

Instituto Tecnológico de Morelia
Subdirección Académica
Departamento de Sistemas y Computación

Morelia, Michoacán, **07/Enero/2022**

OFICIO N° D. 138/2022

**ASUNTO: Autorización de tema y asignación de asesor
de proyecto para Titulación Integral.**

Patricia Molina Vázquez

Jefe de la División de Estudios Profesionales

PRESENTE

Por este medio le informo que el proyecto del alumno **JOSE LUIS MAGALLAN ALATORRE**, con número de control **17121091** de la carrera de **INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**, denominado **"HIGIENE DE CIBERSEGURIDAD UTILIZANDO HERRAMIENTAS DE MACHINE LEARNING PARA EL INSTITUTO DE INVESTIGACIONES EN ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)."**, ha sido **REGISTRADO y AUTORIZADO** como tema para la **TITULACIÓN** bajo la opción: **TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN**, haciendo la designación de **HEBERTO FERREIRA MEDINA** como **ASESOR DEL PROYECTO**.

Agradezco la atención al presente y aprovecho para enviar un afectuoso saludo.

ATENTAMENTE

Excelencia en Educación Tecnológica®
"Técnica, Progreso de México"®



JOSÉ MANUEL CUIN JACUINDE
Jefe del Depto. de Sistemas y Computación



J. GUADALUPE RAMOS DÍAZ
Presidente de la Academia de Sist. y Computación

C.c.p. Alumno
C.c.p. Archivo
MYVF/



Av. Tecnológico #1500, Col. Lomas de Santiaguito, C.P. 58120, Morelia, Michoacán.
Tel. (443) 3121570 Ext. 233, e-mail: sistemas@morelia.tecnm.mx
tecnm.mx | morelia.tecnm.mx



2022 *Ricardo Flores*
Año de Magón
PROLEGEMER DE LA REVOLUCIÓN MICHUANA



Instituto Tecnológico de Morelia
Subdirección Académica
Departamento de Sistemas y Computación

Morelia, Michoacán, 13/septiembre/2022

OFICIO N° 074.13/2022

ASUNTO: CONSTANCIA DE
PROYECTO INTEGRADOR

C. JOSÉ MANUEL CUIN JACUINDE
JEFE DEL DEPTO. DE SISTEMAS Y COMPUTACIÓN

Por medio del presente manifiesto que el trabajo titulado “HIGIENE DE SEGURIDAD UTILIZANDO HERRAMIENTAS DE MACHINE LEARNING PARA EL INSTITUTO DE INVESTIGACIONES EN SUBSISTEMAS Y SUSTENTABILIDAD (IIES UNAM)”, que fue desarrollado por el (la) alumno (a) **JOSÉ LUIS MAGALLÁN ALATORRE**, con número de control **17121091** egresado(a) de la Carrera de Ingeniería en Tecnologías de Información y Comunicaciones de este Instituto, quien lo desarrolló en el período de agosto de 2020 a diciembre de 2021 y en el transcurso de las asignaturas de Taller de Investigación I, Taller de Investigación II y Sistemas de Gestión de la Seguridad Informática, materia de la especialidad de Seguridad de la Información (2019-1), por lo tanto posee los elementos necesarios para ser considerado como una alternativa para que obtenga el grado de Ingeniero en Tecnologías de Información y Comunicaciones, por la opción “Titulación Integral por Proyecto de Investigación”.

Sin otro particular, reciba un cordial saludo.

ATENTAMENTE

Excelencia en Educación Tecnológica®
“Técnica, Progreso de México”®

C. HEBERTO FERREIRA MEDINA
ASESOR

 **EDUCACIÓN**
SECRETARÍA DE EDUCACIÓN PÚBLICA
 **TECNOLÓGICO NACIONAL DE MÉXICO**
INSTITUTO TECNOLÓGICO DE MORELIA
INGENIERÍA EN SISTEMAS COMPUTACIONALES

C.c.p. Archivo
RCJ/rfs*



Av. Tecnológico #1500, Col. Lomas de Santiaguito, C.P. 58120, Morelia, Michoacán.
Tel. (443) 3121570 Ext. 233, e-mail: sistemas@morelia.tecnm.mx
tecnm.mx | morelia.tecnm.mx





Instituto Tecnológico de Morelia
Subdirección Académica
Departamento de Sistemas y Computación

Morelia, Mich., 06/septiembre/2022
OFICIO N°: DSC 353 /2022

Asunto: Liberación de proyecto para titulación integral y
autorización de impresión definitiva

Patricia Molina Vázquez

Jefa de la Div. De Estudios Profesionales

Por este medio, le informo que ha sido liberado el siguiente proyecto para la Titulación Integral.

Nombre del Egresado:	JOSE LUIS MAGALLAN ALATORRE
No. Control:	17121091
Carrera:	INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIONES
Opción de Titulación:	TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACION
Nombre del Proyecto:	HIGIENE DE CIBERSEGURIDAD UTILIZANDO HERRAMIENTAS DE MACHINE LEARNING PARA EL INSTITUTO DE INVESTIGACIONES EN ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)"

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados

ATENTAMENTE

*Excelencia en Educación Tecnológica®
"Técnica, Progreso de México"®*

 HEBERTO FERREIRA MEDINA	 ANASTACIO ANTOLINO HERNANDEZ	 ABEL ALBERTO PINTOR ESTRADA	 JUAN JESUS RUIZ LAGUNAS
PRESIDENTE Y ASESOR	SECRETARIO	VOCAL PROPIETARIO	VOCAL SUPLENTE

C.p. Asesor
Alumno interesado
Archivo



Av. Tecnológico #1500, Col. Lomas de Santiaguito, C.P. 58120, Morelia, Michoacán.
Tel. (443) 3121570 Ext. 233, e-mail: sistemas@morelia.tecnm.mx
tecmm.mx | morelia.tecnm.mx



2022 Flores
Año de Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA



INSTITUTO TECNOLÓGICO DE MORELIA

**DIVISIÓN DE ESTUDIOS PROFESIONALES
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN**

TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN

**HIGIENE DE CIBERSEGURIDAD UTILIZANDO
HERRAMIENTAS DE MACHINE LEARNING PARA
EL INSTITUTO DE INVESTIGACIONES EN
ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)**

**QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

PRESENTA:

JOSE LUIS MAGALLAN ALATORRE

ASESOR:

HEBERTO FERREIRA MEDINA

MORELIA, MICHOACÁN

Junio, 2022



INSTITUTO TECNOLÓGICO DE MORELIA

DIVISIÓN DE ESTUDIOS PROFESIONALES
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN

TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN

**HIGIENE DE CIBERSEGURIDAD UTILIZANDO
HERRAMIENTAS DE MACHINE LEARNING PARA
EL INSTITUTO DE INVESTIGACIONES EN
ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)**

QUE PARA OBTENER EL TÍTULO DE:

**INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

PRESENTA:

JOSE LUIS MAGALLAN ALATORRE

ASESOR:

DR. HEBERTO FERREIRA MEDINA

COASESORES:

MTI. FROYLAN HERNÁNDEZ RENDÓN

DR. SERGIO ROGELIO TINOCO MARTÍNEZ

MTI. ALBERTO VALENCIA GARCÍA

MORELIA, MICHOACÁN

Junio, 2022

Agradecimientos

Quiero dar las gracias a mis padres y mis hermanos, que tuvieron paciencia con el temperamento que pude llevar a presentar en varias ocasiones cuando sentía que el tiempo se venía encima y no podría terminar o presentar un mal resultado, a mis amigos más cercanos, que entendieron mi ausencia y cuando tenía oportunidad se reunían conmigo, tanto para discutir cosas relacionadas con el proyecto, como hablar de cosas banales que me ayudaban a liberar estrés, frustración y sentirme libre de volver a trabajar arduamente en el proyecto.

Agradezco a las personas que estuvieron cerca de mí durante el proyecto, a mis asesores, el Dr. Heberto Ferreira Medina y al MTI. Alberto Valencia García, que me tomaron bajo su tutela, y siempre que tenía una duda, un problema o simplemente no sabía cómo desenvolverme en una actividad estuvieron dispuestos a darme una mano para salir del asunto.

También agradezco al Dr. Sergio Tinoco Martínez, y al MTI. Froylan Hernández Rendón de la ENES Morelia, por su apoyo técnico. Agradezco a la MGTI. Atzimba López M. por su colaboración en el desarrollo de esta tesis. A la DGAPA UNAM por su apoyo con el proyecto PE106021; "Propuesta de mejora a la enseñanza del aprendizaje automático aplicado a la Ciencia de Datos a gran escala; dirigido a académicos y estudiantes de la licenciatura en Tecnologías para la Información en Ciencias (LTICs) en la ENES Morelia". Y, por último, agradezco a todos los profesores del Instituto Tecnológico de Morelia que me dieron clases, asesorías y calificaron justamente, apoyándome a adquirir todos los conocimientos que poseo ahora. Gracias a todos.

Resumen

La higiene en la ciberseguridad, es una actividad que forma parte de la protección de los datos, tanto para los usuarios, como los que se almacenan en servidores de red, debe considerarse también el monitoreo y control de amenazas a todos los equipos que conforman la red de una institución pública o empresa privada. Estas actividades deben apegarse a los estándares de limpieza en ciberseguridad, desde la seguridad en la parte física (espacios o sites de alojamiento), el endurecimiento de servicios (hardening) y hasta la administración del hardware y software en servicios de red.

Para garantizar la seguridad en cualquier empresa o institución que haga uso de las Tecnologías de la Información y Comunicaciones (TICs), se recomienda tener en cuenta las buenas prácticas propuestas por la comunidad informática, incluyendo estándares de seguridad de la información, se recomienda seguir una metodología ya establecida para lograr mejores resultados.

El objetivo de este proyecto es mantener el control de la seguridad de la información ante amenazas empleando herramientas de Machine Learning (ML), para el análisis y limpieza de logs de monitoreo (datasets), que surgen de la recopilación de información de los servicios de red y de la aplicación de métodos de análisis; como la regresión lineal y otros métodos del aprendizaje no supervisado.

Para lograr lo antes mencionado se propone un sistema de gestión de la seguridad informática, que sigue las normas de la familia ISO 27000, para mantener el control de la seguridad, la utilización adecuada del software y hardware dedicados a la seguridad de la información y además de la administración de las herramientas de control de amenazas para este propósito.

Índice

Agradecimientos.....	2
Resumen	3
Índice.....	4
Índice de figuras y tablas.....	7
Capítulo 1. Introducción	9
1.1 Nombre del proyecto	9
1.2 Justificación del proyecto	9
1.3 Datos de la empresa	11
1.3.1. Nombre de la empresa.....	11
1.3.2. Misión.....	11
1.3.3. Visión	11
Capítulo 2. Antecedentes	12
2.1 Institución.	12
2.2 Problemática	13
2.3 Alcances y limitaciones de las soluciones.....	16
Capítulo 3. Marco teórico.	17
3.1. Auditoría Informática y planeación preliminar	17
3.2. Familia de normas ISO 27000.....	18
3.3. Sistema de Gestión de la Seguridad Informática	19
3.4. Higiene en Ciberseguridad.....	20
3.5. Políticas de seguridad	21
3.6. Red Privada Virtual	21
3.7. VLAN en la red	22
3.8. Firewall.....	22

3.9. Machine Learning.....	25
3.10. WireShark	26
3.11. Anaconda Navigator.....	27
3.12. Python 3.8	27
3.13. JupyterLab	28
3.14. Librería Numpy.....	28
3.15. Pandas	29
3.16. SciKit-Learn.....	30
Capítulo 4. Procedimientos y actividades.....	31
4.1. Descripción de las actividades	31
4.1.1. Actividad 1: Auditoría informática.....	31
4.1.2. Actividad 2: Higiene en ciberseguridad	33
4.1.3. Actividad 3: Levantamiento de Firewall.....	34
4.1.4. Actividad 4: Creación y revisión de políticas de seguridad	35
4.1.5. Actividad 5: Revisión y aseguramiento de infraestructura de TI....	36
4.1.6. Actividad 6: Monitoreo y análisis de datos usando herramientas de Machine Learning.....	37
4.1.7. Actividades extra.....	38
Capítulo 5. Resultados	39
5.1 Auditorías	39
5.2 Firewall en funcionamiento.....	40
5.3. Seguridad básica de la red.....	42
5.3.1. Cuentas de administradores de la red	42
5.3.2. Portal cautivo (Disclaimer de uso de red)	42
5.3.3. Actualización de firmware	43

5.3.4. VPN.....	45
5.3.5. Escaneo a la red	46
5.4. Políticas de seguridad en la red	47
5.5. Configuración de la red inalámbrica	48
5.6. Esquemas de red principal	50
5.7. Instalación de la nueva red inalámbrica y pruebas de funcionamiento ...	51
5.8. Instalación, limpieza y cambio de switches en la red principal	52
5.9. Análisis de datos con herramientas de Machine Learning	54
5.9.1. Importación y preparación de logs	55
5.9.2. Limpieza de datasets	56
9.9.3. Modelo de regresión lineal	57
5.9.4. Modelo de aprendizaje no supervisado con K-means.....	61
5.10. Instalación de equipos de cómputo	68
Conclusiones.....	69
Recomendaciones.....	70
Retrospectiva del Proyecto.....	71
Referencias bibliográficas	73
Anexos	76
Anexo A. Instalación de la red de pruebas y oficina del del proyecto	76
Anexo B. Código del modelo de aprendizaje no supervisado con K-means..	77
Anexo C. Informes de auditorías.....	80
Hoja de Visto Bueno por parte de los asesores	90



INSTITUTO TECNOLÓGICO DE MORELIA

DIVISIÓN DE ESTUDIOS PROFESIONALES

**DEPARTAMENTO DE SISTEMAS Y
COMPUTACIÓN**

**TITULACIÓN INTEGRAL POR PROYECTO DE
INVESTIGACIÓN**

HIGIENE DE CIBERSEGURIDAD UTILIZANDO HERRAMIENTAS DE MACHINE LEARNING PARA EL INSTITUTO DE INVESTIGACIONES EN ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PRESENTA:

JOSE LUIS MAGALLAN ALATORRE

ASESOR:

DR. HEBERTO FERREIRA MEDINA

MORELIA, MICHOACÁN

OCTUBRE 2022



Morelia, Mich., **31 de octubre de 2022**
OFICIO No.: D.E.P.T./T/2170/2022

ASUNTO: Autorización de Impresión Definitiva.

**JOSE LUIS MAGALLAN ALATORRE
PASANTE DE LA CARRERA DE
INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**

Por este medio, tengo el agrado de comunicar a usted que el Jurado designado para su Recepción Profesional, ha informado a esta Jefatura de la División de Estudios Profesionales, su aceptación para la Impresión Definitiva de su trabajo de titulación por la opción TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN, que lleva por nombre:

“HIGIENE DE CIBERSEGURIDAD UTILIZANDO HERRAMIENTAS DE MACHINE LEARNING PARA EL INSTITUTO DE INVESTIGACIONES EN ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)”

Por lo anterior, esta Jefatura le autoriza la impresión definitiva de su trabajo de titulación, esperando que el logro del mismo sea congruente con sus aspiraciones profesionales.

ATENTAMENTE

Excelencia en Educación Tecnológica®
“Técnica, Progreso de México”



PATRICIA MOLINA VÁZQUEZ
JEFA DE LA DIV. DE EST. PROFESIONALES

C.c.p.- Servicios Escolares
Para agregar a empastado final
Archivo
PMV/lmca





Instituto Tecnológico de Morelia
Subdirección Académica
Departamento de Sistemas y Computación

Morelia, Mich., 06/septiembre/2022
OFICIO N°: DSC 353 /2022

Asunto: Liberación de proyecto para titulación integral y
autorización de impresión definitiva

Patricia Molina Vázquez

Jefa de la Div. De Estudios Profesionales

Por este medio, le informo que ha sido liberado el siguiente proyecto para la Titulación Integral.

Nombre del Egresado:	JOSE LUIS MAGALLAN ALATORRE
No. Control:	17121091
Carrera:	INGENIERÍA EN TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Opción de Titulación:	TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACION
Nombre del Proyecto:	HIGIENE DE CIBERSEGURIDAD UTILIZANDO HERRAMIENTAS DE MACHINE LEARNING PARA EL INSTITUTO DE INVESTIGACIONES EN ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)"

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados

ATENTAMENTE

Excelencia en Educación Tecnológica®
"Técnica, Progreso de México"®

HEBERTO FERREIRA MEDINA	ANASTACIO ANTOLINO HERNANDEZ	ABEL ALBERTO PINTOR ESTRADA	JUAN JESUS RUIZ LAGUNAS
PRESIDENTE Y ASESOR	SECRETARIO	VOCAL PROPIETARIO	VOCAL SUPLENTE

C.p. Asesor
Alumno interesado
Archivo



Av. Tecnológico #1500, Col. Lomas de Santiaguito, C.P. 58120, Morelia, Michoacán.

Tel. (443) 3121570 Ext. 233, e-mail: sistemas@morelia.tecnm.mx

tecnm.mx | morelia.tecnm.mx



2022 Flores
Año de Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

CONSTANCIA DE EXENCIÓN DE EXAMEN PROFESIONAL

de acuerdo con el instructivo vigente de Titulación, que no tiene como requisito la sustentación del Examen Profesional para efecto de obtención de Título, en las opciones VIII, IX y Titulación Integral, el jurado HACEN CONSTAR que el (la) C. Jose Luis Magallan Alatorre

numero de control 17121091 egresado (a) del Instituto Tecnológico de Morelia,
clave 16DIT0012H que cursó la carrera de

Ingeniería en Tecnologías de la Información y Comunicaciones

completó satisfactoriamente con lo estipulado en la opción: "Titulación Integral por Proyecto de Investigación" con trabajo denominado "Higiene de Ciberseguridad Utilizando Herramientas de Machine Learning para el Instituto de Investigaciones en Ecosistemas y Sustentabilidad (ITES-UNAM)"

El (la) Presidente (a) del Jurado le hizo saber al sustentante el Código de Ética Profesional y le tomó la Promesa de Ley, una vez escrita y leída la firmaron las personas que en el acto protocolario intervinieron, para los efectos legales a que haya lugar, se asienta la presente en la ciudad de Morelia, Michoacán, el 10 del mes de Febrero del año 20 23.

PRESIDENTE (A)

Heberto Ferreira Medina
Cédula Prof. 9875495
Dr. en Tecnologías de Información y Análisis de Datos



SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLOGICO NACIONAL
DE MEXICO
DIRECCIÓN DE ASUNTOS ESCOLARES
Y APOYO A ESTUDIANTES

SECRETARIO (A)

Anastacio Antonio Hernandez
Dr. en C. en Ing. Eléctrica y en Sistem. Comput.
Cédula Prof. 7355312

VOCAL

Abel Alberto Pintor Estrada
Miembro. En. Ciencias en C. de la Computac.
Cédula Prof. 10228740



INSTITUTO TECNOLÓGICO DE MORELIA

**DIVISIÓN DE ESTUDIOS PROFESIONALES
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN**

TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN

**HIGIENE DE CIBERSEGURIDAD UTILIZANDO
HERRAMIENTAS DE MACHINE LEARNING PARA
EL INSTITUTO DE INVESTIGACIONES EN
ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)**

**QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

PRESENTA:

JOSE LUIS MAGALLAN ALATORRE

ASESOR:

HEBERTO FERREIRA MEDINA

MORELIA, MICHOACÁN

Junio, 2022



INSTITUTO TECNOLÓGICO DE MORELIA

DIVISIÓN DE ESTUDIOS PROFESIONALES
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN

TITULACIÓN INTEGRAL POR PROYECTO DE INVESTIGACIÓN

**HIGIENE DE CIBERSEGURIDAD UTILIZANDO
HERRAMIENTAS DE MACHINE LEARNING PARA
EL INSTITUTO DE INVESTIGACIONES EN
ECOSISTEMAS Y SUSTENTABILIDAD (IIES, UNAM)**

QUE PARA OBTENER EL TÍTULO DE:

**INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

PRESENTA:

JOSE LUIS MAGALLAN ALATORRE

ASESOR:

DR. HEBERTO FERREIRA MEDINA

COASESORES:

MTI. FROYLAN HERNÁNDEZ RENDÓN

DR. SERGIO ROGELIO TINOCO MARTÍNEZ

MTI. ALBERTO VALENCIA GARCÍA

MORELIA, MICHOACÁN

Junio, 2022

Agradecimientos

Quiero dar las gracias a mis padres y mis hermanos, que tuvieron paciencia con el temperamento que pude llevar a presentar en varias ocasiones cuando sentía que el tiempo se venía encima y no podría terminar o presentar un mal resultado, a mis amigos más cercanos, que entendieron mi ausencia y cuando tenía oportunidad se reunían conmigo, tanto para discutir cosas relacionadas con el proyecto, como hablar de cosas banales que me ayudaban a liberar estrés, frustración y sentirme libre de volver a trabajar arduamente en el proyecto.

Agradezco a las personas que estuvieron cerca de mi durante el proyecto, a mis asesores, el Dr. Heberto Ferreira Medina y al maestro Alberto Valencia García, que me tomaron bajo su tutela, y siempre que tenía una duda, un problema o simplemente no sabía cómo desenvolverme en una actividad estuvieron dispuestos a darme una mano para salir del asunto.

También agradezco al Dr. Sergio Tinoco Martínez, y al MTI. Froylan Hernández Rendón de la ENES Morelia, por su apoyo técnico. Agradezco a la MGTI. Atzimba López M. por su colaboración en el desarrollo de esta tesis. A la DGAPA UNAM por su apoyo en el proyecto PE106021, y, por último, agradezco a todos los profesores del Instituto Tecnológico de Morelia que me dieron clases, asesorías y calificaron justamente, apoyándome a adquirir todos los conocimientos que poseo ahora. Gracias a todos.

Resumen

La higiene en la ciberseguridad, es una actividad que forma parte de la protección de los datos, tanto para los usuarios, como los que se almacenan en servidores de red, debe considerarse también el monitoreo y control de amenazas a todos los equipos que conforman la red de una institución pública o empresa privada. Estas actividades deben apegarse a los estándares de limpieza en ciberseguridad, desde la seguridad en la parte física (espacios o sites de alojamiento), el endurecimiento de servicios (hardening) y hasta la administración del hardware y software en servicios de red.

Para garantizar la seguridad en cualquier empresa o institución que haga uso de las Tecnologías de la Información y Comunicaciones (TICs), se recomienda tener en cuenta las buenas prácticas propuestas por la comunidad informática, incluyendo estándares de seguridad de la información, se recomienda seguir una metodología ya establecida para lograr mejores resultados.

El objetivo de este proyecto es mantener el control de la seguridad de la información ante amenazas empleando herramientas de Machine Learning (ML), para el análisis y limpieza de logs de monitoreo (datasets), que surgen de la recopilación de información de los servicios de red y de la aplicación de métodos de análisis; como la regresión lineal y otros métodos del aprendizaje no supervisado.

Para lograr lo antes mencionado se propone un sistema de gestión de la seguridad informática, que sigue las normas de la familia ISO 27000, para mantener el control de la seguridad, la utilización adecuada del software y hardware dedicados a la seguridad de la información y además de la administración de las herramientas de control de amenazas para este propósito.

Índice

Agradecimientos.....	2
Resumen	3
Índice.....	4
Índice de figuras y tablas.....	7
Capítulo 1. Introducción	9
1.1 Nombre del proyecto	9
1.2 Justificación del proyecto	9
1.3 Datos de la empresa	11
1.3.1. Nombre de la empresa.....	11
1.3.2. Misión.....	11
1.3.3. Visión	11
Capítulo 2. Antecedentes	12
2.1 Institución.	12
2.2 Problemática	13
2.3 Alcances y limitaciones de las soluciones.....	16
Capítulo 3. Marco teórico.	17
3.1. Auditoría Informática y planeación preliminar	17
3.2. Familia de normas ISO 27000.....	18
3.3. Sistema de Gestión de la Seguridad Informática	19
3.4. Higiene en Ciberseguridad.....	20
3.5. Políticas de seguridad	21
3.6. Red Privada Virtual	21
3.7. VLAN en la red	22
3.8. Firewall.....	22

3.9. Machine Learning.....	25
3.10. WireShark	26
3.11. Anaconda Navigator.....	27
3.12. Python 3.8	27
3.13. JupyterLab	28
3.14. Librería Numpy.....	28
3.15. Pandas	29
3.16. SciKit-Learn.....	30
Capítulo 4. Procedimientos y actividades.....	31
4.1. Descripción de las actividades	31
4.1.1. Actividad 1: Auditoría informática.....	31
4.1.2. Actividad 2: Higiene en ciberseguridad	33
4.1.3. Actividad 3: Levantamiento de Firewall.....	34
4.1.4. Actividad 4: Creación y revisión de políticas de seguridad	35
4.1.5. Actividad 5: Revisión y aseguramiento de infraestructura de TI....	36
4.1.6. Actividad 6: Monitoreo y análisis de datos usando herramientas de Machine Learning.....	37
4.1.7. Actividades extra.....	38
Capítulo 5. Resultados	39
5.1 Auditorías	39
5.2 Firewall en funcionamiento.....	40
5.3. Seguridad básica de la red.....	42
5.3.1. Cuentas de administradores de la red	42
5.3.2. Portal cautivo (Disclaimer de uso de red)	42
5.3.3. Actualización de firmware	43

5.3.4. VPN.....	45
5.3.5. Escaneo a la red	46
5.4. Políticas de seguridad en la red	47
5.5. Configuración de la red inalámbrica	48
5.6. Esquemas de red principal	50
5.7. Instalación de la nueva red inalámbrica y pruebas de funcionamiento ...	51
5.8. Instalación, limpieza y cambio de switches en la red principal	52
5.9. Análisis de datos con herramientas de Machine Learning	54
5.9.1. Importación y preparación de logs	55
5.9.2. Limpieza de datasets	56
9.9.3. Modelo de regresión lineal	57
5.9.4. Modelo de aprendizaje no supervisado con K-means.....	61
5.10. Instalación de equipos de cómputo	68
Conclusiones.....	69
Recomendaciones.....	70
Retrospectiva del Proyecto.....	71
Referencias bibliográficas	73
Anexos	76
Anexo A. Instalación de la red de pruebas y oficina del del proyecto	76
Anexo B. Código del modelo de aprendizaje no supervisado con K-means..	77
Anexo C. Informes de auditorías.....	80
Hoja de Visto Bueno por parte de los asesores	90

Índice de figuras y tablas

Organigrama 1: Organización del IIES.....	12
Tabla 1: Tipos de Firewall.....	23
Figura 1: Topología inicial de la red.....	34
Tabla 2: Equipo de cómputo para la realización del proyecto.....	39
Figura 2: Página principal de Fortigate 600C.....	40
Figura 3: Interfaces de la red de pruebas.....	41
Figura 4: Cuentas de administradores.....	42
Figura 5: Muestra de portal cautivo en la red.....	43
Figura 6: Actualización de firmware disponible.....	44
Figura 7: Versión 5.6.1 del Fortigate 600C.....	44
Figura 8: Conexión a VPN exitosa con FortiClient.....	45
Figura 9: Escaneos de red no protegida.....	46
Figura 10: Muestras de políticas de seguridad.....	47
Figura 11: Auditoría de security fabric.....	48
Figura 12: Administración de los puntos de acceso de manera gráfica.....	49
Figura 13: Mejores prácticas de configuración de los puntos de acceso.....	49
Figura 14: Administración de los servicios de la red en el IIES.....	50
Figura 15: Topología de la red del IIES.....	51
Figura 16: Instalación de puntos de acceso.....	52
Figura 17: Limpieza y cambio de switch.....	53
Figura 18: Diferencia de velocidad entre interfaces Gigabit y Fast.....	53
Figura 19: VLANs e interfaces de un switch.....	54
Figura 20: Archivos logs descargados.....	55

Figura 21: Datasets exportados en archivos .csv.....	55
Figura 22: Importación, visualización y exportación de logs.....	56
Figura 23: Muestra del Dataset original.....	57
Figura 24: Copia del dataset limpio de valores vacíos.....	57
Figura 25: Modificación de datos del dataframe.....	58
Figura 26: Gráfica de direcciones IP y código de estado.....	59
Figura 27: Gráfica de direcciones IP y Bytes transferidos.....	59
Figura 28: Gráfica de tipos de peticiones por dirección IP.....	60
Figura 29: Error al entrenar el modelo de regresión lineal.....	61
Tabla 3: Parte de la tabla para el modelo de aprendizaje no supervisado.....	62
Figura 30: Muestra del dataframe con los datos escalados.....	63
Figura 31: Pruebas de valores MinMaxScaler.....	64
Figura 32: Pruebas de valores StandardScaler.....	64
Figura 33: Función para graficar los resultados.....	65
Figura 34: Resultados StandardScaler.....	66
Figura 35: Resultados MinMaxScaler.....	66
Figura 36: Valor de puntuación silhouette.....	67
Figura 37: Instalación y pruebas del servidor QNAP “NAS-CEEMBio”.....	68
Anexos – Figura 1: Oficina y espacio de pruebas.....	75
Anexos – Cuadro 1: Código de Python de programación del modelo.....	76

Capítulo 1. Introducción

1.1 Nombre del proyecto

Higiene de ciberseguridad utilizando herramientas de Machine Learning para el Instituto de Investigaciones en Ecosistemas y Sustentabilidad (IIES, UNAM).

1.2 Justificación del proyecto

La razón para realizar este proyecto es porque el monitoreo y control de amenazas continuas a los servicios de la red es una actividad fundamental a realizar. Las buenas prácticas, metodologías u otras formas probadas de llevar a cabo lo mencionado antes, ya que se considera una necesidad para cualquier empresa que haga uso de las tecnologías de la información y la comunicación.

Herramientas como la familia de normas ISO 27000, en *Global Suite Solutions (2015)* establecen una serie de pasos que ayudan a garantizar el control de seguridad; otras herramientas que se pueden emplear serían el uso de software o hardware especializado en la seguridad (como los firewalls perimetrales) y la revisión, actualización y mantenimiento a las herramientas con las que se buscan y controlan amenazas ya es una tarea fundamental a realizar en casi cualquier institución.

Las implicaciones que pueden tener los resultados son:

- Garantizar la integridad de los datos: haciendo referencia a tanto los datos de acceso al sistema como al volumen completo de datos. Como lo explica *Astera (2021)* “La integridad de los datos es la precisión, integridad y confiabilidad general de la información. Puede especificarse por la falta de variación entre dos instancias o actualizaciones consecutivas de un registro, lo que indica que su información está libre de errores.” El beneficio principal de los resultados es asegurarse de que la información ingresada al sistema sea real y únicamente modificada por las personas con los permisos y credenciales para ello.

- Proveer respaldos de datos en caso de pérdida, ataque, etc y la seguridad de los mismos. El sitio *ESET SGSI (2016)* explica que una de las buenas prácticas de la seguridad de la información son los respaldos periódicos de información, para que, en diversos casos que pueden surgir, el impacto en el trabajo y/o registros no sea tan fuerte. Las causalidades podrían ser ataques de terceros, ataques internos, desastres naturales, etc.
- Uso de Machine Learning para la revisión y monitoreo más flexible y rápida de datos sospechosos. Aplicar machine learning a software o procedimientos agiliza la obtención de resultados sin tanto trabajo para el administrador, siendo más sencillo programar un algoritmo para ingresar los datos y se realice el procedimiento, básicamente automatizando la obtención de gráficas y muestras en los resultados.
- Una conexión segura para los usuarios de la red y puedan sentir que sus datos personales no corren tanto riesgo. Llevar de la mano de la integridad de los datos, brindar una conexión segura para los usuarios, protegida por reglas y limitando la comunicación a sólo lo que los usuarios necesitan es un paso para garantizar dicha integridad y hace al usuario sentir la confianza de usar la red (teniendo precaución y uso responsable de su parte).

Los beneficiados de dichos resultados son:

- Usuarios académicos y administrativos que hagan uso de la red
- Otros administradores de la red
- Estudiantes usuarios de la red