UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

Opción de Titulación:

Artículos profesionales de alto nivel

Tema:

PLANTEAMIENTO DE UNA POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS AMBIENTES DE ENSEÑANZA VIRTUALES MOOC EN ECUADOR.

Autores:

Galo Stiven Rocha Freire
Beker Arnaldo Ortiz Sánchez

Director:

José Luis Aguayo Morales

CUENCA – ECUADOR
2023

Autores:

Galo Stiven Rocha Freire
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
grochaf@est.ups.edu.ec

Beker Arnaldo Ortiz Sánchez
Ingeniero en Ciencias de la Computación.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
bortizs@est.ups.edu.ec

Dirigido por:

José Luis Aguayo Morales
Ingeniero en Electrónica y Telecomunicaciones.
Magister en Ciberseguridad.
Magister en Sistemas Informáticos Educativos.
Magister en Redes de Comunicación.
jaguayo@ups.edu.ec

DEDICATORIA

Arnaldo Ortiz

Dedico mi tesis a mi familia especialmente a mis padres que me apoyaron tanto económicamente, como con sus acciones de aliento y preocupación cada día durante el Posgrado.

A la empresa Celebrity Cruises la cual me brindo de conocimiento en distintos ámbitos tecnológicos que fueron de utilidad durante el posgrado universitario y la realización de este artículo.

A mi Tutor de Proyecto el cual estuvo siempre pendiente durante las revisiones y guiándonos de la mejor manera durante todo el proceso, con profesionalismo, buena actitud, preocupación y responsabilidad.

A mi compañero Galo Rocha que junto a mi persona realizo la presente tesis con mucha dedicación buscando siempre la perfección en este trabajo final.

A mis docentes ingenieros por sus cátedras que me han servido en la presente tesis, así como sé que me servirá en mi futuro profesional.

Galo Rocha

Dedico mi tesis a mis padres quienes me han apoyado incondicionalmente en cada paso que doy, por sus consejos, por su preocupación al momento de ayudarme en mi vida profesional y en el transcurso del posgrado.

A mi familia, mis hermanos, abuelitos, tíos y primos, por apoyarme con consejos y ánimos cuando lo necesitaba, por nunca dejarme desviar del camino y por enseñarme a enfocarme en cumplir mis metas.

A mi tutor del proyecto quien siempre estuvo pendiente en cada paso que se dio en el proceso de creación del mismo, por su entrega y dedicación para sacar en adelante un excelente entregable para la titulación del posgrado.

A mi compañero Arnaldo Ortiz, con quien hemos dado el 100% de nuestro interés al momento de la crear este entregable, por su dedicación y empeño demostrado a lo largo del proyecto.

A mis docentes por sus cátedras impartidas a lo largo del posgrado, las cuales me han ayudado en mi vida profesional y me han ayudado a tener un nuevo enfoque de profesionalismo.

AGRADECIMIENTO

A mi tutor el ingeniero José Luis Aguayo Morales . Sin usted y sus virtudes, su paciencia y constancia esta tesis no lo hubiese logrado. Sus consejos fueron siempre de mucha utilidad al momento de realizar las distintas actividades en el presente trabajo. Usted formo parte importante de mi carrera universitaria y el presente posgrado con sus aportes profesionales que lo caracterizan. Gracias por sus orientaciones.

A mis padres que han sido mi motor que impulsa mis sueños y aspiraciones, gracias por apoyarme cada día de mi vida en especial en mi carrera universitaria y el presente posgrado que esta por culminar, agradezco de todo corazón por compartir un logro importante más junto a mi familia la cual siempre creyó en mí.

A mis compañeros los cuales me acompañaron por este trayecto académicos, compartiendo una serie de emociones por este largo proceso, deseándoles lo mejor en su vida futura y profesional y esperando mantener contacto con todos para seguir compartiendo momentos únicos e inolvidables como los que he pasado en el posgrado.

Tabla de Contenido

Planteamiento de una política de gestión de seguridad de la información para los ambientes de enseñanza virtuales MOOC en Ecuador.

Autor(es):

Galo Stiven Rocha Freire
Beker Arnaldo Ortiz Sánchez

Resumen

En Ecuador, la educación en línea en los últimos años se ha vuelto cada vez más importante, y los sistemas MOOC han surgido como una alternativa accesible para la formación continua de estudiantes y profesionales. Sin embargo, el uso creciente de estas plataformas también ha dado lugar a preocupaciones sobre la seguridad de la información y la protección de los activos digitales de los usuarios. Además, es indispensable que las instituciones educativas ecuatorianas implementen políticas efectivas de seguridad de la información para proteger tanto el sistema MOOC como los activos de los usuarios que lo utilizan.

Para desarrollar una política de seguridad efectiva para un sistema MOOC utilizando el estándar ISO 27001, se sigue una metodología rigurosa y estructurada. En primer lugar, se realiza una evaluación de riesgos para identificar los activos críticos y las amenazas potenciales a la seguridad del sistema MOOC usando la metodología magerit. Luego, se definen los objetivos de seguridad y los requisitos de cumplimiento para garantizar que la política de seguridad cumpla con las normas y regulaciones aplicables. A continuación, se establecen los controles de seguridad necesarios para mitigar los riesgos identificados. Además, se establecen medidas para la gestión de incidentes de seguridad y se desarrolla un plan de capacitación y concientización en seguridad para el personal involucrado en el sistema MOOC.

El resultado es una política que puede mitigar los riesgos y garantizar la privacidad de los usuarios. Esto implica que las instituciones educativas necesitan implementar medidas preventivas para identificar y reducir los riesgos potenciales, como la implementación de medidas de autenticación y autorización, la encriptación de datos y la capacitación del personal para proteger los datos de los usuarios, incluyendo información personal, registros académicos y otra información sensible, así como también la protección del sistema contra posibles amenazas cibernéticas. Esta política se evaluó por medio de un retorno sobre la inversión de seguridad (ROSI).

Abstract

In Ecuador, online education in recent years has become increasingly important, and MOOC systems have emerged as an accessible alternative for the continuous training of students and professionals. However, the increasing use of these platforms has also given rise to concerns about information security and the protection of users' digital assets. In addition, it is essential that Ecuadorian educational institutions implement effective information security policies to protect both the MOOC system and the assets of the users who use it.

To develop an effective security policy for a MOOC system using the ISO 27001 standard, a rigorous and structured methodology is followed. First, a risk assessment is performed to identify critical assets and potential threats to the security of the MOOC system. Security objectives and compliance requirements are then defined to ensure that the security policy complies with applicable standards and regulations. Next, the necessary security controls are established to mitigate the identified risks and the procedures for their implementation and maintenance are defined. In addition, measures are established for the management of security incidents and a security training and awareness plan is developed for the personnel involved in the MOOC system. Finally, the security policy is regularly reviewed and updated to ensure its continued effectiveness and an internal audit is performed to ensure its compliance with the requirements of ISO 27001.

The result is a policy that can mitigate risks and ensure user privacy. This implies that educational institutions need to implement preventive measures to identify and reduce potential risks, such as the implementation of authentication and authorization measures, data encryption, and staff training to protect user data, including personal information, records academics and other sensitive information, as well as system protection against possible cyber threats. This policy will be evaluated by means of a Return on Security Investment (ROSI) calculator.

1 INTRODUCCIÓN

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas basadas en el estándar ISO 27001 para gestionar la seguridad de la información en términos de confidencialidad, integridad y disponibilidad. Su implementación en ambientes de enseñanza virtual (MOOC) ofrece ventajas para los administradores y los usuarios, evitando el mal uso de la información y estableciendo políticas beneficiosas.

El uso de los MOOC ha aumentado significativamente en el mundo, especialmente por el COVID-19, donde estos ambientes virtuales permitieron mantener una educación continua, cómoda, segura y de calidad. Mantener un correcto SGSI en los MOOC permite evitar posibles riesgos informáticos y gestionar de manera efectiva las políticas en la plataforma, obteniendo así ventajas en términos de confiabilidad y prestigio con los usuarios consumidores.

En Latinoamérica, el nivel de uso de ambientes virtuales de enseñanza es menor que en otros continentes, y en muchos casos se prefiere la modalidad presencial. En consecuencia, la minoría de MOOC existentes en la región no suelen tener un SGSI adecuado, especialmente en aquellos cursos de corta duración que no toman en cuenta políticas de seguridad de la información.

En Ecuador, las instituciones universitarias han implementado medios de enseñanza virtual con el objetivo de certificar a sus estudiantes en distintas áreas de la educación, ofreciendo flexibilidad de horarios, economía y rapidez. Aunque es un gran método de enseñanza, es importante que los recursos e información personal almacenados en estos sistemas cumplan con los estándares de SGSI, ISO 27001, para garantizar la integridad de la institución educativa y sus usuarios consumidores después de finalizado el curso.

El SGSI aplicado en los sistemas MOOC se basará en tres enfoques: gestión de activos, relacionado con políticas empleadas para el correcto manejo de recursos del ambiente virtual; integridad personal, que protege al usuario y su información personal, incluyendo métodos de pago y login; y control de accesos, enfocado en temas de licenciamiento con el MOOC, protocolos de encriptación y uso normalizado de la cuenta.

2 DETERMINACIÓN DEL PROBLEMA

La seguridad de los activos en una MOOC es un tema complejo y delicado que requiere una atención constante y minuciosa. Es crucial tener en cuenta que los activos de una organización en un ambiente virtual de enseñanza pueden ser objeto de divulgación no deseada, lo que puede tener consecuencias negativas en términos de pérdidas económicas y de credibilidad. Si las clases grabadas son difundidas gratuitamente por otros medios, puede generarse una competencia desleal que lleve a la pérdida de usuarios en la comunidad virtual.

Otro factor que puede afectar seriamente la credibilidad de una MOOC es la validez de los certificados emitidos al cumplir los hitos o al culminar el curso. Si estos certificados no tienen validez en el mundo laboral, puede afectar la satisfacción y la confianza de los usuarios.

Además, es importante considerar la integridad personal y la seguridad bancaria de los usuarios en la MOOC, ya que cualquier información personal o bancaria mal gestionada puede resultar en demandas por parte de los usuarios o en sanciones regulatorias.

En cuanto al control de accesos, los activos importantes de la organización pueden ser objeto de robo o divulgación indebida, lo que requiere de medidas de seguridad eficaces. Por ejemplo, es importante establecer límites para compartir cuentas y fomentar el uso normalizado por la cuenta principal.

Frente a estos desafíos, es imprescindible contar con una política SGSI para MOOC, enfocada en la gestión de sus recursos. De esta manera, se pueden prevenir estos problemas y garantizar la continuidad del ambiente virtual en el largo plazo.

3 MARCO TEÓRICO

3.1 QUE ES UN MOOC

Massive Online Open Courses que da paso a las siglas MOOC cuyo significado es cursos online masivos y abiertos. El cual no es otra cosa más que la evolución de la educación común, brindando un igual o mejor aprendizaje por medio de métodos online que benefician a estudiantes y maestros en varios aspectos personales, como por ejemplo economía, tiempo, recursos, facilidad, retroalimentación y flexibilidad de elección en la mayor parte de aspectos dentro de estos cursos online. (Rivas, 2015)

El inicio de los MOOC relata (Pernías Peco & Luján Mora, sf) la creación de un curso sobre conectividad el cual sorprendió por la acogida que tuvo. Sebastian Thrun en el año 2011 ya que fue el contribuidor más grande en el mundo de los MOOC con la expansión de una gran cantidad de cursos en la universidad de Stanford sobre inteligencia artificial, en el cual acogió más de 160.000 estudiantes. (Excellence, 2013)

El potencial de un sistema MOOC consiste en la flexibilidad de compactar nodos en este caso de conocimiento, lo que ocasiona que cuanto mayor sea la cantidad de nodos, más información abarcará el curso y se proveerá mayor aprendizaje para el estudiante.

Con la actual popularidad de estos cursos online, la privatización de estos ha sido inminentes, pero no perjudicial dado que en su mayoría estos suelen poseer una mejor calidad de educación con profesores certificados y mejor planteamiento educacional dentro del MOOC y si en el caso no fuera así aún existen un sinfín de MOOC gratis provenientes de excelentes universidades y empresas de todo el mundo. (Guerrero, 2019)

Dentro de lo que abarca SGSI para MOOC se debe tener en cuenta que los recursos e información personal almacenados en estos sistemas mantengan todos los estándares para la gestión de la seguridad ISO 27001, para que así la institución educativa como sus usuarios consumidores mantengan su integridad, aun después de terminado el curso. (Universidad Veracruzana, 2013)

Este SGSI aplicado en los sistemas MOOC se basará en tres enfoques que permitirán abarcar de mejor manera todos los respectivo a políticas e información los cuales son: Gestión de activos la cual estará relacionado con políticas empleada al usuario para el correcto manejo de recursos del ambiente virtual. (Varela, 2020) Integridad personal: La cual protege al usuario y su información personal, incluyendo métodos de pago y login en caso de existir. Por último, tenemos el control de accesos está enfocado en temas de licenciamiento con el MOOC, protocolos de encriptación y uso normalizado de la cuenta. (Noreña, 2015)

3.2 ¿QUÉ SE ENTIENDE POR ENSEÑANZA VIRTUAL?

La enseñanza virtual se ha convertido en un avance educativo que utiliza herramientas tecnológicas para brindar educación de manera remota, lo que ofrece numerosas ventajas, como la flexibilidad de tiempo y recursos económicos. Gracias a las tecnologías de la información y comunicación, esta forma de educación permite a los estudiantes y profesores interactuar sin necesidad de estar en el mismo lugar físico, creando así un entorno de enseñanza remota. Esta modalidad de enseñanza ha surgido debido a la necesidad de recurrir a formas de aprendizaje sin tener que acudir físicamente a una institución, ya sea por parte del maestro o del alumno, debido a razones como la ubicación geográfica, la cual puede limitar el acceso a la educación en un determinado lugar o país. Además, el tiempo es otro factor determinante, ya que muchas personas tienen ocupaciones laborales, deportivas o personales que limitan su horario de estudio. La enseñanza virtual permite una mayor flexibilidad y accesibilidad, lo que la hace ideal para personas con horarios ocupados. Este tipo de enseñanza se utiliza principalmente para la obtención de maestrías, certificados y títulos de tercer nivel. La enseñanza virtual ha demostrado ser una alternativa viable y eficaz para la educación en línea, y su uso continuará expandiéndose a medida que la tecnología siga evolucionando. Como tal, es importante estudiar y comprender esta modalidad de enseñanza para poder mejorar y optimizar su implementación en el futuro. (Anonimo, 2020)

3.3 RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN UN SISTEMA MOOC

Para la correcta gestión de la seguridad de la información en un sistema de enseñanza virtual se debe detallar aquellos recursos que se van a utilizar durante el proceso de educación de un MOOC, desde el principio de este. Incluso antes de que el usuario comience su primera sesión, lo ideal será obtener todos los activos existentes desde la creación del MOOC o la inscripción del usuario.

Se debe entender que un sistema MOOC tendrá escasos activos tecnológicos físicos o en su mayoría ninguno pues el modelo de negocio es ese. Levar la presencialidad a los niveles más bajos y que el usuario no necesite manejar nada físicamente durante el proceso de aprendizaje.

Tabla 1: Activos Tecnológicos de un sistema MOOC

TABLA DE ACTIVOS TECNOLÓGICOS DE UN SISTEMA MOOC		
CATEGORIA	**ACTIVO**	**EJEMPLO**
DATOS IDENTIFICACIÓN	Título	Indicar
	Web del curso	Indicar
	Institución	Universidad, Institución gubernamental, Empresa, Organización
	Plataforma	Coursera, Udemi, UCAM, UGR
	Ámbito	Arte y Humanidad, Ciencias y Salud, Tecnológico, Jurídico, Científico
	Equipo	Docente, Técnico, Acceso a los perfiles
	Inscripción	Abierta por periodos, permanentemente, es exclusiva o permanece cerrada

	Cursos relacionados	No hay, hay uno, hay varios
	Fecha de cumplimiento	Fecha
ASPECTOS DESCRIPTIVOS	Relevancia del curso	Bajo, Medio, Ato
	Destinarios	Exclusivo, Publico General
	Prerrequisitos	Hay o no Hay y cuales
	Duración del curso	No aparece, indefinido, acotado
	Dedicación	No aparece, indefinido, acotado
	Introducción	Temática del contenido, resolución de las actividades, otra
	Videos	Si hay o no hay
	Objetivos del curso	Si hay o no hay y cuales son
	Funcionamiento del sistema	Orientado desde el curso, Orientado desde la plataforma, Otra
ASPECTOS FORMATIVOS	Plan de trabajo	Por semanas, Por módulos, Por retos
	Módulos	Bloques, Unidades
	Método de trabajo	Indicar
	Evaluación	Indicar
	Certificación	Hay o no Hay y si es Pago o Gratuita
	Acreditación	Medallas, insignias, credenciales, certificados
ASPECTOS INTERACTIVOS	Actividades	Indicar
	Herramientas TIC	Indicar
	Nivel interactividad	Trabajo colaborativo o en pares

Los activos tecnológicos estarán seccionados por cuatro divisiones las cuales permitirán identificar de mejor manera cada activo y su clasificación. De igual manera un ejemplo de cada uno de estos para comprender de donde son provenientes y si son manejados directamente con el MOOC o esta compartida con los usuarios que utilizan la plataforma. La privacidad y seguridad de esta información, estará regularizada por cada una de las políticas establecidas por la plataforma, el servidor de alojamiento del curso y los servicios externos que pueden llegar a manejarlo. (Excellence, 2013)

3.3.1 INTEGRIDAD

Las políticas deberán ser presentadas al usuario que desee ingresar al sistema de aprendizaje y el mismo deberá aceptar o rechazar estas políticas de seguridad y confidencialidad de la información. No deberá estar obligado a aceptarlas en ninguna condición ya sea por su Institución Educativa, o Empresa donde trabaje. En caso de incumplir una política, será penalizado de acuerdo con la gravedad del asunto tanto si el usuario o la plataforma educativa lo causen.

Perjudicar la integridad personal de un usuario se basaría en la filtración o venta de información intencional o no intencional del mismo. Producido por un ataque informático o a su vez una entidad fraudulenta en cuanto al cumplimiento de las políticas. Intentando aprovechar la información de los usuarios para su beneficio. (Aicad, 2022)

3.3.2 CONFIDENCIALIDAD

En este apartado se habla sobre aquellas credenciales que le usuario necesita para ingresar a los distintos recursos del curso, una vez ya inscrito en el mismo. Dentro de estos se tiene accesos a la plataforma, accesos a una clase específica, credenciales de reuniones privadas, claves de acceso a pruebas y lecciones, entre otras que el ambiente virtual crea conveniente cifrar y poner restricción en el sistema.

La seguridad de cada uno de los recursos se basará en métodos criptográficos de contraseñas, además de un sistema de defensa ante intentos de intrusión normado por prácticas de seguridad de la información proporcionado por la ISO

27001 para evitar ataques informáticos y mantener la información segura. (Fernández, 2019)

Los acuerdos con el usuario en cuanto a credenciales deberán ser especificadas dentro de las políticas y términos del ambiente virtual. El no cumplimiento de estos términos podrá ser juzgado por ambas partes.

3.3.3 DISPONIBILIDAD

El usuario que hace uso del MOOC, dependiendo de las políticas establecida durante el proceso de matriculación tendrá que exigir el horario y tiempo en el cual estará disponible el sistema de enseñanza virtual. Teniendo en cuenta que este deberá estar disponible durante el tiempo que se estableció y de igual manera en los horarios ya previstos, esto dependiendo del país que maneje el MOOC.

Al no tener disponibilidad del ambiente virtual y sus recursos, se estará infringiendo un término dentro de las políticas establecidas, ya sea que el hecho suceda por un ataque informático o una mala práctica en los servidores de sistema virtual, este tendrá que responder por los prejuicios ocurridos hacia el usuario.

3.4 COIP

El Código Orgánico Integral Penal del Ecuador, fue creado con el fin de “regular el poder punitivo del Estado, normalizar las contravenciones penales, definir el proceso para el juzgamiento de las personas, promover la reivindicación social de las personas procesadas y la compensación integral de las víctimas”. (Ecuador, 2017)

3.5 DELITOS INFORMÁTICOS

Son acciones ilegales, sin autorización, que se hace uso en diferentes dispositivos e internet, su objetivo es vulnerar o dañar bienes de otros usuarios, los delitos informáticos tienen diferentes naturalezas, como pueden ser: suplantación de identidad, fraude de CEO, robos bancarios, entre otros. (Ecuador, 2017)

3.6 DELITOS INFORMÁTICOS RECURRENTES EN ECUADOR

En Ecuador desde algunos años atrás, se cuenta con leyes sancionatorias para los delitos informáticos con penas privativas de la libertad, estos se los reconoce en el COIP, con la evolución constante de la tecnología, la comunicación va a pasos agigantados, los delitos informáticos también han ido cambiando, pero se siguen manteniendo los ataques tradicionales. (Primicias, 2019)

En Ecuador los delitos más frecuentes según la página web de primicias del Ecuador, indica 4 delitos informáticos con un alto índice de denuncias.

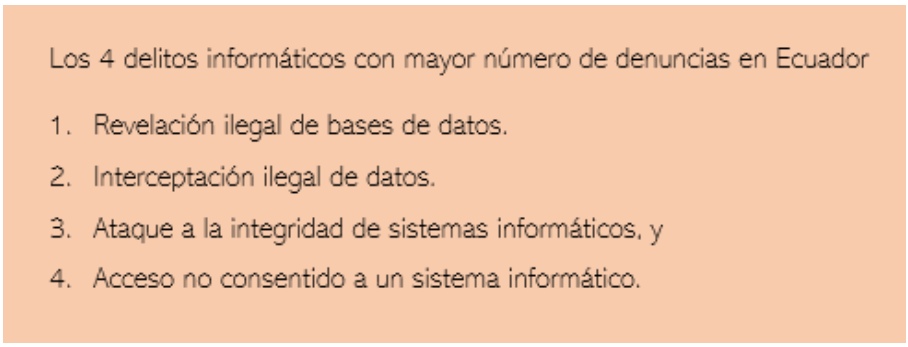

Figura 1: Delitos informáticos en Ecuador (Primicias, 2019)

Estos 4 artículos están penados con prisión preventiva dependiendo la causa probable y de la intención y afección con que estos se den para la organización afectada.

3.7 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP)

En el Ecuador, en 2021 se creó LOPDP (Alonso, 2023), para entregar las pautas sobre el manejo y tratamiento de datos personales entregados o pertenecientes a cualquier organización, haciendo énfasis sobre quien recae la responsabilidad de la protección de los datos y sus sanciones, a esto se crea un nuevo rol, al cual se le delega la responsabilidad de generar los planes de contingencia, los cambios estructurales, etc., todo eso depende de la naturaleza de la organización, también se informó sobre los derechos a los titulares de los datos, entre estos está el derecho de oposición, el de enseñanza virtual, entre otros, esta ley sanciona dependiendo de la gravedad de la afección realizada con un porcentaje sobre la facturación anual de la organización.

3.8 ATAQUES CIBERNÉTICOS EN ECUADOR

En los últimos años Ecuador ha sido blanco de diversos ciber ataques, según un reportaje hecho por el comercio (Comercio, 2021) , a partir del teletrabajo que se dio por la pandemia el ciber ataque en el Ecuador subió un 75%, seguidos por Perú, Panamá y Guatemala, todo esto presentado por un análisis entregado por la tecnología de soluciones de Kaspersky instaladas en usuarios de la región, todo esto se da por el aumento de técnicas de recepción de datos que en los últimos años esto han crecido, lamentablemente en Latinoamérica no existe una cultura de protección de su información, todo esto por falta de campañas de concientización sobre estos temas, o inculcación temprana sobre medios tecnológicos sus beneficios y consecuencias, a continuación se detalla casos de ciber ataques en el Ecuador.

3.9 ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Por todo lo visto anteriormente Ecuador en 2017, formo un comité de Ciberseguridad, con organismos estatales y privados. Para generar una estrategia nacional de Ciberseguridad, el MINTEL el 16 de junio de 2017, informó sobre una herramienta, tanto para el sector público como privado, con seis ejes de operación que contienen temas como: circunstanciales y prioritarios para el país: Gobernanza y combinación gubernamental; Resiliencia cibernética; Lucha contra la ciberdelincuencia; Ciberdefensa nacional y ciber inteligencia; Destrezas y capacidades de ciberseguridad; y Cooperación internacional (Informaciòn, 2022), la ministra enfatizó que esto se lo realizó para proteger la información de la ciudadanía y la seguridad de los estados del ciberespacio, también con la entrega de esta estrategia, se mencionó que el Ecuador se sumará al convenio de Budapest el cual es un instrumento para combatir crímenes y delitos digitales

4 Resultados y discusión

4.1. MEDIDAS DE PROTECCIÓN DE LOS DERECHOS DE AUTOR EN LA INFORMACIÓN DENTRO DE UN SISTEMA MOOC

La creación de contenido online se ha establecido de manera muy fuerte dentro de internet dado que es una manera de darse a conocer con el mundo de manera sencilla y de expandirse con mayor facilidad. Aunque compartir todo este contenido por la red tiende a que los autores peligren que otras personas con malas prácticas se adueñen de su contenido como propio.

Dentro de un sistema MOOC se encontrarán infinidad de recurso estudiantil, entre estos archivos de multimedia, documentos de texto, hojas de cálculo, presentaciones, etc. Es por ello que es necesario registrar el contenido que se sube a la red como propia, dado que puede ser utilizado por otros usuarios que en su mayoría desean obtener beneficios monetarios de este contenido. Por eso se tienen las siguientes alternativas para el registro. (Romero, 2018)

4.1.1 LICENCIAS ONLINE

Existen plataformas digitales que ofrecen este servicio de licenciamiento a recursos online, entre la más conocida esta Safe Creative que expide licencias de copyright las cuales son autorizados en la mayor parte de países del mundo. Otra opción esta de la mano de la organización Creative Common la cual no reserva por completo la propiedad de los derechos de autor sino más bien solo una parte, esto es conocido como copyleft y permite a los usuarios usar el contenido siempre y cuando lo citen, además de permitir replicar o modificar el recurso teniendo en cuanta que no podrán beneficiarse económicamente de él.

4.1.2 DEPOSITO NOTARIAL

Los autores de contenido pueden realizar un depósito ante la notaría de su obra, declarando ser el autor, esto no avala que sea de su propiedad, pero puede ser

beneficioso en caso de un proceso judicial. El depositante puede elegir la cantidad de documentos que desea incluir en el acta y sumar más en el futuro sin ningún límite, este método suele ser útil para resguardar secretos industriales y proyectos en constantes cambios, como programas informáticos o páginas web.

4.1.3. CERTIFICADOS

La organización mundial de la propiedad intelectual son los únicos que pueden dar estos certificados, para ello ha creado Wipo prood el cual es un servicio en la línea que ayuda a proteger los derechos de autor de los recursos digitales por un costo de 20 dólares por ítem. El sistema funciona por medio de sellos llamados tokens o huella digital, que de igual manera como es el caso del depósito notarial no avala que el recurso sea de autoría propia, pero si demuestra la existencia de un documento que prueba que se presentó el recurso como propio.

4.1.4 MÉTODOS PROPIOS

Existen una serie de métodos que cada autor ha decidido ejecutar con el fin de registrar su recurso, en la mayoría de las situaciones, esto no brinda una protección adecuada ya que existen diversas formas de vulnerar estas medidas de seguridad o vacíos legales dentro de estas prácticas, dado que no se avala de ninguna manera que los recursos pertenezcan a un determinado autor. Entre estos métodos tenemos:

- Creación de marcas de agua con el nombre de autor o compañía en recursos online, ya sean multimedia, informáticos de texto o creación de software.
- Bloqueos de escritura y modificación de archivos en su mayoría documentación de ofimática y líneas de código web.
- Métodos de criptografía para la confidencialidad del recurso por medio de contraseñas y encriptación de información.

4.2. ACTIVOS PARA LA EJECUCIÓN DE LA POLÍTICA

En el entorno actual, donde la tecnología desempeña un papel fundamental en la mayoría de las organizaciones, es crucial identificar y proteger los activos tecnológicos más importantes. En este sentido, se han seleccionado tres activos estratégicos que merecen una atención especial: la Propiedad Intelectual, los Servicios en un sistema MOOC y el Recurso Humano. Estos activos han sido respaldados con datos estadísticos que demuestran su relevancia y la necesidad de implementar medidas de seguridad adecuadas para salvaguardar su integridad y confidencialidad.

a) Propiedad Intelectual

Datos estadísticos recientes respaldan la importancia de proteger la propiedad intelectual frente a ataques cibernéticos. Según el informe de la Comisión Europea sobre la situación de los derechos de propiedad intelectual en la Unión Europea, se estima que el 25% de las empresas europeas han experimentado algún tipo de infracción de propiedad intelectual en los últimos cinco años.
Además, un estudio realizado por la Organización Mundial de la Propiedad Intelectual (OMPI) reveló que los ataques cibernéticos relacionados con la propiedad intelectual han aumentado en un 65% en los últimos dos años. Estos ataques van desde el robo de información confidencial hasta la manipulación de derechos de autor y el uso no autorizado de material protegido.

En el ámbito internacional, el informe de la Oficina de Propiedad Intelectual de los Estados Unidos (USPTO) destaca que el 35% de las empresas estadounidenses han sufrido algún tipo de infracción de propiedad intelectual, con pérdidas estimadas en más de $200 mil millones de dólares anuales.
Estos datos estadísticos refuerzan la necesidad de implementar medidas de seguridad sólidas y políticas de protección de la propiedad intelectual. La alta probabilidad de incidentes relacionados con la propiedad intelectual y los impactos significativos que pueden resultar de ellos hacen que la protección de este activo sea una prioridad para las organizaciones.

Es por ello por lo que se toma la propiedad intelectual como un activo crítico debido a que tiene un alto valor estratégico para la organización y es objetivo de

ataques cibernéticos cada vez más sofisticados. La probabilidad de que ocurra un incidente relacionado con la propiedad intelectual es alta, y el impacto de tal incidente podría ser significativo, incluyendo la pérdida de ingresos, la pérdida de ventaja competitiva y la erosión de la reputación.

b) Servicios de un MOOC

Existen datos estadísticos relevantes que respaldan la necesidad de proteger los servicios de MOOC frente a los ataques cibernéticos. Según el informe anual de ciberseguridad de Symantec, en el último año se registró un aumento del 48% en los ataques dirigidos a plataformas educativas en línea, lo que incluye los servicios de MOOC. Estos ataques pueden involucrar desde intentos de robo de información personal de los usuarios hasta interrupciones del servicio y ataques de denegación de servicio distribuido (DDoS).

Además, un estudio realizado por la firma de seguridad informática Kaspersky reveló que el 62% de las instituciones educativas han experimentado al menos un incidente de seguridad en línea en los últimos años. Estos incidentes pueden incluir el acceso no autorizado a los servicios de MOOC, el robo de datos de usuarios y la manipulación de contenido.

En cuanto al impacto de estos incidentes, el informe de seguridad cibernética de Cisco señala que el tiempo promedio de inactividad debido a un ataque cibernético en el sector educativo es de aproximadamente 7.6 horas. Esta interrupción puede resultar en una pérdida significativa de confianza por parte de los usuarios y la posible disminución de los ingresos asociados con los servicios de MOOC.

Estos datos estadísticos subrayan la importancia de implementar medidas sólidas de seguridad y protección de la privacidad en los servicios de MOOC. Dado el alto riesgo y el impacto potencialmente significativo de los incidentes relacionados con los servicios de MOOC, es fundamental adoptar un enfoque proactivo para garantizar la integridad, la confidencialidad y la disponibilidad de estos servicios educativos en línea.

c) Recurso Humano

Los datos estadísticos respaldan la importancia de abordar los riesgos relacionados con el recurso humano en materia de seguridad de la información. Según el informe de Verizon sobre investigaciones de brechas de datos, el factor humano estuvo involucrado en aproximadamente el 33% de las brechas de datos analizadas. Esto incluye tanto errores involuntarios como acciones maliciosas llevadas a cabo por empleados o contratistas.

Además, un estudio realizado por la firma de seguridad informática IBM reveló que las amenazas internas representan el 60% de todos los incidentes de seguridad reportados por las organizaciones. Estas amenazas pueden incluir la divulgación no autorizada de información confidencial, el acceso no autorizado a sistemas y la manipulación malintencionada de datos.

En cuanto al impacto de estos incidentes, el informe de la consultora Ponemon Institute sobre el costo de las brechas de datos señala que el factor humano contribuye al costo promedio de una brecha de datos en un 23%. Esto incluye los gastos asociados con la investigación, la mitigación, la notificación y las posibles acciones legales.

Estos datos estadísticos destacan la importancia de educar y concientizar al personal sobre las mejores prácticas de seguridad de la información, así como implementar controles y políticas adecuadas. El recurso humano debe ser considerado un factor crítico en la cadena de seguridad de la información, y se deben tomar medidas para mitigar los riesgos asociados con errores, descuidos y conductas malintencionadas.

5 CREACIÓN DE LA POLÍTICA

5.1. POLÍTICA PROPUESTA

Para desarrollar una política de seguridad de la información, es importante seguir una serie de pasos claves. En primer lugar, es necesario definir el objetivo, alcance y vigencia de la política, de manera que se establezcan claramente los objetivos a cumplir y los límites dentro de los cuales se aplicará. Luego, es esencial definir quiénes serán los responsables de su implementación y seguimiento, así como especificar la autoridad de emisión, revisión y publicación. Es fundamental que se definan claramente las medidas de seguridad que se deben tomar y se comuniquen de manera efectiva a todos los empleados para asegurar su cumplimiento. Por último, es importante actualizar y revisar continuamente la política para garantizar su eficacia a largo plazo y hacer ajustes en caso de ser necesario.

Al seguir estos pasos, se puede desarrollar una política de seguridad de la información efectiva que proteja adecuadamente los activos de la organización y minimice los riesgos de seguridad. Presentando así la siguiente política.

A. Introducción

Esta política tiene como objetivo establecer un marco de seguridad y gestión de recursos en el Sistema MOOC (Massive Open Online Course), con el fin de garantizar el uso seguro y efectivo de los recursos, proteger los derechos de autor, la privacidad de los usuarios y asegurar la calidad del aprendizaje virtual.

B. Objetivo

El objetivo principal de esta política es asegurar el uso seguro y efectivo de los recursos en el Sistema MOOC, protegiendo los derechos de autor, la privacidad de los usuarios y la calidad del aprendizaje virtual.

C. Alcance

La política de gestión de recursos en el Sistema MOOC tiene un alcance amplio y se aplica a todos los recursos utilizados, así como a todos los usuarios involucrados en la plataforma. Esto incluye archivos, audios, videos y cualquier

otro material utilizado para la enseñanza virtual. La política abarca aspectos técnicos y legales, asegurando el cumplimiento de los derechos de autor, la protección de la privacidad y la implementación de medidas de seguridad. Con una vigencia de un año dividida en dos periodos, se busca una implementación completa seguida de una evaluación y monitoreo para identificar mejoras en futuras auditorías.

D. Principios de la Política de la Información

Los siguientes principios deben ser seguidos para asegurar la gestión efectiva de los recursos en el Sistema MOOC:

I. Protección de los derechos de autor.
II. Privacidad de los usuarios.
III. Uso responsable y efectivo de los recursos.
IV. Cumplimiento de las normas y regulaciones aplicables.

E. Compromiso de la Dirección

La dirección del Sistema MOOC se compromete a respaldar y cumplir con esta política, asignando los recursos necesarios para su implementación y garantizando su seguimiento.

F. Roles y Responsabilidades

Se establecen los siguientes roles y responsabilidades:

I. Área Legal: Responsable de garantizar el cumplimiento de los derechos de autor y tomar acciones legales en caso de infracciones.
II. Área de Soporte Informático: Encargada de administrar los accesos, monitorear los recursos y brindar soporte técnico.
III. Área de Gestión Académica: Responsable de la administración de los recursos y la carga de contenido.
IV. Área de Recursos Humanos: Encargada de la capacitación de los usuarios sobre las políticas de seguridad y recursos.
V. Área de Recursos Financieros: Provee el capital necesario para la implementación de programas de capacitación y otras medidas de seguridad.

G. Gestión de la Seguridad de los Recursos Humanos

Se deben establecer medidas de seguridad para la gestión de los recursos humanos, incluyendo la contratación, capacitación y concientización sobre las políticas de seguridad y recursos.

H. Gestión de Activos

Se debe realizar un inventario de los activos utilizados en el Sistema MOOC, incluyendo los recursos digitales y físicos. Debe establecerse un proceso de gestión y protección de estos activos.

I. Clasificación de la Información

La información utilizada en el Sistema MOOC debe ser clasificada de acuerdo con su nivel de confidencialidad y criticidad. Se deben establecer controles de acceso y protección adecuados para cada categoría de información.

J. Prevención de Fugas de Información

Se deben implementar medidas para prevenir la filtración o divulgación no autorizada de información confidencial. Esto incluye controles técnicos, políticas de uso aceptable y concientización de los usuarios.

K. Control de Acceso

El acceso a los recursos en el Sistema MOOC debe ser controlado y limitado a los usuarios autorizados. Se deben establecer niveles de permisos y restricciones de acceso para garantizar la privacidad de los usuarios y la protección de los recursos.

L. Gestión del Ciclo de Vida de la Identidad

Se deben establecer procesos para la gestión adecuada del ciclo de vida de la identidad de los usuarios en el Sistema MOOC, incluyendo la creación, modificación y eliminación de cuentas de usuario.

M. Seguridad Física y del Entorno

Se deben implementar medidas de seguridad física para proteger los recursos físicos utilizados en el Sistema MOOC, como servidores, equipos de almacenamiento y cualquier otro dispositivo.

N. Seguridad en el Trabajo en la Nube o Cloud

Si se utiliza la nube para almacenar o procesar información en el Sistema MOOC, se deben establecer medidas de seguridad adecuadas, como la encriptación de datos y la selección de proveedores confiables.

O. Seguridad en la Operativa

Se deben establecer procedimientos y controles para garantizar la seguridad en las operaciones diarias del Sistema MOOC, incluyendo la gestión de copias de seguridad, la protección contra malware y la monitorización de eventos de seguridad.

P. Seguridad en las Telecomunicaciones

Se deben implementar medidas de seguridad para proteger las comunicaciones y transmisiones de datos en el Sistema MOOC, como la encriptación de la información y el uso de redes seguras.

Q. Seguridad en el Ciclo de Vida del Desarrollo de Sistemas

Se deben aplicar prácticas de seguridad en todas las etapas del ciclo de vida del desarrollo de sistemas utilizados en el Sistema MOOC, desde el diseño y la implementación hasta las pruebas y la puesta en producción.

R. Seguridad en los Proveedores

Se deben establecer criterios de seguridad para la selección y evaluación de proveedores externos que brinden servicios o suministren recursos al Sistema MOOC, asegurando su confiabilidad y cumplimiento de las políticas de seguridad.

S. Gestión de Incidentes

Se debe establecer un proceso de gestión de incidentes para responder y mitigar rápidamente cualquier incidente de seguridad que pueda afectar los recursos del Sistema MOOC.

T. Continuidad de Negocio

Se deben implementar medidas de planificación y gestión de la continuidad de negocio para garantizar la disponibilidad y recuperación de los recursos en el Sistema MOOC en caso de interrupciones o desastres.

U. Cumplimiento Regulatorio

El Sistema MOOC debe cumplir con todas las normas y regulaciones aplicables en cuanto a protección de datos, privacidad y derechos de autor.

V. Auditorías de Seguridad y Gestión de Vulnerabilidades

Se deben realizar auditorías periódicas de seguridad y gestión de vulnerabilidades para evaluar y mejorar continuamente la seguridad de los recursos en el Sistema MOOC.

W. Gestión de Excepciones

Se debe establecer un proceso para gestionar las excepciones a las políticas de seguridad y recursos, asegurando que sean debidamente justificadas y aprobadas por la dirección.

X. Sanciones Disciplinarias

Cualquier usuario que viole esta política estará sujeto a sanciones disciplinarias de acuerdo con el reglamento establecido por la plataforma del Sistema MOOC. El reglamento especificará los eventos o conductas que serán sancionados, así como el alcance y las medidas disciplinarias que se aplicarán.

Las sanciones disciplinarias pueden incluir, entre otras, la suspensión temporal de la cuenta del usuario, la eliminación permanente de la cuenta, la restricción de acceso a ciertos recursos o funcionalidades, y la aplicación de medidas legales correspondientes, según la gravedad de la violación cometida.

Es responsabilidad del área legal y la dirección del Sistema MOOC establecer y mantener actualizado el reglamento de sanciones disciplinarias, asegurándose de que sea comunicado de manera clara a todos los usuarios. Las sanciones se aplicarán de manera justa y consistente, garantizando el cumplimiento de las normas y la protección de los derechos de autor, la privacidad de los usuarios y la calidad del aprendizaje virtual en el Sistema MOOC.

Y. Revisión y Actualización de la Política

Esta política será revisada y actualizada de forma periódica para garantizar su relevancia y eficacia. Se establecerá un plan de auditoría y monitoreo de su implementación, así como de identificación de posibles mejoras.

La política de gestión de recursos en el Sistema MOOC busca garantizar el uso seguro y efectivo de los recursos, proteger los derechos de autor, la privacidad de los usuarios y asegurar la calidad del aprendizaje virtual. Todos los usuarios del Sistema MOOC deben cumplir con esta política y se espera que colaboren activamente en su implementación y cumplimiento.

5.2. COSTO BENEFICIO (ROSI)

Para mejorar la relación costo-beneficio, es fundamental implementar medidas de control en nuestros activos de información. De esta manera, podemos comparar el nivel de riesgo anterior con el nivel de riesgo posterior tras la implementación de los controles y así determinar si el beneficio obtenido justifica los costos incurridos. En resumen, antes de aplicar cualquier control, es necesario evaluar el riesgo actual y luego determinar si los controles propuestos son adecuados para reducir el riesgo a un nivel aceptable, en la tabla 2, se menciona los activos a los cuales se enfoca el presente proyecto.

ACTIVO	CONTROLES IMPLEMENTADOS	NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO	CONTROLES A IMPLEMENTAR	NUEVO NIVEL DE RIESGO	RIESGO RESIDUAL
Propiedad intelectual	Ninguno	Alto	Mitigar	Medidas de protección a los recursos (Licencias online, block chain, deposito notarial, certificados, marca de agua, metodos de criptografía)	Bajo	Aceptable
Servicios de MOOC	Ninguno	Alto	Mitigar	Implementar medidas de seguridad informática en toda la plataforma, esto incluye (servidor, página web, base de datos, recursos del sistema)	Medio	Aceptable
Recurso humano	Ninguno	Alto	Mitigar	Implementar control de accesos, monitoreos, capacitación del personal	Bajo	Aceptable

Tabla 2: Implementación de controles

Para calcular el costo beneficio de una politica de seguridad es recomendable implementar la metodología ROSI esta se utilizada para evaluar el costo y el valor de una política de seguridad. Es importante utilizar esta metodología porque permite tomar decisiones informadas sobre la inversión en seguridad y justificar los recursos asignados a ella.

$$Rosi = \frac{((N° \ incidentes * Costo) - Inversión)}{Inversión}$$

Figura 2: Formula ROSI

En la Figura 2, podemos apreciar la fórmula para el cálculo del ROSI, algunas de las razones por las cuales es necesario utilizar la metodología ROSI para determinar el costo beneficio de una política de seguridad son:

1) Evaluación de riesgos: Esta ayuda a evaluar los riesgos asociados con las amenazas de seguridad y determinar las medidas necesarias para mitigarlos. Al comprender los riesgos y las posibles consecuencias, se pueden tomar decisiones más acertadas sobre la asignación de recursos y la implementación de controles de seguridad.
2) Toma de decisiones basada en datos: Se basa en datos concretos y mediciones tangibles para evaluar el costo y el valor de una política de seguridad. Esto proporciona una base objetiva para tomar decisiones informadas y priorizar las inversiones en seguridad de acuerdo con su rendimiento esperado.
3) Justificación de recursos: Ayuda justificar la asignación de recursos a la seguridad al demostrar su valor y beneficio para la organización. Al calcular el retorno de la inversión en seguridad, se puede demostrar cómo las medidas de seguridad contribuyen a la protección de activos críticos, la reducción de riesgos y la minimización de pérdidas potenciales.
4) Optimización de recursos: Permite identificar las áreas en las que se obtiene un mayor retorno de la inversión en seguridad. Esto ayuda a optimizar el uso de los recursos disponibles, asegurando que se asignen adecuadamente a las áreas de mayor riesgo o donde se espera un mayor impacto en la protección de activos.

5) Comunicación efectiva: Proporciona una forma estructurada de comunicar los resultados y el valor de las inversiones en seguridad a los diferentes interesados, como la alta dirección y los responsables de la toma de decisiones. Esto facilita la comprensión de los beneficios y los riesgos asociados con la política de seguridad, lo que a su vez puede respaldar la obtención de recursos adicionales o el apoyo necesario.

Por estas razones esta metodología es recomendada y asi evaluar el costo y el beneficio de la política de seguridad, lo que permite tomar decisiones basadas en datos, justificar la asignación de recursos, optimizar su uso y comunicar de manera efectiva los resultados y beneficios a los interesados.

6 Conclusiones

Al incluir la ley de Orgánica de Protección de Datos Personales por medio de los roles definidos y las responsabilidades, así como el control fugas y accesos asignadas en la política propuesta se puede fomentar la transparencia y responsabilidad en la gestión de los datos personales y crear un ambiente de confianza entre los usuarios y el MOOC. La consideración de esta Ley es esencial para garantizar una política efectiva que beneficie al SGSI en la gestión de recursos para el MOOC, y a su vez, proteja la privacidad y seguridad de los datos personales de los usuarios en línea.

El COIP en el Ecuador es una ley que establece el marco jurídico para la prevención y persecución de los delitos en el país. En cuanto a las políticas de seguridad, el COIP puede tener un impacto significativo, ya que establece los delitos relacionados con la seguridad y las sanciones correspondientes como: Tipificación de delitos, prevención y disuasión, investigación y persecución protección de datos personales, colaboración con autoridades. Teniendo un impacto directo en la política de seguridad ya que al definir las restricciones de la política se puede salvaguardar la integridad legal del MOOC, definiendo los delitos relacionados con la seguridad, estableciendo sanciones y estableciendo procedimientos legales para la investigación y persecución de delitos.

El uso de la metodología ROSI en una política de seguridad en un MOOC puede ser beneficioso para asegurar la protección de los activos digitales, garantizar la privacidad de los estudiantes y promover la confianza en el entorno educativo en línea. Al aplicar esta metodología, se pueden obtener los siguientes resultados como evaluación precisa de riesgos, optimización de recursos, justificación de inversiones, confianza de los estudiantes, cumplimiento normativo. Todo esto puede mejorar la protección de los activos digitales, garantizar la privacidad de los estudiantes y promover la confianza en el entorno educativo en línea. Al evaluar los riesgos, optimizar

los recursos, justificar las inversiones y cumplir con las regulaciones, se crea un ambiente más seguro y confiable para el aprendizaje en línea.

Referencias

Aicad. (15 de 01 de 2022). *Seguridad de la infromación* . Obtenido de https://www.aicad.es/

Alonso, C. (22 de 02 de 2023). *Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador.* Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/

Anonimo. (2020). *GCF Global*. Recuperado el 2 de Septiembre de 2022, de https://edu.gcfglobal.org/es/educacion-virtual/que-es-la-educacion-virtual/1/

Comercio, E. (31 de 08 de 2021). *Ecuador es el país de Latinoamérica con mayor aumento en ciberataques*. Obtenido de https://www.elcomercio.com/

Ecuador. (27 de 05 de 2017). *Obtenido de Delitos informáticos establecidos en el COIP y como prevenirlos*. Obtenido de https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Excelencia., E. E. (19 de 06 de 2019). *Escuela Europea De Excelencia. Obtenido de Beneficios de una certificación ISO*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/03/beneficios-de-una-certificacion-iso-por-que-su-empresa-deberia-obtenerla/

Excellence, I. (10 de 12 de 2013). *Blog especializado en Seguridad de la*. Obtenido de https://www.pmg-ssi.com/2013/12/iso27001-origen/

Fernández, L. (12 de 06 de 2019). *Control de acceso: qué es y cómo ayuda a proteger nuestros datos*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/

Guerrero, D. (26 de 05 de 2019). *BLOGSCIENCE MOOCS*. Obtenido de https://blogscienceusmp.blogspot.com/

Informaciòn, M. d. (16 de 06 de 2022). *El Gobierno Nacional presentó la Estrategia Nacional de Ciberseguridad*. Obtenido de https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-presento-laestrategia-nacional-de-ciberseguridad/.

Pernías Peco, P., & Luján Mora, S. (ssf de sf de sf). *Los MOOC: orígenes, historia y tipos.* Obtenido de https://rua.ua.es/: https://rua.ua.es/dspace/bitstream/10045/105190/1/Pernias_Lujan-Mora_2014_Comunicacion-y-Pedagogia.pdf

Pirani, A. (15 de 09 de 2018). *ISO 27001: de qué se trata y cómo implementarla*. Obtenido de https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

Primicias. (11 de 09 de 2019). *Los cuatro delitos informáticos más recurrentes en Ecuador.* Obtenido de https://www.primicias.ec/noticias/tecnologia/estos-delitos-informaticos-mas-recurrentes-ecuador

Rivas, M. R. (12 de 05 de 2015). *Un estudio sobre los componentes*. Recuperado el 2022, de https://www.revistacomunicar.com/verpdf.php?numero=44&articulo=44-2015-03

Romero, I. (15 de 05 de 2018). *maneras de proteger los contenidos originales en internet*. Obtenido de

https://cincodias.elpais.com/cincodias/2020/10/21/legal/1603232054_463916.html