito de incumbencia profesional. Las respuestas obtenidas fueron las siguientes:

Tabla N: Incumbencia profesional del CP con la formación en S y C SI

Respuesta	%
Muy de acuerdo	33%
De acuerdo	43%
Poco de acuerdo	17%
Nada de acuerdo	7%
Total general	100%

Fuente: elaboración propia

Ante una profesión contable que actualmente se encuentra interpelada debido al fuerte impacto de las tic´s, tres cuartas partes de los encuestados están de acuerdo en que la formación del profesional en Ciencias Económicas en temas de seguridad informática, permitiría ofrecer servicios profesionales relacionados a la temática.

La consulta sobre si la formación en "Seguridad y Control en Sistemas Informáticos", otorgaría al graduado de su unidad académica, un perfil profesional diferencial respecto a la de otras ofertas académicas de la región, proporcionó las siguientes respuestas:

Tabla O: Perfil diferencial del graduado en Ciencias Económicas

Respuesta	%
Muy de acuerdo	30%
De acuerdo	50%
Poco de acuerdo	20%
Nada de acuerdo	0%
Total general	100%

Fuente: elaboración propia

La amplia mayoría considera que la formación en “Seguridad y Control de Sistemas Informáticos” brindaría un diferencial a sus graduados respecto a otras unidades académicas.

3.2.3 **Conclusiones preliminares sobre el Análisis de la Encuesta.**

La realización de las encuestas a miembros de DUTI representantes de diferentes Universidades Nacionales, nos permitió tener un mayor conocimiento respecto al abordaje de la disciplina a nivel nacional y nos posibilitó intercambiar información relacionada con planes de estudios.

Se destaca que la totalidad de los encuestados consideró de suma importancia el dictado de temas relacionados con "Seguridad y Control de Sistemas Informáticos" en las carreras de CP y LA, para la gestión estratégica de negocios, lo cual conforma un dato muy relevante a tener en cuenta en el desarrollo de este trabajo. Sin embargo se verifica que en la mayoría de las Facultades de Ciencias Económicas se imparte esta temática dentro de los contenidos de la materia principal de TI y no se cuenta con una asignatura específica que profundice este espacio de conocimiento.

3.3 Situación: Facultad de Ciencias Económicas de la UNT

3.3.1 **Misión, Visión, Principios y Valores**

La Facultad de Ciencias Económicas de la UNT tiene más de setenta años de trayectoria institucional. Fue fundada por Ley Nº 13.050, del 29 de setiembre de 1947, cumpliendo con la previsión del proyecto del Dr. Juan B. Terán que contemplaba una sección de estudios comerciales para la Universidad, poniendo de manifiesto cuan claro estaba en la sociedad de la época la necesidad de que la organización económica en nuestra región requería personas aptas para interpretar científicamente los fenómenos de nuestra producción y riqueza[61].

La Misión, Visión y Valores de la FACE están estrechamente ligados con los de la Universidad Nacional de Tucumán, por pertenecer a esta última. Las mismas se detallan a continuación:

3.3.1.1 *Misión*

"Promover la excelencia académica y la formación de profesionales competentes en el campo de las Ciencias Económicas, capaces de generar y liderar cambios, con valores éticos necesarios para contribuir a un desarrollo socioeconómico sostenible".

3.3.1.2 *Visión*

"Constituirnos como una institución académica de prestigio en las Ciencias Económicas con proyección nacional e internacional, formando profesionales que contribuyan al desarrollo, transformación y crecimiento de la sociedad"[62].

3.3.1.3 *Principios y Valores*

- Equidad para la consecución de los objetivos
- Respeto entre los miembros de la Comunidad de la FACE-UNT y hacia la Sociedad.

---

[61] Resolución N° 542- HCD-18. Plan de Desarrollo de la carrera de Contador Público. Facultad de Ciencias Económicas, UNT. Publicada el 28 de noviembre de 2018.

[62] Resolución 173D18: *Misión, Visión y Valores de la FACE*. Facultad de Ciencias Económicas, Universidad Nacional de Tucumán. Publicada el 23 de abril de 2018.

- Conducta Ética y Profesional en el desarrollo de las actividades de cada miembro de nuestra Comunidad de la FACE-UNT
- Innovación para estar a la vanguardia del conocimiento.
- Inclusión como herramienta de contención.
- Compromiso Social para contribuir al desarrollo, transformación y crecimiento de la Sociedad.
- Excelencia académica para lograr estándares de alta calidad en docencia, investigación, extensión y gestión.

Se destaca que la FACE buscar promover la excelencia académica y la formación de profesionales competentes en el campo de las Ciencias Económicas, constituyéndose como una institución de prestigio, con proyección nacional e internacional, considerándose fundamental el principio de "innovación", para estar a la vanguardia del conocimiento.

Para ello ha presentado un "Plan Estratégico Institucional 2019-2022" [63], en donde se plantean las perspectivas y ejes transcendentales, como una herramienta de gestión que permitirá trabajar en base a estrategias, para el desarrollo de la visión planteada. Por su relevancia, se transcribe un párrafo del "análisis del entorno" que se realiza en el mencionado documento: "*el acelerado proceso de difusión de las tecnologías de la información y de las comunicaciones a nivel global se asocia a profundas transformaciones en el modo de operar de los sistemas productivos, económicos, sociales y culturales. La cantidad de información disponible, el desdibujamiento de los límites de tiempo y espacio, la creación de redes y el intercambio de conocimiento, entre otros aspectos, representan una revolución en los modos de funcionamiento social nunca antes visto*". Esta afirmación indica que la institución es consciente del fuerte impacto que tienen las TIC en el modo de dirigir, administrar y operar las

[63] Resolución N° 093-HCD-19. "Plan Estratégico Institucional 2019-2022". Facultad de Ciencias Económicas, UNT. Publicado el 12 de abril de 2019.

organizaciones en la actualidad. Además, considera que el contexto económico, social y tecnológico está provocando cambios a los que debe adaptarse. Asimismo, se percata que la rapidez actual en la transferencia de conocimientos genera una demanda de formación continua cada vez mayor por parte de los profesionales y las organizaciones.

3.3.2 **Espacio epistemológico: Sistemas de Información.**

Los programas de estudio de las carreras de Contador Público y Licenciatura en Administración de la FACE de la UNT, contienen en su diseño curricular una materia principal y obligatoria sobre Sistemas y Tecnologías de la Información denominada "Sistemas de Información I", de 83 horas de carga horaria total, dividida en 6 horas semanales entre clases teóricas y prácticas, ubicada en el primer cuatrimestre de segundo año de la currícula.

El programa de la asignatura, incluye conceptos y elementos teóricos y prácticos que le permiten al futuro egresado aprender, internalizar y comprender los aspectos epistemológicos relacionados a los Sistemas y las Tecnologías de información en el ambiente de las organizaciones y los negocios, considerando que los mismos deberán actuar en ambientes altamente informatizados. Asimismo, brinda las competencias para comprender y desarrollar modelos en distintas herramientas informáticas[64].

Los objetivos generales planteados para esta asignatura se detallan a continuación:

a) Conocer, comprender e internalizar los conceptos relacionados con los sistemas de información y las características de la información que brindan.

b) Conocer las tecnologías de información y como coadyuvan a la toma de decisiones y a la gestión organizacional.

c) Concientizar sobre la ética y la seguridad en el manejo de la información.

---

[64] Masclef, M. A. (2018). Programa de Asignatura: "Sistemas de Información I", para el período lectivo 2019. Instituto de Administración, Facultad de Ciencias Económicas, Universidad Nacional de Tucumán.

d) Propiciar que el alumno se apropie de una jerga epistemológica que le será de utilidad en el resto de las materias de la currícula y en su ejercicio profesional.

e) Integrar los conocimientos con los de otras materias fomentando la transferencia de conceptos.

f) Utilizar aplicaciones para el desarrollo de modelos por medio de aplicativos informáticos.

Se enfatiza que el tercer objetivo general de la materia, plantea a la seguridad en el manejo de la información, como un concepto que debe ser aprendido e internalizado por el alumno para alcanzar aquellos conocimientos que se consideran fundamentales para la formación del perfil profesional del futuro egresado.

Conforme la Resolución 1271/2018[65] que aprueba el plan de estudio, los contenidos mínimos propuestos para la asignatura, son los siguientes:

a) Fundamentos de los sistemas de información en los negocios.

b) Aspectos tecnológicos de los medios de procesamiento y comunicaciones: hardware, software, bases de datos y telecomunicaciones.

c) Aplicaciones empresariales

d) Metodología de análisis, diseño e implementación de los sistemas de información.

e) Evaluación de sistemas aplicativos.

f) Seguridad de los sistemas de información

g) Aspectos éticos y sociales de los sistemas de información

Es destacable que la materia "Sistemas de Información I" plantea como contenido mínimo obligatorio a la "seguridad de los sistemas de información", temática que es abordada necesariamente dentro del programa de la asignatura. Esto nos permite inferir que el tema es

[65] Resolución 1271/2018 HCS. Aprobación del nuevo plan de estudios de la carrera de Contador Público, plan 2018. Universidad Nacional de Tucumán, Tucumán 29 de noviembre de 2018.

percibido por los responsables de la cátedra como importante y necesario en la formación del graduado en ciencias económicas, dentro de la disciplina de los sistemas y la administración.

3.3.3 **Asignaturas electivas: Carrera de Contador Público.**

Además de la materia principal y obligatoria, la carrera de CP cuenta actualmente con una asignatura optativa denominada "Sistemas de Información II", de 63 horas. Para cursarla, el alumno debe contar con un mínimo de 20 materias aprobadas, entre los cuales se encuentran "Sistemas de Información I" y "Sistemas Administrativos y Control Interno I"

Considerando el perfil del graduado generalista de amplio alcance, con una especialización técnico – funcional, la asignatura proporciona al futuro egresado conceptos avanzados y formación sobre nuevas tendencias relacionadas a los Sistemas y las Tecnologías de información en el ambiente de las organizaciones y los negocios, permitiendo el conocimiento de nuevos modelos de negocios e ingresos y estrategias de comercialización que se generan a partir de la aplicación de tecnologías. Brinda además las competencias para diseñar e implementar estrategias de sistemas y tecnología, tanto en empresas tradicionales como en *startups* tecnológicas. Proporciona herramientas conceptuales para tomar decisiones respecto de la contratación de software, infraestructura, o plataformas como servicio[66].

La asignatura plantea como contenidos mínimos obligatorios los siguientes temas:

a. Estrategia, Sistemas de Información y Tecnología: Impacto de los Sistemas de Información y la tecnología sobre las organizaciones y empresas de negocios. Sistemas y Tecnologías para lograr ventajas competitivas. Usos estratégicos.

b. Cómputo en Nube: aspectos técnicos. Aspectos del negocio. Modelos de Entrega de Servicios en la Nube: IaaS, PaaS y SaaS.

c. Big Data: definición, aplicaciones, beneficios, desventajas.

---

[66] Masclef, M.A. (2018). Programa de Asignatura: "Sistemas de Información II", para el período lectivo 2019. Instituto de Administración, Facultad de Ciencias Económicas, Universidad Nacional de Tucumán.

d. Comercio electrónico: características. Infraestructura tecnológica. Plataformas de comercio electrónico. Pasarelas y plataformas de pago. Comercio móvil. Desafíos en la implementación: técnicos y de negocios.

e. Modelos de Negocios y Modelos de Ingresos en Internet: Mercados de larga cola: demanda, almacenamiento y recomendación. Modelos de Negocios creados sobre productos / servicios gratuitos.

f. Metodología *Lean Startup*: Pivotaje. Desarrollo de Clientes (*Customer Development*). Experimentos. Prototipos. Producto Mínimo Viable (MVP)[67].

Se observa que este curso propicia un ámbito de conocimiento específico referido a la tecnología para la gestión de organizaciones y los negocios en internet. Sin embargo, no se tratan aspectos relativos a seguridad y control de sistemas informáticos.

3.3.4 **Asignaturas electivas: carrera Licenciatura en Administración.**

Adicionalmente a la materia principal y obligatoria, la Licenciatura en Administración cuenta con dos materias optativas actualmente implementadas: "Sistemas de Información II", descripta anteriormente y "Análisis y Diseño de Sistemas", de 63 horas.

Esta última asignatura justifica su relación con el perfil profesional del graduado de la siguiente manera: "*Los profesionales en ciencias económicas en algún momento del ejercicio de su profesión, muy probablemente participen en un proyecto de desarrollo o implementación de sistemas, ya sea como usuarios, administradores de una unidad de negocios, como líderes de un equipo de proyecto, miembros del departamento de SI o tal vez incluso como Gerentes del Departamento Sistemas y Tecnologías de Información. Entender el ciclo de vida, nuevas metodologías, herramientas y técnicas del desarrollo de sistemas, así como tener la capacidad para su aplicación, garantizan el éxito de los proyectos de desarrollo en que participe. Un*

[67] Resolución 1271/2018 HCS. Aprobación del nuevo plan de estudios de la carrera de Contador Público, plan 2018. Universidad Nacional de Tucumán, Tucumán 29 de noviembre de 2018.

aspecto fundamental de la formación, lo constituye el creciente requerimiento de profesionales en ciencias económicas para cubrir cargos de analistas funcionales, dentro de organizaciones o empresas que se dedican al desarrollo de software.

En todos estos sentidos, la materia proporciona conceptos avanzados, metodologías actuales y el entrenamiento en el análisis y diseño de un sistema real, en este trabajo, se complementa la teoría con modelos que se van desarrollando según el tipo de problema u oportunidad que el alumno presenta. Es decir que se trata de una práctica, tal como se presentará en el ejercicio profesional"[68].

La misma plantea contenidos mínimos a dictarse en el cursado, los cuales se detallan a continuación:

a) Desarrollo de sistemas y cambio organizacional.

b) Rediseño de procesos de negocios.

c) Metodologías de desarrollo: El ciclo de vida de los sistemas, Prototipos, Paquetes de Software y Outsourcing.

d) Desarrollo por usuario Final, Metodologías Agiles de Desarrollo, Desarrollo basado en componentes y servicios web. Metodología: Diagnóstico, Factibilidad.

e) Diseño lógico, Diseño físico, Programación, Implementación. Análisis funcional.

f) Administración de Proyectos de Tecnologías de la Información. El rol del Profesional en Ciencias Económicas[69].

Por lo tanto, se concluye que la asignatura otorga formación en metodologías para el análisis y diseño de sistemas de información. No se explicita en su programa que se impartan conceptos

[68] Masclef, M.A. (2018). Programa de Asignatura: "Análisis y Diseño de Sistemas / Computación II". Instituto de Administración, Facultad de Ciencias Económicas, Universidad Nacional de Tucumán.

[69] Resolución 2075/2013 HCS. Aprobación del plan de estudios de la Licenciatura en Administración plan 2014. Universidad Nacional de Tucumán, Tucumán, 20 de septiembre de 2013.

relativos a seguridad y control, sin embargo, estos constituyen requisitos inherentes al diseño, en donde entran en consideración.

3.3.5 **Otras consideraciones relevadas en la Institución.**

Respecto a la oferta de posgrado, se constata que la unidad académica, hasta el año 2019, no contaba con ninguna carrera en donde se impartan cursos relacionados con "Seguridad y Control de Sistemas Informáticos".

Se verifica que en el año 2020 comenzó el dictado de una nueva carrera de posgrado: "Especialización en Auditoría y Contabilidad"[70]. En el plan de estudios de la misma, se observa un curso ubicado en el segundo cuatrimestre de segundo año, denominado "Seguridad Informática", de solo 20 horas de duración, siendo este, el único curso relacionado con esta temática, hasta el momento, en carreras de posgrado ofrecidas en la FACE UNT.

3.3.6 **Conclusiones preliminares sobre el Espacio epistemológico: Sistemas de Información".**

Se pudo constatar que la FACE cuenta actualmente con un espacio disciplinar de "Sistemas y Tecnologías de la información" perteneciente al Instituto de Administración. El mismo está formado por una materia principal y obligatoria en donde se imparten conceptos generales e introductorios en la temática. Esta asignatura cuenta con una unidad donde se imparten conceptos amplios pero básicos referidos a la seguridad informática. La cantidad de contenidos que se dictan, no posibilita una mayor profundización y la ubicación de la materia en la currícula trae aparejado un alumnado que no aún no adquirió una madurez y una base conceptual que permita la aprehensión de estas conceptualizaciones.

En el rol de vigilancia epistemológica que les cabe a los responsables de la disciplina y de las competencias e incumbencias profesionales que se esperan de los egresados de las carreras

[70] Facultad de Ciencias Económicas (27/09/2019). Inician las inscripciones para la Especialización en Auditoría y Contabilidad. Recuperado el 27 de septiembre de 2019 de https://face.unt.edu.ar

de Ciencias Económicas, se han implementado un conjunto de asignaturas que coadyuvan a la formación en Sistemas y Tecnologías de la Información. Esto se logra, introduciendo los conceptos disciplinares y herramentales, conocimientos que se amplían, complementan y re contextualizan posteriormente, profundizando aspectos de mayor complejidad y abordando las últimas tendencias en una disciplina caracterizada por lo creciente, complejo y volátil de sus cambios y las oportunidades que representa para los profesionales y las organizaciones. Es por ello que este espacio disciplinar también cuenta con las dos materias optativas anteriormente descriptas en donde se retoman, recontextualizan y amplían temas abordados en la materia principal.

En este contexto se considera que la asignatura de "Seguridad y Control de Sistemas Informáticos", brindaría conocimientos y competencias que permitirían completar la formación del graduado en lo que refiere a sistemas y tecnologías de información.

Por último, se hace referencia a que la FACE tiene la oportunidad potencial de desarrollar una propuesta de posgrado relacionada a la temática abordada, dadas las exigencias demandadas por el mercado regional y la escasa oferta de formación local y regional al respecto.

3.4 Acreditación de la Carrera de Contador Público en todas las Universidades del país[71]

3.4.1 **Antecedentes.**

En el año 2013, de acuerdo al plenario N° 122 del Consejo de Universidades y la Resolución Ministerial N° 1723, se incluyó a la carrera de Contador Público en el régimen del artículo 43 de la Ley de Educación Superior. El mismo establece que los planes de estudio de carreras correspondientes a profesiones reguladas por el Estado, cuyo ejercicio pudiera comprometer el

[71] Resolución 3400-E/2017. Ministerio de Educación de la Nación. República Argentina, Ciudad de Buenos Aires, aprobada el 08/09/2017.

interés público, poniendo en riesgo de modo directo la salud, la seguridad o los bienes de los habitantes, deben tener en cuenta la carga horaria mínima, los contenidos curriculares básicos y los criterios sobre intensidad de la formación práctica que establezca el Ministerio de Educación en acuerdo con el Consejo de Universidades. Asimismo, entre otros aspectos, se establece que la carrera debe ser acreditada periódicamente por la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU)[72].

A partir de ello, en septiembre de 2017 y tras la aprobación de la propuesta para tal fin por el Consejo Interuniversitario Nacional, se aprobó la Resolución 3400/17 que establece los contenidos curriculares básicos, la carga horaria mínima, los criterios de intensidad de la formación práctica y los estándares para la acreditación de la carrera correspondiente al título de Contador Público, así como la nómina de actividades reservadas para quienes hayan obtenido el respectivo título. Asimismo, se implantó un plazo máximo de doce meses para que los establecimientos universitarios adecuen sus carreras de grado de Contador Público a las disposiciones precedentes.

La Resolución antes mencionada contiene un anexo[73] que la reglamenta. Teniendo en cuenta el objeto problema de este trabajo, se destacan los aspectos desarrollados a continuación, por considerarse relevantes:

Dentro del área temática "Administración y Tecnologías de la Información" contempla como contenidos curriculares básicos y obligatorios, entre otros a:

a) Metodología de análisis, diseño e implementación de Sistemas de Información.

b) Aspectos tecnológicos de los medios de procesamiento y comunicaciones: utilización de software de base, utilitarios y redes

[72] Ley de Educación Superior N° 24.521. República Argentina. Sancionada el 20/07/1995 y promulgada el 07/08/1995 B.O.

[73] Anexo I, II, III y IV de Resolución 3400-E/2017. Ministerio de Educación de la Nación. República Argentina, Ciudad de Buenos Aires, 20/07/2017.

c) Evaluación de sistemas aplicativos

d) Seguridad en los sistemas de información

Los contendidos curriculares mínimos son considerados esenciales y deben cubrir la matriz básica de los lineamientos curriculares y planes de estudios. Estos se expresan en función de la información conceptual y teórica considerada imprescindible, teniendo en cuenta las competencias que se desean lograr.

En este aspecto y según la información relevada y analizada en el espacio epistemológico de la disciplina de los Sistemas de Información[74] se puede afirmar que la FACE da cumplimiento a la exigencia de la normativa en la materia principal y obligatoria "Sistemas de Información I", en la cual se imparten nociones generales al respecto. Luego estos conceptos, con excepción al punto "d", se profundizan y recontextualizan en las asignaturas optativas actualmente implementadas.

En este apartado nos detenemos en el último ítem "d) Seguridad en los Sistemas de Información", el cual establece específicamente que es un contenido curricular básico y obligatorio para la formación del Contador Público. Por lo tanto, se considera que no es suficiente la instrucción otorgada en la materia del ciclo básico, sino que se requiere una profundización al respecto, que permita madurar y analizar con mayor detalle la problemática de las organizaciones y los negocios actuales bajo el ámbito de la seguridad de la información, como diferencial estratégico para sobrevivir en un entorno sumamente competitivo.

Por otra parte, se destaca que en la Resolución se establece un total de 600 hs., para las áreas de "Administración, Tecnologías de la Información y Economía". Ello representa un cuarto del total de carga horaria mínima para la formación teórica y práctica de la carrera (2700 hs.).

[74] Véase punto 3.3 del capítulo N° 3

Otro aspecto estudiado en este documento y en el que se hace referencia, son las actividades profesionales reservadas para el CP. Teniendo en cuenta el ámbito del presente trabajo, se realiza un análisis de las siguientes:

- *"Diseñar, dirigir e implementar sistemas de información (...)":* dado el ámbito altamente informatizado de desempeño de los profesionales en Ciencias Económicas, se hace indispensable la formación en competencias de control y seguridad informática para el correcto diseño, dirección e implementación de Sistemas de Información.

- *"Dirigir y realizar procedimientos de auditoría (...)":* la tecnología y los sistemas de información han experimentado avances notables y han impactado fuertemente en el desempeño y las formas de estructurar, administrar y conducir las organizaciones. Por lo tanto, se torna de vital importancia para el profesional de Ciencias Económicas, contar con conocimientos suficientes para realizar una valoración de riesgos informáticos, analizar los objetivos y alcances de una auditoría de recursos de TI y diseñar e implementar la metodología para efectuarla.

3.4.2 **Conclusiones preliminares sobre la "Acreditación de la Carrera de Contador Público en todo el país".**

Se constató que para dar cumplimiento a la resolución 3400/17, en la FACE UNT se realizaron modificaciones en el programa de estudios de la materia principal y obligatoria, y como consecuencia se produjeron cambios en las optativas ofrecidas por la disciplina.

Asimismo, es importante aclarar en este punto, que en la encuesta a los integrantes de DUTI se indagó sobre las acciones realizadas por cada cátedra para dar cumplimiento al requerimiento de la CONEAU para la acreditación de la carrera de CP. Se obtuvieron las siguientes respuestas:

Tabla P: Accionar de la cátedra tras el requerimiento de la Resolución 3400/17

Acción realizada por la Cátedra	% del total
El tema ya se encontraba incluido en el plan de estudios	70%
Se realizaron modificaciones para incluir el tema	17%
No sabe / No Conoce	13%
Total de respuestas:	**100.00%**

Fuente: elaboración propia

En la tabla "P" se evidencia que la amplia mayoría manifiesta que la temática en cuestión ya se encontraba incluida en el plan de estudios de la carrera de CP. Esto nos permite inferir que esta ya era percibida como una necesidad para el perfil profesional, antes que surgiera la exigencia de la norma.

Por otra parte, se pudo constatar que la FACE, debido a la importancia que comporta el Proceso de Autoevaluación Institucional para la acreditación de la carrera de CP, decidió la creación de una Comisión Permanente, con el objetivo principal de abordar los requerimientos de este proceso y generar los mecanismos necesarios para lograr la participación activa de toda la comunidad[75].

Finalmente, se aprovecha este apartado para hacer mención que en las Jornadas DUTI, llevadas a cabo en la UBA en el año 2018 se consideró propicio el ámbito para el desarrollo de una mesa panel sobre "Acreditación de la Carrera de Contador Público". En la misma fueron expositores docentes de algunas unidades académicas seleccionadas, abriendo posteriormente un enriquecedor debate respecto a los contenidos de TI, que a criterio del claustro, debían formar parte de la currícula de esta carrera. Se concluyó, entre otros aspectos que Seguridad Informática, es un contenido que debe estar presente indefectiblemente en la formación del profesional en Ciencias Económicas. Se hace mención a que dicha mesa panel contó con la

[75] "Se reunió la Comisión Permanente para el Proceso de Autoevaluación Institucional de nuestra Facultad" (12/04/2019). En sitio web de la Facultad de Ciencias Económicas, recuperado el 15 de abril de 2019.

participación de la Prof. Alejandra Masclef, directora de esta Tesis de Maestría, en representación de la FACE de la UNT.

3.5 Aprobación del Nuevo Plan de Estudios de la Carrera de CP en la UNT

3.5.1 **Generalidades.**

Considerando lo expresado en la Resolución Ministerial anteriormente analizada, la FACE de la UNT, realizó un proceso de revisión de su plan de estudio vigente para la carrera de Contador Público, con el objetivo de efectuar las adecuaciones correspondientes a fin de ajustarse a lo establecido en ella. Como resultado de este procedimiento, se propuso un nuevo plan de estudio con una estructura curricular más equilibrada y coherente al perfil profesional de acuerdo a lo requerido por el Ministerio de Educación de la Nación en particular y a las exigencias de la sociedad en general.

Por lo tanto, mediante la Resolución 463/2018[76], se aprobó el "Plan de Estudios 2018" para la carrera de Contador Público, elevándolo a consideración del Honorable Consejo Superior (HCD) de la Universidad Nacional de Tucumán[77]. Según establece, este plan entrará en vigencia en el período lectivo inmediato posterior a su aprobación, año 2019.

3.5.2 **Antecedentes del Plan de Estudios 2018.**

Hace varios años, en la FACE se venía generando un movimiento de docentes, estudiantes, egresados y autoridades que percibía la necesidad de replantear el plan de estudios vigente y la formación impartida, con la finalidad de actualizar los contenidos y metodologías de enseñanza de las asignaturas, en relación al avance del conocimiento y de las nuevas técnicas y tecnologías que el mercado requiere. Por lo que se realizaron modificaciones en el plan de estudio 1983, mediante la aprobación del Plan 2010 y posteriormente en el año 2013 se generó una propuesta

[76] Resolución 463HCD18. Expte. 56.380/18 Facultad de Ciencias Económicas, UNT. San Miguel de Tucumán, 29 de octubre de 2018.

[77] Resolución 1271 HCS. Expte. 56.380/018. Honorable Consejo Superior de la Universidad Nacional de Tucumán, del 27 de noviembre de 2018.

con modificaciones. Estas últimas produjeron cambios de forma, no de fondo y solucionaron inconvenientes que habían sido observados en la implementación del plan de estudios planteado.

3.5.3 **Diseño curricular.**

Para el nuevo plan de estudios, se definió una duración de carrera de cinco años, con treinta materias obligatorias y dos optativas, las cuales pueden ser elegidas por el alumno de un grupo variado de asignaturas propuestas, lo que le permitirá adquirir una formación más profunda en la orientación de su preferencia y le facilitará la articulación en carreras de posgrado.

Además, dicha resolución establece que las materias optativas planteadas deben contribuir a la formación del alumno en competencias claramente definidas, respondiendo al perfil del graduado establecido.

3.5.4 **Propuesta de reformulación académica.**

La organización del plan de estudios 2018, responde a criterios firmes de amplio espectro, que incorpora los cambios ocurridos en el mercado, especialmente en las disciplinas de franco e impactante desarrollo, como son las nuevas tecnologías de información. Por tal motivo, se evidencia que la asignatura propuesta sobre “Seguridad y Control de Sistemas Informáticos”, da respuesta a un área de vacancia disciplinar, que no estaba siendo considerada en los anteriores planes de estudio de la carrera.

Por otra parte, dentro de los objetivos específicos planteados en este plan de estudios para la carrera, se resalta la adquisición por parte del egresado de una adecuada capacitación en la técnica contable para aplicarla al diseño e implementación de sistemas de información y de control.

3.5.5 **Organización del nuevo Plan de Estudios.**

El plan de estudios está integrado por asignaturas pertenecientes a las siguientes áreas temáticas: contabilidad e impuestos; economía; jurídica; administración y tecnologías de la

información; matemática y humanística. Se observa que el área de "Tecnología de la información" ha adquirido un vasto espacio curricular independiente y determinado.

3.5.6 **Entrevista a Docentes intervinientes en la aprobación del nuevo Plan.**[78]

Para una toma de conocimiento más exhaustiva de la situación, se entrevistaron a docentes intervinientes en el proceso de diseño y aprobación del nuevo plan de estudios de la carrera de Contador Público. Específicamente a representantes de la "Comisión de Implementación y Seguimiento del Plan de Estudios de Contador 2018" y a miembros del "Honorable Consejo Directivo de la Facultad de Ciencias Económicas UNT", quienes participaron en el proceso de debate y aprobación de este programa de estudios.

Se aclara que la "Comisión de implementación y Seguimiento del Plan de Estudios", es un órgano asesor del Decano, encargado de diseñar estrategias de seguimiento y regulación que acompaña la implementación de los cambios curriculares. El trabajo de esta ella, impacta favorablemente en la carrera, al poner en práctica sistemáticamente acciones tendientes a mejorar el desarrollo curricular[79].

Del análisis de las entrevistas, se constató que la Resolución Ministerial antes mencionada, exigía una mayor carga horaria en temas relacionados a "Administración" y a "Tecnologías de la Información". Por este motivo se adicionaron horas de clases presenciales a "Sistemas de Información I" y se incorporaron materias optativas de la disciplina, para complementar la formación del estudiante. Estas últimas, fueron planteadas como un espacio de especialización, teniendo en cuenta las áreas de formación reglamentadas por el Ministerio de Educación de la Nación.

---

[78] Véase Anexo "B"

[79] Resolución N° 093-HCD-19. "Plan Estratégico Institucional 2019-2022". Facultad de Ciencias Económicas, UNT. Publicado el 12 de abril de 2019.

Cabe destacar que la Comisión de Implementación del Plan de Estudios considera muy importante la formación en Sistemas y Tecnologías de la Información dentro de este nuevo programa ofrecido.

Todos los encuestados manifestaron que la asignatura de “Seguridad y Control en Sistemas Informáticos” fue bien recibida y que no hubo mayores discusiones para lograr su inclusión y su posterior aprobación definitiva, dada la evidente importancia para el perfil del egresado. Además, consideran que este curso cubre necesidades actuales y futuras, ya que la tecnología de la información tiene una fuerte influencia en todas las labores realizadas por los contadores egresados, especialmente las relacionadas a la auditoría. Así también, afirman que esta asignatura permite a la unidad académica, ofrecer una formación diferencial respecto a otras instituciones de la región.

Se observa que existe consenso respecto a que la materia propuesta permitiría ofrecer un nuevo servicio ante una profesión que actualmente está interpelada. Por lo que, también consideran, que dado el avance de la tecnología y el estado de la economía digital, las asignaturas que actualmente son optativas en el área de “TI”, necesariamente deberían pasar a ser, en un futuro próximo de carácter obligatorio.

3.5.7 **Conclusiones preliminares respecto a la “Aprobación del Nuevo Plan de Estudios de la Carrera de Contador en la UNT”.**

En base al análisis anteriormente expuesto, durante el proceso de reformulación del plan de estudios de la Carrera de CP, la cátedra de “Sistemas de Información I”, presentó la propuesta de inclusión de una asignatura sobre Seguridad y Control de Sistemas Informáticos, para ser incorporada como curso optativo para las carreras de Contador Público y Licenciatura en Administración. La misma fue aprobada para formar parte de ambas carreras, valorándose como positivos todos los aspectos desarrollados en la propuesta, desde el punto de vista de las

exigencias ministeriales y los requerimientos técnicos que demanda el mercado laboral y de los negocios actuales.

3.6 Próxima acreditación de la Carrera de Licenciatura en Administración

Actualmente la carrera de Licenciatura en Administración no está transitando un proceso de acreditación por la CONEAU.

Dada la tendencia global, es de esperar que el nuevo perfil del egresado exija fuertes competencias en sistemas y tecnologías de la información para la gestión de las organizaciones en entornos altamente informatizados. Entre ellos, muy probablemente, estarán presentes conceptos y problemáticas propias del ámbito de la seguridad informática, como ser: diseño e implementación de una estrategia corporativa bajo el ámbito de la Seguridad Informática; metodologías para la evaluación y gestión del riesgo; certificación de estándares internacionales de resguardo de la seguridad de la informaron; seguridad de la información en relación a los RRHH; diseño y puesta en marcha de planes de contingencia, de recuperación ante desastres y de continuidad de negocio, entre otros.

3.7 Planes de estudios analizados para el desarrollo del programa de asignatura

Para finalizar con este capítulo, a continuación se detallan los programas de estudios relativos a la temática que fueron consultados y analizados en conjunto con la bibliografía de la disciplina, para la elaboración del programa de asignatura propuesto en este trabajo.

a) Programa de Asignatura: Auditoría y Control de los Sistemas de Información – Facultad de Ciencias Económicas, UBA[80]

[80] BRIANO, Juan Carlos y otros (2006). Programa de Asignatura: Auditoría y Control de Sistemas de Información (Materia N° 659). Departamento de Sistemas. Carrera de Licenciado en Sistemas de Información de las Organizaciones. Facultad de Ciencias Económicas, Universidad de Buenos Aires.

b) Programa de Asignatura: Seguridad, Control y Auditoría de Sistemas – Especialización en Gestión Estratégica de las Tecnologías de la Información, UNR[81]

c) Programa de estudios: Maestría en Seguridad Informática – Facultad de Ciencias Económicas Facultad de Ciencias Ingeniería y Ciencias Exáctas, UBA[82]

d) Programa de estudios: Diplomatura en Seguridad de la Información – UCASAL, AGASI y Fundación Libertad[83].

e) Programa de estudios: Diplomatura en seguridad de la información – Cibercrimen – Universidad Siglo XXI[84]

f) Programa de estudios: Master en Seguridad de la Información y Continuidad de Negocios. EADIC y Universidad Católica San Antonio de Murcia, España. [85]

g) Programa de estudios: Master en Ciberseguridad – Deloitte, IMF *Business School* y Universidad Camilo José Cela[86]

h) Programa de Estudios: Experto Universitario en Ciberseguridad y Protección de Sistemas - Deloitte, IMF *Business School* y Universidad Camilo José Cela[87]

---

[81] Programa de Asignatura "Seguridad, Control y Auditoria de Sistemas" de la carrera de posgrado "Especialización en Gestión Estratégica de la Tecnología. Facultad de Ciencias Económicas, Universidad Nacional de Rosario. Aprobado por: Resolución no14385-C.D. del 19-12-2006

[82] Programa de estudios: Maestría en Seguridad Informática. Sitio web de la Maestría en Informática de la UBA.

[83] Programa de estudios: Diplomatura en Seguridad de la Información (s.f.). Sitio web de la Diplomatura en Seguridad de la Información. Universidad Católica de Salta.

[84] Programa de estudios: Diplomatura en seguridad de la información – Cibercrimen (s.f.). Sitio web de la Universidad Siglo XXI:

[85] Programa de estudios: Master en Seguridad de la Información y Continuidad de Negocios (s.f.) Sitio web de. EADIC.

[86] Programa de estudios: Master en Ciberseguridad Sitio web del Master en Seguridad Informática (s.f). Sitio Web de IMF *Business School*.

[87] Programa de Estudios: Experto Universitario en Ciberseguridad y Protección de Sistemas (s.f.). Sitio Web de IMF *Business School*.

Capítulo Nº 4: Propuesta de Asignatura sobre Seguridad y Control de Sistemas Informáticos

4.1 Introducción

En este capítulo se desarrolla el programa de asignatura propuesto como materia optativa para ser incorporada a las carreras de Contador Público y Licenciatura en Administración, de la Facultad de Ciencias Económicas de la UNT, el cual representa el objetivo principal de esta Tesis de Maestría.

Este apartado no solo desarrolla las unidades de estudio de la asignatura, sino que también plantea una fundamentación de la materia, su relación con otras y con el perfil profesional y los objetivos generales y específicos para cada unidad de estudio. Finalmente se describen las habilidades conceptuales, procedimentales y actitudinales que se espera alcance el alumno y la bibliografía que se utilizaría para el dictado del mismo.

4.2 Marco Referencial

4.2.1 Identificación de la Asignatura.

Teniendo en cuenta la recopilación bibliográfica realizada, el trabajo de campo ejecutado y descripto en el capítulo anterior y el análisis de planes de estudio referidos a la disciplina impartida en otras unidades académicas nacionales e internacionales, se confeccionó este programa de asignatura. El mismo con el objetivo de proponerlo, por intermedio de la Secretaría Académica de la FACE de la UNT, como materia optativa para las carreras de Contador Público y Licenciatura en Administración.

A continuación, se describe la identificación de la Asignatura propuesta:

a) **Nombre**: Seguridad y Control de Sistemas Informáticos

b) **Carrera**: Contador Público (Plan 2018) y Licenciatura en Administración (Plan 2014)

c) **Curso y cuatrimestre**: Segundo cuatrimestre de cuarto año.

d) **Plan de estudios**: CP 2018 (Res. 463-HCD-18). LA 2014 (Res. 363-HCD-13)

e) **Pre correlativas exigidas para su cursado**: Sistemas Administrativos y Control Interno I / Organización Contable de Empresas I

f) **Otros requisitos exigidos por resoluciones vigentes**: Los alumnos de la Carrera de Contador Público para cursar esta asignatura deberán contar con un mínimo de 18 materias aprobadas, entre estas la pre correlativa requerida.

g) **Carga horaria**: 78 horas.

4.2.2 Contenidos Mínimos.

Los contenidos mínimos se expresan en función de la información conceptual y teórica considerada imprescindible y de las competencias que se desean lograr. Se plantean a continuación aquellos que han sido considerados para este curso:

a. Conceptualización de seguridad y control de los sistemas de información: confidencialidad, integridad y disponibilidad.

b. Estructura para la seguridad y el control de los sistemas de información. Comité de seguridad.

c. Gestión de la seguridad de la Información. Plan de concientización.

d. Evaluación y gestión del riesgo. Amenazas, vulnerabilidades e impacto.

e. Principios y técnicas de control en sistemas de información. Tecnologías y herramientas para la seguridad informática. Seguridad física y lógica.

f. Normas, estándares y legislación de seguridad de la información. Tratamiento de los datos personales.

g. Incidentes de seguridad, plan de contingencia y continuidad del negocio.

h. Control interno. Controles generales y de aplicación.

i. Auditoría de Sistemas. Metodologías, enfoques, función y organización. Objetivos y alcances. Planificación de la auditoría. Informes del auditor

4.2.3 Fundamentación de la Asignatura.

En este separado se realiza un análisis minucioso respecto a la misión que cumple la materia dentro del plan de estudios y su relación y coordinación de enfoques y conocimientos previos con otras asignaturas.

4.2.3.1 Importancia de la Asignatura dentro del Plan de Estudios.

La tecnología y los sistemas de información han experimentado avances notables, impactado en un grado nunca antes visto sobre el desempeño y las formas de estructurar, administrar y conducir las organizaciones. Lo anteriormente expresado, se reconoce ampliamente en la fundamentación de los planes de estudios y en las competencias e incumbencias profesionales que se esperan de los egresados de las carreras de Ciencias Económicas.

Esta realidad conlleva a la necesidad de implementar un conjunto de asignaturas que complementen los contenidos cubiertos en “Sistemas de Información I”, prevista como obligatoria en la currícula en 2° año, la cual introduce en los conceptos disciplinares y herramentales, que se amplían, complementan y recontextualizan en la asignatura optativa “Sistemas de Información II”, profundizando aspectos de mayor complejidad y abordando las últimas tendencias en una disciplina caracterizada por lo creciente, complejo y volátil de sus cambios y las oportunidades que representa para los profesionales y las organizaciones.

Teniendo en cuenta que la organización de los planes de estudios vigentes responden a criterios de amplio espectro e incorporan los cambios ocurridos en el mercado, especialmente en las disciplinas de franco y espectacular desarrollo, como son las nuevas tecnologías de información y dando respuestas a los requerimientos sociales y económicos, se propicia que con el cursado de la asignatura “Seguridad y Control en Sistemas Informáticos”, se brinda una formación que permite completar la capacitación optativa del graduado, en lo que refiere a sistemas y tecnologías de la información, permitiéndole adquirir habilidades específicas en esa temática.

4.2.3.2 Relación de la Asignatura con el Perfil Profesional.

Considerando el perfil del graduado generalista de amplio alcance, con una especialización técnico – funcional, el desarrollo profesional puede vincularse y sustentarse por la materia prima del graduado y la organización: la información.

Como resultado de esto, surgen demandas crecientes en cuanto a seguridad, control y disponibilidad de mecanismos de verificación, que requieren familiarizarse con conceptos y técnicas afines a las características y vulnerabilidades generadas por el uso de los recursos informáticos y tecnológicos.

La materia proporciona al futuro egresado conceptos avanzados y formación sobre competencias en lo referido a la seguridad informática y control, requeridas para actuar en el ambiente de las organizaciones y los negocios altamente informatizados, permitiendo reconocer riesgos, vulnerabilidades y amenazas. Brinda además las competencias para diseñar, implementar y gestionar un sistema de seguridad de la información. Permite conocer los requerimientos de seguridad al trabajar interconectado y con vinculación en la web. Proporciona herramientas conceptuales para tomar decisiones en caso de participar de un comité de seguridad. Brinda conceptos de control interno y auditoria informática. Permite conocer el marco legal, estándares y normativas sobre la temática.

Específicamente:

a) El alumno recibirá una adecuada capacitación, aplicable al diseño, implementación y dirección de sistemas de información, su seguridad y control, abarcando tanto la información como los activos informáticos, otorgando valor agregado a la gestión y posibilitando el logro de los objetivos propuestos por la entidad.

b) Asimismo, las técnicas de “Auditoría en Sistemas” permitirán emitir opinión fundada sobre la razonabilidad y confiabilidad del funcionamiento de los sistemas empresariales y como consecuencia, de la información financiera y no financiera reportada por ellos.

c) Brindará competencias para conformar equipos interdisciplinarios con otras áreas del conocimiento, como por ejemplo integrando comités de seguridad.

d) Las habilidades adquiridas contribuirán a la formación de competencias necesarias para el desenvolvimiento eficiente de las actividades propias de la profesión en el contexto actual.

4.2.3.3 Articulación con la materia pre correlativa: Sistemas Administrativos y Control Interno I/ Organización Contable de Empresas.

Dada la naturaleza de la temática abordada en la asignatura, se torna de fundamental importancia contar con conocimientos previos sobre diseño e interpretación de sistemas administrativos y estructuras, lo que permitirá al alumno conceptualizar la medición del riesgo en cada uno de los procesos identificados y a partir de esto, poder determinar cuáles son las medidas de seguridad informática más adecuadas a aplicar, considerando el nivel de riesgo aceptado por la dirección y las características propias del diseño organizacional. El conocimiento de estructuras también posibilitará al alumno, una mayor comprensión de temas relativos a la estructura organizativa necesaria para la seguridad y el control de la información. Asimismo, los aprendizajes previos sobre control interno, serán re contextualizados con el objetivo de profundizar en temas relacionados a auditoria de sistemas y de TI.

4.2.3.4 Articulación con las materias del mismo año.

Por tratarse de una materia optativa, el alumno puede cursarla una vez aprobadas las pre correlativas y las condiciones indicadas en el Reglamento Académico, lo que brinda múltiples opciones de articulación. Brinda conceptos avanzados y formación sobre seguridad y control en todos los aspectos relacionados a los Sistemas y las Tecnologías de información en el ambiente de las organizaciones y los negocios. Aporta competencias para trabajo en grupo y colaborativo, resolución de problemas, capacidad de expresión y exposición, tanto oral como escrita

4.2.3.5 Articulación con las materias de otros años.

a) De años anteriores: Es recomendable para facilitar y ampliar la comprensión de los aspectos disciplinares contar con conocimientos en "Sistemas Administrativos y de Control Interno I" y "Derecho Empresario I", ya que esta última brinda los esquemas para la compresión de las conceptualizaciones jurídicas y las ciencias del derecho; dotando de conocimientos jurídicos y herramientas para la reflexión y el análisis de este campo disciplinar.

Sería deseable que los alumnos hayan adquirido competencias en el uso del Aula Virtual, dado que en la materia se trabajará intensivamente con la misma y que hayan desarrollado experiencia de trabajo con casos, exposiciones orales y escritas.

b) De años posteriores: Brinda conceptos avanzados y formación sobre aspectos particulares relacionados a la seguridad y el control de los Sistemas y las Tecnologías de información en el ambiente de las organizaciones y los negocios. Capacita en el uso del Aula Virtual y el trabajo con casos.

El cursado de las materias optativas "Análisis y Diseño de Sistemas" y "Sistemas de Información II", brindaría al egresado una completa formación disciplinar en Sistemas y Tecnologías de Información, que le permitiría abordar los múltiples y variados desafíos que se presentan hoy a los profesionales y las organizaciones.

4.3 Objetivos de la Asignatura

Según Steiman (2007) "*desde la lógica tecnológica, los objetivos tratan de enunciar qué aprendizajes, en relación con los contenidos, se espera que realicen los alumnos como "productos" parciales y finales de la cursada de una unidad curricular. Los objetivos representan ser la descripción de la ejecución, entendida como realización de una actividad, que se pretende que los alumnos estén en condiciones de realizar antes de que se les considere competentes. El objetivo, desde este punto de vista, describe un resultado previsto, antes que el proceso mismo"* (p. 18).

4.3.1 Objetivos Generales.

Se plantean como objetivos generales, es decir aquellos que están relacionados directamente con el desarrollo global del alumno, los siguientes aspectos:

a. Conocer, comprender e internalizar conceptos avanzados relacionados con sistemas y tecnologías de información, complementarios a los abordados en la asignatura Sistemas de Información I, lo cual permite ampliar conceptos emergentes relacionados con la disciplina Sistemas y Tecnologías.

b. Identificar soluciones a problemas, requerimientos legales y regulatorios y desafíos a través de conocimientos aprendidos sobre tecnologías, metodologías y procesos y otras materias de la currícula.

c. Propiciar que el alumno sea capaz de realizar implementaciones exitosas en equipo y trabajo interdisciplinario.

d. Conocer las tendencias emergentes en seguridad de la tecnología de la información, lo cual es clave en un sector que experimenta un cambio drástico y acelerado como parte de su naturaleza.

e. Reconocer los desafíos y oportunidades que las tecnologías significan para una organización y los profesionales.

f. Integrar los conocimientos con los adquiridos en otras materias, propiciando la transferencia de conceptos.

4.3.2 Objetivos Específicos.

Se plantean como objetivos específicos de la asignatura, es decir los relacionados al segmento de conocimiento que compete a la materia, los siguientes puntos:

a. Reconocer la importancia de la seguridad de la información en las organizaciones.

b. Identificar los activos de información y su valor para la organización.

c. Distinguir riesgos, vulnerabilidades y amenazas.

d. Dimensionar el impacto económico y reputacional para la organización ante un incidente en la seguridad de la información.

e. Comprender el rol de los integrantes de la organización en la implementación de un Sistema de Gestión de Seguridad de la Información.

f. Reconocer las principales tecnologías y herramientas para implementar un SGSI.

g. Reconocer los riesgos y vulnerabilidades, su gestión y cuantificación en función al tipo de organización. Identificar las acciones para mitigarlos.

h. Diferenciar categorías de productos de seguridad.

i. Comprender los requerimientos de seguridad al trabajar interconectado y con vinculación en la web.

j. Conocer y concientizar sobre la legislación vigente y las principales normativas aplicadas a la seguridad de la información en Argentina.

k. Comprender como la aplicación de los estándares internacionales pueden contribuir a mejorar el nivel de protección.

l. Reconocer un incidente de seguridad de la información.

m. Conocer sobre la gestión de incidentes y las acciones para la mitigación y reporte.

n. Comprender y diseñar un plan de continuidad de negocios y una estrategia de recuperación ante desastres.

o. Interpretar el sistema de control interno y sus componentes en un entorno computarizado.

p. Identificar los conceptos y aplicación de los controles de entorno y programados en un sistema de información computarizado.

q. Analizar los objetivos y alcances de una auditoría a los recursos informáticos en una organización y la metodología para efectuarla.

r. Interactuar en ambientes virtuales y colaborativos como la plataforma Moodle

4.4 Contenidos y Habilidades

4.4.1 Habilidades conceptuales.

En este apartado se realiza un desarrollo de los contenidos conceptuales (hechos, datos, conceptos, características, etc.) propuestos para ser desarrollados en el transcurso del dictado de la asignatura. Los mismos están agrupados en unidades de estudio, para facilitar su comprensión e internalización por parte del alumno.

Tabla Q: Contenidos conceptuales de la Asignatura Seguridad y Control de SI

Unidad Nº 1: **Introducción a la Seguridad y el Control de la información**
Definición y alcance de la seguridad de la información, seguridad informática y activos de información. Aspectos estratégicos y tácticos. Valor de los sistemas de información. Sistema de Gestión de Seguridad de la Información. Plan de Seguridad. Estado y problemáticas actuales de Seguridad de la información en organizaciones regionales.
Unidad Nº 2: **Estructura organizativa para la seguridad y el control**
Control y estructura organizativa del ente y del área específica de Tecnología. Gobierno de TI. Funciones y puestos. Diseño de una estrategia de Seguridad de la Información. Rol del comité de seguridad.
Unidad Nº 3: **Metodologías de evaluación y gestión del riesgo**
Disponibilidad, integridad y confidencialidad de la información. Evaluación y gestión del riesgo: fases, alcance, modelos y valoraciones. Vulnerabilidades, amenazas e impacto: definición, alcance, tipología y probabilidad de ocurrencia. Inventario de activos de la información; cuantificación y valoración.

Unidad Nº 4: **Tecnologías y herramientas para la seguridad informática**
Seguridad física y lógica. Seguridad en componentes de hardware, software, bases de datos, comunicaciones, dispositivos móviles, páginas web. Cifrado de datos y firma digital. Copias de Seguridad. Ciclo de vida, clasificación y destrucción segura de la información. Servicios en la nube: tipología y contratación; consideraciones legales y de seguridad. Tendencias.
Unidad Nº 5: **Normas, estándares y legislación sobre seguridad de la información**
Legislación nacional aplicable en seguridad de la información y protección de datos personales. Principales marcos de referencia, normativas y estándares de seguridad, nacionales e internacionales. Relación de las Normas Técnicas Profesionales, con el ambiente de la tecnología informática. Contratos informáticos. Delito informático.
Unidad Nº 6: **Seguridad de la información con proveedores, clientes y RR HH**
Medidas de seguridad con proveedores y clientes. Tercerización de servicios. Aspectos de seguridad con empleados: acuerdos de confidencialidad y finalización de la relación laboral; programas de capacitación y concientización. Ingeniería Social. Protección de puestos de trabajo: objetivos; implementación de buenas prácticas.
Unidad Nº 7: **Incidentes de seguridad, continuidad de negocio y plan de contingencias**
Definición y clasificación de incidentes. Impacto económico. Valuación y métricas. Respuestas ante incidentes. Recuperación de Desastres. Plan de Contingencias. Pruebas y simulacros.
Unidad Nº 8: **Control Interno**
Contenidos: Definición, alcance e importancia. Dificultades propias del entorno informático para las tareas de auditoría. Sistema de control interno: Importancia y componentes. Controles generales y de aplicación. Pruebas.

Unidad Nº 9: **Auditoría de Sistemas**
Contenidos: Conceptualización de auditoría informática, en entornos informatizados y de sistemas; objetivos y alcances. Marco de referencia. Prácticas de control y estándares de auditoría. Programa y realización de una auditoría: Proceso, estrategia, planificación, asignación de recursos, características del auditor, técnicas de auditoría, tipos de controles y riesgos. Gestión de logs. Informe de auditoría.

Fuente: elaboración propia

4.4.2 Habilidades Procedimentales.

En este apartado se realiza un desarrollo de los contenidos procedimentales propuestos para ser alcanzados en el transcurso del dictado de la asignatura:

a. Interpretar y relacionar los conceptos disciplinares del marco teórico, entre sí, con otros conocimientos previos y con la praxis.

b. Reconocer y re contextualizar conocimientos respecto de Sistemas, tecnologías y herramientas informáticas desde el enfoque de la seguridad informática.

c. Diseñar soluciones para problemáticas organizacionales relacionadas con la seguridad informática.

d. Reconocer incidentes que pueden abordarse con procedimientos y tecnologías de la disciplina.

e. Interpretar marcos normativos y regulatorios.

f. Interpretar resultados.

g. Resolver y responder consignas, cuestionarios y casos

h. Apropiarse de una jerga epistemológica adecuada para su posterior desempeño profesional.

i. Utilizar en forma activa y eficiente los recursos del Aula Virtual.

j. Utilizar herramientas multimedia del aula virtual permitiendo el desarrollo de habilidades de redacción, elaboración y explicación.

k. Desarrollar habilidades de expresión oral y escrita.

4.4.3 Habilidades Actitudinales.

En este punto, se realiza un desarrollo de los contenidos actitudinales, valores y actitudes, que se esperan sean alcanzados por parte de los alumnos durante el transcurso del dictado de la asignatura:

a. Resignificar conocimientos e ideas previas

b. Responsabilidad y respeto en el cumplimiento de condiciones y plazos

c. Tolerancia a las dificultades y a las normas

d. Respeto a la diversidad de opinión

e. Desarrollo de capacidades de comunicación inter e intrapersonal

f. Proactividad

g. Fomentar la capacidad de análisis y toma de decisiones

h. Concientización respecto a la temática abordada

4.5 Bibliografía Propuesta

Finalmente se plantea un listado de libros y artículos de consulta que posibilitará al alumno aprender, comprender y profundizar los conceptos desarrollados y explicados en las clases presenciales.

4.5.1 Básica (obligatoria).

- Keneth C. Laudon y Jane P. Laudon (2016). *Sistemas de Información Gerencial*. 14ª Edición. Pearson, México.

- Lardent, A. R. (2001). *Sistemas de Información para la gestión empresarial: Procedimientos, seguridad y auditoría.* 1º Edición. Prentice Hall. Argentina.

- Ralph Stair y George Reynolds (2017). *Principios de Sistemas de Información.* 10º Edición. Cengage Learning Editores, México.

- Castello, Ricardo J. (2008). *Auditoría de sistemas y tecnologías de información.* Creative Commons, Córdoba, Edición digital. [on line]. Recuperado de: http://e-conomicas.eco. unc.edu.ar/archivos/_3/ AudSistLibro08.pdf

- Saroka, Raúl H. (2002). *Sistemas de Información en la era digital.* Argentina. Fundación OSDE. Unidad 3: La Seguridad de los Sistemas de Información.

- Instituto Nacional de Ciberseguridad del Gobierno de España, Ministerio de Economía y Empresa (2018). Guías de estudio sobre Ciberseguridad. Blog "Protege tu empresa".

- Ley 26.326 (2000). Protección de datos personales.

- García, M. A. (2019). Apuntes de cátedra sobre Seguridad de la Información, Sistemas de Información I, Facultad de Ciencias Económicas, UNT.

- Masclef, M. A. (2017). Apuntes sobre Comité de Seguridad de la Información según Norma ISO. Sistemas de Información I, Facultad de Ciencias Económicas UNT.

4.5.2 Complementaria.

- Baca Urbina G. (2016). Introducción a la Seguridad Informática. Primera Edición digital. México. Grupo Editorial Patria.

- Cansler, l., Elissondo, l., Godoy, l., y Rivas, R., (2015). Informe Nº 15 – Auditoría en ambientes computarizados. FACPCE -CECYT. Argentina.

- Directrices generales COBIT (Control Objetives for Information and Related Technology). ISACA (Information System Audits and Control Association).

- IRAM, Instituto Argentino de Normalización (2019). Norma ISO/IEC 27002: Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.

- IRAM, Instituto Argentino de Normalización (2012). Norma ISO/IEC 27005: Tecnología de la información. Gestión del riesgo de seguridad de la información. Subcomité de Seguridad en Tecnología de la Información.

- IRAM, Instituto Argentino de Normalización (2015). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad en Tecnología de la Información.

- IRAM, Instituto Argentino de Normalización (2018). Norma ISO/IEC 31000: Gestión del riesgo. Directrices. Subcomité de Seguridad en Tecnología de la Información.

- Jeimy J., Cano, M. (2013) La inseguridad de la información: una visión estratégica. Colombia. Alfaomega Colombiana S.A.

- Normas COSO (2004). Marco referencial para la Administración del Riesgo (Risk Management).

- Perez, J.C.M. (2015). Protección de datos y Seguridad de la Información. 4º Edición actualizada. España. Editorial RA-MA.

- Resolución técnica N° 37 (2013). Normas de Auditoría, revisión, otros encargos de aseguramiento, certificación y servicios relacionados. Federación Argentina de Consejos Profesionales de Ciencias Económicas. Argentina

- Spina M. L. (2017). Compendio Normativo en Derecho Informático. Diplomado en Gobierno de TI, Seguridad y Auditoría. UCASAL. Argentina.

4.6 Estrategias Didácticas

4.6.1 Metodología de enseñanza.

Seguridad y Control en Sistemas Informáticos es una materia teórico – práctica. Para cada una de las instancias, se debe tener en cuenta los siguientes aspectos:

Las clases teóricas se dictarán en dos instancias semanales de 1.30 hs. de duración a todo el grupo de alumnos de la cohorte. En la misma se desarrollarán los temas con apoyo de

presentaciones y material audio visual, se propiciará la lectura previa del material, fomentando la participación e interacción entre alumnos y docentes.

Los contenidos prácticos se abordarán en una segunda instancia semanal de 1.30 hs de duración a la cohorte, sobre los contenidos teóricos desarrollados en la clase de la misma semana. Durante las mismas, los alumnos podrán trabajar con ejemplos o resoluciones de casos que se soliciten, estos ayudarán a los estudiantes a analizar, debatir y aprender. Se prevé además la participación de invitados que disertarán sobre su experiencia profesional respecto de los temas abordados en clases teóricas. Asimismo, se realizarán clases de tutoría sobre los trabajos de campo de los asistentes.

En caso de no poder efectuar las clases de manera presencial, por cuestiones de fuerza mayor, se habilitará una sala de videoconferencia, para el dictado de las mismas.

Un requisito para la aprobación del curso será que los alumnos deberán desarrollar un trabajo de campo integrador, que se expondrá al final del cursado.

Por otro lado, el Aula Virtual se encontrará desarrollada en Moodle 3.0, propiciando una modalidad *b-learning*, se utilizará como complemento y apoyo a las instancias teóricas y prácticas, la misma contará con las presentaciones de las clases, material adicional, guía didáctica de la materia, videos, cuestionarios para autoevaluación, casos de discusión, foros de debate y de consulta, encuestas, notas y todas las novedades que hacen el cursado de la materia, entre otras actividades y contenidos.

La evaluación de los contenidos se efectuará sobre los conceptos abordados en las clases teórico – prácticas.

La cátedra ofrecerá consultas teóricas y prácticas en forma presencial y a través del Aula Virtual. Además se brindarán consultas para que los alumnos puedan revisar sus exámenes parciales y finales.

4.7 Recursos Didácticos

a) Libros y apuntes de cátedra.

b) Disertaciones de profesionales invitados a las clases.

c) *Software*: Sistema operativo, Google Drive, procesador de textos, hoja de cálculo, aplicativos de seguridad informática

d) Pizarra

e) Proyector

f) Sistema de sonido

g) Diapositivas y material multimedia

h) Videos / Imágenes

i) Aula Virtual

4.8 Condiciones para aprobar y obtener la promocionalidad

4.8.1 Régimen de Aprobación.

Promoción y régimen de aprobación con examen libre (Art 8, d, y Art. 9 a y e del Reglamento Académico).

4.8.2 Características de la materia.

Seguridad y Control en Sistemas Informáticos es una materia teórico – práctica.

Para promocionar la asignatura debe aprobarse, con 6 (seis) o más.

4.8.3 Régimen de promoción.

a) Acreditar el 75% de asistencia a las clases

b) Nº de parciales: 2 (dos)

c) Trabajo de campo final aprobado

d) Nota para promocionar: seis (6) puntos, como promedio final, pudiendo tener aplazado o estar ausente justificado en solo un (1) parcial, el cual deberá ser recuperado

4.8.4 Inasistencias: a parciales.

- Justificada: Recupera el parcial. La justificación deberá ajustarse a lo establecido en el Reglamento Académico. (Art. 12º y 13º Reglamento Académico).

- Injustificada: se considera como obtenido cero (0) puntos. (Art. 12º Reglamento Académico).

4.8.5 Recuperación de parciales.

Cantidad de parciales a recuperar: 1 (uno)

Pueden recuperar:

a) Los alumnos ausentes justificados.

b) Los aplazados en el primer o segundo parcial.

c) Los alumnos que teniendo todos los parciales aprobados, obtuvieran un promedio menor a 6 (seis), recuperarán el parcial de menor nota, más avanzado cronológicamente.

De no cumplirse estos requisitos, el alumno queda en condición de libre.

4.8.6 Examen libre.

El alumno podrá rendir la materia en carácter de libre en los turnos habilitados para esta condición. Dicho examen constará de dos (2) partes:

a) Examen práctico sobre un caso de estudio o desarrollo de campo, conforme lo solicite la cátedra.

b) Una vez aprobado el examen antedicho, se deberá rendir otro examen de evaluación teórica. (Art. 9 e) Reglamento Académico).

La nota mínima de aprobación de la materia en esta condición es de cuatro (4) puntos.

Las fechas de parciales y recuperaciones se fijarán por la cátedra y serán informadas conforme indica la Secretaría Académica.

4.8.7 Momentos de Evaluación.

a) Parcial: Se evaluarán 2 parciales teórico-prácticos.

b) Trabajo final: se requiere la elaboración, presentación y aprobación del mismo

4.8.8 Metodología de Evaluación.

Se evalúa en instancias escritas individuales, de 1.30 hs. de duración, a todos los alumnos de la cohorte en forma conjunta.

- Trabajo final: se requiere la elaboración, presentación de material multimedial y aprobación del mismo de carácter individual. El mismo debe ser auténtico y evidenciar la comprensión de los contenidos trabajados durante el cursado.

Se utilizarán rúbricas para indicar lo que se espera del desempeño del alumno, tanto en las instancias de evaluación escritas como en el trabajo final

Capítulo N º 5: Resultados y Conclusiones

5.1 Resultados de la Tesis de Maestría

A continuación, se realiza una compilación de las actividades ejecutadas y los resultados obtenidos en el transcurso del proceso de elaboración de este trabajo final de Maestría.

En el Capítulo N° 1, se realizó una recopilación bibliográfica, para dar cumplimiento al objetivo planteado de definir y entender, en toda su dimensión teórica, el concepto de gestión estratégica de la seguridad de la información, identificando su relevancia en el campo de la Ciencia de la Administración. Asimismo, se concluyó como postulado que la Seguridad Informática es un área de vacancia disciplinar en las carreras de Ciencias Económicas, específicamente dentro de la disciplina de la Administración, la cual no está considerando la realidad actual y por lo tanto no se están incorporando en la formación de sus profesionales, aspectos propios del ámbito de la seguridad informática de vital importancia en el entorno de las organizaciones y los negocios actuales. El objetivo de la seguridad informática no solo consiste en prevenir los potenciales ataques, sino también abarca el diseño e implementación de los planes de recuperación en caso de haberse concretado daños. Esta área disciplinar posibilita la continuidad del negocio, aspecto estrictamente necesario para la labor profesional de la administración.

En este capítulo se transcribieron los aspectos más relevantes y generales al respecto. Cabe destacar, con el material relevado, clasificado y ordenado se confeccionó un dossier que será utilizado como material de lectura por los alumnos que cursen la asignatura optativa propuesta.

A continuación, en el Capítulo N° 2, se analizaron reportes especializados, con el objetivo de reconocer el estado actual de la seguridad de la información en organizaciones. Se pudieron dimensionar las problemáticas, las principales preocupaciones y las tendencias en Latinoamérica y el mundo al respecto. Se observó que este ámbito teórico práctico de

conocimiento está expandiéndose fuertemente en el último tiempo, entre otros aspectos, debido al crecimiento de las superficies de ataque, a la concientización por parte de las organizaciones por el resguardo de sus activos de la información y los incrementales beneficios económicos obtenidos por parte de los ciber delincuentes. Además, se evidenció que es necesario se lleven a cabo acciones conjuntas entre las diferentes partes involucradas a fin de fortalecer y ampliar los espacios de capacitación y formación pertinentes.

Posteriormente, en el Capítulo N° 3 se describió el proceso de análisis realizado, respecto al estado de la disciplina de la Seguridad Informática en las carreras de Ciencias Económicas. Además, se realizó una interpretación de la información relevada tanto a nivel nacional como local, para probar el postulado de este trabajo: "la Seguridad Informática es un área de vacancia disciplinar en las carreras de Ciencias Económicas, específicamente dentro de la disciplina de la Administración".

El relevamiento de la situación externa, mediante el intercambio de información con integrantes de DUTI, permitió comprobar que la temática es considerada de suma importancia para el ejercicio de la administración estratégica de negocios en entornos informatizados. Sin embargo, se verifica que en la mayoría de las unidades académicas se imparte dicha temática dentro de los contenidos básicos de la materia principal de TI, sin contar con una asignatura específica que profundice y re contextualice este espacio de conocimiento.

En el ámbito local, se realizó un análisis del proceso de acreditación de las carreras de CP y LA, y de los contenidos mínimos requeridos por las resoluciones ministeriales, entre los cuales se encuentra el tema tratado. También se constató el estado actual de la disciplina de los "sistemas y tecnologías de la información" en general y de la "seguridad informática" en particular. La situación corroborada a nivel nacional se verifica de igual modo para la FACE UNT.

Para dar respuesta a esta situación en la institución antes mencionada, se consideró el diseño de una propuesta curricular referida a “Seguridad y Control de Sistemas Informáticos”, la cual brindaría conocimientos y habilidades que permitirían ampliar la formación del graduado en lo que refiere a sistemas y tecnologías de información.

Por otra parte, se entrevistó a docentes del HCD y de la comisión de implementación del plan de estudio de CP y consideraron como positivo todos los aspectos a desarrollar en la propuesta de asignatura, desde el punto de vista de las exigencias ministeriales y los requerimientos técnicos que demanda el mercado laboral y de los negocios. Además algunos de ellos, manifestaron que la materia debería formar parte de la currícula obligatoria de las carreras antes mencionadas.

Finalmente, se realizó una reflexión destacando la oportunidad potencial que posee la FACE, de desarrollar una propuesta de posgrado relacionada a la temática abordada, dadas las exigencias del mercado regional y la escasa oferta de formación al respecto.

Finalmente, en el Capítulo N° 4 se dio cumplimiento al objetivo general de esta tesis de elaborar una propuesta curricular referida a Seguridad y Control de Sistemas Informáticos, a fin de proponerlo como materia optativa dentro de las carreras de CP y LA de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán.

Cabe destacar, que la propuesta fue presentada el 5 de noviembre de 2018 a la FACE[88] y luego de los tratamientos pertinentes, la asignatura fue incorporada a los planes de estudios de CP (plan 2018) y LA (plan 2014).

Asimismo, se constató entre los docentes de la FACE entrevistados[89], que la propuesta realizada tuvo aceptación generalizada por parte la “Comisión de seguimiento e implementación del Plan de Estudios” y hubo consenso en su tratamiento para su inclusión en

[88] Véase Anexo “C”

[89] Véase Anexo “B”

los programas de estudios. Además, señalaron que esta materia ofrece una formación diferencial respecto a otras propuestas curriculares de la región. Consideran que es primordial que el profesional en Ciencias Económicas posea conocimientos en seguridad y control de sistemas informáticos, no solo para desempeñarse en organizaciones altamente informatizadas, sino también para generar un nuevo espacio de desempeño profesional.

Representantes del Honorable Consejo Directivo afirman que hubo pleno consenso para la aprobación de la asignatura propuesta en los planes de estudio. La misma fue adecuada, sin presentarse oposiciones ni objeciones para su implementación.

5.2 Reflexiones finales sobre el ámbito de la Seguridad Informática

Teniendo en cuenta la información relavada y el trabajo de campo realizado, a continuación se realizan reflexiones finales, respecto a la incorporación de esta disciplina dentro de los planes de estudios de las carreras de CP y LA, para una efectiva administración estratégica de negocios.

a) Dada la situación actual de los negocios y de la economía digital imperante a nivel mundial, es de fundamental importancia que el graduado en Ciencias Económicas adquiera conocimiento para la gestión de la seguridad de la información, propicie, internalice y transmita estos conceptos a la organización y posea las habilidades necesarias para formar parte en un comité de seguridad, estando capacitado para participar en entornos interdisciplinarios.

b) Las certificaciones internacionales en TI, como ser el conjunto de normas ISO 27000, son cada vez más exigidas por clientes y proveedores. Por lo tanto, son la llave de acceso a nuevos mercados, posibilitando de este modo la expansión de las organizaciones a nivel global.

c) La capacitación del personal en temas relacionados a la Seguridad Informática constituye un requisito imprescindible para el normal desarrollo de las actividades de una organización. Los ataques internos a través de la ingeniería social, el fraude y la fuga de información son actualmente una de las mayores preocupaciones de los directivos de las compañías regionales.

d) Es necesario que el administrador vele por el mantenimiento del valor de la organización, parte de la cual se encuentra en su información, por lo que deberá contar con un fuerte dominio de conceptos relacionados a la Seguridad de la Información, que garanticen la confidencialidad, integridad y disponibilidad de la información, asegurando de este modo la confianza de todo el entorno organizacional.

e) Los directivos de negocios en conjunto con los profesionales de la administración, deben diseñar estrategias corporativas, contemplando amenazas y riesgos informáticos, para lograr la estabilidad y el posicionamiento en mercados. Es por ello que el profesional debe estar capacitado para diseñar e implementar metodologías para la evaluación y gestión del riesgo, planes de contingencia, de recuperación ante desastres y de continuidad de negocio, entre otros.

5.3 Conclusión Final

El diseño curricular de la asignatura presentada constituye una propuesta académica en donde se explicitan contenidos disciplinares, prácticas y habilidades esperadas para la práctica didáctica en el aula y explicita acuerdos que conforman aquello que puede objetivarse del contrato didáctico que se establece con los alumnos y con la institución. Este se basa en una selección de objetivos de aprendizaje y contenidos que deben dar lugar a la creación de experiencias apropiadas que tengan efectos acumulativos, manteniendo sobre el mismo una revisión constante para realizar oportunas reacomodaciones. En dicho marco, el programa está conformado por experiencias de aprendizaje planificadas y dirigidas en orden a conseguir los objetivos educativos propuestos.

En concordancia con lo antes expresado, se reconoce la importancia de la temática conforme lo relevado en las carreras de Ciencias Económicas de diferentes casas de estudio, aspecto que también se evidencia en los contenidos curriculares exigidos por la resolución ministerial para la acreditación de la carrera de CP. En este sentido la propuesta de una materia específica sobre Seguridad y Control de Sistemas Informáticos implica consolidar los conocimientos, destrezas

y habilidades, requeridas en esta área de conocimiento, procurando abordar una temática cada vez más usual en el contexto actual y cubriendo un área de vacancia disciplinar en la Facultad de Ciencias Económicas de la UNT.

5.4 Divulgación de Resultados

Los resultados y conclusiones parciales de este trabajo fueron socializados en los siguientes eventos académicos de investigación:

- Autor y Expositor: *"Implementación del "Modelo 5S", para el fortalecimiento de la seguridad física de la información, en área funcional de empresa de transportes"*. IIº Congreso de Administración del Jardín de la República. Encuentro Inter-Regional ADENAG Centro Oeste y Noroeste Argentino". Facultad de Ciencias Económicas (U.N.T), 23 de marzo de 2018, Tucumán. Número ISBN: 978-987-754-143-4. Páginas: 159 - 174

- Autor y Expositor: *"Proceso de Implementación de Propuesta de Asignatura sobre Seguridad y Control de Sistemas Informáticos para la Administración estratégica de Negocios"*. II Encuentro de Innovación en la Enseñanza con la Red de Facultades de Ciencias Económicas del Norte Argentino y V Encuentro de Innovación en la Enseñanza de las Ciencias Económicas. Facultad de Ciencias Económicas, Universidad Nacional de Jujuy, 25 y 26 de octubre de 2018, Jujuy. Número ISBN: 978-987-3926-48-8. Páginas: 304 - 312

- Autor y Expositor: *"Seguridad Informática, área de vacancia disciplinar en la Ciencia de la Administración"*. 35° Congreso Nacional de ADENAG. Facultad de Ciencias Económicas (U.N.T), 23 y 24 de mayo de 2019, Tucumán. Número ISBN: 978-987-754-192-2. Páginas: 588 - 616

- Autor y Expositor: *"Análisis del Proceso de Inclusión de Contenidos sobre Seguridad de la Información en las Carreras de Ciencias Económicas, en el Contexto de la Acreditación de CONEAU"*. XIV Jornadas de Docentes Universitarios en Sistemas y Tecnologías de la Información (DUTI). Facultad de Ciencias Económicas, Universidad Nacional de La Plata. 3 a 5 de octubre de 2019, La Plata, Buenos Aires.
- Autor y Expositor: "*Inclusión de Contenidos Curriculares sobre Seguridad y Control de la Información en las Carreras de Ciencias Económicas, en el Contexto de la Acreditación de la CONEAU"*. Encuentro Regional ADENAG, zonas Centro Oeste y Noroeste, organizado por las facultades de Ciencias Económicas de la Universidad Nacional de Córdoba y la Universidad Nacional de Tucumán - Administración 4.0. 19 y 20 de marzo de 2020. Número
- Autor y Expositor: "*El Profesional de Ciencias Económicas en el ámbito de la Seguridad de la Información: Percepciones Interdisciplinarias"*. IV Encuentro de "Innovación en la Enseñanza" con la Red de Facultades de Ciencias Económicas del Norte Argentino y VII Encuentro de "Innovación en la Enseñanza de las Ciencias Económicas". Facultad de Humanidades, Ciencias Sociales y de la Salud, Universidad Nacional de Santiago del Estero, 10 al 12 de noviembre de 2020.

Anexos

Anexo A: Encuesta a integrantes de DUTI – Año 2018

1.1. Objetivo Específico de la Encuesta

Efectuar un intercambio de información con la Asociación de Docentes Universitarios en Sistemas y Tecnologías de la Información sobre la temática e *indagar* sobre los contenidos de seguridad informática impartidos en otras instituciones educativas nacionales de nivel superior del país.

1.2. Instrumento Utilizado

La presente encuesta tiene como objetivo relevar información entre los integrantes de DUTI, acerca de los contenidos relacionados a "Seguridad y Control de Sistemas Informáticos" impartidos en las facultades de Ciencias Económicas del país.

La misma es anónima y los datos serán utilizados en una investigación que se está llevando a cabo por miembros de la Cátedra de Sistemas de Información I, de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán.

Agradecemos su valiosa colaboración al responder este cuestionario, que solo le llevará unos minutos...

Empecemos...

1- Indique la Universidad Nacional a la que pertenece

2- Indique la Unidad Académica a la que pertenece

3- Indique el estamento docente al que pertenece

a) Profesor Titular

b) Profesor Asociado

c) Profesor Adjunto

d) Profesor Jefe de Trabajos Prácticos

e) Profesor Auxiliar

f) Otro

4- ¿Cuántas asignaturas OBLIGATORIAS referidas a "Sistemas y Tecnologías de la Información" se dictan para la carrera de CONTADOR PÚBLICO NACIONAL (CP) en su unidad académica?

a) Solo 1 asignatura

b) 2 asignaturas

c) 3 asignaturas

d) 4 asignaturas

e) Más de 5 asignaturas

f) Ninguna asignatura obligatoria

5- ¿Cuántas asignaturas ELECTIVAS/OPTATIVAS referidas a "Sistemas y Tecnologías de la Información" se dictan para la carrera de CP en su unidad académica?

a) Solo 1 asignatura

b) 2 asignaturas

c) 3 asignaturas

d) 4 asignaturas

e) Más de 5 asignaturas

f) Ninguna asignatura electiva / optativa

6- ¿Cuántas asignaturas OBLIGATORIAS referidas a "Sistemas y Tecnologías de la Información" se dictan para la carrera LICENCIATURA EN ADMINISTRACIÓN (LA) en su unidad académica?

a) Solo 1 asignatura

b) 2 asignaturas

c) 3 asignaturas

d) 4 asignaturas

e) Más de 5 asignaturas

f) Ninguna asignatura obligatoria

7- ¿Cuántas asignaturas ELECTIVAS/OPTATIVAS referidas a "Sistemas y Tecnologías de la Información" se dictan para la carrera LA en su unidad académica?

a) Solo 1 asignatura

b) 2 asignaturas

c) 3 asignaturas

d) 4 asignaturas

e) Más de 5 asignaturas

f) Ninguna asignatura electiva / optativa

8- ¿El plan de estudios de la carrera de CP incluye una asignatura exclusivamente relacionada a "Seguridad y Control de Sistemas informáticos" o similar?

a) Si

b) No

9- Considerando que el plan de estudios de la carrera de CONTADOR PÚBLICO incluye una asignatura relacionada a "Seguridad y Control de Sistemas informáticos" o similar. Escriba el nombre de dicha asignatura

10- ¿El plan de estudios de la carrera LA incluye una asignatura relacionada a "Seguridad y Control de Sistemas informáticos" o similar?

a) SI

b) No

11- Considerando que el plan de estudios de la carrera LICENCIATURA EN ADMINISTRACIÓN incluye una asignatura relacionada a "Seguridad y Control de Sistemas informáticos" o similar. Escriba el nombre de la Asignatura

12- ¿La asignatura principal y obligatoria relacionada a "Sistemas y Tecnologías de la Información" contempla una unidad específica referida a Seguridad y Control de Sistemas Informáticos?

a) Si

b) No

13- Considerando que la asignatura principal y obligatoria relacionada a "Sistemas y Tecnologías de la Información" contempla una unidad específica referida a Seguridad y Control de Sistemas Informático. ¿Cuáles de los contenidos que se enumeran a continuación se incluyen dentro de dicha unidad? Indique los que correspondan:

a) Introducción a la seguridad y el control: Integridad, disponibilidad y confidencialidad de la información

b) Desarrollo de una estructura para la seguridad y el control

c) Metodologías de evaluación y gestión del riesgo

d) Tecnologías y herramientas para la seguridad informática

e) Seguridad en los principales recursos tecnológicos de la organización

f) Requerimientos legales y normativas regulatorias de seguridad de la información

g) Seguridad de la información con colaboradores, proveedores y clientes

h) Incidentes de seguridad y plan de contingencias

i) Control interno y auditoría de sistemas

j) Gestión de la seguridad de la Información y buenas prácticas

k) Otros

14- ¿La oferta académica de GRADO cuenta con una carrera (exceptuando CP y LA) donde se impartan asignaturas relacionadas a "Seguridad y Control de Sistemas Informáticos"?

a) Si

b) No

15- Considerando que la oferta académica de GRADO cuenta con una carrera (exceptuando CP y LA) donde se imparten asignaturas relacionadas a "Seguridad y Control de Sistemas Informáticos". Escribir el nombre de la Carrera

16- ¿La oferta académica de POSGRADO cuenta con una carrera en donde se impartan cursos relacionados a "Seguridad y Control de Sistemas Informáticos"?

a) Si

b) No

c) No sabe / No conoce

17- Considerando que la oferta académica de POSGRADO cuenta con una carrera en donde se impartan cursos relacionados a "Seguridad y Control de Sistemas Informáticos". Escriba el nombre de la Carrera.

18- Considera importante el dictado de temas relacionados con "Seguridad y Control de Sistemas Informáticos" en las carreras de CP y LA, para la gestión estratégica de negocios

a) Si

b) No

19- La Resolución 2017-3400-APN-ME - para la acreditación de la Carrera de Contador Público, define los contenidos curriculares básicos de la misma y dentro del área temática "Administración y tecnologías de la Información" sugiere la inclusión de "Seguridad en los sistemas de información". Para dar cumplimiento a este requerimiento, en el plan de estudios vigente en su unidad académica:

a) Se realizaron modificaciones para incluir el tema

b) El tema ya se encontraba incluido en el plan de estudios

c) No sabe / No Conoce

20- Comentarios finales y/o sugerencias. Indique

Anexo B: Entrevista semi estructurada FACE

1. ¿Cuál fue el criterio tomado para la selección de materias optativas en los nuevos planes de estudios?

2. ¿Qué aspectos se tuvieron en cuenta para seleccionar las materias optativas relacionadas con tecnologías de la información en los planes de estudio recientemente implementados?

3. Al considerar el tramo de materias optativas ¿En qué contribuye para el futuro profesional esta formación específica?

4. ¿Qué grado de importancia se le atribuye al bloque de materias optativas sobre "TI" en la formación del profesional en ciencias económicas?

5. ¿Cómo considera que contribuye la formación en "Seguridad y Control de Sistemas Informáticos" específicamente para las carreras de CP y LA?

6. ¿Qué aspectos relacionados a "Seguridad y Control de Sistemas Informáticos considera que deberían ser impartidos en las carreras de ciencias económicas?

7. ¿Cómo considera que queda posicionada la materia dentro del programa de estudio de las carreras de Ciencias Económicas?

8. ¿Considera que la formación en tecnologías de la información es fundamental en el perfil del graduado en Ciencias Económicas?

9. ¿Qué grado de consenso hubo entre los miembros de la "Comisión de seguimiento e implementación del plan de estudios" / HCD sobre la incorporación de la materia dentro de los nuevos planes de estudio?

10. ¿Consideraron que esta asignatura otorgaría una formación diferencial respecto a otras unidades académicas de la región?

Información relevada en Anexo B

Teniendo en cuenta la temática del trabajo, a continuación se transcriben los comentarios más relevantes manifestados por los entrevistados:

1.1 Representante de la Comisión de Diseño e Implementación del nuevo Plan de Estudios de la Carrera de Contador Público

Nos manifiesta que, al recibirse la Resolución Ministerial para la acreditación de la carrera de CP, la Comisión encargada del diseño e implementación del nuevo plan de estudios, observó que el área de "Administración y TI" tenía una carga horaria menor a la requerida por la exigencia. Además, notaron en este documento, basa la formación de la disciplina antes mencionada, en dos pilares: Finanzas y "Tecnologías de la Información", lo cual es considerado como el perfil deseado.

Asimismo, indica que estuvo bajo análisis, solicitar la obligatoriedad de la materia "Sistemas de Información II" en el nuevo plan de estudios. Esto con el objetivo de cumplir los requerimientos en cuanto a contenidos y carga horaria de la disciplina. Finalmente, se decidió aumentar la carga horaria a "Sistemas de Información I", para suplir la deficiencia encontrada.

Además, la comisión evidenció que se esperarían egresados del nuevo plan de estudios a partir del año 2024, por lo que consideró imposible concebir un perfil profesional sin un fuerte dominio en TI.

El entrevistado afirma que un mayor uso de las tecnologías para el manejo de la información, generará una mayor cantidad de vulnerabilidades en los circuitos operativos y técnicos, aumentando de este modo los riesgos.

Seguidamente, nos manifiesta que la asignatura de "Seguridad y Control en Sistemas Informáticos" fue bien recibida en la comisión y que no hubo mayores discusiones para lograr su inclusión en el plan de estudios. También considera que el bloque optativo de asignaturas de "TI", debería ser elegido por la mayoría de los alumnos, pues esta formación lo prepararía para

desempeñarse idóneamente en los mercados actuales. Indica que la asignatura propuesta cubre necesidades actuales y futuras. En este aspecto, hace hincapié en la necesidad de otorgar formación en la protección de datos personales y en la gestión de bases de datos.

Así también indica que, debido al avance de las TIC, el Contador tiene ámbitos de incumbencia que están fuertemente identificados en la actualidad: primero el asesoramiento y planificación fiscal y laboral con una visión macro y el segundo el control. Este último mediante la integración de mecanismos de seguridad para reducir riesgos en los sistemas. Seguidamente expresa que, en la Argentina, no hay profesionales capacitados en aspectos de seguridad informática para la gestión de las organizaciones: "*El profesional en Ciencias Económicas desconoce muchas normativas al respecto"*.

En relación al armado de los bloques de materias optativas en el nuevo plan de estudios, se fortaleció la rama jurídica-contable y la disciplina de Administración. Se integraron materias de TI debido a que el mundo está ampliamente integrado por la tecnología. Esto se justifica ya que el Contador tiene que estar preparado para ser un usuario demandante de aquel que tiene a su cargo el diseño y los mecanismos de control de los sistemas de información.

Además, afirma que en la "comisión" hubo consenso respecto a la incorporación de materias sobre "TI" en el nuevo plan de estudios.

Los encargados del diseño de este nuevo programa de estudios no quieren para el alumno una formación que se limite a lo que establece la Resolución Ministerial, ya que ella es muy técnica. Es por ello que a través de las asignaturas optativas se intenta ofrecer al estudiante una actualización y una visión más integral sobre las personas, procesos y organizaciones.

Reflexiona en que la formación en TI es fundamental en el perfil del graduado en ciencias económicas. Considera que en un futuro cercano la tecnología tendrá una fuerte influencia en todas las labores realizadas por el contador.

Finalmente señala que la asignatura propuesta ofrece una formación diferencial respecto a otras instituciones de la región. Considera que el Contador debe poseer conocimientos en control de sistemas informáticos indispensablemente, para desempeñarse como un buen auditor, situación que se fortificará con el correr de los años.

1.2 Representante N°1 del Honorable Consejo Directivo de la Facultad de Ciencias Económicas UNT

El entrevistado indica que según su punto de vista, no ha habido una gran estrategia para el armado de materias optativas, sin embargo se observó una preferencia de las asignaturas del área de administración.

Considera que la carrera de CP tiene que realizar un cambio de enfoque. Tiempo atrás, su incumbencia más importante eran los impuestos y la auditoría, pero actualmente el primero de ellos tendería a desaparecer. Por tal motivo, esta profesión debería enfocarse hacia un perfil de "gestión" o de "control y auditoría", aunque hace mención a que las Facultades de Ciencias Económicas no tienen bien claro el perfil que quieren para para sus egresados.

Asimismo, manifiesta que el presidente de la FACPCE en la apertura del último Congreso Nacional de Ciencias Económicas, planteó que la profesión del Contador tiene que reorientarse rápidamente, debido a que las labores impositivas tenderán a desaparecer.

Por otra parte, considera que la comisión de diseño e implementación del nuevo plan de estudios no tuvo un criterio definido para la selección de materias optativas del bloque de TI.

Además, manifiesta que la carrera de CP es una carrera muy enfocada a lo operativo y que las materias de "TI" le aportan al egresado una mirada sistémica y general. También señaló que la asignatura de "Seguridad y Control de Sistemas Informáticos", le permitirá al egresado observar el proceso contable desde otro lugar: no desde lo operativo, sino desde el control y la veracidad de la salida de la información.

Seguidamente señala que el HCD no ve como fundamental la formación en aspectos de TI, pero si la ve como importante. Algunos consideran que la formación en tecnologías debe ser impartida fuera de la universidad, pues confunden esta instrucción con la enseñanza de herramientas.

Afirma que hubo pleno consenso para la aprobación de la asignatura propuesta. Esta fue adecuada y nadie se opuso o realizó alguna objeción al respecto. Considera que si la carrera se enfoca al "control y la auditoría" la materia sería fundamental, y debería pasar a ser obligatoria. Además, señaló que la misma generará una formación diferencial en la oferta académica, respecto a otras instituciones de la región, con un gran valor agregado para la profesión.

Finalmente hace referencia a que el contador cumple una función de fedatario y tiene que asegurar la validez de la información presentada a los interesados: clientes, proveedores, accionistas, inversores, etc.

1.3 Representante N°2 del Honorable Consejo Directivo de la Facultad de Ciencias Económicas UNT

El entrevistado indicó que el criterio de incluir en los programas de estudios materias optativas, fue ofrecer un espacio de especialización. Por eso es que las optativas dependen de una materia principal. Sin embargo, en la carrera de CP, las áreas de formación estaban normalizadas por Resolución Ministerial.

Reflexiona que el espacio optativo debería servirle al alumno para estar a la vanguardia en un área de conocimiento. Sin embargo, se observa este generalmente elige la asignatura por el horario y por la escasa oferta académica actual.

Además, considera que en la carrera de CP se observa que no hay una definición clara respecto a la formación en tecnologías, habilidades blandas e investigación; se centran en lo normativo, propio de la epistémica de la profesión.

También comenta que el bloque de materias en “TI” contribuye a la formación actual que necesita el profesional universitario, el cual se desenvolverá en el mundo laboral digital

Opina que la asignatura propuesta permitiría ofrecer un nuevo servicio profesional (CP), ante una profesión que actualmente está interpelada. En el caso de los LA permitiría una profundización en el análisis de los modelos y procesos de negocios.

Considera que, dado el avance de la tecnología y el estado de la economía digital, las materias que actualmente son optativas en el área de “TI”, deberían pasar a ser obligatorias para la carrera de CP y LA. Además, señala que la formación en Seguridad Informática es fundamental para la formación del perfil del profesional en Ciencias Económicas.

Finalmente comentó que hubo consenso para la incorporación de la asignatura de “Seguridad y Control de Sistemas Informáticos” en los planes de estudio. Además, considera que la asignatura brindaría una formación diferencial respecto a otras ofertas académicas de la región y brindará un espacio interesante para la práctica profesional.

Anexo C: Presentación del Programa de Asignatura

"Seguridad y Control de Sistemas Informáticos"

UNIVERSIDAD NACIONAL DE TUCUMAN
FACULTAD DE CIENCIAS ECONOMICAS

"2018 - Año del Centenario de la Reforma Universitaria"

CENTENARIO
DE LA REFORMA UNIVERSITARIA

San Miguel de Tucumán, 5 de Noviembre de 2018.

Sr. Decano
Facultad de Ciencias Económicas
Universidad Nacional de Tucumán
Mg. José Luis Jiménez
S / D

Ref.: Presentación Programa 2018 Seguridad y Control en Sistemas Informáticos

De mi consideración:

Por la presente me dirijo a Ud. y por su intermedio a quien corresponda, adjuntando Programa 2018 de la asignatura "**Seguridad y Control en Sistemas Informáticos**", teniendo en cuenta las consideraciones de la Resolución 463-HCD-18 del 29/10/2018.

Sin otro particular, saludo a Usted con distinguida consideración.

Prof. María Alejandra Masclef
Titular
Sistemas de Información I

FACULTAD DE CIENCIAS ECONOMICAS
- 6 NOV. 2018
MESA DE ENTRADAS

Anexo D: Aprobación del Programa Analítico "Seguridad y Control de Sistemas Informáticos"

UNIVERSIDAD NACIONAL DE TUCUMAN
FACULTAD DE CIENCIAS ECONÓMICAS

"2018 - Año del Centenario de la Reforma Universitaria"

1918 2018 CENTENARIO DE LA REFORMA UNIVERSITARIA

521 HCD 18

San Miguel de Tucumán, 28 NOV 2018

Expte. 55.811/18

VISTO:

La presentación efectuada por el Cra. María Alejandra Masclef, Profesora Titular de la cátedra Sistema de Información I de esta Facultad, mediante la cual eleva a consideración del H. Consejo Directivo el Programa Analítico de la asignatura optativa SEGURIDAD Y CONTROL DE SISTEMAS INFORMATICOS [Planes 2010/2014], para ser aplicado a partir del Período Lectivo 2019; y

CONSIDERANDO:

Que se ha dado intervención a las Comisiones de Implementación y Seguimiento de Planes de Estudios de las carreras de Contador Público Nacional y Licenciatura en Administración quienes se expiden aconsejando se apruebe el Programa presentado;

Que puesto a consideración del Cuerpo como Asunto a Consideración Directa, y el acuerdo unánime de los Consejeros presentes;

POR ELLO:

EL H. CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS ECONÓMICAS

En su Sesión Extraordinaria de fecha 20 de noviembre de 2018

RESUELVE:

Art. 1º Aprobar el Programa Analítico de la asignatura optativa SEGURIDAD Y CONTROL DE SISTEMAS INFORMATICOS [Planes 2010/2014], de las carreras de Contador Público Nacional y Licenciatura en Administración para ser aplicado a partir del Período Lectivo 2019, el que como Anexo forma parte integrante de la presente.

Art. 2º Hágase saber y resérvese en la Secretaria de Asuntos Académicos a sus efectos.

MG. CHRISTINE ADRIANE ISGRO
SECRETARIA DE ASUNTOS ACADEMICOS
FACULTAD DE CIENCIAS ECONOMICAS
UNT

MG. JOSE LUIS ANTONIO JIMENEZ
DECANO
FACULTAD DE CIENCIAS ECONÓMICAS
UNT

FACULTAD DE CIENCIAS ECONÓMICAS
- 1 MAR. 2019
MESA DE ENTRADAS

Anexo E: Encuesta a integrantes de DUTI – Año 2019

1.1 Objetivo Específico de la Encuesta

En el contexto de las “XIV Jornadas de Docentes Universitarios en Sistemas y Tecnologías de la Información” realizadas desde el 3 al 5 de octubre de 2019, en la Facultad de Ciencias Económicas de la Universidad Nacional de La Plata, se instrumentó una segunda encuesta, realizada por profesores de las diferentes Facultades de Ciencias Económicas del país.

El objetivo de la misma, fue relevar la situación actual de las diferentes unidades académicas, respecto a los planes de estudios vigentes y su relación con la formación del alumno sobre “Sistemas y Tecnologías de la Información” en general y, "Seguridad y Control de Sistemas Informáticos" en particular, luego de transcurrida la primera etapa del proceso de acreditación de la CONEAU.

1.2 Instrumento Utilizado

1- Indique la Universidad a la que pertenece

2- Indique la Unidad Académica a la que pertenece

3- Indique el estamento docente al que pertenece

a) Profesor Titular

b) Profesor Asociado

c) Profesor Adjunto

d) Jefe de Trabajos Prácticos

e) Auxiliar Docente

4- Considera importante el dictado de temas relacionados con "Seguridad y Control de Sistemas Informáticos" en las carreras de "Contador Público" y "Licenciatura en Administración", para la "Gestión Estratégica de Negocios"

a) Si

b) No

5- La Resolución 2017-3400-APN-ME - para la acreditación de la Carrera de Contador Público, define los contenidos curriculares básicos de la misma y dentro del área temática "Administración y Tecnologías de la Información" establece la inclusión de "Seguridad en los Sistemas de Información". Para dar cumplimiento a este requerimiento, en el plan de estudios de su unidad académica:

a) Se realizaron modificaciones para incluir el tema

b) El tema ya se encontraba incluido en alguna de las asignaturas.

c) No sabe / No Conoce

SOLO SI RESPONDE LA A): Indique las modificaciones realizadas para incluir el tema en el Plan de Estudios.

a) El tema fue incluido dentro de la materia principal de "TI" / "Sistemas de Información"

b) El tema fue incorporado en otra asignatura, no relacionada con la disciplina de Sistemas/TI. (Ejemplo: Auditoría)

c) Se incorporó una materia específica en el plan de estudio sobre la temática en cuestión

d) Otro. Indique

SOLO SI RESPONDE LA C): La asignatura incorporada tiene la siguiente característica.

a) Es Obligatoria

b) Es Electiva / Optativa

6- Considerando el plan de estudio vigente (posterior al proceso de acreditación) para la carrera de Contador Público ¿Qué ponderación le otorga a la formación, en general, respecto a "Sistemas y Tecnologías de la Información"?

a) Excesiva

b) Suficiente

c) Insuficiente

d) No Sabe / No Conoce

7- Considerando el plan de estudio vigente para la carrera de Licenciatura en Administración ¿Qué ponderación le otorga a la formación, en general, respecto a "Sistemas y Tecnologías de la Información"?

a) Excesiva

b) Suficiente

c) Insuficiente

d) La Unidad Académica no otorga el título de "Licenciado en Administración"

e) No Sabe / No Conoce

8- Teniendo en cuenta el Plan de Estudio vigente para la carrera de Contador Público ¿Cómo considera la formación en “Seguridad y Control de Sistemas Informáticos”? (teniendo en cuenta que esta temática forma parte de los contenidos curriculares mínimos obligatorios de la carrera)

a) Excesiva

b) Suficiente

c) Insuficiente

d) No Sabe / No Conoce

9- Teniendo en cuenta el Plan de Estudio vigente para la carrera "Licenciatura en Administración" ¿Cómo considera la formación en “Seguridad y Control de Sistemas Informáticos”?

a) Excesiva

b) Suficiente

c) Insuficiente

d) No Sabe / No Conoce

10- Indique su nivel de acuerdo respecto a la siguiente frase: “en la Argentina, no hay suficientes profesionales capacitados en aspectos sobre seguridad informática para la Dirección y Gestión de las Organizaciones”

a) Muy de acuerdo

b) De acuerdo

c) Poco de acuerdo

d) Nada de acuerdo

11- ¿Considera que el alumno de "Contador Público" debería necesariamente recibir formación en su carrera de grado sobre “Seguridad y Control de Sistemas Informáticos” para efectuar tareas de auditoria?

a) Muy de acuerdo

b) De acuerdo

c) Poco de acuerdo

d) Nada de acuerdo

12- ¿Considera que la formación sobre “¿Seguridad y Control en Sistemas Informáticos”, permitiría al graduado en Ciencias Económicas ampliar su ámbito de incumbencia profesional?

a) Muy de acuerdo

b) De acuerdo

c) Poco de acuerdo

d) Nada de acuerdo

13- ¿Considera que una formación en “¿Seguridad y Control en Sistemas Informáticos”, otorgaría al graduado de su unidad académica un perfil profesional diferencial respecto a la de otras ofertas académicas de la región?

a) Muy de acuerdo

b) De acuerdo

c) Poco de acuerdo

d) Nada de acuerdo

Anexo F: Encuesta a expertos de la "Seguridad de la Información" – Año 2020

1.1 Objetivo Específico de la Encuesta

En el contexto de la Diplomatura en “Estrategia de ciberseguridad e inteligencia en cibercrimen” organizada por la Universidad del Norte Santo Tomás de Aquino (UNSTA), en desarrollo entre los meses de Septiembre y Diciembre de 2020, se diseñó y realizó una encuesta a los participantes, en su mayoría expertos de la "Seguridad de la Información", relevando aspectos relacionados a su experiencia de trabajo y precepción de conocimientos respecto de profesionales Ciencias Económicas, con los que han tenido oportunidad de trabajar, para una adecuada gestión y dirección de organizaciones, contemplando el ámbito de la Seguridad y el Control de la Información.

1.2 Instrumento Utilizado

Herramienta: Formulario de Google (bit.ly/Encuesta SI)

1. Indique "Sexo"
2. Indique el nombre de la provincia en la que actualmente reside
3. Indique rango de edad
4. ¿Cuál es su formación Universitaria de Grado? (Ejemplo: Ingeniero en Computación, Abogado, Contador Público, etc.)
5. ¿Cuál es su formación Universitaria de Posgrado? (Ejemplo: Magister de la Universidad de Buenos Aires en Seguridad Informática, Magister en Administración, etc.)
6. ¿Cuál es su formación específica en el ámbito de la "Seguridad de la Información"? (Ejemplo: Diplomatura, Certificación internacional, Capacitación empresarial, Autodidacta, etc.)
7. ¿En qué aspectos de la "Seguridad de la Información" trabaja actualmente?

8. ¿Cuál es su desempeño profesional en el ámbito de la "Seguridad de la Información"? (Ejemplo: Gerente del Departamento de Sistemas en empresa privada)

9. En el ejercicio de su profesión en el campo de la "Seguridad de la Información" ¿ha tenido que trabajar conjuntamente con un profesional en Ciencias Económicas (Contador Público, Lic. en Sistemas de Información, Lic. en Administración, Lic. en Economía, etc.)?

10. ¿Qué rol cumplía el profesional en Ciencias Económicas con el que tuvo que trabajar conjuntamente?

11. ¿El profesional en Ciencias Económicas contaba con la formación y utilizaba la jerga epistemológica adecuada para comprender / interpretar lo que se le solicitaba?

12. ¿Qué aspectos considera que debería incluir la formación de un profesional en Ciencias Económicas, para desempeñarse idóneamente en un "Comité de Seguridad"?

13. ¿Considera necesaria la formación de los Profesionales en Ciencias Económicas en el área disciplinar de la "Seguridad de la Información"?

14. Indique sus comentarios o consideraciones finales, si lo desea

1.3 Desarrollo

Se encuestaron a profesionales relacionadas con el ámbito de la Seguridad de la Información, de doce provincias, las cuales se detallan a continuación:

- Buenos Aires
- Catamarca
- Chaco
- Ciudad Autónoma de Buenos Aires
- Corrientes
- Jujuy
- Mendoza
- Misiones

- Neuquén
- Río Negro
- Santiago del Estero
- Tucumán

1.4 Resultados

De las respuestas recopiladas, el 70% corresponde a personas de sexo masculino y el 30% restante de sexo femenino.

En cuanto al rango etario de la muestra, el mismo se detalla a continuación:

Franja etaria	**%**
20 a 30 años	13%
31 a 40 años	30%
41 a 50 años	47%
51 a 60 años	10%
Total	**100%**

Fuente: elaboración propia

El 85% de los encuestados cuentan con título universitario de grado. Las carreras indicadas, se detallan a continuación:

- Abogado
- Analista en Sistemas
- Contador Público
- Ingeniero Electrónico
- Ingeniero en Computación
- Ingeniero en Informática
- Ingeniero en Sistemas de Información
- Ingeniero Industrial
- Licenciado en Informática

- Licenciado en Relaciones Internacionales
- Licenciado en Sistemas de Información

El 47% de los indagados cuentan con un título universitario de posgrado. Los programas cursados por ellos, se detallan a continuación:

- Especialista en Educación Superior y TIC
- Especialista en Ingeniería
- Integración Regional
- Maestría en Administración y Dirección de Empresas
- Maestría en Informática
- Maestría en Ingeniería de Software
- Especialidades no especificadas

En cuanto a la formación específica en el ámbito de la "Seguridad de la Información", el 83% respondió haber realizado una especialización, diplomatura, certificación internacional o capacitación empresarial al respecto.

El 87% de los encuestados, actualmente se desempeña laboralmente en el ámbito de la “Seguridad de la Información” o afines. Se destacan algunos puestos donde se desempeñan profesionalmente:

- Administrador de Sistemas
- Analista de Seguridad de la Información
- Analista Protección de Activos
- Consultor de Ciberseguridad
- Encargado de Investigaciones y auditoría de Seguridad de la Información
- Jefe de departamento de Seguridad de la Información y Ciberseguridad
- Jefe de Gobierno, Riesgo y Cumplimiento de la Seguridad de la Información
- Jefe de Marco Normativo y Plataformas Seguridad

- Jefe de Seguridad de la Información
- Supervisor de Auditoría Interna de TI
- Supervisor de Seguridad Informática

Con el afán de recabar información acerca de los conocimientos que consideran, deberían poseer los profesionales Ciencias Económicas, para una adecuada gestión y dirección de organizaciones, contemplando el ámbito de la Seguridad y el Control de la Información; se indagó a los encuestados si en ámbito laboral y relacionado a la "Seguridad de la Información", habían tenido que trabajar conjuntamente con un profesional en Ciencias Económicas. El 70% de ellos respondió afirmativamente, indicando que el rol que cumplían estos últimos era algunos de los siguientes:

- Analista Funcional
- Cliente
- Director de Área funcional
- Gerente de Área
- Miembro de equipo de trabajo
- *Project Manager*
- *Tester*
- Usuario

A los que respondieron afirmativamente el enunciado anterior, se les consultó si el profesional en Ciencias Económicas, a su criterio, contaba con la formación y utilizaba la jerga epistemológica adecuada para comprender o interpretar lo que se le solicitaba o lo que se estaba planificando y/o implementando. Las respuestas fueron las siguientes:

Respuesta	%
Si	5%
Parcialmente	52%
No	43%
Total	**100%**

Fuente: elaboración propia

Se enfatiza, en concordancia con el objetivo del presente trabajo, que el 95% de los encuestados manifiesta que el profesional en Ciencias Económicas comprendía parcialmente o no comprendía lo que se le requería, lo que se planificaba y/o implementaba o se estaba evaluando respecto de “Seguridad de la Información” en un sentido amplio.

Así mismo, se indagó sobre los aspectos que consideran, debería incluir la formación de los profesionales en Ciencias Económicas, para desempeñarse idóneamente en un "Comité de Seguridad". Las respuestas más relevantes fueron las siguientes:

- Normativas generales en ciberseguridad y metodologías de evaluación del riesgo
- Conocimientos en Seguridad de la Información y Ciberdelitos, para la concientización del personal
- Auditoría de Sistemas y estándares de seguridad
- Planes de continuidad del negocio y de contingencias
- Políticas, normas, roles y cumplimiento para la Seguridad de la Información
- Fundamentos de un Sistema de Gestión de Seguridad de la Información. Por ejemplo: familia de normas ISO 27000

Se destaca que el 70% de los encuestados, consideraron necesaria la formación de los Profesionales en Ciencias Económicas en el área disciplinar de la "Seguridad de la Información”, para una adecuada gestión y dirección de organizaciones.

Para finalizar se hace mención a algunos de los comentarios realizados por los consultados. Consideran que el profesional debería ser idóneo en la temática, para responsabilizarse de los activos de la información que son de su incumbencia profesional.

Además, manifiestan que en general los Planes de Estudios de las carreras relacionadas a las Ciencias Económicas están desactualizados y adolecen de formación en Sistemas de Información.

Asimismo, indican que la Seguridad de la Información es absolutamente necesaria para la gestión de cualquier organización pública o privada; y que la gestión estratégica de negocios incorpora un pensamiento que resulta útil únicamente si el área de seguridad es considerada una unidad de negocios.

1.5 Conclusiones

Con el desarrollo, generalización y agresivo crecimiento, en el ámbito tecnológico, y en el de generación, vinculación y disponibilidad de datos e información, nos encontramos frente a un contexto que poco tiene que ver con el modo de instrumentar los procedimientos y los mecanismos para la toma de decisiones, como se venían desarrollando. En este mismo sentido la cantidad de información y la dependencia de las organizaciones de la misma, torna imprescindible dotar de seguridad y garantizar la integridad, disponibilidad y confidencialidad de la información.

Del análisis de los resultados, surge que el 70% de los encuestados trabajó interdisciplinariamente con profesionales en Ciencias Económicas, en el transcurso de su trayectoria laboral. Como lo indican, estos últimos se desempeñaban en diferentes roles relacionados con el análisis, diseño, testeo, administración de proyectos, etc., relacionados con los Sistemas y las Tecnologías de la Información. Esto pone de manifiesto los diferentes roles y funciones de ejercicio profesional, que el graduado en Ciencias Económicas puede asumir

relacionado al mencionado tema, incluyendo además el desempeño de actividades y/o responsabilidades en el ámbito de la Seguridad de la Información, objeto de este trabajo.

En este sentido se considera relevante, que el 95% de los consultados manifiesta que el profesional en Ciencias Económicas, con el que tuvo que trabajar interdisciplinariamente, no comprendía lo que se le solicitaban respecto a la temática de la “Seguridad de la Información”, o lo comprendía parcialmente.

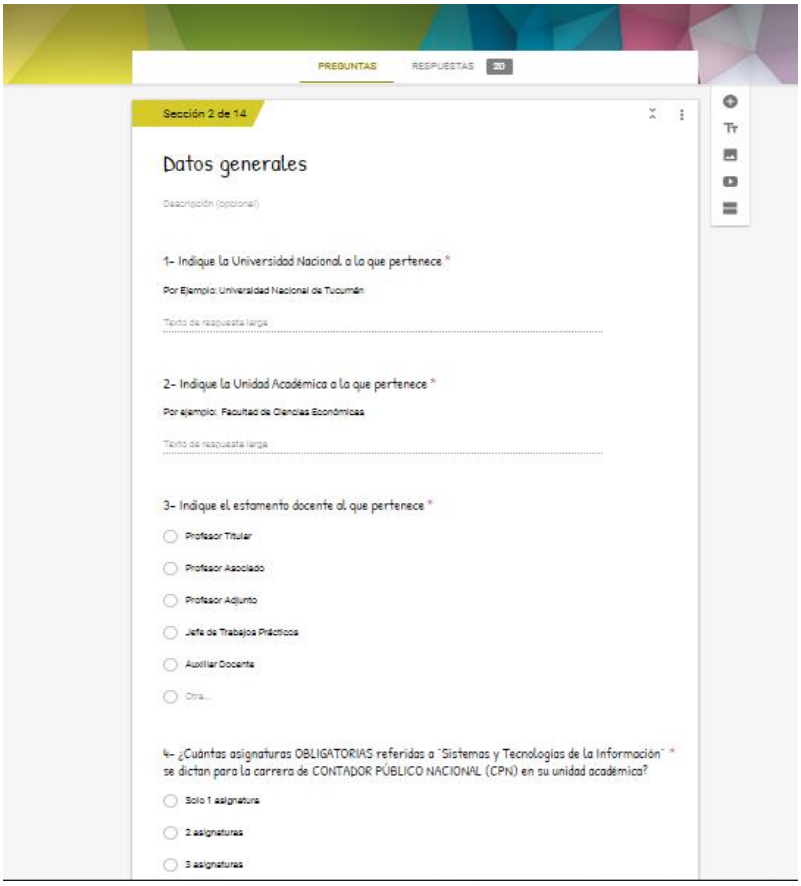
Dados los avancen tecnológicos en materia de almacenamiento, recuperación y análisis de datos y las nuevas formas de tele trabajo y movilidad, la Seguridad y el Control de la Información, son contenidos esenciales en el diseño curricular de las carreras de Contador Público y Licenciado en Administración. Sin embargo, conforme relevamientos anteriores, puede observarse la falta de contenidos sobre la temática en las currículas de Ciencias Económicas, en el presente trabajo podemos relevar la percepción y los inconvenientes, al momento de trabajar interdisciplinariamente con profesionales de áreas de Tecnologías de la Información y Seguridad.

Finalmente se hace referencia a que el 70% de los encuestados, consideraron necesaria la formación de los Profesionales en Ciencias Económicas en el área disciplinar de la "Seguridad de la Información”, para una adecuada gestión y dirección de organizaciones.

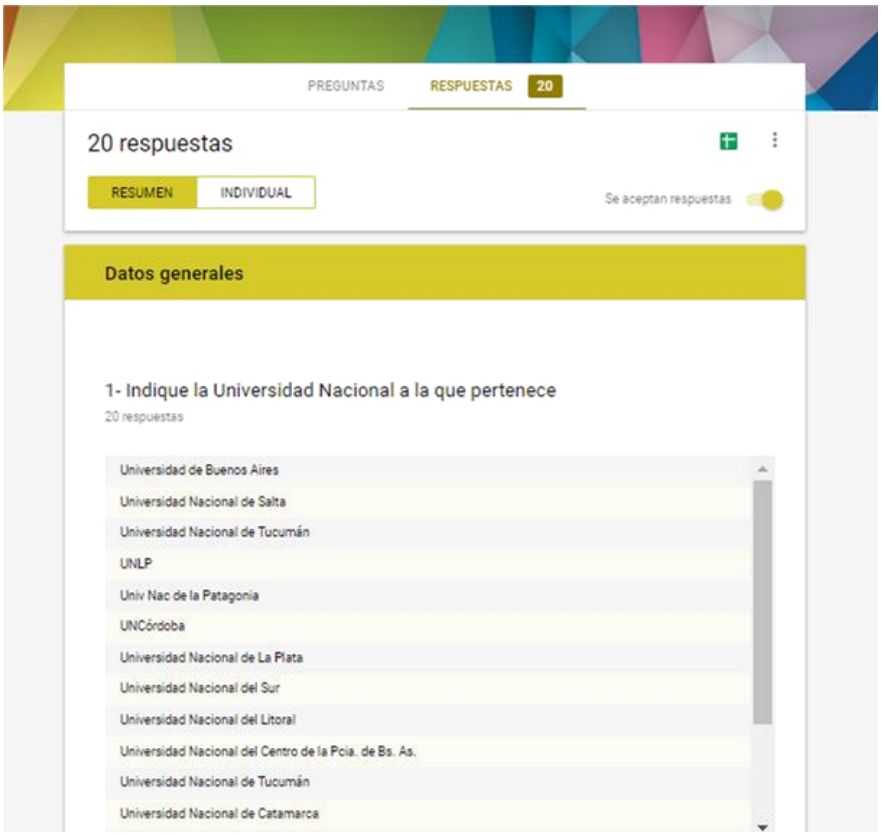
Apéndice

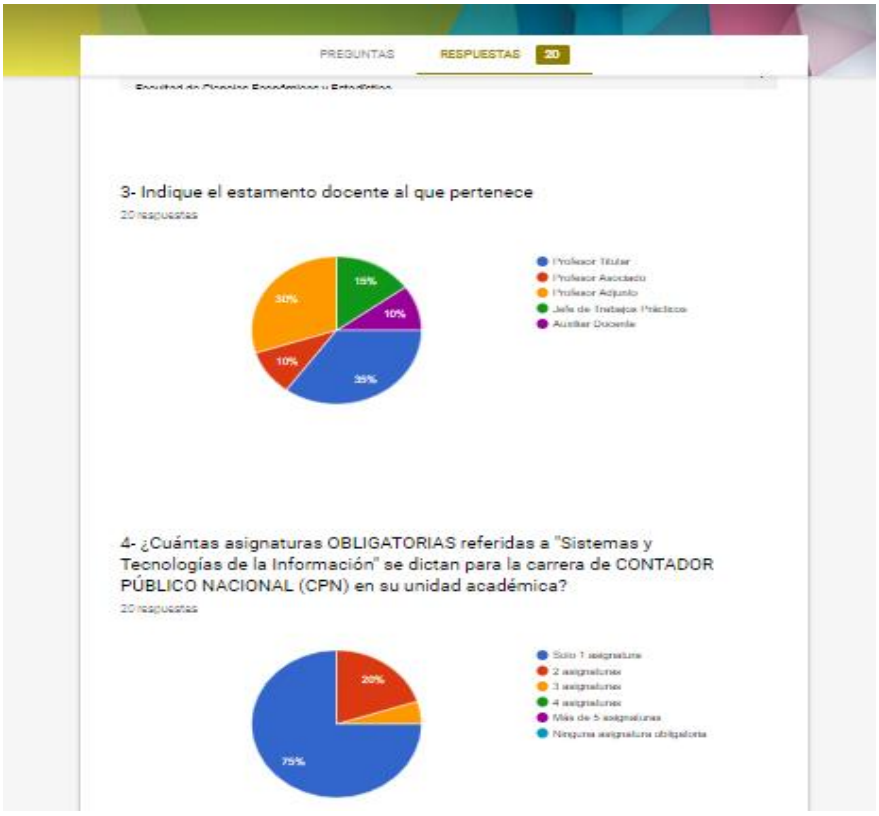
Presentación de la Encuesta. Herramienta utilizada: “Formulario de Google”

Diseño del cuestionario. Preguntas:



Análisis de las respuestas:





Abreviaturas

- **AWS**: Amazon *Web Services*
- **CIO**: *Chief Information Officer*
- **CONEAU**: Comisión Nacional de Evaluación y Acreditación Universitaria
- **CP**: Contador Público
- **DUTI**: Asociación de Docentes Universitarios en Sistemas y Tecnologías de la Información de Facultades de Ciencias Económicas Nacionales
- **FACE**: Facultad de Ciencias Económicas
- **FACPCE**: Federación Argentina de Consejos Profesionales en Ciencias Económicas
- **GDPR**: Reglamento General de Protección de Datos
- **HCD**: Honorable Consejo Directivo
- **HCS**: Honorable Consejo Superior
- **LA**: Licenciatura en Administración
- **N°**: Número
- **OEA**: Organización de los Estados Americanos
- **PDS**: Plan Director de Seguridad
- **Pymes**: Pequeñas y medianas empresas
- **Res.**: Resolución
- **SGSI**: Sistema de Gestión de Seguridad de la Información
- **S y C SI:** Seguridad y Control de Sistemas Informáticos
- **S y TI:** Sistemas y Tecnologías de la Información
- **TI**: Tecnologías de la Información
- **TIC**: Tecnologías de la Información y la Comunicación
- **UBA**: Universidad de Buenos Aires
- **UNICEN**: Universidad Nacional del Centro de la Provincia de Buenos Aires
- **UNT**: Universidad Nacional de Tucumán

Bibliografía

Bibliografía Específica

- Baca Urbina G. (2016). *Introducción a la Seguridad Informática*. 1ra edición ebook. México. Grupo Editorial Patria.
- Cano M. J. J. (2013). *Inseguridad de la información: Una visión estratégica.* Bogotá. Alfaomega.
- Castello, R. J. (2008). *Auditoría de sistemas y tecnologías de información*. Córdoba, Edición digital. En internet: http://e-conomicas.eco.unc.edu.ar/archivos/_3/AudSistLibro08.
- Collazo J. y Saroka R. H. (2010). *Informática en las Organizaciones.* 1º edición, Buenos Aires, Argentina. EDICON
- Coraminas, J. (1961). *Breve diccionario epistemológico de la lengua castellana.* 3° ed. Madrid, España. Editorial Gredos.
- Gallo, F.D. (2010). *"Inseguridad Informática".* España. Editorial Cooma.
- Lardent, A. R. (2001). *Sistemas de información para la gestión empresaria: procedimientos, seguridad y auditoría.* 1ª ed. Buenos Aires, Argentina. Pearson Education.
- Steiman, J. (2007). *Más Didáctica en la educación superior.* Cap. 1: Los proyectos de cátedra. Buenos Aires, Argentina. Miño y Dávila-UNSAM.
- Torres A. (2017). *Hackearán tu mente.* 1° Edición. Argentina Grupo editorial Planeta SAIC.
- Usandivaras de Hlawaczek, S. E. T. (2012). *Preparación de Tesis MBA.* 1° edición. Argentina. Universidad Nacional de Tucumán, Facultad de Ciencias Económicas.

Informes Especializados

- Academia ESET Latinoamérica (10 de enero de 2019) Tendencias 2019: privacidad e intrusión en la aldea global Recuperado el 10 de enero de 2019 de: https://empresas.eset-la.com/novedad/tendencias-2019-privacidad-e-intrusion-en-la-aldea-global
- Academia ESET Latinoamérica (s.f.). ESET Security Report 2018. Recuperado el 15 de julio de 2018 de: https://empresas.eset-la.com/novedad/eset-security-report-2018

- Bravo R. (2018). Doble Virus. Update trending. Revista Info Tecnology. Año 22, N° 252, septiembre 2018, pág. 20.

- Cobb, S. (2019). GDPR: ¿El primer paso hacia una ley de privacidad global? Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

- Encuesta de Seguridad Informática: Las empresas y los nuevos desafíos en Seguridad. Publicación (15/08/2018). Binder Dijker Otte y Taquión. Recuperado el 20 de septiembre de 2018 de: https://www.bdoargentina.com/es-ar/publicaciones/categoria-de-publicaciones/ grupo-de-publicaciones/encuesta-de-seguridad-nformatica

- Garcia, M.A. Masclef M. A. (2018). "Implementación del "Modelo 5S", para el fortalecimiento de la seguridad física de la información, en área funcional de empresa de transportes". Argentina. Libro II "IIº Congreso de Administración del Jardín de la República" y "Encuentro Inter-Regional ADENAG Centro Oeste y Noroeste Argentino". 1° ed. comprendida ISBN: 978-798-3926-48-8.

- Gutiérrez Amaya, C. (2019). Asistentes de voz para el hogar: cuando tus dispositivos nunca se apagan. Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

- Gutierrez C. (2020). Transformación digital y seguridad de la información: el reto para las empresas. Academia ESET Latinomérica. Tendencias 2020: La tecnología se está volviendo cada vez más inteligente ¿Y nosotros?

- Harley, D. (2019). Coinminers: el nuevo chico del barrio. Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

- Jake Moore (2020). El futuro del trabajo: abrazando una nueva realidad. Welivesecurity de ESET Latinoamérica. Tendencias en Ciberseguridad para el 2021: mantenerse seguros en tiempos de incertidumbre.

- Masclef, M. A. (2016). Infraestructura de Seguridad de la Información. Cátedra de Sistemas de Información I. Facultad de Ciencias Económicas UNT, Tucumán, Argentina.

- Myers L., Cobb, S. (2019). Privacidad recargada: ¿Será ella quién decida que negocios sigan en pie? Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

- Myers, L. (2019). Las Máquinas aprenden, los Humanos no tanto. Academia ESET Latinoamérica. Tendencias 2019: privacidad e intrusión en la aldea global.

- OEA y AWS (2018). Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción a las TIC. *White paper series*, 3° edición. Publicado el 28 de agosto de 2018. Chile.

- OEA y AWS (2018). Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción a las TIC. *White paper series*, 3° edición. Publicado el 28 de agosto de 2018 en Chile.

- Welivesecurity (2020). Tendencias en Ciberseguridad para el 2021: mantenerse seguros en tiempos de incertidumbre. Recuperado de internet el 29 de enero de 2021 de: https://www.welivesecurity.com/wp-content/uploads/2020/12/ Cybersecurity_Trends_2021 _ES.pdf

Programas de Estudios

- Briano, Juan Carlos y otros (2006). Programa de Asignatura: Auditoría y Control de Sistemas de Información (Materia N° 659). Departamento de Sistemas. Carrera de Licenciado en Sistemas de Información de las Organizaciones. Facultad de Ciencias Económicas, Universidad de Buenos Aires.

- Masclef, M. A. (2018). Programa de Asignatura: “Sistemas de Información I”, para el período lectivo 2019. Instituto de Administración, Facultad de Ciencias Económicas, Universidad Nacional de Tucumán.

- Masclef, M.A. (2018). Programa de Asignatura: “Análisis y Diseño de Sistemas / Computación II”. Instituto de Administración, Facultad de Ciencias Económicas, Universidad Nacional de Tucumán.

- Masclef, M.A. (2018). Programa de Asignatura: “Sistemas de Información II”, para el período lectivo 2019. Instituto de Administración, Facultad de Ciencias Económicas, Universidad Nacional de Tucumán.

- Presentación del Master en Seguridad de la Información y Continuidad de Negocios (Ciberseguridad). EADIC y Universidad Católica San Antonio de Murcia, Cohorte 2019/2020 (s.f). Recuperado el 15 de agosto de 2018 de: https://www.eadic.com/documentos-informativos/Master-Ciberseguridad.pdf

- Programa de Asignatura “Seguridad, Control y Auditoria de Sistemas” de la carrera de posgrado “Especialización en Gestión Estratégica de la Tecnología. Facultad de Ciencias Económicas, Universidad Nacional de Rosario. Aprobado por: Resolución no14385-C.D. del 19-12-2006

- Programa de estudios: Diplomatura en Seguridad de la Información (s.f.). Sitio web de la Diplomatura en Seguridad de la Información. Universidad Católica de Salta. Recuperado el 15 de Julio de /2018 de: http://sistemas.ucasal.edu.ar/CursosUcasal/cursos/844/ diplomatura_en_seguridad_ informatica.xhtml

- Programa de estudios: Diplomatura en seguridad de la información – Cibercrimen (s.f.). Sitio web de la Universidad Siglo XXI: Recuperado el 21 de septiembre de 2018 de: https://contenidos.21.edu.ar/landings/cloud21/diplomatura-en-seguridad-de-la-informacion. php?

- Programa de Estudios: Experto Universitario en Ciberseguridad y Protección de Sistemas (s.f.). Sitio Web de IMF *Business School*. Recuperado el 20 de noviembre de 2018 de: https://www.imf-formacion.com/cursos-superiores/curso-seguridad-sistemas

- Programa de estudios: Maestría en Seguridad Informática (s.f). Sitio web de la Maestría en Informática de la UBA. Recuperado el 03 de octubre de 2018 de: http://www.economicas.uba.ar/posgrado/posgrados/seguridad-informatica/

- Programa de estudios: Master en Ciberseguridad Sitio web del Master en Seguridad Informática (s.f). Sitio Web de IMF *Business School*. Recuperado el 29 de noviembre de 2018 de: https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica

- Programa de estudios: Master en Seguridad de la Información y Continuidad de Negocios (s.f.) Sitio web de. EADIC. Recuperado el 16 de octubre de 2018 de:https://www.eadic-becas.com/documentos-informativos/Master-Ciberseguridad.pdf

Normativas

- Anexo I, II, III y IV de Resolución 3400-E/2017. Ministerio de Educación de la Nación. República Argentina, Ciudad de Buenos Aires, 20/07/2017. Recuperado el 12 de diciembre de 2018 de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279433/res3400.pdf

- Federación Argentina de Consejos Profesionales en Ciencias Económicas, CECYT (2008). Resolución Técnica N° 16: Marco Conceptual de las Normas Contables Profesionales. Argentina.

- IRAM, Instituto Argentino de Normalización (2007). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad en Tecnología de la Información.

- IRAM, Instituto Argentino de Normalización (2012). Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad".

- IRAM, Instituto Argentino de Normalización (2012). Norma ISO/IEC 27005: Tecnología de la información. Gestión del riesgo de seguridad de la información. Subcomité de Seguridad en Tecnología de la Información.

- Ley de Educación Superior N° 24.521. República Argentina. Sancionada el 20/07/1995 y promulgada el 07/08/1995 B.O. Recuperado el 09 de diciembre de 2018 de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25394/texact.htm

- Resolución 1271 HCS. Expte. 56380-018. Honorable Consejo Superior de la Universidad Nacional de Tucumán, del 27 de noviembre de 2018.

- Resolución 1271/2018 HCS. Aprobación del nuevo plan de estudios de la carrera de Contador Público, plan 2019. Universidad Nacional de Tucumán, Tucumán 29 de noviembre de 2018.

- Resolución 173D18: Misión, Visión y Valores de la FACE. Facultad de Ciencias Económicas, Universidad Nacional de Tucumán. Publicada el 23 de abril de 2018.

- Resolución 2075/2013 HCS. Aprobación del plan de estudios de la Licenciatura en Administración plan 2014. Universidad Nacional de Tucumán, Tucumán, 20 de septiembre de 2013.

- Resolución 3400-E/2017. Ministerio de Educación de la Nación. República Argentina, Ciudad de Buenos Aires, aprobada el 08/09/2017. Recuperado el 03 de diciembre de 2018de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279433/norma.htm

- Resolución 463HCD18. Expte. 56.380/18 Facultad de Ciencias Económicas, UNT. San Miguel de Tucumán, 29 de octubre de 2018.

- Resolución N° 093-HCD-19. "*Plan Estratégico Institucional 2019-2022*". Facultad de Ciencias Económicas, UNT. Publicado el 12 de abril de 2019.

- Resolución N° 542- HCD-18. "*Plan de Desarrollo de la carrera de Contador Público*". Facultad de Ciencias Económicas, UNT. Publicada el 28 de noviembre de 2018.

Consultas a Sitios Web

- Administración (s.f.). En Wikipedia. Recuperado el 30 de enero de 2019 de https://es.wikipedia.org/wiki/Administraci%C3%B3n

- Aprendizaje Automático. En Wikipedia. Recuperado el 14 de enero de 2019 de: https://es.wikipedia.org/wiki/Aprendizaje_autom%C3%A1tico

- Control (s.f.). En definion.es, recuperado el 22 de febrero de 2019 de: https://definicion.de/control/

- Cuarta Revolución Industrial en Latinoamérica: ¿cómo lo llevan los gobiernos? (s.f.) ISOTools, plataforma tecnológica para la gestión de la excelencia. Recuperado el 24 diciembre de 2018 de: https://www.isotools.org/2018/12/14/cuarta-revolucion-industrial-latinoamerica-hacen-gobiernos

- El plan para reconvertir el aparato militar (23/07/2018). Diario Clarín: Clarin.com. Buenos Aires, Argentina. Recuperado el 23 de julio de 2018 de: https://www.clarin.com/politica/mauricio-macri-anuncia-plan-reforma-fuerzas-armadas_0_ rkz _JEQEX.html

- Glosario de términos de ciberseguridad: una guía de aproximación para el empresario. INCIBE (s.f). Recuperado el 20 de febrero de 2018 de: https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

- Herrera J. (29/11/2018). Mercados rezan porque surjan señales de paz comercial. Diario Ámbito Financiero: ámbito.com. Buenos Aires, Argentina. Recuperado el 29 de noviembre de 2018 de: https://www.ambito.com/mercados-rezan-porque-surjan-senales-paz-comercial-n5002285

- Información (s.f.). En Wikipedia. Recuperado el 30 de enero de 2019 de: https://es.wikipedia.org/wiki/ Informaci%C3%B3n

- Inician las inscripciones para la Especialización en Auditoría y Contabilidad. En el sitio de web de la FACE UNT, recuperado el 27 de septiembre de 2019 de https://face.unt.edu.ar/web/blog/inician-las-inscripciones-para-la-especializacion-en-auditoria-y-contabilidad/

- Kevin Mitnick (s.f). En Wikipedia. Recuperado el 30 de enero de 2021 de: https://es.wikipedia.org/wiki/Kevin_Mitnick

- Mendoza M. A. (2015). Conceptos básicos de Seguridad de la Información. Sitio web de la academia ESET Latinoamérica. Recuperado el 15/ de agosto de 2018 de: https://www.academiaeset.com/default/std/myevents/45357

- Mendoza M. Á. (2015). Conceptos básicos de Seguridad de la Información. Sitio web de la academia ESET Latinoamérica. Recuperado el 23 de septiembre de 2018 de: https://www.academiaeset.com/default/std/myevents/45357

- Plan Director de Seguridad. Colección: Protege tu empresa (s.f). Sitio web de INCIBE. Recuperado el 15 de diciembre de 2018 de: https://www.incibe.es/sites/ default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

- Riesgo (s.f). Real Academia Española. En Diccionario de la lengua española: Recuperado el 20 de julio de 2018 de: http://dle.rae.es/srv/fetch?id=WT8tAMI

- Se reunió la Comisión Permanente para el Proceso de Autoevaluación Institucional de nuestra Facultad (12/04/2019). En el sitio web de la Facultad de Ciencias Económicas, recuperado el 15 de abril de 2019 de: https://face.unt.edu.ar/web/blog/se-reunio-la-comision-permanente-para-el-proceso-de-autoevaluacion-institucional-de-nuestra-facultad/

- SGSI: Blog especializado en sistemas de gestión de seguridad de la información ¿Cómo asegurar la seguridad de la información en las organizaciones?(s.f.) Recuperado el 22 de noviembre de 2018 de: https://www.pmg-ssi.com/2018/11/como-asegurar-la-seguridad-de-la-informacion-en-las-organizaciones/