ANEXO III: FORMULARIO DE PROYECTOS DE I+D

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

1. Título del Proyecto de I+D.

Análisis, investigación y proyección de las acciones de Ciberseguridad en la UNO.

2. Departamento/Instituto de radicación:

Instituto de Ingeniería y Nuevas Tecnologías.

3. Línea de Investigación y Desarrollo de pertenencia:

Prioritaria	X	Complementaria	

Denominación: Técnicas criptográficas y de seguridad en telecomunicaciones aplicadas a nuevas amenazas.

4. Tipo de Proyecto:

Acreditable	X	Reconocimiento institucional	

5- Período de vigencia:

01/03/2023 al 31/12/2024

6. Justificación del Proyecto

Hoy en día la seguridad de la información y la preservación de los sistemas de información se ha convertido en uno de los aspectos más críticos que toda organización debe cuidar, es por esta razón que en las distintas universidades del país se está dando un enfoque más profundo a la investigación en esta disciplina.

Sin embargo, ese enfoque que se da puede pasar a ser un punto secundario de la formación académica, ya que tan solo se toca una pequeña parte de los conocimientos, de las normas legales, documentos o papers que se encuentran buscando en internet.

Si esta actividad se da como secundaria, como ser una parte complementaria del desarrollo de software o como un tema agregado al laboratorio de redes, no se le estará dando la real importancia que tiene hoy en día el estudio de la seguridad y su proyección en el futuro.

Ese enfoque secundario se da en la mayoría de las organizaciones ya que no tienen lugares adecuados y dedicados a este fin.

7. Estado actual del conocimiento sobre el tema.

Para poder describir el estado actual en que se encuentra el estudio de la seguridad informática, es necesario primeramente comprender las dos áreas básicas que integrarán este proyecto, las cuales son la seguridad de la información y la tecnología de virtualización.

1. Seguridad de la información:

   Se puede definir a la seguridad de la información como el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener los siguientes principios básicos:

   - La integridad.
   - La autenticidad.
   - La confidencialidad.
   - La disponibilidad.
   - El no repudio.

   Integridad de la información:
   La información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación, no ha sido manipulada por terceros de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.

   Autenticidad de la información:
   La información pertenece a quien dice haberla generado.
   Este principio asegura que la información procedente de un usuario verifica que es quien dice ser y se debe garantizar que el origen de los datos es correcto.

Confidencialidad de la información:
La información sólo debe ser conocida por las personas que necesitan conocerla y que han sido autorizadas para ello.
Este principio asegura que la información no va a ser divulgada de manera fortuita o intencionada.

Disponibilidad de la información:
La información debe estar disponible siempre para las personas autorizadas para accederla y tratarla, y además puede recuperarse en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción.
Este principio asegura que la información esté disponible cuando sea necesario.

No repudio:
Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación.

2. Virtualización:

La virtualización hace referencia a una tecnología que permite la ejecución de varias máquinas virtuales sobre una máquina física con el objetivo de aprovechar al máximo los recursos de un sistema y que su rendimiento sea mayor.

Máquina virtual:
Se define a una máquina virtual como una representación virtual o emulación de un sistema físico. La máquina física en la que se ejecutan las máquinas virtuales se las conoce con el nombre de "Host".

La virtualización permite crear varias máquinas virtuales, cada una con su propio sistema operativo (SO) y aplicaciones, en una única máquina física.

Existen máquinas virtuales de todo tipo, estas pueden ser:

- Máquinas virtuales Windows.
- Máquinas virtuales Android.
- Máquinas virtuales Mac.

- Máquinas virtuales iOS.
- Máquinas virtuales Java.
- Máquinas virtuales de Python.
- Máquinas virtuales Linux.
- Máquinas virtuales VMware.
- Máquinas virtuales Ubuntu.

Una máquina virtual no puede interactuar directamente con un sistema físico.
En su lugar, necesita una capa de software llamada middelware.

A este middelware se lo conoce con el nombre de "Hipervisor" y tiene la finalidad de coordinar a las distintas máquinas virtuales entre ellas y al mismo tiempo coordinar a estas con el hardware físico subyacente.

El hipervisor asigna recursos de computación físico, como procesadores, memoria y almacenamiento, a cada máquina virtual y mantiene cada máquina virtual separada de las otras para que no interfieran entre sí.

Existen dos tipos principales de hipervisores.

Hipervisores de tipo 1:
Se ejecutan directamente en el hardware físico (normalmente un servidor), ocupando el lugar del sistema operativo.

Normalmente, se utiliza un producto de software independiente para crear y gestionar máquinas virtuales en el hipervisor.

Algunas herramientas de gestión, como vSphere de VMware, permiten seleccionar un sistema operativo huésped para instalar en la MV.

Puede utilizar una MV como plantilla para otras y duplicarla para crear nuevas. En función de sus necesidades, también es posible crear varias plantillas de MV para distintos fines, como pruebas de software, bases de datos de producción y entornos de desarrollo.

Hipervisores de tipo 2:
Se ejecutan como una aplicación dentro de un sistema operativo de host y normalmente se dirigen a plataformas de escritorio o portátiles de un solo usuario.

Con un hipervisor de tipo 2, se puede crear manualmente una máquina virtual y luego instalar un sistema operativo anfitrión en él.

Es posible utilizar el hipervisor para asignar recursos físicos a la MV, estableciendo manualmente la cantidad de núcleos de procesador y memoria.

Algunas de las ventajas al utilizar la virtualización como herramienta de trabajo:

- Mejor utilización de recursos.
- Escalabilidad.
- Portabilidad.
- Flexibilidad.

Pero haremos hincapié en este aspecto en particular:

- Seguridad: las máquinas virtuales mejoran la seguridad de varias formas en comparación con los sistemas operativos que se ejecutan directamente en el hardware.

  Una MV es un archivo que un programa externo puede escanear para detectar software malicioso.

  Se puede crear una instantánea completa de la MV en cualquier momento y, a continuación, restaurarla a ese estado si se infecta con un programa malicioso, haciendo que la MV vuelva en el tiempo de manera eficaz.

  La rápida y fácil creación de las MV también permite eliminar completamente una MV en riesgo, y luego volver a crearla rápidamente, acelerando la recuperación de las infecciones de malware.

Otro aspecto importante a tener en cuenta es el modelo de dedicación que deben tener:

- Máquinas virtuales públicas o de multi-inquilino:
- Máquinas virtuales en las que múltiples usuarios comparten una infraestructura física común.

Este es el abordaje más rentable y escalable para el suministro de máquinas virtuales, pero carece de algunas de las características de aislamiento que pueden preferir las organizaciones con estrictos mandatos de seguridad o conformidad.

- Máquinas virtuales de único inquilino:
  Existen dos modelos para este tipo: hosts e instancias dedicados.
  - Host dedicado: implica el alquiler de una máquina física completa y el mantenimiento de acceso y control continuo de esa máquina, su hardware y el software que se instale en ella.

    Este modelo proporciona la máxima flexibilidad y transparencia de hardware, control y colocación de carga de trabajo, y también ofrece algunas ventajas para determinado software de "traiga su propia licencia".

  - Instancia dedicada: ofrece el mismo aislamiento de inquilino único y el mismo control sobre la colocación de la carga de trabajo, pero no está acoplado con una máquina física específica.

    Así, por ejemplo, si una instancia dedicada es reiniciada, podría terminar en una nueva máquina física, una máquina dedicada a la cuenta individual, sin embargo, una nueva máquina, posiblemente en una ubicación física diferente.

Habiendo expuesto las dos áreas que integran este proyecto, lo que se pretende lograr con la conjunción de los principios de la seguridad y tecnologías de virtualización es el de identificar, conocer y estudiar los distintos tipos de ciberataque de los que se puedan ser objeto, como así también poder establecer patrones de conducta de los atacantes y formular o implementar metodologías de contención y mitigación en el futuro para proteger a las organizaciones, siempre realizando todas las acciones dentro de un entorno seguro y controlado.

8. Objetivos general y específicos

Se identifican dos líneas principales de investigación de interés; a saber:

1. Estudiar las amenazas y ataques cibernéticos definiendo posibles futuras tendencias de las ciberagresiones a las organizaciones, para detectar el comportamiento de los atacantes que puedan afectar la integridad, la confidencialidad, la autenticidad y la disponibilidad de la información.

2. Desarrollar una metodología de análisis de incidentes para identificar las acciones de mitigación, de contención y de respuesta inmediata ante los efectos de una ciberagresión o ciberataque en tiempo real, con la finalidad de poder conocer los distintos tipos de ciberataques de los que puede ser objeto una organización, determinando los siguientes aspectos:

    a. Cómo y cuándo ocurrió una violación de la seguridad.
    b. Identificar cuáles fueron los activos informáticos comprometidos y afectados.
    c. Qué atacantes tomaron o cambiaron procesos.
    d. Contener y remediar los incidentes que se identificaron.
    e. Buscar violaciones adicionales a la seguridad.

9. Hipótesis de la Investigación

El proyecto está enfocado en estudiar y obtener metodologías que sean aplicables para el análisis de eventos e incidentes de ciberseguridad o ciberataques.

Es poder dotar a las organizaciones de un método confiable, eficaz y basado en un modelo lógico fundamentado, que permita identificar, minimizar y contener amenazas de ciberseguridad para lograr preservar el activo de la información.

Así mismo, se busca garantizar que los alumnos de la universidad puedan acceder a mejores conocimientos, u poder ofrecerles a los mismos laboratorios de informática dotadas de componentes hardware y software competentes, que posibilitan una mayor apropiación

del conocimiento adquirido en cada una de las asignaturas que requieren el empleo de esta técnicas y metodologías.

10. Metodología a utilizar.

Con el advenimiento de las nuevas tecnologías, los nuevos desarrollos de software, el diseño de nuevos componentes electrónicos basados en software y los nuevos servicios de las tecnologías de la nube, tratar de establecer las acciones de mitigación, contención y respuesta inmediata ante los efectos de una ciberagresión o ciberataque en tiempo real, parecería un trabajo muy difícil de realizar.

Pero con el empleo de las tecnologías de computación, ahora es posible desarrollar herramientas virtuales que permiten realizar las acciones de mitigación, contención y respuesta inmediata ante los efectos de una ciberagresión o ciberataque en un entorno educativo en tiempo real.

Empleando la virtualización no solo se pude analizar, desarrollar e implementar acciones de protección de los sistemas informáticos, sino que también se está trabajando en un entorno completamente controlado y protegido, preservando en todo momento la seguridad de la organización.

Hoy en día, el empleo de las máquinas virtuales en los laboratorios está emergiendo como respuesta ante esta necesidad de poder identificar, analizar y adoptar medidas preventivas ante los ciberataques.

El empleo de estas herramientas se ha incrementado y adaptado en diferentes aplicaciones y han brindado diferentes soluciones a otros organismos, que necesitan de la seguridad como un elemento esencial para preservar la integridad de la organización.

Para poder llevar a cabo el proyecto se lo puede dividir en etapas a los efectos de poder comprender la manera de ejecutarlo:

Etapa 1: Estudio de casos de ciberataques.
Etapa 2: Identificación de los distintos tipos de ciberataques.
Etapa 3: Empleo de herramientas y modelado de técnicas de acción contra ciberataques.
Etapa 4: Simulación de incidentes y ejecución de las acciones de mitigación.

Etapa 5: Análisis y explotación de los resultados.

En lo que se refiere a la búsqueda bibliográfica, al tratarse de un área tan nueva y cambiante, hay que aclarar que la mayoría de la información no se encuentra en la bibliografía tradicional, sino que hay que realizar búsquedas y acceder a sitios especialmente dedicados a esta área de la informática, como así también la información que publican las organizaciones especializadas en esta temática.

En lo que se refiere a la adquisición de equipamiento e insumos, la necesidad de contar con el equipamiento informático inicial es primordial para poder crear el entorno de trabajo necesario para poder ejecutar las etapas en las que se ha dividido el proyecto.

En lo que se refiere al diseño del entorno de trabajo se deben tener en cuenta los siguientes aspectos:

1. Equipos de trabajo: Se deben definir la cantidad mínima de que se pueden implementar por área de trabajo tales como:
2. Equipos de escritorio: destinados a los investigadores u operarios.
3. Equipos de red: equipos destinados a configurar la red a utilizar (Switches, routers, APS, UTM). Equipos de almacenamiento: equipos destinadas a almacenar las herramientas requeridas para trabajar y salvaguardar la información.
4. Equipos de servidores: son los equipos informáticos que proporción los diversos servicios necesarios para que se pueda implementar el entorno de trabajo, tales como:
    a. Servidores Web.
    b. Servidores de Almacenamiento.
    c. Servidores de bases de datos.
    d. Servidores de acceso remoto.
    e. Servidores de correo.
    f. Servidores de servicios (DNS, AD, DHCP, entre otros)

11. Resultados Esperados

El aporte original de esta línea de investigación se basa en proponer una nueva metodología de Ciberseguridad, desarrollando un abordaje proactivo hacia las amenazas antes que éstas comprometan las organizaciones, a fin de estar preparado ante estos ataques mediante una defensa dinámica de tal manera de impedir, mitigar o reducir los efectos de una ciberagresión o ciberataque.

Las líneas de investigación planteadas para este proyecto tienen como alcance desarrollar una metodología proactiva de análisis de eventos que ocurren ante los ciberataques antes que el objetivo propuesto por el agresor haya sido alcanzado.

El principal resultado esperado es desarrollar una metodología propia de análisis de eventos o incidentes aplicable a las fases iniciales de una ciberagresión o ciberataque que pudiera ocurrir sobre uno o más activos esenciales de una organización (estos pueden ser la información, sus procesos, su infraestructura de comunicaciones, etc.)

12. Antecedentes y funciones previstas del Grupo de Investigación en el área temática/disciplina

Los integrantes del equipo poseen conocimientos avanzados sobre el tema de trabajo.
El director tiene antecedentes de haber realizado una especialización en Seguridad Informática y Criptografía y una maestría en Ciberdefensa.
Ambos integrantes del proyecto son docentes de la UNO y en otras universidades.

13. Transferencia de Resultados.

Este proyecto busca como primera línea de trabajo obtener resultados que permitan identificar y estudiar los ciberataques que se realizan sobre las organizaciones.

Como segundo aspecto puede resultar importante para el modelado del comportamiento del agresor, especialmente en las etapas previas del ciberataque, como ser la exploración o reconocimiento inicial, la adquisición intrusiva de servicios o procesos computacionales de la infraestructura, y permitir también que sea posible el desarrollo de herramientas defensivas acordes a la debilidad a la que se encuentre expuesta la organización.

Como último aspecto se puede mencionar la consolidación de un grupo de trabajo en la UNO con conocimientos específicos sobre la ciberseguridad y el desarrollo de las capacidades institucionales para la detección y manejo de amenazas a la seguridad de la información.

El desarrollo de recursos humanos necesitará la participación de personal con conocimientos básicos del área de la Licenciatura en Informática. Por esta razón y para dar soporte a la actividad se solicitará un becario con dedicación a este proyecto.

14. Viabilidad y Factibilidad Técnica

El Proyecto reúne características, condiciones técnicas y operativas que aseguran el cumplimiento de sus metas y objetivos.

Para poder estudiar los ciberataques hay que crear las condiciones que responden a una estrategia de investigación que posibilite obtener los resultados deseados dentro del marco de desarrollo de las TI, para lo cual la herramienta más adecuada sería ejecutar las acciones de investigación dentro de un laboratorio de seguridad informática que este orientado a esta área en particular.

Además, también se busca maximizar las inversiones económicas, ya que aporta a otras áreas de la ingeniería informática en su conjunto, respondiendo a las necesidades organizacionales, además de no superponer esfuerzos ni duplicar acciones.

15. Aspectos Éticos.

Los principales valores morales que se deben preservar son la privacidad, la propiedad, la confianza y la veracidad de la información.

La ética informática busca identificar, analizar la naturaleza y el impacto social de las tecnologías de la información y la comunicación, en este caso particular centrándose en preservar la seguridad de la información, además, de dar cumplimiento a las políticas que dirigen nuestras acciones en el área informática y al mismo tiempo haciendo un uso ético de estas tecnologías.

Por los motivos planteados anteriormente, la finalidad de este proyecto se enfoca en explotar los beneficios que produce el empleo de las TI aplicadas al campo de la seguridad informática y no orientarse a explotar acciones de intrusión u obtención de información que estén en oposición con las normas y leyes que lo rigen.

16. Aspectos de Seguridad Laboral, Ambiental y Bioseguridad requeridos

No aplica para este tipo de investigación.

17. Intervención de terceros

No aplica para este tipo de investigación.

18. Cronograma de Actividades.

1er Año

Actividad	Mes											
	1	2	3	4	5	6	7	8	9	10	11	12
Estudio de las técnicas y herramientas de Informática de seguridad sobre sistemas Windows y Linux, pasibles de ser utilizadas en la detección y respuesta frente a un incidente de Ciberseguridad.	X	X	X	X								
Estudio de casos de ciberataques y selección de una metodología de trabajo para comprender y definir las fases comunes de un ciberataque.				X	X							
Implementación del laboratorio de seguridad.						X	X	X	X	X		
Elaboración de informe final, explotación de los resultados obtenidos durante el primer año.											X	X

2do Año

Actividad	Mes											
	1	2	3	4	5	6	7	8	9	10	11	12
Ampliación del laboratorio de seguridad	X	X	X									
Definición de un conjunto inicial de métodos y herramientas para aplicar en el caso de la detección de un ciberataque y como dar respuesta a dicha agresión.				X	X	X						
Estudio y simulación de incidentes y ejecución de las acciones de mitigación.							X	X	X			
Elaboración de informe final, explotación de los resultados obtenidos y preparación de la transferencia.										X	X	X

19. Presupuesto

Presupuesto del Primer año de ejecución

	Rubro	**Descripción**	**Monto**
1	Bienes de consumo	No aplica	
2	Servicios no personales	Mantenimiento general delos equipos	
3	Servicios técnicos y profesionales	No aplica	
4	Servicios comerciales y financieros	No aplica	
5	Pasajes y viáticos	Inscripción a congreso Viaje a congreso Publicaciones en revista	$100.000
6	Bienes de uso	No aplica	
7	Equipamiento	UN (1) servidor de alto desempeño para simulación del entorno de trabajo Dell poweredge T440 Intel® Xeon® de 2.a generación y hasta 16 núcleos por procesador 512 GB DE RDIMM Hasta 8 discos SAS/SATA (HDD/SSD) de 3,5 in con un máximo de 128 TB Hasta 16 discos SAS/SATA (HDD/SSD) de 2,5 in con un máximo de 61 TB RDIMM / LRDIMM	$595.000
Total 1° Año			**$695000**

Presupuesto del Segundo año de ejecución

	Rubro	Descripción	Monto
1	Bienes de consumo		
2	Servicios no personales		
3	Servicios técnicos y profesionales		
4	Servicios comerciales y financieros		
5	Pasajes y viáticos	Inscripción a congreso Viaje a congreso Publicaciones en revista	$100,000
6	Bienes de uso		
7	Equipamiento		
Total 2° Año			**$100.000**

Rubros

1. Bienes de consumo: insumos de laboratorio, útiles de oficina, librería, fotocopias, etc.
2. Servicios no personales: alquiler de equipos y mantenimiento, etc.
3. Servicios técnicos y profesionales: traducciones, desgrabaciones, data-entry, etc.
4. Servicios comerciales y financieros: imprenta, internet, transporte y almacenamiento, etc.
5. Pasajes y viáticos en ámbito nacional, inscripciones a congresos nacionales o internacionales.
6. Bienes de uso: libros, revistas, programas de computación, etc.
7. Equipamiento

20. Referencias bibliográficas

- INCIBE. Instituto Nacional de Ciberseguidad de España, «https://www.incibe.es/protege-tu-empresa/herramientas.
- INCIBE. Instituto Nacional de Ciberseguidad de España, «https://www.incibe-cert.es,» 2019. [En línea]. Available: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_protocolos_seguridad_red_sci.pdf. [Último acceso: 12 07 2019].
- INCIBE. Instituto Nacional de Ciberseguidad de España, «https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf

- T. A. Johnson, Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, St.Louis, Missouri. USA: CRC Press, 2015.
- The Mitre Corporation, «MITRE ATT&CK,» 22 Nov 2018. «https://attack.mitre.org/.
- Universidad internacional de Valencia, «https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme
- Universidad internacional de Valencia, «https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-seguridad-informatica-y-por-que-es-tan-importante
- Intelligence and National Security Alliance (INSA). (31 de Ago de 2018). Intelligence and National Security Alliance, «https://www.insaonline.org/wp-content/uploads/2018/08/INSA-Managing-Cyber-Attack-Critical-Infrastructure.pdf
- Normas ISO para la seguridad informática, «http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html