Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 46 – 62, noviembre 2023

www.concienciadigital.org

Política de control de vulnerabilidades en el proceso "B" del área de admisión y nivelación de la Universidad Católica de Cuenca

Vulnerability control policy in the "B" process of the admission and leveling area of the Catholic University of Cuenca

[1] Kerly-Gardenia Ordoñez Almeida https://orcid.org/0000-0003-1207-1263
Universidad Católica de Cuenca, Cuenca - Ecuador.
kerly.ordonez@ucacue.edu.ec

[2] Carlos Andrés Torres Soto https://orcid.org/0009-0003-5893-6047
Universidad Católica de Cuenca, Cuenca – Ecuador.
atorres@ucacue.edu.ec

[3] Laura Alexandra Ureta Arreaga https://orcid.org/0000-0001-5328-8085
Universidad Católica de Cuenca, Cuenca – Ecuador.
laura.ureta@ucacue.edu.ec

Artículo de Investigación Científica y Tecnológica
Enviado: 18/08/2023
Revisado: 12/09/2023
Aceptado: 02/10/2023
Publicado: 03/11/2023
DOI: **https://doi.org/10.33262/concienciadigital.v6i4.2.2752**

Cítese: Ordoñez Almeida, K. G., Torres Soto, C. A., & Ureta Arreaga, L. A. (2023). Política de control de vulnerabilidades en el proceso "B" del área de admisión y nivelación de la Universidad Católica de Cuenca. *ConcienciaDigital*, 6(4.2), 46-62. https://doi.org/10.33262/concienciadigital.v6i4.2.2752

CONCIENCIA DIGITAL, *es* una revista multidisciplinar, **trimestral,** que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. https://concienciadigital.org
La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 46 – 62, noviembre 2023
www.concienciadigital.org

Palabras claves:
Riegos; amenazas; vulnerabilidades; ciberseguridad; ciberdelincuencia, controles, políticas.

Resumen

Introducción: La Universidad Católica de Cuenca, a la vez de ir alineada en alcance de la calidad educativa, innovación y crecimiento institucional, también busca el mejoramiento continuo en sus diferentes dependencias respecto a la seguridad de la información y así evitar posibles amenazas a sus activos de información, pudiendo iniciar con el área de Admisión y Nivelación con alcance al proceso "B" correspondiente a la toma de los exámenes de Odontología de la Institución. **Objetivo:** Obtener la política de control de vulnerabilidades en el proceso "B" del Área de Admisión y Nivelación de la Universidad Católica de Cuenca. Con la finalidad de que posteriormente sean implementadas en la institución. **Metodología:** La metodología utilizada fue la ISO 27002:2013, la principal herramienta de apoyo fue Excel y sus diferentes hojas lo que facilitó el análisis, seguido la herramienta tecnológica de análisis de gestión de riesgo PILAR 7.4.9 (25.10.2021). **Resultados:** El análisis de los riesgos, amenazas y vulnerabilidades empezó con el levantamiento del inventario de activos de información del subproceso (b) del área de admisión y nivelación correspondiente a la toma de los exámenes de Odontología de la Institución, donde se obtuvieron 33 AI, los cuales fueron clasificados por tipo de AI. **Conclusión:** El alma mater, se ha mantenido participando en diferentes rankings internacionales como; webometrics, permitiéndole escalar 3 puesto a favor de 28 al 25, concluyendo que la institución constantemente genera acciones para escalar posiciones de excelencia académica. **Área de estudio general:** Tecnología de la información. **Área de estudio específica:** Ciberseguridad.

Keywords:
Risks; threats; vulnerabilities; cybersecurity; cybercrime, controls, policies.

Abstract

Introduction: The Catholic University of Cuenca, while being aligned in the scope of educational quality, innovation and institutional growth, also seeks continuous improvement in its different departments regarding information security and thus avoid possible threats to its information assets, being able to start with the Admission and Leveling area with scope to the "B" process corresponding to the taking of the Institution's Dentistry exams. **Objective:** Obtain the vulnerability control policy in the "B" process of the Admission and Leveling Area of the Catholic University of Cuenca. In order that they are subsequently

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 46 – 62, noviembre 2023

implemented in the institution. **Methodology:** The methodology used was ISO 27002:2013, the main support tool was Excel and its different sheets which facilitated the analysis, followed by the technological risk management analysis tool PILAR 7.4.9 (25.10.2021). **Results:** The analysis of the risks, threats and vulnerabilities began with the collection of the inventory of information assets of the sub process (b) of the admission and leveling area corresponding to the taking of the Dentistry exams of the Institution, where 33 Ais were obtained, which were classified by type of AI. **Conclusion:** The alma mater, has been participating in different international rankings such as; webometrics, allowing it to climb 3 places in favor of 28 to 25, concluding that the institution constantly generates actions to climb positions of academic excellence.

Introducción

Según aportan, Fernández & Ascón (2021), desde un inicio, cuando existieron los equipos informáticos, no fue un desconocimiento para la sociedad la facilidad que podrían traer al mundo moderno con su operatividad y eficacia, así como la incertidumbre que ha venido causando en el pasar de los años al saber que la información se encuentre almacenada en varios dispositivos tecnológicos con diferentes características, marcas y modelos sin conocer claramente el tratamiento que podrían tener los datos, el riesgo y vulnerabilidades que se podrían exponer.

Según el criterio de Ríos (2019) y Ordóñez et al. (2020), el poder entregar una información básica sobre datos personales se ha vuelto una detonante para las personas, ya que no conocen con severidad que tratamiento podrían tener su información desde una computadora, ya sea que se encuentre en la comodidad de un hogar o hasta en la mejor empresa de "confianza", no siendo un desconocer para la sociedad los múltiples ciberataques que realizan hackers o personas maliciosas que han existido desde un comienzo hasta llegar a actualizarse cada vez mejor con equipos altamente sofisticados como se ha observado a lo largo de los años.

Por otra parte, expresa Muñoz et al. (2019), los riesgos tecnológicos no se hicieron esperar a nivel internacional, sin desestimar a los grandes elefantes empresariales como

SolarWinds, FireEye, Equifax, Telefónica y otras que fueron víctima de ataque en el mundo de las vulnerabilidades tecnológicas, de presa fácil para un ciber atacante siendo irónico que para SolarWinds, una empresa que brinda servicios de seguridad e infraestructura tecnológica a más empresas estadounidenses, haya sido un blanco de ataque.

No obstante, rescatando el aporte de valoración de APD (2018) y Ranchal (2020), se debe suponer que los atacantes debieron haber analizado a profundidad la vía de ataque, estando en una situación compleja al enfrentarse a una empresa que brinda seguridad tecnológica. Claramente se puede apreciar que en el mundo tecnológico ni las empresas que brindan mayor seguridad en la información de sus datos podrían asegurar el respaldo total de la información, viéndolo desde ese punto de vista ni WhatsApp podría ser tan seguro con su sistema de encriptación de punto a punto como para que no haya intentado atacar un hacker de sombrero malicioso.

Manteniendo la idea, Holguín & Lema (2019), mencionan que al vivir un mundo completamente digital, las empresas se ven en la necesidad de no solo abastecerse con una infraestructura robusta sino tener una mirada más amplia donde no se vean involucrados los datos y sean expuesto por diferentes riesgos tecnológicos, no proviniendo estos solo de los hackers, sino desde un terremoto donde se encuentra expuesto el servidor de una organización o un ataque de ransomware, hasta que un administrativo de una empresa "XYZ" deje abierta su computadora y exponga sus credenciales de acceso en un membrete pegado a la esquina del computador.

Es por ello que Vaca & Orellana (2020) y Guerra et al. (2021), mencionan que las empresas cada vez mejoran su equipo técnico, para que mediante el análisis que sepan brindar, solidifiquen el área tecnológica considerando a los activos de información que tengan mayor impacto en ser vulnerables respecto a la información que es tratada, ya siendo estas desde las pequeñas, medianas y grandes empresas, y así no poner en riesgo el cumplimiento de sus objetivos.

Por otra parte, Monges & Jiménez (2021), recuerdan brevemente el holocausto que se empezó a vivir a finales del 2019 como; cuarentena, mascarillas, caída de las bolsas de

valores, temor en los negocios, sistemas hospitalarios colapsados, angustia en las personas, cambio de pensamiento forzado, desempleo, educación en tiempos de COVID-19, clases virtuales, entre más angustias que se observó a lo largo de la cúspide del COVID-19 la cual tuvo que enfrentar la humanidad de forma abrupta, donde los profesionales competentes en ciberseguridad tuvieron que redoblar sus esfuerzos para acaparar con la seguridad de todo lo que engloba el hardware y software para su continuidad.

Según Ordóñez et al. (2020), la seguridad de la información en la actualidad, ha sido un tema muy nombrado en el medio común, y en los últimos años aún más, con la llegada del COVID-19 que tuvo a más de una empresa ajustada a la zozobra al escuchar los diferentes robos de información que existían en hospitales, en empresas de telecomunicaciones, entre otras, donde la información ha sido el blanco vulnerable para que los ciber atacantes hagan de las suyas extrayendo los datos a sabiendas de que seguramente se van a lucrar bien del hurto generado.

Por otra parte, según Rosero & Llerena (2021), indican que, en el dominio de los recursos humanos laborales, los empleados tenían que ajustarse a las disposiciones de sus jefaturas, entre las más comunes han sido trasladar su equipo de cómputo al hogar ajustándose al llamado teletrabajo, realizando una conexión directa al internet de su hogar, sin tomar en consecuencia las facilidades que se le brindaba a los hacker al poner en riesgo la información del trabajo, exponiéndola no solo desde un punto de red libre de posibles restricciones, sino realizando análisis desde que Proveedor de Servicio de internet (PSI) tienen los empleados y cuál sería la red más fácil de atacar.

Citando brevemente a las aplicaciones Wireshark y Sniffer entre las más comunes, permitiendo al ciber atacante supervisar el tráfico de Internet en tiempo real y capturar todo el tráfico de datos que entra y sale de un equipo informático.

Siguiendo el hilo de lo anteriormente expuesto según Zuñiga et al. (2021), menciona que, en la misma temporada de la terrorífica pandemia, existieron empresas como las financieras que vieron la forma de mantener siempre a buen recaudo sus bases de datos con la información de los clientes, hasta el principal objetivo que es precautelar, asegurar

y brindar solidez de confianza a sus clientes creyendo que su dinero deberá estar siempre seguro y disponible, todo ello mediante la entrega de una Red Privada Virtual (VPN) a sus empleados desde la comodidad del teletrabajo que se encuentren realizando, permitiendo de cierta forma canalizar y asegurar el tráfico de la información.

Por otra parte, Pazmiño et al. (2020), mencionan que, los riesgos tecnológicos son amenazas que están latentes en el medio digital, desde una Tablet, teléfonos, laptops, smartwatch, UPC, y cualquier dispositivo tecnológico que tenga el servicio de internet trasmitiendo paquetes de datos en las redes, siendo estas herramientas utilizadas en la vida laboral para procesar información, donde las empresas se ven expuestas a grandes consecuencias de amenazas sino ponen atención en el asunto, pudiendo ser afectadas directamente las estrategias y objetivos de ingresos.

De igual forma la revista Forbes EC (2021), indica que, en el caso de Ecuador no fue la excepción en el círculo de las empresas atacadas por ciberdelincuentes como fue la Corporación Nacional de Telecomunicaciones (CNT), donde los hackers secuestraron sus sistemas con la finalidad de liberarlo a cambio de grandes sumas de dinero o bien llamado el término técnico ataque de ransomware.

Siguiendo la idea, respecto a lo que indica la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional República del Ecuador, 2021), en su capítulo VI, artículo 37; seguridad de datos personales, menciona la valoración que deberá brindar el responsable o encargado del tratamiento de datos personales para mantener técnicas de seguridad y respaldo ante cualquier incidente y así precautelar la Confidencialidad Integridad y Disponibilidad (CID) de los datos, adicional deberá realizar constantes pruebas de ataques obteniendo posteriormente un plan de mitigación de riesgos ante las posibles amenazas analizadas.

Metodología

La investigación realizada fue de tipo cualitativa y de corte transversal, el universo de inventario levantado fue de 33 activos de información del sub proceso (b) del área de admisión y nivelación correspondiente a la toma de los exámenes de Odontología de la Institución.

La metodología utilizada fue la ISO 27002:2013, la principal herramienta de apoyo fue Excel y sus diferentes hojas lo que facilitó el análisis, seguido la herramienta tecnológica de análisis de gestión de riesgo PILAR 7.4.9 (25.10.2021), donde se logró insertar los activos de información, y posteriormente se obtuvieron las amenazas.

Cabe mencionar que en primera instancia fue considerada la aplicación PIRANI para los diferentes análisis siendo descartada por no ser una herramienta Open Source. Todos los hallazgos encontrados se plasman en las siguientes tablas, las cuales se explican más adelante.

Tipos de (AI)

Los activos de información fueron categorizados en base al rol que desempeña cada uno de ellos sin subestimar la importancia que tienen para la institución.

Valoración de los activos de información (AI)

Una vez que se realizó el levantamiento de los activos de información, se efectuó la valoración de menor = 1; moderado =2; y mayor =3 analizando la criticidad de cada uno de ellos en base al impacto y afectaciones que podrían causar en la continuidad del negocio sirviendo de apoyo las 3 características básicas que predomina la seguridad de la información, como lo es la Confidencialidad, Integridad y Disponibilidad (CID).

Clasificación del (AI)

Los AI fueron clasificados mediante análisis de la necesidad del negocio; confidencial, de uso interno y público como se describe en la siguiente tabla 1.

Tabla 1

Descripción de la clasificación que se analizó en cada AI

Clasificación	Descripción
Confidencial	Información de alta importancia para la institución, la cual deberá ser bien protegida, por el valor de su data y los diferentes aportes que brinda a la organización. Solo podrá tener acceso el usuario interno autorizado.

Uso interno	Información sensible, interna a áreas o proyectos que se debe tener acceso controlado y solo al usuario interno.
Público	Información que puede ser uso del usuario interno y externo.

Importancia del (AI)

Para obtener la importancia se realizó la suma de la valoración de los AI y seguido a ello se obtuvo el promedio =(C2+I2+D2)/3 el cual dio como resultado valores menores a 3, obteniendo y clasificando la importancia de cada activo de información, observar la tabla 2.

Tabla 2

Descripción de la importancia obtenida de cada AI

Importancia	Descripción	Valor
Grave	En caso de pérdida o difusión no autorizada existe un alto porcentaje de pérdida de objetivos, y estrategias institucionales.	**1**
Importante	En caso de pérdida o difusión no autorizada existe un posible porcentaje de pérdida de la imagen, confianza y reputación institucional.	**2**
Prescindible	En caso de pérdida o difusión no autorizada existe un bajo porcentaje de pérdida de la situación organizacional actual.	**3**

Selección de los AI con importancia grave

Una vez realizado el análisis se consideró los activos con importancia grave para la mitigación de la vulnerabilidad respecto al riesgo encontrado los AI, los cuales se desagregan en los siguientes: UCC-AN-EI-02, se analizó el riesgo que se podría tener en la pérdida de los datos, en caso de que el proveedor del servicio no realice backup de forma periódica sobre la data aun resaltando la confianza y transparencia de su trabajo, UCC-AN-EI-03, el riesgo fue de una posible caída del servicio, donde podría verse afectada la TRIADA CID interrumpiendo la continuidad de los procesos de negocio (matriculación y sincronización con otros sistemas de transferencia de conocimiento docente-estudiante), UCC-AN-EI-04, por consiguiente, el riesgo encontrado fue aplicaciones defectuosas, considerando de que podría ocurrir una desactualización en los

certificados, UCC- AN-AS-14, el riesgo identificado fue; que el proveedor desaparezca ya que no existe una penalidad en el contrato, UCC-AN-AS-15, el riesgo fue; denegación de servicio, ya que los usuarios internos y externos intentan un sin número de ocasiones en acceder a la vez en el mismo dominio como lo es en temporadas de matrículas y de esta forma afecte a la disponibilidad del servicio, UCC-AN-DI-16, el riesgo analizado fue; degradación del rendimiento y la violación de la confidencialidad y acuerdos de privacidad, donde los protocolos de bases de datos puedan permitir el acceso no autorizado a datos, la corrupción o la disponibilidad, UCC-AN-AS-31, el riesgo encontrado fue; certificados desactualizados, pudiendo recaer en inyección de códigos maliciosos, UCC-AN-EI-32, por último, se tiene al activo de información del Servidor UCC-AN-EI-32 donde el riesgo sería; que ataquen a los servidores AWS de la institución mediante sistemas de capturas de credenciales de acceso como el ataque de fuerza bruta y considerando que el administrador de dicho servidor mantenga credenciales de accesos débiles.

Una vez Identificados los AI con riesgo grave los cuales fueron 8, la concentración fue en las amenazas y las vulnerabilidades de los AI.

Análisis e identificación de las amenazas

Para identificar las amenazas se ingresaron los AI apoyados en la aplicación PILAR 7.4.9 (25.10.2021) herramienta con licencia de uso y basada en las normas ISO 27000 y todas sus sub divisiones, esta permitió crear, clasificar, identificar y analizar las amenazas de cada AI creado.

Una vez que fueron creados los AI, se entregó el criterio de valoración calificados del 1 al 10 en la disponibilidad [D], integridad [I], confidencialidad [C], autenticidad de los datos y la información [A], habilidad y servicios de los datos [T], valor [V] y datos personales [DP].

En el activo de información UCC-AN-AS-31, fue analizada la integridad, comprendiéndose qué; sí desde las operaciones técnicas realizan carga de información de alta importancia institucional con errores de fondo, podría verse comprometida la

integridad al estar la información expuesta en la página web institucional de conocimiento público nacional e internacional. Con el mismo criterio fueron analizados todos los AI.

Análisis e identificación de las vulnerabilidades en las amenazas

Una vez encontradas las amenazas, fueron identificadas y analizadas las vulnerabilidades.

Para obtener el análisis de la matriz de valoración de riesgos se definió la importancia de: crítico, alto, relevante, moderado y bajo, con la descripción y políticas en cada una de ellas, así como se explica en la tabla 3.

Tabla 3

Descripción de la tabla de valoración de la matriz de riesgos

Importancia	Descripción	Políticas para la toma de medidas
Crítico	Riesgo no aceptable	**1**
Alto	Riesgo no deseable	**2**
Relevante	Riesgo moderado	**3**
Moderado	Riesgo tolerable	**4**
Bajo	Riesgo aceptable	**5**

Por lo cual, se dio inicio al levantamiento de la matriz de riesgo, como se explica el análisis a mayor énfasis en el apartado de los resultados y discusión.

Resultados

El análisis de los riesgos, amenazas y vulnerabilidades empezó con el levantamiento del inventario de activos de información del sub proceso (b) del área de admisión y nivelación correspondiente a la toma de los exámenes de Odontología de la Institución, donde se obtuvieron 33 AI, los cuales fueron clasificados por tipo de AI, posteriormente se dio el criterio de valor y su importancia mediante la CID donde el 24.32% de AI afectaban a la confiabilidad, el 26.34% afectaban a la integridad y el mismo porcentaje afectaba a la disponibilidad, lo que permitió rescatar el primer resultado de análisis, encontrando 8 AI

de importancia grave los cuales se convirtieron en la mirada de análisis profundo, sin subestimar los restantes.

Por consiguiente, los AI graves fueron analizadas las amenazas y vulnerabilidades teniendo en la primera columna la numeración de los riesgos, le continua el código del AI, le sigue la lista de amenazas, y de igual forma sus vulnerabilidades encontradas.

En las siguientes tres columnas se encuentra la valoración de la CID, en la cual se realizó la suma de cada valor dado en la CID apegados a la tabla 3, y seguido a ello se obtuvo el promedio =(C+I+D)/3 el cual dio como resultado valores menores a 3, obteniendo el impacto del riesgo institucional, todo ello realizando la pregunta ¿Cuál es la probabilidad de que la vulnerabilidad se materialice? dando como resultado la matriz de riesgos.

De igual forma los AI fueron agrupados, ya que, por citar el caso, el activo UCC-AN-AS-14 y UCC-AN-AS-15 son sistemas que cumplen diferentes roles sin dejar de tener las mismas probabilidades de amenazas y vulnerabilidades, agrupándolos como; RG01, RG02, RG03 y RG04, tratándolos más adelante como control de vulnerabilidad cero unos C-V01, control de vulnerabilidad cero dos C- V02, control de vulnerabilidad cero tres C-V03 y control de vulnerabilidad cero cuatro C-V04.

Encontrándose 3 vulnerabilidades de impacto crítico, 3 de impacto alto, 6 relevantes, 12 moderado y 2 bajo, siendo un total de 26 vulnerabilidades a las que se dio tratamiento a cada una de ellas.

Análisis e identificación de controles en las vulnerabilidades

Seguido, se realizó una nueva matriz donde se obtiene el análisis de los resultados finales, teniendo el criterio en la primera columna de; dominio de control, que hace referencia a la clasificación de los controles acorde al dominio dado por la ISO 27002:2013, en la segunda columna se tiene; la categoría de seguridad que hace referencia a la sub clasificación que tiene una categoría de control, en la siguiente columna se encuentra el nombre del control, le sigue la descripción, de igual forma se tiene a los códigos de vulnerabilidades que se ven comprometidos, y por último la adaptación de los controles que se deberá implementar en la institución.

Para poder analizar los controles, se tomó el análisis de agrupamiento de los AI, donde el dominio de control de seguridad física y ambiental recae en las vulnerabilidades de C-V01 que pertenecen a los activos de información UCC-AN-EI-02, UCC-AN-EI-03, UCC-AN-EI-04 y UCC-AN-EI-32 estos generalmente se encuentran en riesgos a daños físico, eléctricos, movimientos telúricos, cambios climáticos severos, mal tratamiento de equipos físicos entre otros que necesitan ser apegados a las buenas prácticas de controles de seguridad física.

De la misma forma, se identificó para los C-V02, C- V03 y C-V04, el dominio de control que es; relación con los proveedores, este pertenece a los activos de información UCC-AN-AS-14, UCC-AN-AS-15, UCC- AN-DI-16 y UCC-AN-AS-31, estos recurrentemente se encuentran expuestos a amenazas de: aplicaciones defectuosas, procesamiento ilegal de datos, manipulación de la información, error en la utilidad del software, abuso de derecho, errores de mantenimiento y actualizaciones de programas de software, desactualización de certificados, avería de origen físico o lógico, difusión de software dañino, robo o manipulación del activo, entre varias, que requieren ser aplicados ciertos controles que hacen referencia a relación con los proveedores.

De igual manera, para los mismos agrupamientos de los activos de información C-V02, C-V03 y C-V04 se identificaron dos dominios más, que hace referencia a control de acceso y a la seguridad en la operativa.

Ajustando a la política un total de 45 controles que deberán ser aplicados en la institución, observar la tabla 4.

Tabla 4

Detalle de los dominios y número de controles

Dominio	Número de controles
Seguridad Física y ambiental	14
Relación con los Proveedores	5
Control de acceso	14
Seguridad en la Operativa	12

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 46 – 62, noviembre 2023

Conclusiones

Una vez realizado el análisis de los activos de información, riesgos, y aplicar los controles en cada vulnerabilidad de las amenazas, se puede concluir en lo siguiente:

- Teniendo presente todo el procedimiento del análisis, este podría servir de apoyo para encontrar la matriz de riesgos en otras áreas de la universidad.
- Al momento de identificar los controles de la ISO 27002:2013, se debe ser muy asertivo para tomar los controles necesarios en una vulnerabilidad específica, más no es necesario adicionar un sinnúmero de controles que no benefician directamente a la vulnerabilidad, ya que podría desviar el foco de los controles de mayor importancia para atacar dicha vulnerabilidad.
- Dentro de las bondades que la herramienta PILAR aportó, fue el amplio abanico de categorizaciones específicas que tiene en el criterio de valor, entregando las amenazas de forma desagregadas.
- La alma mater, actualmente se ha mantenido participando en diferentes rankings internacionales como; webometrics, lo que le ha permitido escalar 3 puesto a favor de 28 al 25, llegando a concluir que la institución constantemente generan acciones para escalar posiciones de excelencia académica, manteniendo firme sus procesos, procedimiento, políticas y manuales que implementa en cada una de sus dependencias, sumando de apoyo a su crecimiento académico, los 45 controles de análisis de vulnerabilidades que son expuestos en el presente estudio.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses en relación con el artículo presentado.

Referencias bibliográficas

APD. (2018, julio 06). 10 empresas afectadas por ciberataques que no imaginarías. https://www.apd.es/empresas-afectadas-por-ciberataques/

Asamblea Nacional República del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Fernández, E., & Ascón, W. (2021). B-Learning. Vía para la preparación en seguridad informática del docente del Politécnico "Julio Antonio Delgado Reyes". EduSol, 21(75), 1-13. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1729-80912021000200016

Forbes EC. (2021, julio 22). Hackeo a CNT genera problemas en la facturación. https://www.forbes.com.ec/negocios/hackeo-cnt-genera-problemas-facturacion-n6763

Guerra, E., Neira, H., Díaz, J., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. Información tecnológica, 32(5), 145-156. https://doi.org/10.4067/S0718-07642021000500145

Holguín, F. Y., & Lema, L. M. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. Revista lbérica de Sistemas e Tecnologias de Informação, 31, 1-17. https://pdfs.semanticscholar.org/e0f8/cf42af8483db9a94996326d630888404d72d.pdf

Monges, M. R., & Jiménez, V. E. (2021). Seguridad de la información en plataformas e-learning en tiempos de pandemia COVID-19. Revista UNIDA Científica, 4(1), 1-13. https://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/9

Muñoz, H., Zapata, L. G., Requena, D. M., & Ricardo, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. Revista Venezolana de Gerencia, 2, 528-541. https://www.redalyc.org/articulo.oa?id=29063446029

Ordóñez, K. G., Garcia, D., Erazo, C. A., & Erazo, J. C. (2020). Impacto del COVID-19 en Educación Superior: Universidad Católica de Cuenca. Revista Arbitrada Interdisciplinaria Koinonía, 5(1), 221-245. https://doi.org/10.35381/r.k.v5i1.781

Ordóñez, K., Guaña, J., García, D., Naranjo, D., & Bonilla, C. (2020). Análisis del uso de los recursos en la plataforma virtual de enseñanza aprendizaje. Revista Ibérica de Sistemas e Tecnologias de Informação(E32), 126-136. https://www.proquest.com/openview/5d92effec869242e21f7c8d9376e034d/1?pq-origsite=gscholar&cbl=1006393

Pazmiño, C. A., Serrano, A. K., & González, M. M. (2020). Las Tics como herramienta para la gestión de riesgos. Revista Científica Mundo de la Investigación y el Conocimiento, 4(1), 173-181. https://doi.org/10.26820/recimundo/4.(1).esp.marzo.2020.173-181

Ranchal, J. (2020, diciembre 30). Los 10 peores incidentes de ciberseguridad en 2020. https://www.muycomputer.com/2020/12/30/ciberseguridad-en-2020/

Ríos, E. E. (2019). SGSI bajo el marco normativo ISO 27001 en el proceso de control de accesos para una empresa: una revisión científica de los ultimos 9 años. [Trabajo de investigación, Universidad Privada del Norte, Lima - Perú]. https://repositorio.upn.edu.pe/bitstream/handle/11537/26449/Trabajo%20de%20Investigación_Total.pdf?sequence=2&isAllowed=y

Rosero, L. F., & Llerena, J. (2021). El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático. [Tesis de grado, Universidad Politécnica Salesiana, Ecuador]. https://dspace.ups.edu.ec/handle/123456789/21699

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 46 – 62, noviembre 2023

Vaca, A. J., & Orellana, I. (2020). Análisis de riesgo financiero en el sector de fabricación de otros productos minerales no metálicos del Ecuador. Revista Economía y Política(32), 1-43. https://doi.org/10.25097/rep.n32.2020.05

Zuñiga, A. R., Jalón, E. J., Andrade, M. E., & Giler, J. L. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19. Revista Universidad y Sociedad, 13(3), 454-459. http://scielo.sld.cu/scielo.php?pid=S2218-36202021000300454&script=sci_arttext&tlng=en

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 46 – 62, noviembre 2023