ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/338050855

Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente

Article *in* RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao · August 2019

CITATIONS
0

READS
17

6 authors, including:

Daisy Imbaquingo
Universidad Técnica del Norte
4 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Erick Herrera
Universidad Técnica del Norte
11 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Israel Herrera
Universidad Técnica del Norte
17 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Optimización del Master Production Schedule en entornos inciertos View project

Product distribution optimization View project

All content following this page was uploaded by Erick Herrera on 19 December 2019.

The user has requested enhancement of the downloaded file.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 22/04/2019
Aceitação/Acceptance: 01/07/2019

Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente

Daisy E. Imbaquingo[1,2], Erick P. Herrera-Granda[1], Israel D. Herrera-Granda[1], Silvia R. Arciniega[1], Verónica L. Guamán[1], MacArthur C. Ortega-Bustamante[1,2]

deimbaquingo@utn.edu.ec, epherrera@utn.edu.ec, idherrera@utn.edu.ec, srarciniega@utn.edu.ec, vlguaman@utn.edu.ec, mc.ortega@utn.edu.ec

[1] Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, 100150, Ibarra, Ecuador.

[2] Facultad de Informática, Universidad Nacional de La Plata, 1900, La Plata, Argentina.

Pages: 349–362

Resumen: El presente trabajo detalla el proceso de evaluación de seguridad del Sistema de Evaluación Docente de la Universidad Técnica del Norte, para establecer objetivos y controles que permitan minimizar las vulnerabilidades del sistema de gestión. Se recolectó información mediante encuestas, entrevistas y reuniones de trabajo, posteriormente se aplicó la metodología Magerit mediante el software PILAR, que permitió el levantamiento de información y activos como hardware, software, y activo humano, para luego realizar una valoración de acuerdo con su incidencia en la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad. La estructura factorial de la encuesta se diseñó mediante análisis factorial exploratorio y los resultados se validaron empleando análisis factorial confirmatorio. Además, se realizó una revisión de la ISO/IEC2001:2013 y la evaluación de cumplimiento basada en la Norma ISO/IEC 2700:2017. Para detectar la seguridad a este sistema se hizo pruebas de penetración en las vulnerabilidades detectadas mediante herramientas de SQLmap y Nmap.

Palabras-clave: Evaluación seguridad sistemas informáticos; ISO/IEC 27002:2017; Análisis factorial exploratorio, Validez, Fiabilidad.

Evaluation of University Informatic Security Systems: Teacher Evaluation System a case study

***Abstract*:** This work details the security evaluation process of Técnica del Norte University teacher evaluation system, in order to establish objectives and controls that minimize the vulnerabilities of the management system. Information was collected through surveys, interviews and work meetings. Next, the Magerit methodology was applied through the PILAR software, which allowed information and assets collection, such as hardware, software, and human assets, and then, an assessment according to its incidence in integrity, confidentiality, availability, authenticity and traceability, was made. The factorial structure of the survey was

designed using exploratory factor analysis and the results were validated by means of confirmatory factor analysis. In addition, a review of ISO / IEC2001: 2013 and an evaluation of compliance based on ISO / IEC 2700: 2017 was performed. To detect the security of this system, penetration tests were made on the detected vulnerabilities, by means of SQLmap and Nmap tools.

Keywords: informatic security system evaluation; ISO/IEC 27002:2017; factorial exploratory analysis; validity; fiability.

1. Introducción

Las organizaciones se enfrentan a un número alto de inseguridades que provienen de varias fuentes, por esta razón los Sistemas de Seguridad de Gestión Informática deberían estar implementados con estándares en cuanto a seguridad, integridad y confidencialidad. Para (Muñoz, 2015) un SGSI para una organización es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de la seguridad de la información.

Las instituciones educativas suelen presentar problemáticas en lo relacionado a la seguridad de la información de los datos que a diario emplean, desde bases de datos información de sus alumnos, docentes y personal administrativo, en el intercambio de información que tienen que realizar entre centros u organismos educativos institucionales.

Dentro de la Universidad Técnica del Norte se usan los sistemas de gestión de información, siendo un activo fundamental la información la misma que necesita protección ante amenazas que afectan diariamente la disponibilidad e integridad de la organización así mismo poder evitar riesgos altos, daños operantes y económicos para la organización. Por lo antes mencionado se debe establecer procedimientos y controles de seguridad los cuales se obtienen del análisis de riesgos, establecer parámetros para poder identificar amenazas que afectan a los activos de la organización, además verificar vulnerabilidades y de esta manera determinar el impacto que tendrá en la institución las posibles amenazas encontradas.

Los problemas de seguridad informática alcanzan a todas las organizaciones que tienen alto volumen de información sea esta financiera o académica, ésta es la razón se vuelve blanco de posibles ataques. La seguridad informática se relaciona con procesos, procedimientos y metodologías que ayudan a salvaguardar los datos, estos procesos se van estructurando con el uso de normas, protocolos, estándares que servirán para minimizar riesgos en una infraestructura tecnológica.

El autor (Baca, 2016) define a la seguridad informática como: la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos a los que se encuentra expuesta.

Según (Romo & Valarezo, 2012) la seguridad de la información está apoyada en 3 pilares fundamentales de la seguridad:

- Confidencialidad: Certifica que solo los usuarios con accesos autorizados puedan acceder a la información. La seguridad que se implementará debe asegurar que solo las personas que tengan acceso a la información fueron autorizadas. Una medida que mitiga este tipo de riesgo es la firma de contratos de confidencialidad o inclusión de este tipo de cláusulas en el contrato de servicio (Ministerio de Energía, 2017).
- Integridad: Hace referencia a que la información sea correcta y no se modifique, ni haya errores. La información puede ser corrompida y se puede basar decisiones en torno a la información, lo cual da la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad (Hidalguense, 2011).
- Disponibilidad: Según (Chilán & Williams, 2017) la disponibilidad es cuando se asegura que los usuarios autorizados tienen el acceso debido a la información siendo la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La información es el núcleo dentro de una organización, como se aprecia en la figura 1, indica la relación que existe dentro de la misma, por ello es necesario mantener un nivel aceptable de protección para estos componentes y minimizar los riesgos a los que puede estar expuesta cualquier tipo de entidad.

2. Materiales y Métodos

2.1. Metodología Magerit V3

MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", fue elaborada por el Consejo Superior de Administración de España, actualizada en 2012 su versión 3, brinda un método sistemático para analizar los riesgos del uso de las tecnologías de la información y la comunicación (Ministerio de Hacienda y Administraciones Públicas de España, 2012), dicha metodología implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones, teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

MAGERIT es la metodología más usada a nivel de Latinoamérica, el beneficio que presenta es que se encuentra disponible en idioma inglés y español, además utiliza la herramienta EAR que es comercial pero la herramienta PILAR BASIC es gratuita, misma que puede ser usada con licencias de prueba. MAGERIT se desarrolla para organizaciones públicas gubernamentales; el ciclo de vida de esta metodología empieza con la identificación de activos, amenazas lógicas y de entorno, establece frecuencias e impacto para poder identificar salvaguardas y gestionar el riesgo residual, dentro de la metodología se considera activos de información al hardware, software, información electrónica, personas, instalaciones, medios de soporte y elementos de comunicación de datos.

La metodología MAGERIT determina los valores de los activos considerando la dimensión de la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad, estableciendo escala de valoración en diferentes niveles: muy alto, alto, medio, bajo, muy bajo y despreciable, en esta metodología se verifica el impacto determinando el valor de

los activos, este, acumulado se calcula mediante el valor del activo y las amenazas a las que afronta, y este impacto repercutido se considera el valor propio y las amenazas (MAGERIT, 2012) . Con respecto a lo establecido se escoge esta metodología por ser la más completa y evalúa todos los pilares de la seguridad informática, con la ayuda del software de complemento, como lo es el PILAR, se puede obtener fácilmente las gráficas de impactos y riesgos acumulados.

2.2. PILAR

PILAR, es un acrónimo de "Procedimiento Informático Lógico para el Análisis de Riesgos", es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

La herramienta soporta todas las fases del método Magerit que son: caracterización de los activos (identificación, clasificación, dependencias y valoración), caracterización de las amenazas y evaluación de las salvaguardas. Además, la herramienta incorpora los inventarios del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis, siendo: tipos de activos, dimensiones de valoración, criterios de valoración y catálogo de amenazas.

Una vez realizado el análisis con MAGERIT, se procedió a ingresar los datos en la herramienta PILAR, la misma que ayudó a evaluar la situación actual y de esta manera proponer soluciones eventuales en el departamento de DDTI de la Universidad Técnica del Norte.

2.3. ISO/IEC 27002:2017

Este es un estándar para la seguridad de la información creada por la Organización Internacional de Normalización y la Comisión Electrotecnia Internacional. La versión más reciente de la norma ISO/IEC 27002:2017, brinda diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a quienes se interesen en iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. Esta norma internacional establece directrices para la seguridad de la información en las organizaciones y las prácticas de gestión de seguridad de la información incluyendo la selección, la implantación y la gestión de los controles. Además, considera el entorno de los riesgos de seguridad de la información de la organización (INEN, 2017).

El valor de esta información se propaga por palabras escritas, números e imágenes, por ejemplo: el conocimiento, conceptos son formas intangibles de información. La información y sus procesos relacionados, los sistemas, las redes y el personal implicado en la operación y manejo de la información y protección son los activos que resultan valiosos para el negocio de las organizaciones y en consecuencia requieren protección contra diversos peligros. La seguridad de la información se consigue mediante la implantación de un conjunto adecuado de controles, lo que incluye políticas, procesos, estructuras organizativas y funciones de hardware y software. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización (INEN, 2017).

La norma ISO/IEC 27002:2017 consta de 14 capítulos de controles de seguridad que en conjunto proporcionan un total de 35 categorías principales y 114 controles.

2.4. Aplicación de Magerit y Pilar

La ejecución del proceso de evaluación docente está basado en la aplicación de varios instrumentos como la autoevaluación, coevaluación y heteroevaluación para de esta manera obtener un diagnostico real de los datos evaluados (CEIDPA, 2018). El DDTI es el encargado de recopilar los datos que se obtengan mediante el sistema de evaluación docente y la información que se obtuvo mediante Magerit y PILAR permitió evaluar la situación en que se encontraba y de esta manera poder proponer soluciones eventuales en el Departamento de Desarrollo de Tecnologías Informáticas (DDTI) de la Universidad Técnica del Norte.

Identificación de Activos

Un activo es algo valioso o de utilidad para la organización, la finalidad de los activos es brindar protección para asegurar de alguna forma la operación del negocio y la continuidad del mismo. En la tabla 1 se muestra los activos identificados en el DDTI – UTN.

Tipo de activo	Activo
Datos y/o información	Bases de Datos de estudiantes y personal académico.
Software	Licencia GNU Oracle Linux 6 Licenciamiento Campus Agreement Microsoft Licencia perpetua Oracle 11g Database and Aplications Licenciamiento Adobe Creative Cloud MLP Ed Subscription Multi Latin American Languagues Licenciamiento Eset NOd 32 Antivirus Licencia ToolBook Licencia GNU Linux Centus Software libre licencia GNU para el Geoportal Licencia de ESRI Arcgis 10.1 Licencia GNU Dbspace para Repositorio Digital Licencia GNU Moodle para aula virtual
Equipamiento Informático (Hardware)	Servidores HP Blade System, equipos Informáticos PC, Laptop's, Call Manager, Gateway de voz, IVR (contestadora automática), Tape Backup, Switchs Core, Switchs de acceso, Cisco ASA, Firewall, Ipx, Router, Antenas y radio enlaces, Access point, Torres, Racks, Cableado estructurado
Redes de Comunicaciones	Red telefónica, Red de datos, Red inalámbrica, Internet
Soportes de Información	Nube Oracle Apex
Equipamiento Auxiliar	Ups, Fibra Óptica
Instalaciones	Departamento de DDTI – UTN
Personal	Miembros del Área de DDTI

Tabla 1 – Clasificación de Activos DDTI - UTN.

Valoración de activos

La valoración del activo se lo puede hacer de forma cuantitativa, es decir asignando una cantidad numérica, también es posible valorar el activo de forma cualitativa, es decir asignado niveles. En este caso de estudio la metodología empleada para la valoración fue la elaboración de una encuesta aplicada a los usuarios del sistema de evaluación docente, mediante la cual se diseñó un constructo aplicando Análisis Factorial Exploratorio AFE que permitió valorar los dominios objetivos y controles estipulados por la norma ISO/IEC 27002:2017, en sus componentes: Aspectos Organizativos, Control de Acceso y Cumplimiento. Posteriormente se validó el instrumento y la estructura factorial mediante Análisis Factorial Confirmatorio AFC, de manera que los datos de valoración que se emplearán en Magerit y Pilar estén dotados de validez y fiabilidad (Batista y Coenders, 2010).

La encuesta estuvo constituida de 10 preguntas de se diseñaron en base a la normativa para permitir valorar las puntuaciones que los usuarios del sistema les otorgaron a los componentes. La evaluación se conformó de 529 encuestas aplicadas a usuarios, docentes y personal administrativo que han utilizado el sistema de evaluación docente. Los resultados obtenidos fueron tratados y ejecutados las pruebas estadísticas empleando el lenguaje de programación R mediante RStudio. Inicialmente se verificó que no existan valores perdidos mediante la librería *mice*, además se obtuvieron las distancias de Mahalanobis para cada variable y mediante estas, en conjunto con los cuantiles de la distribución chi cuadrada para un *pvalue* de 0.999, se estableció un puntaje de corte de 29,5883, mediante el cual se detectaron y eliminaron 15 observaciones atípicas por lo que la base de datos con la que se trabajó estuvo conformada de 514 encuestas.

Como el AFE y AFC son técnicas estadísticas paramétricas, se verificó los supuestos para estas. Inicialmente para el supuesto de aditividad se obtuvo la matriz de correlación bivariada para todas las posibles combinaciones de preguntas, donde se observó que ninguna de las parejas de variables alcance una correlación perfecta en rango de 0,95 a 1, por lo que se alcanza el supuesto de aditividad.

Posteriormente para verificar los supuestos de linealidad, normalidad, homogeneidad y homocedasticidad se ejecutó un análisis de regresión lineal falsa basado en los residuos estandarizados obtenidos para los cuantiles $\chi^2\chi^2$. Los resultados obtenidos se resumen en la figura 1.

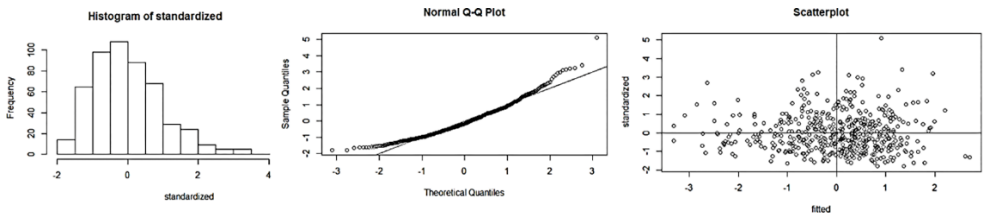


Figura 1 – Histograma, QQ Plot y Scatter Plot de los valores estandarizados obtenidos para los cuantiles $\chi^2\chi^2$

El supuesto de normalidad se verifica mediante la visualización del histograma para la regresión realizada a partir de los cuantiles, donde las frecuencias se distribuyeron con una tendencia normal centrada entre $-2{-}2$ a 22. De la misma manera el supuesto de linealidad se verifica ya que los cuantiles cumplen con una tendencia lineal creciente en el intervalo de $-2{-}2$ a 22. Finalmente los supuestos de homogeneidad y homocedasticidad se verificaron mediante el criterio de esfericidad mediante un Scatter plot donde se visualiza homogeneidad de la distribución en los cuatro cuadrantes con ligeros problemas en el semiplano negativo pero en el intervalo de $-2{-}2$ a 22 se tienen resultados aceptables.

Para el diseño del AFE es necesario adicionalmente la verificación de los supuestos de suficiencia de correlación y suficiencia de muestreo (Pettersson & Turkheimer, 2010). Mediante el paquete psych se ejecutó el test de suficiencia de correlación de Bartlett obteniéndose un p-value de $2{,}72 \times 10^{-303} 2{,}72 \times 10^{-303}$ mediante el cual se acepta suficiencia de correlación con un elevado nivel de significancia. Por su parte para demostrar la suficiencia de muestro se efectuó el test de Kaise-Meyer-Olkin KMO, en el que se obtuvo un índice de suficiencia factorial KMO de 0,84 por lo que se acepta este supuesto ya que presentó un nivel cercano a 1 y por encima de 0.7.

Para determinar el número de factores a emplearse se ejecutó un análisis paralelo y por medio de un Scre Plot se visualiza el punto de inflexión. En la figura 2 se muestran los resultados del análisis paralelo donde se pueden visualizar 2 puntos probables para 2 y 6 factores, por lo que un valor dentro de este intervalo puede ser seleccionado. En este estudio se emplearon 3 factores ya que coincide con los dominios a analizar.

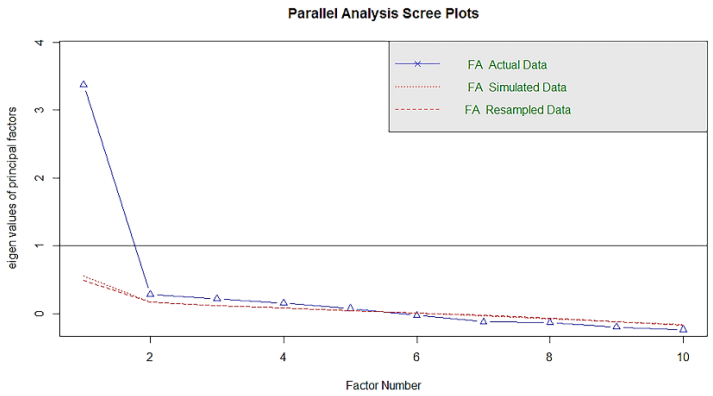


Figura 2 – Scree plot del análisis paralelo

Una vez seleccionado el número de factores a crear en la estructura factorial se ejecuta el AFE para 3 factores empleando un método de rotación factorial oblicuo mediante *oblimin* que permite a los factores ser correlacionados cuando son rotados y la estimación de ajuste matemático empleada es *ml* para emplear el criterio de máxima verosimilitud el cual es más apropiado en AFE.

Después de ejecutar varias pruebas experimentales y cotejando con el AFC se retiró la pregunta 2 (¿Considera usted que el sistema académico protege su información?) ya que saturaba a dos factores en más de 0,3 para las diferentes configuraciones empleadas, además la pregunta 9 (¿Considera usted que se debería implementar la política de obligatoriedad de cambio de contraseña cada cierto periodo de tiempo?) fue retirada debido a que no fue capaz de saturar a ningún factor en más de 0,3 en ninguna de las configuraciones. Los resultados para la estructura factorial sugerida por el AFE con sus saturaciones, comunalidades y singularidades, se muestran en la figura 3.

```
Standardized loadings (pattern matrix)
             ML3   ML2   ML1    h2    u2
pregunta1   0.40  0.00 -0.02 0.159 0.841
pregunta3   0.24  0.52  0.03 0.529 0.471
pregunta4   0.13 -0.21  0.20 0.062 0.938
pregunta5   0.00  0.01  1.00 0.995 0.005
pregunta6   0.73 -0.08  0.03 0.453 0.547
pregunta7   0.58  0.24 -0.03 0.609 0.391
pregunta8   0.50  0.12 -0.03 0.359 0.641
pregunta10 -0.01  0.93  0.00 0.858 0.142

                       ML3  ML2  ML1
SS loadings           1.54 1.45 1.04
Proportion Var        0.19 0.18 0.13
Cumulative Var        0.19 0.37 0.50
Proportion Explained  0.38 0.36 0.26
Cumulative Proportion 0.38 0.74 1.00
```

```
Standardized loadings
(pattern matrix)
             ML1   ML2   h2   u2
pregunta1   0.38  0.08 0.15 0.85
pregunta3   0.74 -0.03 0.55 0.45
pregunta4  -0.06  0.48 0.23 0.77
pregunta5   0.07  0.40 0.17 0.83
pregunta6   0.60  0.13 0.37 0.63
pregunta7   0.78  0.05 0.60 0.40
pregunta8   0.58  0.04 0.34 0.66
pregunta10  0.84 -0.09 0.72 0.28

                       ML1  ML2
SS loadings           2.71 0.42
Proportion Var        0.34 0.05
Cumulative Var        0.34 0.39
Proportion Explained  0.86 0.14
Cumulative Proportion 0.86 1.00
```

```
Standardized loadings (pattern matrix)
             ML1   ML2   h2   u2 com
pregunta1   0.03  0.36 0.15 0.85 1.0
pregunta3   0.55  0.22 0.53 0.47 1.3
pregunta6  -0.07  0.74 0.46 0.54 1.0
pregunta7   0.29  0.53 0.60 0.40 1.5
pregunta8   0.15  0.48 0.36 0.64 1.2
pregunta10  0.93 -0.02 0.85 0.15 1.0

                       ML1  ML2
SS loadings           1.51 1.45
Proportion Var        0.25 0.24
Cumulative Var        0.25 0.49
Proportion Explained  0.51 0.49
Cumulative Proportion 0.51 1.00
```

Figura 3 – Pruebas efectuadas para el diseño de la estructura factorial

Como se visualiza en la figura 4, inicialmente se ejecuta el AFE para 3 factores donde se determinó que las preguntas 1, 6, 7, 8 pueden pertenecer a un primer factor, mientras la 3 y la 10 a un segundo factor. Inicialmente se visualiza que las preguntas 4 y 5 pueden pertenecer a un tercer factor, sin embargo, la pregunta 4 no presenta una saturación superior a 0,3, por lo que se ejecutan dos pruebas más inicialmente para 2 factores donde las saturaciones de 4 y 5 si superan a 0,3 por lo que se puede considerar ubicarlas en un factor sin embargo existe incertidumbre en las preguntas 4 y 5 por lo que se someterá a análisis factorial confirmatorio. En todas las tres pruebas efectuadas se obtuvieron índices CFI (Comparative Fit Index) de 0.999, 0,973 y 0,994 respectivamente y índices de Tucker y Lewis de 0.98, 0,99 y 0,978 respectivamente por lo que se acepta la confiabilidad de factoreo del AFE. Adicionalmente se ejecuta una prueba de alfa de Cronbach para verificar la validez de los dos primeros factores obteniendo valores de 0,79 y 0,7 respectivamente por lo que entran en la categoría de aceptable.

Finalmente, mediante análisis factorial confirmatorio se valida la estructura factorial (Rosseel & Lavaan, 2012), donde se obtuvo una saturación insuficiente de la pregunta 5 por lo que se retiró de la estructura factorial. De esta manera se obtuvo que, las saturaciones superan en todos los casos a 0,3 y ningún factor está correlacionado. Además, el índice de Tucker y Lewis y el NNFI (Non Normed Fit Index) obtenidos son de 0,991 el cuál entra en la categoría de excelente >0,95, además el CFI fue de 0,995 ubicándose en la categoría de excelente y los índices RMSEA (Root Mean Square Error of Approximation) y SRMR (Standardized Root Mean Residual) alcanzaron valores de 0,030 y 0,021 lo cual demuestra la validez del constructo debido a que estos valores están por debajo de 0,05.

Una vez validado el instrumento los valores obtenidos a partir de la encuesta fueron empleados para efectuar la valoración de activos en el software pilar. La figura 4 muestra la valoración de activos efectuada estadísticamente en conjunto con los datos suministrados por el DDTI.

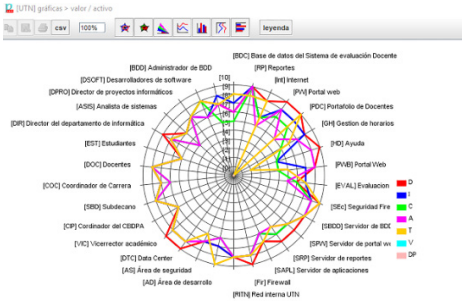


Figura 4 – Valoración de activos en PILAR

Identificación de amenazas

La identificación de amenazas consiste en identificar posibles amenazas que pueden afectar a cada uno de los activos anteriormente identificados. Para ello fue necesario revisar documentación acerca de políticas de seguridad del sistema a evaluar, por ejemplo, verificar si existen políticas para el acceso al sistema de evaluación docente. Una vez valorados los activos Pilar asocia a cada uno de los activos del sistema de evaluación docente, amenazas posibles para dicho activo. En la figura 5 se realiza la valoración de la frecuencia, se toma en cuenta dos factores importantes: probabilidad de ocurrencia, que es el registro de ocurrencia de una amenaza cuando se materializa una amenaza y porcentaje de degradación que es el daño que causó el incidente ocurrido (Fernandez & Daniel, 2016).

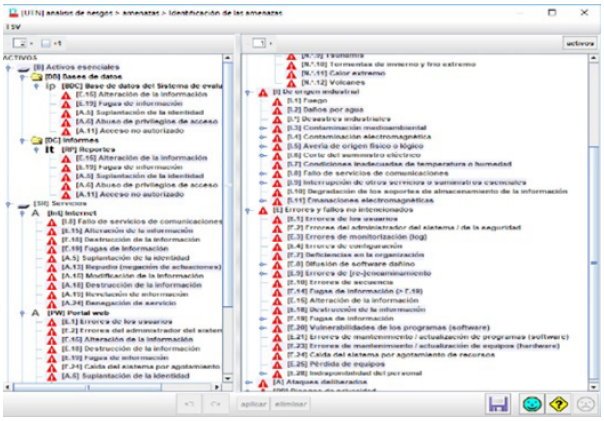
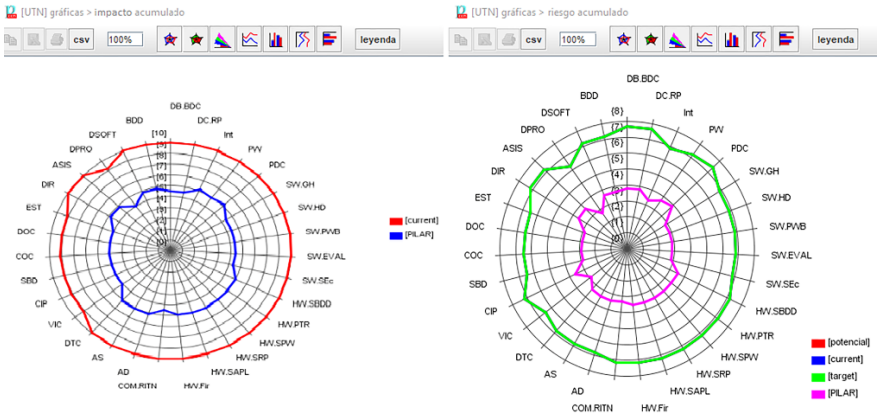


Figura 5 – Amenazas del sistema de evaluación docente.

Impacto

El impacto es el daño que se originó en los activos una vez que las amenazas se materializaron. Para la estimación de impacto se lo hace mediante los siguientes factores: la materialización de una amenaza puede afectar a todo un recurso informático o solo a una parte de este, la materialización de una amenaza puede afectar a partes claves de información o a partes independientes, una vez materializada la amenaza es temporal o permanente. Los impactos pueden traer consigo impactos cualitativos o cuantitativos, por ejemplo, pérdidas económicas, mala imagen de los clientes hacia la empresa entre muchas otras (Fernandez & Daniel, 2016). Dentro de PILAR se puede obtener el impacto acumulado para cada activo, amenaza y la dimensión de valoración, el resultado está descrito en función de la degradación y el valor acumulado; por lo tanto, mientras más grande sea la degradación, mayor será el impacto acumulado, y este permitirá identificar que salvaguardas se deben aplicar en la organización para mitigar los riesgos, como se muestra en la Figura 6.



(a) (b)

Figura 6 – Impacto (a) y Riesgo Acumulado del Sistema de Evaluación Docente (b)

Riesgo

La figura 6, literal (b), presenta la valoración de riesgos, que es un proceso que debe seguir la secuencia: identificación de activos, identificación de amenazas y la estimación de vulnerabilidades de amenazas sobre cada activo. Para la valoración de riesgos existen cuatro zonas: Bajo (0 a 3) indica que el riesgo es bajo; por lo tanto, no es necesario emplear salvaguardas adicionales, Medio (3 a 6), indica que el riesgo es medio; por lo tanto, se debe considerar la implementación de salvaguardas, Alto (6 a 9), indica que el riesgo es alto; por consiguiente, es obligatorio emplear salvaguardas para mitigar riesgos, Crítico (9 a 12), indica que el riesgo es crítico; por que es obligatorio emplear salvaguardas adicionales para minimizar el riesgo.

3. Resultados y Discusión

Una vez que se realizó el análisis mediante la metodología se procede a evaluar el cumplimiento d los controles del sistema de Evaluación Docente mediante la Norma ISO/IEC 27002:2017, donde se pudo evidenciar que se cumple un 53% de los controles de la norma ISO/IEC 27002:2017. Los ítems que el sistema cumplió a cabalidad acorde con la norma antes mencionada se detallan en la tabla 2.

Aspecto general	Objetivo de control	Control	Cumple
Políticas de seguridad de la información	Dirección de gestión de la seguridad de la información	Políticas de seguridad de la información	SI
		Revisión de las políticas para la seguridad de la información	NO
Organización de la seguridad informática	Organización interna	Roles y responsabilidades de seguridad de la información	NO
		Separación de funciones	SI
		Contacto con las autoridades	SI
		Contacto con los grupos de interés especial	NO
	Dispositivos móviles y teletrabajo	Política de dispositivos móviles	NO
Seguridad en recursos humanos	Antes del empleo	Investigación de antecedentes	SI
		Términos y condiciones de empleo	NO
	Durante el empleo	Responsabilidades de dirección	SI
		Conciencia, educación y formación en seguridad de la información.	NO
		Proceso disciplinario	NO
	Finalización o cambio de empleo	Responsabilidades ante la finalización o cambio de empleo	NO
Gestión de activos	Responsabilidad de los activos	Inventario de activos	SI
		Propiedad de activos	SI
		Uso adaptable de activos	SI
		Devolución de activos	SI
Control de acceso	Requisito de negocio para el control de acceso	Política de control de acceso	NO
		Acceso a redes y servicios de red	NO
	Gestión de acceso de los usuarios	Registro y retiro de usuario	SI
		Provisión de acceso a usuarios	NO
		Gestión de la información secreta de autentificación de los usuarios	NO
		Revisión de los derechos de acceso de usuario	NO
		Retiro y ajuste de los derechos de acceso	NO
	Responsabilidades del usuario	Uso de la información secreta de autentificación	NO
	Control de acceso a sistemas y aplicaciones	Procedimientos seguros de inicio de sesión	NO
		Sistema de gestión de contraseñas	NO
		Control de acceso al código fuente del programa	SI

Aspecto general	Objetivo de control	Control	Cumple
Criptografía	Controles criptográficos	Política de uso de los controles criptográficos	SI
		Gestión de llaves	NO
Seguridad física y del entorno	Áreas seguras	Perímetro de seguridad física	SI
		Controles físicos de entrada	SI
		Protección contra amenazas externas y ambientales.	NO
Seguridad física y del entorno	Equipos	Ubicación y protección de equipos	NO
		Instalaciones de suministro	NO
		Seguridad del cableado	SI
		Mantenimiento de los equipos	SI
Seguridad de las operaciones	Procedimientos y responsabilidades operacionales	Documentación de procedimientos de operación	SI
		Gestión de cambios	SI
		Gestión de capacidades	SI
		Separación de ambientes de desarrollo, pruebas y producción	SI
	Protección contra un malware	Controles contra un malware	SI
	Copias de seguridad	Copias de seguridad de la información	SI
	Registro y monitoreo	Registro de eventos	NO
		Protección de la información de registro	SI
	Control del software operacional	Instalación del software en los sistemas operativos	SI
	Gestión de la vulnerabilidad técnica	Gestión de las vulnerabilidades técnicas	NO
		Restricciones en la instalación del software	NO
	Consideraciones sobre la auditoria de sistemas de información	Controles de auditoria de sistemas de información	SI
Seguridad en las telecomunicaciones.	Gestión de la seguridad de redes	Controles de red	SI
		Seguridad de los servicios de red	SI
		Separación en las redes	SI
	Requisitos de seguridad de los sistemas de información	Análisis de requisitos y especificaciones de seguridad de la información.	SI
Adquisición. Desarrollo y mantenimiento del sistema	Seguridad en el desarrollo y en los procesos de soporte	Política de desarrollo seguro	SI
		Procedimientos de control de cambios en el sistema	SI
	Datos de prueba	Protección de datos de prueba	NO
Relaciones con proveedores	Gestión de la provisión de servicios del proveedor	Monitoreo y revisión de los servicios de proveedores	NO
		Gestión de cambios en los servicios de proveedores.	SI

Aspecto general	Objetivo de control	Control	Cumple
Gestión de incidentes de seguridad de la información	Gestión de los incidentes de seguridad de la información y mejoras	Responsabilidades y procedimientos	NO
		Informe de los eventos de seguridad de la información	NO
		Informe de debilidades de seguridad de la información	NO
		Respuesta a incidentes de seguridad de la información	SI
		Aprendizaje de los incidentes de seguridad de la información	NO
		Recopilación de evidencias	SI
Aspectos de seguridad de la información para la gestión de la continuidad del negocio.	Continuidad de seguridad de la información	Planificación de la continuidad de seguridad de la información	NO
	Redundancias	Disponibilidad de las instalaciones de procesamiento de la información	NO
Cumplimiento	Cumplimiento de los requisitos legales contractuales	Identificación de la legislación aplicable de los requisitos contractuales.	SI
		Derechos de propiedad intelectual	SI
		Protección de los registros	SI
		Protección y privacidad de la información de carácter personal	NO

Tabla 2 – Clasificación de Activos DDTI – UTN

4. Conclusiones

El factor que aumenta significativamente el nivel de riesgo de los activos de información es el escaso proceso que se aplica y adhiere al problema expuesto para evitar aquellas situaciones que pueden afectar la disponibilidad, integridad y confidencialidad de la información que se manipula. La aplicación del estándar ISO/IEC 27002:2017 es de suma importancia para la correcta evaluación de controles que garanticen la seguridad de la información del sistema de Evaluación docente de la UTN. La evaluación de riesgos del sistema de evaluación docente es indispensable para el departamento de informática de la Universidad Técnica del Norte, puesto que se considera a la información como un activo institucional. El uso de la Metodología MAGERIT permite realizar un análisis de riesgos mediante la identificación de activos del sistema de evaluación docente y fue de ayuda para identificar el estado actual de la seguridad de la información. La situación actual del sistema de evaluación docente evidencia un nivel considerable de cumplimiento de políticas de seguridad de información, tanto física como de gestión (51%), por lo que requiere de un compromiso de autoridades y docentes para un cumplimiento total de la normativa. De igual manera se requiere que en los departamentos de tecnología de las universidades cuenten con personal calificado que se encargue de la seguridad de la información de los ERP, pues al realizar un análisis de vulnerabilidades tres herramientas brindaron información exacta de los puntos críticos que se deben revisar para evitar estar expuestos a hackers informáticos.

Referencias

Baca, G. (2016). *Introducción a la Seguridad Informática*. Mexico: Grupo Editorial Patria, S.A. de C.V.

CEIDPA. (2018). *Evaluación integral del desempeño del personal académico de la UTN para el período septiembre 2018 - agosto 2019*. Ibarra.

Chilán, S. E., & Williams, P. P. (2017). Apuntes teóricos introducctorios sobre la seguridad de la información. *Revista Científica Dominio de las Ciencias*, 284–295.

Fernandez, A., & Daniel, G. (2016). Complex vs. simple asset modeling approaches for information security risk assessment: Evaluation with MAGERIT methodology. *Sixth International Conference on Innovative Computing Technology (INTECH)* (págs. 542 - 549). Dublin, Ireland: IEEE Xplore.

Hidalguense, U. T. (2011). *Auditoria*. Mexico: UTHH.

INEN. (2017). *Norma INEN ISO/IEC 27002*. QUITO: INEN.

MAGERIT. (Octubre de 2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XXgJlGa21PY.

Ministerio de Energía, T. y. (2017). *Protección de la Información*. Madrid: Ministerio de Energía, Turismo y Agenda Digital España.

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *Magerit - version 3.0. Metodología de Analisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Hacienda y Administraciones Publicas de España.

Muñoz, M. (2015). *Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001*.

Pettersson, E., & Turkheimer, E. (2010). Item selection, evaluation, and simple structure in personality data. *Journal of research in personality, 44(4)*, 407–420.

Romo, V. D., & Valarezo, C. J. (2012). Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana Sede Guayaquil. Guayaquil.

Rosseel, Y., & Lavaan. (2012). An R Package for Structural Equation Modeling. *Journal of Statistical Software, 48(2)*, 1–36.

© 2019. This work is published under https://creativecommons.org/licenses/by-nc-nd/4.0(the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.

View publication stats