**ANÁLISIS DE RIESGOS A SISTEMAS WEB DE INSTITUCIONES DE EDUCACIÓN SUPERIOR**

**HIGHER EDUCATION INSTITUTIONS WEB SYSTEM RISK ANALYSIS**

**M. en I. Jocelyn Guadalupe Arenas Hernández**

jarenash1300@alumno.ipn.mx,

ESIME Culhuacán, IPN, México

**Ing. Mayra Ugalde Eduardo**

mugaldee1300@alumno.ipn.mx

ESIME Culhuacán, IPN, México

**M. en I. Lidia prudente Tixteco**

lprudente@ipn.mx

ESIME Culhuacán, IPN, México

**Resumen**

En los últimos años ha habido un gran incremento en el uso de las Tecnologías de la Información y las Comunicaciones (TIC) en las instituciones educativas, las cuales se utilizan en sus sistemas web para el almacenamiento, procesamiento, recuperación y distribución de información.

Las Instituciones de Educación Superior (IES) almacenan un gran volumen de datos provenientes de los procesos ejecutados, entre los que se encuentran: datos personales de estudiantes, docentes y administrativos, datos financieros, historial académico y otros, que actualmente son procesados por los sistemas de información. Si bien los sistemas web presentan ventajas como optimización y automatización de procesos, reducción de costos operativos, disponibilidad e integridad de la información almacenada, interacción con otros sistemas y escalabilidad, presentan también vulnerabilidades que los convierten en un objetivo estratégico para que los ciberdelincuentes planifiquen un ataque a la Institución.

Este trabajo de investigación presenta un análisis de riesgos utilizando la metodología RAQUM para evaluar los riesgos de un sistema web en una Institución de Educación Superior, identificando las principales amenazas y vulnerabilidades de los activos involucrados.

**Palabras clave: sistemas web, análisis de riesgos, vulnerabilidades, amenazas, ciberseguridad, controles de seguridad**

**Summary**

There has been a great increase in the use of Information and Communication Technologies (ICT) in educational institutions, which are used in their web systems for the storage, processing, retrieval, and distribution of information.

Higher Education Institutions (HEIs) store a large volume of data from the processes executed, among which are: personal data of students, teachers and administrative staff, financial data, academic history and others, which are currently processed by information systems. Although web systems have advantages such as optimization and automation of processes, reduction of operating costs, availability and integrity of stored information, interaction with other systems, and scalability, they have vulnerabilities that make them a strategic target for cybercriminals to plan an attack on the institution.

This paper presents a risk analysis using the RAQUM methodology to evaluate the risks of a web system in a Higher Education Institution, identifying the main threats and vulnerabilities of the assets involved.

Keywords: web systems, risk analysis, vulnerabilities, threats, cybersecurity, security controls

**Introducción.**

Un sistema web es un conjunto de aplicaciones dinámicas y complejas que se ejecutan por medio de un servidor web y los usuarios acceden a este mediante un navegador web sin necesidad de tener una aplicación en el escritorio. Las aplicaciones web son diseñadas para una gran variedad de usos y pueden ser utilizadas por cualquier persona, organización e institución. Existen diferentes tipos de sistemas web como lo son: sistema de gestión de personal, sistema de control académico, sistema administrativo, entre otros. En la Figura 1 se muestra un diagrama con los elementos que componen el sistema Web, los cuales son: el FrontEnd, BackEnd y la base de datos.



Figura . Diagrama de elementos de un sistema web. Elaboración propia.

En el caso de los procesos escolares, la normatividad establece los procesos de admisión, de inscripción, la permanencia del estudiante, el egreso y la titulación, definidos a través de procesos documentados basado en las normas internas o con base en las normas ISO/IEC y utilizando a las tecnologías de la información para que vía un sistema web se registren los aspirantes y se inscriban los alumnos. Además de incorporar estándares y buenas prácticas de seguridad, para proteger la información bajo el resguardo de la institución, evitando caer en sanciones por falta de protección de los datos personales de los usuarios (ANUIES, 2022).

Una de las principales razones por las cuales los sistemas web son vulnerables es debido a que los desarrolladores cometen errores de codificación y/o seguridad que permiten a personas no autorizadas acceder a datos sensibles y a su vez conseguir derechos de acceso administrativo a la propia aplicación web o incluso al servidor. Las vulnerabilidades más frecuentes en los sistemas web son: configuraciones incorrectas de seguridad, cross-site scripting (XSS), algoritmos de cifrado débiles y falsificación de solicitudes del lado del servidor (El financiero, 2023).

De acuerdo con el Global Threat Analysis Report de Radware 2022, los ataques a aplicaciones web crecieron significativamente, con la mayoría de los ataques dirigidos a aplicaciones y servicios que utilizan HTTPS y HTTP (Radware, 2023).

Los ataques DDoS experimentaron un crecimiento del 150% en comparación con el año 2021, mientras que los ataques a aplicaciones web y API aumentaron un 128%. Los ataques de inyección de código y SQL también incrementaron, representando más del 25% de los ataques a aplicaciones web. Estos aumentos significativos se debieron en gran medida a la creciente dependencia de las organizaciones en tecnologías digitales y la exposición a nuevas vulnerabilidades. Las industrias más atacadas en el 2022 y su porcentaje se encuentran representadas en la gráfica de la Figura 2 (Radware, 2023).



Figura . Industrias más atacadas en el 2022. (Radware, 2022)

(Prudente Tixteco, L., 2017), exponen que no solo las grandes organizaciones se encuentran expuestas a ataques informáticos, sino que también las instituciones de educación, principalmente las universidades, institutos y centros de investigación son un blanco transcendental para los ciberdelincuentes y como consecuencia corren un mayor riesgo, debido al tipo de información que gestionan como los son: las investigaciones y desarrollos científicos y tecnológicos, así como los datos personales de los estudiantes y personas involucradas en la institución.

(Mairaj Inamdar, 202), en este artículo se evalúan varios mecanismos de detección de ataques a sistemas web y su resistencia frente a diversas técnicas de ataque con el objetivo de medir la defensa disponible contra estos e identificar las brechas para construir soluciones eficaces para las diferentes técnicas de defensa en aplicaciones web.

Por lo anterior, el realizar un análisis de riesgos permite la evaluación de los riesgos de los activos de información para determinar el estado de seguridad en el que se encuentran y ayuda a definir un plan de implementación de controles de seguridad para prevenir los riesgos de los sistemas web y así evitar la materialización de estos en un impacto perjudicial e irreversible a las instituciones de educación superior que los emplean.

**Desarrollo.**

A continuación se describen brevemente algunas definiciones importantes para el entendimiento de los componentes del análisis de riesgos.

* *Activo de Información*
	+ Recurso que aporta valor a la institución.
* *Vulnerabilidad*
	+ Debilidad, falta o carencia de seguridad de la información.
* *Amenaza*
	+ Ente con la capacidad de explotar una vulnerabilidad.
* *Riesgo*
	+ Probabilidad de ocurrencia de la amenaza.
* *Control*
	+ Medidad y mecanismos implementados para reducir el riesgo.
* *Impacto*
	+ Materializión del riesgo.

La interacción de los elementos que componen el análisis de riesgos se presenta en la Figura 3, donde cada uno de estos tiene un papel fundamental para proteger y salvaguardar la información de una organización e institución de las amenazas que las asechan día con día.



Figura 3. Interacción de elementos que componen el análisis de riesgos. Elaboración propia.

***Análisis De Riesgos***

El análisis de riesgos tiene como propósito la identificación de los riesgos asociados a los activos de información del proceso crítico de una organización o institución, con base en el cálculo de la probabilidad de que una amenaza explote una vulnerabilidad y cuyo impacto afecte directamente al proceso crítico. De esta manera es posible determinar e implementar los controles pertinentes para llevar a cabo un adecuado tratamiento del riesgo, ya sea aceptándolo, mitigándolo o transfiriéndolo, de acuerdo con la decisión que sea tomada por los directivos responsables.

Un análisis de riesgos se puede desarrollar de forma cualitativa, cuantitativa o mixta dependiendo de la información que se disponga de la institución u organización y de la metodología a emplear.

Para este caso se realizó un análisis de riesgos a un sistema web de una institución de educación superior, donde se empleó la metodología Risk Assessment Qualitative Methodology (RAQUM), la cual es una metodología mixta para la evaluación del riesgo propuesta por el Maestro en Seguridad de la Información Darío Medina Ramírez.

RAQUM se encuentra compuesta por distintas etapas, las cuales se detallan en la Figura 4. Todo el proceso de análisis de riesgos desde la primera hasta la última fase se debe de documentar y comunicar con las áreas y responsables correspondientes.



Figura 4. Etapas de la metodología RAQUM. Elaboración propia.

El Análsis de Riesgos se inició definiendo el alcance, objetivo, limitantes y metas del análisis de riesgos, posterior a esto se llevó a cabo la identificación de activos y sus responsables el sistema web como lo indica la metodología antes mencionada, obteniendo los siguientes activos de información considerados como críticos:

1. Servidor web
2. Página web
3. Servidor de Base de Datos
4. Base de Datos

Después, se continuó con el reconocimiento de las amenazas y vulnerabilidades de cada uno de da uno de los activos de información identificados, obteniendo un listado de estas, como se muestra en las Tablas 1 y 2.

Tabla 1. Vulnerabilidades Identificadas. Elaboración propia.

| **Activo** | **Vulnerabilidades** |
| --- | --- |
| 1. ***Servidor web***
 | * Uso de contraseñas débiles para establecer conexiones remotas
* Falta de bitácoras de registro de eventos
* Falta de bitácoras de registro de eventos
* Falta de controles de protección contra el código malicioso
* Falta de documentación de la política de acceso
* Falta de documentación del procedimiento de control de instalación de software y sistemas operativos
 |
| 1. ***Página web***
 | * Ausencia de procesos documentados para revisar el cumplimiento de requerimientos legales.
* Falta de documentación de un plan de recuperación
* Falta de procedimientos de gestión de cambios
 |
| 1. ***Servidor de base de datos***
 | * Falta de procedimientos de aceptación donde se establezcan criterios de operación y funcionalidad
* Falta de proceso de administración de asignación de claves a usuarios
* Uso de contraseñas débiles para establecer conexiones remotas
* Falta de bitácoras de registro de eventos
 |
| 1. ***Base de datos***
 | * Falta de implementación de mecanismos de cifrado de información
* Falta de documentación de los procedimientos de control de acceso y uso de contraseñas
* Falta de documentación de los procedimientos de respaldo de la información
* Falta de procedimientos para la gestión de cambios
* Falta de procedimientos para dar de alta y de baja a usuarios con acceso
* Falta de bitácoras de registro de eventos
* Falta del procedimiento documentado de revisión de cumplimiento de requerimientos legales
* Falta de documentación del plan de recuperación
 |

Tabla . Amenazas identificadas. Elaboración propia.

| **Activo** | **Amenazas** |
| --- | --- |
| 1. ***Servidor web***
 | * Ataques de contraseñas
* Implantación de código malicioso
* Acceso no autorizado
* Deterioro del servidor
* Fallas en la operación y funcionalidad del servidor web
* Incidentes
* Robo de información
* Respaldos no disponibles
 |
| 1. ***Página web***
 | * Fallas en la operación y funcionalidad de la página web
* Fallas en la operación y funcionalidad de la página web
* Pérdida de datos relacionados con el proceso
* Pérdida de información
* Alteración de la información
* Pérdida de confianza
* Errores del personal
 |
| 1. ***Servidor de base de datos***
 | * Acceso no autorizado
* Falsificación de sistemas operativos
* Elevación de privilegios
* Pérdida de datos relacionado con el proceso
* Deterioro del equipo
* Incidentes
* Indisponibilidad
 |
| 1. ***Base de datos***
 | * Clasificación errónea de la información
* Respaldos no disponibles
* Errores del personal
* Errores en el proceso
* Acceso no autorizado
* Alteración de la información
* Errores en el manejo de la información
 |

Después se realizó la evaluación de los riesgos con base en las directrices que estipula la metodología, utilizando una matriz de riesgos. Para determinar el riesgo se calcula:

$$Riesgo= \left(Probabilidad\*Impacto\right)+\left(Cal.Vulnerabilidad\*Cal. Amenaza\*0.01 \right)$$

En la Tabla 3 se describen los valores de cada uno de los cuadrantes de la matriz de riesgos que van del 1 al 5, cada uno de estos representados por el color correspondiente, siendo el valor 1 y 2 de color verde (bajo), 3 color amarillo (medio), 4 y 5 de color rojo (alto), así como la descripción de estos.

Tabla . Descripción de los cuadrantes de la matriz de riesgos. Elaboración propia.

| **Cuadrante** | **Descripción** |
| --- | --- |
| ***5*** | Requieren respuestas inmediatas basadas en estrategias y acciones que proporcionen valor, mejoras y resultados rápidos. |
| ***4*** | Requieren acciones planteadas y asociadas a una estrategia de corto plazo. |
| ***3*** | Sugieren acciones planeadas de mediano plazo y actividades de monitoreo continua. |
| ***2*** | Sugieren acciones de largo plazo y monitoreo periódico. |
| ***1*** |

Se obtuvo como resultado el nivel de riesgo de cada uno de los activos de información como se muestra en la matriz de riesgos representada en la Figura 5, donde el activo con un mayor nivel de riesgos es la Base de Datos, seguida del Servidor Web y el Servidor de Base de Datos, con un nivel de riesgo medio se encuentra la Página Web.



Figura 5. Matriz de riesgos

***Controles de Seguridad***

Posterior a esto, se realizó un SoA (State of Applicability) con el cual se logró identificar los controles aplicables de la norma ISO/IEC 27001:2013 (ISO, 2017) y se obtuvo un listado de controles para brindar un adecuado tratamiento a los riesgos identificados en cada uno de los activos. A continuación se presentan los controles que son aplicables a la Base de Datos resultante con mayor riesgo después de la evaluación de riesgo.

Tabla 4. Controles seleccionados - base de datos. Elaboración propia.

| **ID Control** | **Nombre del control** |
| --- | --- |
| ***A.8.1.3*** | Uso aceptable de los activos |
| ***A.8.2.1*** | Clasificación de la información |
| ***A.8.2.2*** | Etiquetado de la información |
| ***A.8.2.3*** | Manipulación de la información |
| ***A.9.1.1*** | Política de control de acceso |
| ***A.9.2.1*** | Registro y baja de usuario |
| ***A.9.2.2*** | Asignación de acceso de usuario |
| ***A.9.2.3*** | Gestión de privilegios de acceso |
| ***A.9.2.5*** | Revisión de los derechos de acceso de usuario |
| ***A.9.2.6*** | Eliminación o reasignación de los derechos de acceso de usuario |
| ***A.9.4.1*** | Restricción del acceso a la información |
| ***A.9.4.2*** | Procedimientos seguros de inicio de sesión |
| ***A.9.4.3*** | Sistema de gestión de contraseñas |
| ***A.10.1.1*** | Política de uso de controles criptográficos |
| ***A.10.1.2*** | Gestión de claves |
| ***A.11.2.4*** | Mantenimiento del equipo |
| ***A.12.1.1*** | Documentación de procedimientos operacionales |
| ***A.12.1.2*** | Gestión de cambios |
| ***A.12.3.1*** | Copias de seguridad de la información |
| ***A.12.4.1*** | Registro de eventos |
| ***A.12.4.3*** | Registros de administrador y operador |
| ***A.14.2.1*** | Política de desarrollo seguro |
| ***A.14.2.8*** | Pruebas funcionales de seguridad de sistemas |
| ***A.14.2.9*** | Pruebas de aceptación de sistemas |
| ***A.17.1.1*** | Planificación de la continuidad de la seguridad de la información |
| ***A.17.1.2*** | Implementación de la continuidad de la seguridad de la información |
| ***A.18.1.1*** | Identificación de la legislación aplicable y de los requisitos contractuales |
| ***A.18.1.2*** | Derechos de propiedad intelectual |
| ***A.18.1.4*** | Protección y privacidad de la información de carácter personal |
| ***A.18.2.2*** | Cumplimiento de las políticas y normas de seguridad |

Del listado de controles resultante, se identificó que de los 114 controles del Anexo A de la norma ISO/IEC 27001:2013 solamente 78 controles son aplicables a los cuatro activos identificados, en la Tabla 6 se muestra la relación de los controles aplicables por dominio.

Tabla 6. Controles por dominio. Elaboración propia.

|  |  |  |
| --- | --- | --- |
| **Dominio** | **Nombre de dominio** | **Controles utilizados** |
| ***A.8*** | Gestión de activos | 7 |
| ***A.9*** | Controles de acceso | 25 |
| ***A.10*** | Criptografía | 4 |
| ***A.11*** | Seguridad física y ambiental | 5 |
| ***A.12*** | Seguridad de las operaciones | 20 |
| ***A.14*** | Adquisición, desarrollo y mantenimiento de sistemas | 6 |
| ***A.17*** | Aspectos de seguridad de la información en la gestión de la continuidad del negocio | 4 |
| ***A.18*** | Cumplimiento | 7 |

**Conclusiones.**

Con base en el análisis de riesgos aplicado, se tiene que los activos implicados un sistema de información de una institución de educación superior presentan niveles de riesgo altos y medios, por lo cual los directivos responsables del sistema web deben de priorizar la implementación del tratamiento de riesgos acordado para cumplir con los principios de la seguridad de la información académica de los estudiantes, de investigaciones y empleados aplicables.

La implementación de las medidas y procedimientos de seguridad de la información identificados ayudarán a mitigar los riesgos y proteger los activos de información en el sistema web de las amenazas a los que se encuentran expuestos, generando la estrategia más adecuada para salvaguardar la información y cumplimientos de normativas aplicables, como por ejemplo, la protección de datos personales.

Entre las actividades contempladas para darle continuidad al trabajo desarrollado se encuentran: implementar el tratamiento de riesgos en su totalidad a los riesgos identificados y priorizar la declaración de aplicabilidad de los controles de seguridad de la información, entre otros.

**Referencias.**

1. Asociación Nacional de Universidades e Instituciones de Educación Superior. (2022). “Estado acutal de las Tecnologías de la Información y Comunicación en las Instituciones de Educación Superior en México-Estudio 2022”, Ciudad de México.
2. El financiero. (2023). “7 de las vulnerabilidades en aplicaciones web más comunes”. Recuperado de: https://www.elfinanciero.com.mx/mundo-empresa/2023/04/17/7-de-las-vulnerabilidades-en-aplicaciones-web-mas-comunes/.
3. Radware. (2023). “2022 Global Threat Analysis Report”, USA.
4. L. Prudente Tixteco, M. D. C. Prudente Tixteco, G. Sánchez Pérez, L. K. Toscano Medina y J. d. J. Vázquez Gómez. (2017). “Recommendations for Risk Analysis in Higher Education Institutions”, SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, pp. 125-130.
5. D. Mairaj Inamdar y S. Gupta. (2020). “A Survey on Web Application Security”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 6, nº 5, pp. 223-228.
6. International Organization for Standardization. (2013). “Information Technology- Security Techniques- Information Security Management Systems-Requirements 27001”.