Seguridad en Entornos de Educación Virtual

Security in Virtual Education Environments

Hernán Santiso[1], Juan Matías Koller[2], Mauricio Gabriel Bisaro[3]

Recibido: mayo 2016 Aceptado: setiembre 2016

Resumen.- En los últimos tiempos se han estado incorporando diferentes tecnologías de información y comunicaciones (TICs) a los ámbitos de educación virtual, hasta el punto de convertirse en herramientas esenciales para el apoyo de los procesos de enseñanza y aprendizaje.
Como consecuencia de este fenómeno, estos entornos se encuentran expuestos a nuevos riesgos tecnológicos que si no son identificados y mitigados de manera apropiada, pueden afectar la seguridad de las plataformas educativas.
El objetivo del proyecto fue el de definir un marco de gestión de riesgo informático para entornos de educación virtual que permita garantizar la protección de la información utilizada en los procesos educativos a través de Internet.
Para ello se realizó un relevamiento de los principales riesgos de seguridad asociados a las plataformas virtuales, y una vez hecho esto se definieron un conjunto de controles asociados a dichos riesgos que conformaron el marco de gestión propuesto.
Por último se desarrollaron modelos técnicos para la aplicación efectiva de tecnologías de seguridad en plataformas de educación virtual, como UTM (Gestión de Amenazas Unificada) para seguridad de los protocolos de red y PKI (Infraestructura de Clave Pública) para mejorar los mecanismos de autenticación a las plataformas.

Palabras Claves: TICs en Educación; Seguridad Informática; Plataformas de Educación Virtual; Marco Normativo; Riesgo.

Summary.- *Over the last years it have been incorporating in the virtual education environments different types of information technologies and communications (ICT), up to become it in essential tools to support the teaching and learning process.*
As consequence of that, these environments have been exposed to new technological risks, which if they are not identified and mitigated appropriately, could affect the security of educational platforms.
The goal of the project was to define a framework to manage information technology risks in virtual education environments which ensure the protection of systems and information involved in educational processes over the Internet.
In order to accomplish this objective we have made a survey to know the most important risks associated with virtual educational platforms, and after that, we have defined a set of controls associated to these risks, which finally composes the framework of management.
Lastly were have developed two technical models to implement information security technologies in virtual education platforms. These are UTM (Unified Threat Management) for the security of network protocols and PKI (Public Key Infrastructure) to improve the authentication to the platforms.

[1] CIADE-IT, Universidad Blas Pascal, Córdoba, Argentina, hsantiso@hotmail.com
[2] CIADE-IT, Universidad Blas Pascal, Córdoba, Argentina, matias_koller@yahoo.com.ar
[3] CIADE-IT, Universidad Blas Pascal, Córdoba, Argentina, Mauricio.bisaro@gmail.com

Keywords *:TICs in Education; Information Security; Virtual Learning Platforms.*

1.- Introducción.- En la última década se ha estado experimentado un crecimiento sostenido en el uso de diferentes de TICs como herramientas de apoyo a los procesos de educación a distancia, hasta el punto de convertirse en un componente central en la planificación y diseño de los programas educativos actuales.

La incorporación de nuevos medios de comunicación dentro de las plataformas de educación virtual como el chat, el streaming de video y los sistemas de voz sobre IP, la aparición de nuevas formas de interacción en línea como las redes sociales y los teléfonos inteligentes, brindan una mayor facilidad de uso a los usuarios logrando una integración más rápida y efectiva de los procesos educativos a las plataformas virtuales.

Sin embargo la inclusión de estas nuevas tecnologías trae aparejado nuevos riesgos, que si no son identificados y mitigados de manera apropiada, generan vulnerabilidades que pueden afectar la seguridad de la información, afectando así al proceso educativo.

Para poder encarar esta problemática de manera eficiente es necesario llevar adelante un proceso de gestión de la seguridad de la información con un enfoque integral de los riesgos que nos permita lograr un adecuado balance entre control y usabilidad, e incorporar en forma exitosa las nuevas tecnologías de seguridad que ayuden a mitigar las amenazas más importantes sin perder facilidad de uso.

De estas observación surge el objetivo del proyecto que fue el de definir un marco de gestión de la seguridad de la información para entornos de educación virtual que sirva de guía para que las organizaciones educativas puedan implementar los mecanismos de protección necesarios para llevar adelante los procesos educativos a través de Internet sin verse afectados por los riesgos tecnológicos.

Adicionalmente y como parte del trabajo, se seleccionaron dos prototipos técnicos que se consideran aplicables a la mayoría de las plataformas de educación a distancia y que atacan temas de interés común, como lo son la seguridad en los protocolos de red y la autenticación.

2.- Desarrollo del trabajo.- Antes de comenzar el desarrollo del trabajo consideramos conveniente realizar una revisión de los estándares y normativas de gestión de seguridad y riesgo informático más difundidos en la comunidad y los trabajos de investigación y publicaciones existentes que hacen referencia al tema bajo estudio. En esta primera etapa se analizaron los siguientes estándares de seguridad:

ISO/IEC/IRAM 27001 [1]:

Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI). Establece que los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 [2], donde se abarcan los siguientes temas: Políticas de seguridad, Organización de la seguridad, Seguridad de los recursos humanos, Gestión de activos, Control de accesos, Cifrado, Seguridad física y ambiental, Seguridad en la Operación, Seguridad en las Comunicaciones, Adquisición de sistemas de información, desarrollo y mantenimiento, Gestión de Proveedores, Gestión de los incidentes de seguridad, Administración de la continuidad de negocio y Cumplimiento (legales, de estándares, técnicas y auditorías)

COBIT [3] :

COBIT (Control OBjetives for Information and Technology related) es un sistema de mejores prácticas para la administración de un sistema de información que plantea los siguientes objetivos:
- Suministrar normas basadas en buenas prácticas para el control de la Información y la Tecnología de Información.
- Proveer a los usuarios de una base sólida para administrar la TI y obtener garantías
- Brindar a los auditores criterios para las tareas de evaluación y auditoría
- Respaldar los esfuerzos conjuntos de la gerencia, los responsables de procesos de negocio y los auditores a fin de propiciar el mejor gobierno de TI

NIST Cybersecurity Framework [4]:

Estándar creado por el Instituto Nacional de Estándares de Tecnología de Estados Unidos, que define un marco de trabajo de ciberseguridad independiente de la tecnología que permita a las organizaciones que poseen infraestructuras críticas.
Su foco principal es la prevención, detección y tratamiento efectivo de los ciberataques, organizando los controles según las siguientes fases relacionadas con un incidente de cibersegurdad: identificar, proteger, detectar, responder y recuperar.

MAGERIT[5]:

Es una metodología de gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, enfocada principalmente a entidades de Administración Pública que ofrece un método sistemático para analizar los riesgos derivados del uso de las TICs, de forma de definir luego las medidas de mitigación más apropiadas.

Se encuentra dividida en tres partes, la primera describe la estructura del modelo de gestión de riesgos, la segunda propone criterios para la identificación y valuación de los activos y ofrece un listado con las amenazas y controles aplicables y la última ofrece una guía de técnicas comúnmente utilizadas en los procesos de análisis de riesgos.

ISO 31000/27005[6] :

Es en la actualidad el marco de gestión de riesgos más ampliamente difundido lo conforman los estándares ISO 31000 (Risk Management) ISO/IEC 27005 (Information Security Risk Management).

Dicha norma divide al proceso de gestión de riesgos en seis fases. Ellas son:

1. Establecer el contexto.
2. Identificación de riesgos.
3. Análisis de riesgo.
4. Evaluación de riesgo.
5. Tratamiento del riesgo.
6. Seguimiento, revisión y mejora del proceso de gestión de riesgos

Por otro lado se procedió a realizar una revisión de los trabajos de investigación y publicaciones existentes donde se describen trabajos de investigación relacionados con el tema bajo estudio. Se mencionan a continuación algunos trabajos revisados:

- An Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS), [7]

ISSN 2301-1092 • ISSN (en línea) 2301-1106

- Facilitating Trust in Privacy-Preserving E-Learning Environments [8]
- Risks and remedies in e-learning system [9]
- A security framework for online distance learning and training [10]
- E-Learning and Information Security Management [11]
- On Security Management in E-learning System [12]
- Security Enhancement for E-Learning Portal [13]

En los mismos se pudo verificar que los mismos se enfocan en la protección de los sistemas informáticos, cubriendo con mayor o menor detalle temas como la seguridad en las plataformas de Educación virtual, el acceso a la información y la conectividad.

Sin embardo no se abordan otros aspectos importantes de la gestión de Seguridad como Políticas de Seguridad, Organización, Legislación, Seguridad Física y Ambiental, temas éstos con referencia escasa o nula en los documentos revisados.

Por esta razón es que decidimos encarar el trabajo con un enfoque integrador de estas dos realidades que por un lado tenga una visión global de la gestión de seguridad y por otro esté adaptado al lenguaje y la realidad de las entidades de educación virtual para que pueda ser entendido y aplicado sin la necesidad de apoyo de expertos en seguridad.

3. Definición del Marco de Gestión de Seguridad de la Información para Educación Virtual.- La primera actividad en la definición del marco de gestión consistió en evaluar cuales son las amenazas informáticas que mayor probabilidad tienen de afectar a un sistema de educación virtual, para luego proponer medidas para su tratamiento.

Para ello se tomó como base el "Catálogo de Amenazas" definido en la normativa Magerit versión 3 y luego de revisar en detalle el mismo se seleccionaron las que a nuestro entender son las amenazas que mayor grado de afectación pueden presentar sobre las plataformas de educación virtual.

Para darles un ordenamiento que ayuda a su mejor comprensión se procedió en dividir las amenazas relacionadas con la información asociada al proceso educativo y aquellas que afectan a los activos o bienes necesarios para utilizar dicha información.

Acto seguido se agruparon las primeras según su causal en accidentales y deliberadas y las segundas en base al tipo de activo afectado según sean Instalaciones y servicios de infraestructura básica, Infraestructura Tecnológica o el Personal. El listado de amenazas definido se incluye en el cuadro de la Figura I.

Tipo		Nombre	Descripción
Amenazas a la información	Afectación accidental de información	Errores en el uso del sistema	Equivocaciones de las personas cuando usan los servicios, datos, etc.
		Errores de operación y mantenimiento de los sistemas	Equivocaciones de personas con responsabilidades de instalación, configuración, operación y mantenimiento de las plataformas.
		Errores de monitoreo (logs)	Inadecuado registro de actividades, registros faltantes, incompletos o incorrectos.
		Alteración o destrucción accidental de la	Alteración o pérdida accidental de la información valiosa.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

		información	
		Debilidades en los procesos	Inexistencia o deficiencias en la definición o implementación de procesos de la organización que afectan la información.
	Afectación deliberada de la información	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
		Destrucción intencional de información	Eliminación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
		Divulgación o fuga de información	Revelación intencional de información a un tercero, con ánimo de obtener un beneficio o causar un perjuicio.
		Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
		Abuso de Privilegios	Se produce cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.
		Suplantación de identidad	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
		Repudio	Negación a posteriori de actos realizados en el pasado. Existen varios tipos: - Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. - Repudio de recepción: negación de haber recibido un mensaje o comunicación. - Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.
		Afectación legal por compromiso de información	Divulgación o modificación no autorizada de información, o que se encuentre afectada por alguna legislación vigente, regulación o contratos. (ej. Datos Personales, Propiedad Intelectual)
		Hacking	Ataques donde se vulneran los mecanismos de seguridad de las plataformas informáticas con el fin de lograr acceder y/o modificar información sensible.
Amenazas a los activos	Instalaciones y	Desastres naturales	Eventos que pueden ocurrir sin intervención humana como causa directa o indirecta, incluyendo incendios, inundaciones, rayos, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.

		Desastres industriales	Sucesos que pueden ocurrir de forma accidental o deliberada, derivados de la actividad humana de tipo industrial. Incluye incendios, inundaciones, explosiones, derrumbes, contaminación química, accidentes de tránsito, contaminación mecánica (Vibraciones, polvo en ambiente), contaminación electromagnética (interferencias de radio, campos magnéticos).
		Fallas en el suministro eléctrico	Corte total del suministro eléctrico, bajas de tensión, sobrecargas.
		Fallo de las comunicaciones	Corte, degradación o intermitencias en el enlace de Internet, datos o telefonía.
		Condiciones inadecuadas de temperatura y humedad	Deficiencias en la climatización de los sitios, excediendo los márgenes de trabajo de los equipos, excesivo calor, excesivo frío, exceso de humedad.
		Fallas en el cableado	Fallas en el sistema de distribución del cableado, cortes o daños en los cables.
		Fallas en otros servicios de Infraestructura	Deficiencias de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante.
	Afectación a la Infraestructura Tecnológica	Falla de Equipamiento	Fallos en los equipos (hardware) que impiden su correcto funcionamiento. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
		Falla de Software	Fallos en los programas que impiden su correcto funcionamiento. Agotamiento de recursos. Carencia de recursos de procesamiento de información suficientes que provoca la degradación o caída del sistema cuando la carga de trabajo es desmesurada.
		Degradación de los soportes de almacenamiento de la información	Por defectos de fabricación o como consecuencia del paso del tiempo
		Manipulación de la tecnología (configuración, programas, equipos)	Alteración intencionada del funcionamiento de los programas, del equipamiento, o de su configuración para obtener un beneficio directo o indirecto del uso de los sistemas.
		Vulnerabilidades de los programas (software)	Defectos en el código que posibilitan una acción perniciosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad de operar de un sistema.
		Pérdida o robo de equipamiento	La pérdida de equipos provoca la carencia de un medio para prestar los servicios, o sea indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la

ISSN 2301-1092 • ISSN (en línea) 2301-1106

			pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
		Ataques de Denegación de Servicio	Consumo de recursos de procesamiento más allá de la capacidad operacional de un sistema generado intencionalmente para provoca la caída del mismo.
		Difusión de software malicioso	Infección y propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
Afectación a las personas		Extorsión o amenazas al personal	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
		Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.
		Indisponibilidad del personal	Cualquier tipo de ausencia del personal como huelgas, ausentismo laboral, bajas no justificadas, bloqueo de los accesos, etc.

Figura I.- Cuadro de Amenazas

Este listado es de carácter orientativo y pretende servir como guía para la implementación de un proceso de gestión de riesgos. Sin embargo su aplicabilidad debe ser analizada en cada caso particular ya que siempre existen diferencias entre una organización y otra, pudiendo suceder que deban incluirse nuevas amenazas no contempladas, como así también que algunas de las definidas no sean aplicables.

Una vez definido el conjunto de amenazas a evaluar, se realizó un cruzamiento de las mismas con los controles de ISO 27002, con el objetivo de determinar las salvaguardas que mejor apliquen al caso de estudio.

Luego se procedió a consolidar los controles seleccionados y agruparlos en tres dominios: Protección de la Información desarrollados ampliamente en los documentos de investigaciones revisadas, y Gestión de la Seguridad y Protección de Infraestructura, que como ya mencionamos encontramos abordados en forma escasa en dichos trabajos.

La selección de los controles incluidos en el marco fue el resultado de un proceso de análisis que incluyó revisar cada una de las amenazas seleccionadas y definir que controles pertenecientes al listado de Controles del Anexo I de la norma 27002, aplican mejor para su mitigación. Luego se procedió a resumir, agrupar y consolidar las salvaguardas para luego incluirlas en el marco de referencia propuesto.

Una vez realizada la actividad se revisaron todos los objetivos de control de la norma ISO 27001 Anexo A, para asegurarnos que ninguno de los dominios quedaba sin ser cubierto por el marco definido. Esta relación se puede observar en el cuadro de la Figura II.

CONTROLES PROPUESTOS	OBJETIVOS DE CONTROL ISO 27001	5.-Política de seguridad	6.-Organización de la información de seguridad	7.-Seguridad de los recursos humanos	8.-Gestión de activos	9.-Control de accesos	10.-Cifrado	11.-Seguridad física y ambiental	12.-Seguridad en la Operación	13.-Seguridad en las Comunicaciones	14.-Adquisición de sistemas, desarrollo y mant.	15.-Gestión de Proveedores	16.-Gestión de los incidentes de seguridad	17.-Administración de la continuidad de negocio	18.-Cumplimiento
Control 1.- Políticas de Seguridad		x													
Control 2.- Roles y responsabilidades en Materia de Seguridad			x												
Control 3.- Auditorías de Seguridad									x			x			
Control 4.- Concientización				x											
Control 5.- Gestión de Incidentes													x		
Control 6.- Contingencia y Recuperación														x	
Control 7.- Cumplimiento de leyes y regulaciones				x											x
Control 8.- Terceras partes												x			
Control 9.- Clasificación de Activos la Información					x										
Control 10.- Identificación y autenticación						x									
Control 11.- Privilegios de acceso						x									
Control 12.- Registro y auditoría					x				x						
Control 13.- Cifrado de información							x				x				
Control 14.- Copias de seguridad							x								
Control 15.- Protección de la red de comunicaciones								x		x					
Control 16.- Gestión de cambios y configuraciones									x		x				
Control 17.- Protección contra malware									x						
Control 18.- Gestión de vulnerabilidades									x						
Control 19.- Política de Desarrollo Seguro									x		x				
Control 20.- Protección del equipamiento								x							
Control 21.- Seguridad Física								x							

Figura II.- Relación entre los controles seleccionados y el Objetivo de Control de la Norma ISO 27001.

Adicionalmente y con el objeto de ayudar a las organizaciones en la definición del ámbito de control a aplicar se definió una matriz de cruzamiento entre amenazas y controles para que cada una pueda decidir que controles tienen mayor aplicabilidad en base a la exposición que las mismas tienen a las amenazas, que se muestra en la Figura III.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

AMENAZAS	CONTROLES	1.- Políticas de Seguridad	2.- Roles y responsabilidades en Materia de Seguridad	3.- Auditorías de Seguridad	4.- Concientización	5.- Gestión de Incidentes	6.- Contingencia y Recuperación	7.- Cumplimiento de leyes y regulaciones	8.- Terceras partes	9.- Clasificación de Activos la Información	10.- Identificación y autenticación	11.- Privilegios de acceso	12.- Registro y auditoria	13.- Cifrado de información	14.- Copias de seguridad	15.- Protección de la red de comunicaciones	16.- Gestión de cambios y configuraciones	17.- Protección contra malware	18.- Gestión de vulnerabilidades	19.- Política de Desarrollo Seguro	20.- Protección del equipamiento	21.- Seguridad Física
Errores en el uso del sistema		X	X		X				X			X										
Errores de operación y mantenimiento de los		X	X		X				X		X		X									
Errores de monitoreo		X							X				X		X							
Exposición accidental de información		X	X		X				X		X	X	X	X								
Alteración o destrucción accidental de la		X	X		X				X		X	X	X		X							
Debilidades en los procesos		X	X		X				X													
Modificación deliberada de la información		X	X						X		X	X	X		X							
Destrucción intencional de información		X	X						X		X	X	X		X							
Divulgación o fuga de información		X	X						X		X	X	X	X								
Acceso no autorizado		X	X						X		X	X	X									
Abuso de Privilegios		X	X						X		X	X	X									
Repudio		X	X						X		X	X	X	X								
Afectación legal por compromiso de		X	X					X	X		X	X	X	X								
Hacking		X	X						X		X	X				X			X	X		
Desastres naturales (fuego, inundaciones,		X	X	X		X	X		X	X					X							
Desastres industriales (fuego, inundaciones)		X	X	X		X	X		X	X					X							
Fallas en el suministro eléctrico		X	X	X		X	X		X												X	X
Fallo de las comunicaciones.		X	X	X		X	X		X												X	X
Condiciones inadecuadas de temperatura y		X	X	X		X	X		X												X	X
Fallas en el cableado		X	X	X		X	X		X												X	X
Fallas en otros servicios de Infraestructura		X	X	X		X	X		X												X	X
Falla de Equipamiento		X	X				X		X												X	
Falla de Software		X	X				X		X						X		X					
Agotamiento de recursos		X	X						X								X					
Degradación de los soportes de		X	X						X						X							
Manipulación de la tecnología (configuración,		X	X						X		X	X	X				X					
Vulnerabilidades de los programas (software)		X	X						X										X			
Robo de equipamiento		X	X						X													X
Ataques de Denegación de Servicio		X	X						X		X		X			X		X				
Difusión de software malicioso		X	X		X				X									X				
Extorsión o amenazas al personal		X	X		X				X													
Ingeniería social		X	X		X				X													
Indisponibilidad del personal		X	X				X		X													

Figura III.- Cruzamiento de Amenazas y Controles.

Este cuadro un ejemplo y puede variar dependiendo de diversos factores, como tipo de organización, relación con terceros, tipo de tecnología, procesos implementados, amenazas entre otras. Por lo tanto se recomienda que cada organización pueda realizar su propio análisis de riesgo para detectar que amenazas le aplican y priorizar así las medidas de seguridad a implementarse.

3.1.- Descripción de los Controles.- Se describen a continuación los controles elegidos junto con la referencia a su correlato en la norma ISO 27001.

Dominio 1: Gestión de la Seguridad

Control 1: Políticas de Seguridad

Se debe definir un conjunto de políticas para la seguridad de la información, que estén aprobadas por la gerencia y que se comuniquen a todos los participantes del proceso, incluso a los alumnos.

Se recomienda definir una política de alto nivel (más genérica) relacionada con el sistema de gestión para la seguridad de la información, que pueda estar apoyada por otras políticas de bajo nivel, específicas a aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, dispositivos móviles y teletrabajo, respaldo de información, protección contra malware, etc.

Las políticas se debe revisar al menos anualmente, o cuando haya cambios significativos de procesos o tecnología.

Ref : ISO 27002 Apartado 5. Políticas de Seguridad.

Control 2: Roles y responsabilidades en Materia de Seguridad

Se deben definir y asignar claramente las responsabilidades para la seguridad de la información y segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés.

Se recomienda definir al menos la responsabilidad de los siguientes roles: Responsable de Seguridad, Responsable de Tecnología, Auditor de Seguridad, Usuarios.

Se deben desarrollar contactos con entidades externas como organizaciones educativas, proveedores de tecnología y seguridad informática y organismos públicos, con objeto de mantenerse actualizado acerca de las tendencias de la industria y la evolución de las amenazas y establecer canales de comunicación para el tratamiento de incidentes de seguridad.

Ref : ISO 27002 Apartado 6.1 Organización Interna.

Control 3: Auditorías de Seguridad

Se deben planificar y acordar actividades de auditoría que involucran la verificación de los aspectos de seguridad de los sistemas y plataformas tecnológicos.

Se recomienda realizar auditorías de seguridad independientes periódicamente que revisen la efectividad de los controles implementados. Incluir mínimamente: Gestión de Accesos, Seguridad de Infraestructura y Seguridad Física.

Se debe realizar auditorías sobre servicios prestados por terceras partes que cubran los temas de seguridad más importantes, para garantizar que se cumplen los requisitos definidos en el contrato de servicio.

Ref : ISO 27002 12.7 Consideraciones de las auditorías de los sistemas de información - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

Control 4: Concientización y Recursos Humanos

Todos los usuarios deberían recibir el entrenamiento apropiado en el conocimiento de temas de seguridad que sean relevantes para su función. Se recomienda implementar concientizaciones de seguridad para administradores, docentes, diseñadores e incluso en caso que sea necesario también a los alumnos.

Toda persona que acceda a los sistemas de la organización o utilice información propietaria deberían aceptar los términos y condiciones del trabajo donde se establecerán las obligaciones relacionadas con la seguridad de información. Esto incluye a empleados directos y contratados, proveedores de servicio, docentes, tutores, diseñadores y alumnos.

Ref: ISO 27002 7.1.2 Términos y condiciones de contratación - 7.2.2 Concienciación, educación y capacitación en SI.

Control 5: Gestión de Incidentes

Se debe implementar y comunicar un procedimiento donde se puedan reportar incidentes de seguridad y que los mismos sean clasificados según su criticidad, atendidos apropiadamente y una vez cerrados se registren en un repositorio único.

Adicionalmente se deberían aplicar los procedimientos necesarios para la adquisición y preservación de la información que puede servir de evidencia para futuras investigaciones.

Ref: ISO 27002 16.1 Gestión de incidentes de seguridad de la información y mejoras.

Control 6: Recuperación

Se deben definir planes de recuperación para contingencias asociadas a la falta de disponibilidad de los sistemas y realizar pruebas periódicas de funcionamiento de los mismos.
Ref: ISO 27002 17.1 Continuidad del negocio.

Control 7: Cumplimiento de leyes y regulaciones

Se deben identificar los requisitos contractuales, normativos y legales asociados al proceso educativo para asegurar su cumplimiento.

Se recomienda poner especial atención en los requisitos relacionados con los derechos de propiedad intelectual del software y los contenidos, en la protección de la información personal de interacción y en los requisitos derivados de aspectos relacionados con la calidad de la educación.

Ref : ISO 27002 7.2 - 18.1 Cumplimiento.

Control 8: Terceras partes

Se deben acordar y documentar los requisitos de seguridad de la información requeridos para mitigar los riesgos generados por el acceso de proveedores y terceras personas a los sistemas de la organización.

Esto incluye a los siguientes actores:

- Proveedores asociados con la cadena de suministro de los servicios de tecnología de información y comunicaciones y servicios de computación en la nube en todos sus niveles.
- Proveedores de desarrollo y mantenimiento de software.
- Personal de Soporte de sistemas y plataformas.
- Diseñadores y productores de contenido.

Se deben incluir los requisitos de seguridad en los contratos de servicios para asegurar su cumplimiento.

Ref : ISO 27002 15 Relación con los suministradores

Dominio 2: Protección de la Información

Control 9: Clasificación de Activos la Información

Todos los activos informáticos deben estar claramente identificados, y se debe mantener un inventario con los más importantes. Esto incluye:

- Software (Sistema Operativo, Aplicaciones y Programas).
- Activos físicos:
    - Hardware de computación y comunicaciones
    - Soportes de almacenamiento (discos, cintas, etc.)
    - Centros de cableados.
    - Equipamiento de soporte (generadores, Sistemas de alimentación ininterrumpida (UPS), aire acondicionado).
- Servicios:
    - Servicios informáticos (servicios en la nube, software como servicio (SaaS), Webhosting, servicio técnico, soporte de aplicaciones).
    - Servicios de comunicaciones (Enlaces de datos, Internet, enlaces telefónicos, celulares).
    - Servicios generales (Calefacción, iluminación, energía eléctrica, aire acondicionado).
- Información:
    - Bases de datos, archivos y documentos.
    - Información operacional y de configuración de sistemas.
    - Registros de actividad y evidencia digital.
    - Contenidos educativos.
    - Exámenes y evaluaciones.

El grado de sensibilidad de los activos y de la información que manejan determinará los controles técnicos y administrativos que se debe aplicar a la protección de los mismos.

Ref : ISO 27002 8.2 Clasificación de la información.

Control 10: Identificación y autenticación
Se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de autenticación.

Los sistemas de gestión de contraseñas deberían ser interactivos y se debe exigir a los usuarios la aplicación de buenas prácticas de seguridad para el uso de contraseñas de calidad.

Se deben considerar mecanismos de autenticación robustos cuando el riesgo lo justifique, en especial en procesos donde toda la interacción es virtual, o cuando es necesario certificar ante algún ente externo las acciones realizadas en el sistema.

Es estos casos es importante evitar el repudio y la suplantación de identidad, en pos de garantizar que el alumno y no un tercero en su nombre es quién ha realizado las actividades educativas, incluyendo la evaluación.

Además se debe prestar especial atención a los mecanismos de autogestión de contraseñas ante olvidos, para lograr que los mismos sean lo suficientemente seguros.

Ref : ISO 27002 9.4 Control de acceso a sistemas y aplicaciones.

Control 11: Privilegios de acceso

Se deber implantar un proceso para la asignación y revocación de derechos de acceso a los usuarios sobre sistemas y servicios, que cumpla con las siguientes premisas:

- Asignar privilegios de acceso de acuerdo a los distintos roles, esto es: alumnos, docentes, tutores, administradores, generadores de contenido, etc.
- La asignación y el uso de privilegios especiales o de administración debe ser restringido y controlado.
- Revisar con regularidad los privilegios de acceso de los usuarios para evaluar si siguen siendo necesarios.
- Retirar los derechos de acceso a un usuario cuando finalice el vínculo con la organización.

Ref : ISO 27002 9.2 Gestión de acceso de usuario, 9.4 Control de acceso a sistemas y aplicaciones.

Control 12: Registro y auditoría

Se deberían producir, mantener y revisar periódicamente registros relacionados con actividad de los usuarios, excepciones, fallas y eventos de seguridad de la información.

Se deben incluir tanto registros de tareas de operación y mantenimiento de los sistemas como así también los eventos relacionados con las actividades educativas.

Los registros deben protegerse contra posibles alteraciones y accesos no autorizados.

Se debe verificar el sincronismo de los relojes en los sistemas y plataformas en relación a una fuente de sincronización única de referencia.

Ref : ISO 27002 12.4 Registro de actividad y supervisión - 8.2 Clasificación de la información.

Control 13: Cifrado de información

Se debe desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información. La misma debe incluir aspectos relacionados al uso y protección de las claves criptográficas a través de todo su ciclo de vida.

La criptografía puede dar apoyo entre otros temas, en los siguientes aspectos:

- Cifrado de comunicaciones web (https, VPNs).
- Métodos de autenticación robusta y validación de documentos (PKI, Certificados, Firma electrónica).
- Cifrado de información confidencial (contenidos, evaluaciones).

Ref : ISO 27002 10.1 Controles criptográficos.- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes

Control 14: Copias de seguridad

Se debe implantar procedimientos de respaldo y recuperación de información que satisfagan tanto los requerimientos contractuales como los requisitos internos de la organización.

Se deben realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema para asegurar su integridad.

Se deberían verificar todos los medios de almacenamiento antes de su eliminación o reutilización para garantizar que la información sensible se hayan extraído o se hayan sobrescrito de manera segura.

Ref : ISO 27002 12.3 Copias de seguridad - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.

Dominio 3: Protección de la Infraestructura Tecnológica

Control 15: Protección de la red de comunicaciones

Se deben adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.

Se debería incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, y los requisitos de administración de los servicios de red, independientemente de si estos se entregan de manera interna o están externalizados.

Se recomienda implementar firewalls de red y aplicación (en especial para protocolo web) para proteger la plataforma de educación virtual y separar las redes donde están publicados a Internet dichos servicios del resto de la infraestructura de uso interno.

Adicionalmente se debería implementar herramientas de seguridad activas de monitoreo de red como IDS/IPS (detección y prevención de intrusiones).

Ref : ISO 27002 13.1 Gestión de la seguridad en las redes.

Control 16: Gestión de cambios y configuraciones
Se deberían implementar procedimientos para controlar la instalación de cambios en los sistemas productivos con el objeto de garantizar que las condiciones de operación segura implementadas se mantengan luego de aplicar los cambios.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

Se recomienda aplicar los cambios en sistemas de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de respaldo y puntos de restauración que permitan retornar los sistemas al estado de estabilidad inicial.

Adicionalmente deberían incluirse principios de seguridad en ingeniería de sistemas para cualquier nueva implementación en un sistema de información.

Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

Ref : ISO 27002 12.1 Responsabilidades y procedimientos de operación 12.5 Control del software en explotación.14.2.2 Procedimientos de control de cambios en los sistemas.- 14.2.5 Uso de principios de ingeniería en protección de sistemas.

Control 17: Protección contra malware

Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

Ref : ISO 27002 12.2 Protección contra código malicioso.

Control 18: Gestión de vulnerabilidades

Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas para evaluar el grado de exposición y tomar las medidas necesarias para mitigar los riesgos asociados.

Se debe probar y aplicar los parches críticos o en su defecto tomar otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas activamente.

Ref : ISO 27002 12.6 Gestión de la vulnerabilidad técnica.

Control 19: Política de Desarrollo Seguro

Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

Se deberían establecer programas de prueba y criterios de aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones que incluyan aspectos de seguridad. Adicionalmente deberían realizarse comprobaciones de seguridad antes de la puesta en producción de un nuevo servicio o plataforma.

Se deberán incluir buenas prácticas de programación segura orientadas a minimizar vulnerabilidades en el software.

Ref : ISO 27002 12.1.4 Separación de entornos de desarrollo, prueba y producción. - 14.2.1 Política de desarrollo seguro de software.

Control 20: Protección del equipamiento

Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado. En este sentido deben incluirse los siguientes aspectos:

- Protección contra cortes de energía, sobrecargas y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.
- Protección del cableado eléctrico y de telecomunicaciones contra la intercepción, interferencia o posibles daños.
- Mantenimiento preventivo del equipamiento con el objeto de garantizar su disponibilidad e integridad.
- Control de ingreso y salida de equipamiento fuera de las instalaciones.

Ref : ISO 27002 11.2 Seguridad de los Equipos

Control 21: Seguridad Física

Los medios de procesamiento de información deben ubicarse en áreas seguras, dentro de los perímetros de seguridad definidos, con barreras de seguridad y controles de entrada que aseguren que estén físicamente protegidos del acceso no autorizado, daño e interferencia. Se deberán incluir los siguientes controles:

- Perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible.
- Protección de áreas seguras mediante controles de acceso físico.
- Protecciones físicas contra desastres naturales, ataques maliciosos o accidentes.
- Separar las áreas de entrega y carga/descarga y otras con acceso público de las instalaciones de procesamiento de información.

Ref : ISO 27002 11.1 Áreas Seguras

A continuación se adjunta un gráfico que muestra el marco definido con sus controles agrupados por procesos y más abajo se detallan los controles sugeridos divididos en 3 Dominios según la aplicabilidad de los mismos: Gestión de la Seguridad, Protección de la Infraestructura, y Protección de la Información.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

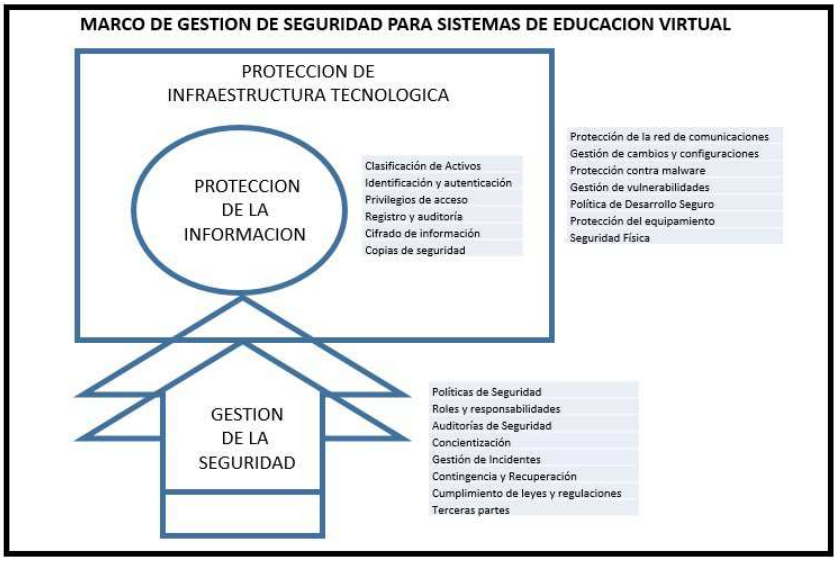

Figura IV.- Marco de gestión de seguridad para sistemas de educación virtual

4. Propuesta para aplicación del Marco de Gestión en una Organización.- Como ya vimos anteriormente, para mitigar en forma eficiente las amenazas se debe implementar un proceso de Gestión de riesgos que permite identificar, priorizar y mitigar los riesgos de afectación de la seguridad de la información, teniendo como principal objetivo realizar un tratamiento de los riesgos a los cuales está expuesta una organización reduciendo su nivel hasta valores tolerables.
El análisis de riesgos mínimamente considera los siguientes elementos:

- **Activos**: que son los elementos propios o ligados a los sistemas de información que dan soporte al proceso educativo.
- **Amenazas**: que son eventos que pueden afectar a nuestros activos de información.
- **Salvaguardas** o Controles: que son medidas de protección a implementar para evitar que las amenazas tengan impacto sobre nuestra información.

Teniendo en cuenta esta premisa, para utilizar el Marco de Gestión propuesto se recomienda seguir la siguiente secuencia.

a) Definir el inventario de activos bajo estudio:

Tomando como referencia el Control 9 (Clasificación de Información) se deberán identificar todos los activos de información asociados al proceso de educación virtual, principalmente la plataforma de educación, la información contenida en la misma, la infraestructura física y tecnológica necesaria para su funcionamiento y los procesos técnicos y administrativos asociados a su correcta operación.

b) Seleccionar el listado de amenazas que consideramos aplicable.

Se deberá revisar el listado de amenazas aplicable a cada activo descripto en el apartado anterior, descartando las improbables y agregando algunas más no incluidas en el listado si fuera necesario. Entre los aspectos que pueden variar la decisión de la elección del conjunto de eventos negativos a incluir en el estudio se encuentran:

- Grado de exposición de la plataforma de educación virtual (principalmente si es accesible desde Internet o sólo puede utilizarse en la red interna de la organización.
- Necesidad de garantizar la identidad de los participantes, más allá del uso de una contraseña.
- Confidencialidad de los contenidos educativos, o de la información relacionada con el proceso educativo, como notas, interacciones, etc.
- Nivel de disponibilidad requerida para la plataforma.
- Requerimientos legales o regulatorios del proceso o de la información contenida (propiedad intelectual, protección de datos personales, calidad del proceso educativo, etc.)

c)Seleccionar las salvaguardas a implementar para mitigar las amenazas.

Ahora tomamos el listado de controles del marco de gestión y seleccionamos para su implementación los que mitiguen las amenazas de mayor riesgo.

d) Una vez seleccionados los controles los mismos servirán como base para la confección de un plan de tratamiento de riesgos, priorizando las acciones mitigantes en base a las necesidades de la organización.

5. Propuestas de implementación de tecnologías de seguridad para Sistemas de Educación virtual.- Uno de los objetivos del trabajo consistió en investigar las tecnologías relacionadas con la seguridad informática que pueden ser utilizadas para mitigar los riesgos detectados.

Como parte de este lineamiento, se trabajó en dos aspectos principales que pueden afectar a las plataformas de educación virtual. Uno de ellos relacionado con los riesgos generados por la accesibilidad desde Internet y el otro con la necesidad de garantizar autenticación y no repudio de las actividades educativas realizadas.

En base a estas premisas se seleccionaron dos tipos de soluciones tecnológicas que pueden ser de gran valor para colaborar con la protección de las plataformas en estos dos temas.

Una de ellas es la tecnología de protección de red denominada UTM (Unified Threat Management en Inglés o Gestión de Amenazas Unificadas) y la segunda hace referencia a la Implementación de un Sistema de Infraestructura de Clave Pública (PKI en Inglés) para la gestión de certificados digitales. A continuación se detallan cada una de ellas:

5.1 Aplicación de tecnologías de UTM para educación virtual.- Como parte del trabajo se propuso implementar como herramienta de seguridad, para brindar protección y cumplir con ciertos controles definidos en esta investigación, el uso de un equipo Firewall del tipo (UTM)

Dicha herramienta tiene el objetivo ayudar mitigar los riesgos que afecten a la plataforma, su interacción y la información que se manipula a través de esta. Como parte de las tecnologías que pueden ser usadas para brindar seguridad al proceso educativo en tres aspectos principales:

- Control de Antivirus a nivel de firewall.
- Control de Spam y software malicioso en correo electrónico.
- Detección y prevención de intrusiones (IPS/IDS).

Para llevar adelante las pruebas técnicas se utilizó un equipo firewall comercial que posee la institución, un perfil de seguridad de antivirus con las configuraciones necesarias para el bloqueo de cualquier virus ante su detección. Sin embargo podría utilizar herramientas de software libre por separado integrando la información en un equipo que administre los eventos y correlacione la información de seguridad.

ISSN 2301-1092 • ISSN (en línea) 2301-1106

Luego se definieron variables como la acción de bloqueo ante detecciones de virus en el tráfico de red de cada servicio de la plataforma, como así también el bloqueo ante la detección de conexiones a servidores de botnets[8].

Adicionalmente se estableció un el perfil para que pueda controlar los correos no deseados, los correos basura y los que contengan malware que son enviados a las casillas de la institución.

Por último se configuraron dos perfiles de protección de intrusiones, uno que proteja las posibles explotaciones de vulnerabilidades que pudieran afectar al servidor de publicación que tiene la plataforma y el restante para detectar y bloquear intentos de intrusión a la base de datos de la plataforma, ya que esta base es la que contiene la información y las tablas de usuarios y controles de acceso a la misma.

5.2 Aplicación de tecnología de PKI para educación virtual.- La propuesta se basa en el diseño de una infraestructura de clave pública para aquellas instituciones que quieran contar con una infraestructura de clave pública de alcance institucional, escalable, que permita la generación y administración de certificados digitales, en forma segura y confiable.

El diseño está basado en un entorno de alta disponibilidad de modo tal que cubre las necesidades para el proceso de gestión del ciclo de vida de los certificados. Está constituido por tres zonas de seguridad interconectadas mediante Firewalls y Switches, todos en modo de alta disponibilidad para evitar que existan puntos únicos de fallo. En la Figura V se detalla el esquema conceptual de cada zona.

Figura V.- Esquema Conceptual – Aplicación PKI para Educación virtual

Diseño Lógico

Esta sección provee una visión de alto nivel del diseño lógico de la infraestructura de claves públicas (PKI) y cubre las decisiones de diseño de arquitectura de la solución en cuanto a las Autoridades de Certificación (CAs) y los certificados a utilizar.

El diseño propuesto utiliza una jerarquía de CAs de dos niveles que contienen en su nivel más alto a la CA Raíz interna propia y en el siguiente nivel a las CA emisora de certificados de firma digital. En este caso hemos optado por una PKI auto-administrada que utiliza la CA Raíz de propia interna como entidad raíz de confianza La figura VI ilustra la jerarquía mencionada.

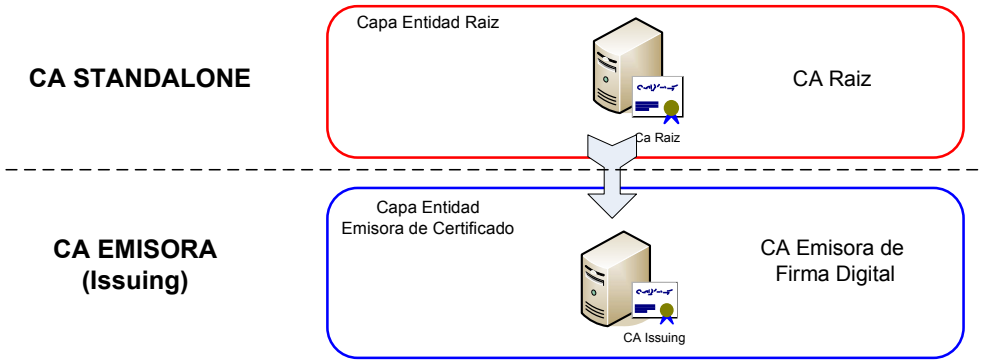

Figura VI.- Jerarquía de CAs

El equipo CA Raíz se usa solo para certificación y revocación de certificados de CA emisora del segundo nivel que será subordinada de la CA Raíz y se utilizara para generación de certificados de firma. Se han planeado inicialmente instalar un servidor de certificados el cual emitirá los certificados de firma digital para los alumnos y docentes.

Las CA emisora se encontrará en línea y utilizara el módulo HSM (Hardware Security Modules) para el resguardo de su clave privada. Los procesos de enrolamiento (Enrollment), renovación (Renewal) y revocación (Revocation), deberán ser llevados a cabo mediante aplicaciones Web.

Seguridad de las Cas

La solución PKI requiere varias capas de seguridad trabajando codo a codo tales como controles de seguridad física, controles de seguridad lógicos y la implementación de procesos de mantenimiento de las CAs. Estos controles de seguridad deberán ser proporcionales a la confianza depositada en la entidad emisora.

En la Figura VI se muestran los controles de seguridad para cada tipo de CA de la solución PKI.

Figura VI.- Controles de Seguridad

ISSN 2301-1092 • ISSN (en línea) 2301-1106

6. Conclusiones y resultados.- Como resultado del trabajo se logró establecer un marco de gestión de la seguridad de la información aplicable a las plataformas de educación virtual, basado en estándares internacionales y con foco específico en la actividad educativa.

Uno de los principales aportes que este trabajo pretende brindar es el de acercar los estándares de seguridad definidos por el mercado a la realidad de una organización dedicada a la educación virtual, colaborando así con la aplicación de las buenas prácticas de seguridad en dichos entornos.

El Marco de Gestión definido es de naturaleza abierta y sus definiciones no buscan ser para nada absolutas, sino que por el contrario pretende ser un punto de partida para enmarcar la actividad de gestión de riesgo y entendemos que el mismo deberá enriquecerse con su aplicación efectiva a través de nuevas definiciones.

Además de ello se lograron identificar y definir los aspectos necesarios para la puesta en práctica de dos tecnologías de seguridad que apuntan a proteger las plataformas educativas, como son los sistemas Unificados de Gestión de Amenazas (UTM), orientados a la protección de las plataformas de cara a su interacción con Internet, y el uso de Infraestructuras de Clave Pública (PKI) para mejorar la autenticación y el no repudio de actividades a través del uso de certificados digitales.

7. Bibliografía.

[1] Organización Internacional de Normalización (ISO). Tecnología de la Información, Técnicas de seguridad, Requisitos para los Sistemas de Gestión de Seguridad de la Información - ISO/IEC 27001:2005

[2] Organización Internacional de Normalización (ISO). Tecnología de la Información, Técnicas de seguridad, Código para la práctica de la gestión de la seguridad de la información ISO/IEC 27002:2005.
http://www.iso27000.es/, 2015, El portal de ISO 27002 en Español

[3] ISACA Information System Audit and Control Association ISACA, A Business Framework for the Governance and Management of Enterprise IT - Preview Version, 2012, http://www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf

[4] American National Institute of Standards and Technology NIST, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[5] Ministerio de Hacienda y Administraciones Públicas de España, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT versión 3.0, 2012

[6] Organización Internacional de Normalización (ISO). Gestión de Riesgos - Principios y Guías - ISO 31000:2009

[7] S Assefa, V Solms , An Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS), 2006, Academy for Information Technology, University of Johannesburg

[8] Mohd Anwar and Jim Greer, Facilitating Trust in Privacy-Preserving E-Learning Environments, 2012, IEEE Transactions on Learning Technologies, VOL. 5, NO. 1

[9] Nikhilesh Barik and Dr. Sunil Karforma, Risks and remedies in e-learning system, 2012, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1

[10] S.M. Furnell, P.D. Onions, U. Bleimann, U. Gojny, M. Knahl ,H.F. Röder and P.W. Sanders, A security framework for online distance learning and training, 1998, Internet Research: Electronic Networking Applications and Policy Volume 8 · Number 3

[11] Najwa Hayaati Mohd Alwi, Ip-Shing Fan, E-Learning and Information Security Management,2010, International Journal of Digital Society (IJDS), Volume 1, Issue 2

[12] Nikhilesh Barik, Argha Barik, Dr. Sunil Karforma, On Security Management in E-learning System, 2012 , Research Scholar ,Burdwan University Dept. Of Computer Science ,Burdwan ,India

[13] A. Jalal and Mian Ahmad Zeb, Security Enhancement for E-Learning Portal, 2008, IJCSNS International Journal of Computer Science and Network Security