Vol.7 No.3 (2023): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.7.3.2023.2793-2808

Information security risk analysis in the recruitment process of a Higher Education Institution in Ecuador, based on ISO 27002 Annex A domain 7.

Análisis de riesgos de seguridad de la información en el proceso de contratación de personal en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7.

Autores:

Arpi-Saquipay, Wilmer Alexander
UNIVERSIDAD CATÓLICA DE CUENCA
Egresado de la Carrera de Software
Cuenca – Ecuador
wilmer.arpi@est.ucacue.edu.ec
https://orcid.org/0009-0003-0699-3752

Cajamarca-Criollo, Olger Antonio
UNIVERSIDAD CATÓLICA DE CUENCA
Docente de la Carrera de Software
Cuenca –Ecuador
ocajamarcac@ucacue.edu.ec
https://orcid.org/0000-0001-8958-584X

Citación/como citar este artículo: Arpi-Saquipay, Wilmer Alexander., Y Cajamarca-Criollo, Olger Antonio. (2023). Análisis de riesgos de seguridad de la información en el proceso de contratación de personal en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7. MQRInvestigar, 7(3), 2793-2808.

https://doi.org/10.56048/MQR20225.7.3.2023.*2793-2808*

Fechas de recepción: 22-JUL-2023 aceptación: 22-AGO-2023 publicación: 15-SEP-2023

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

El proceso de contratación de personal para una institución u organización hoy en día es muy importante, debido a que durante este procedimiento se podrá conocer habilidades, capacidades y destrezas, con la finalidad de entender si una tercera persona podrá contribuir de manera positiva a una entidad; considerando en este caso que, los contratados garanticen la seguridad de la información al ser instruidos sobre sus funciones antes, durante y tras el cambio o cese del trabajo. Previo a la aplicación del instrumento para la recolección de los datos se hace una revisión bibliográfica sobre la seguridad de la información considerando la ISO 27002, posteriormente se conceptualiza la triada de la seguridad de la información, la ISO 27001/27002 y del Anexo A el dominio 7. En la presente investigación se empleó una metodología cuantitativa para analizar el riesgo de la seguridad de la información en el proceso de contratación. Los resultados obtenidos dejan en evidencia que el análisis de los controles de la ISO 27002 permiten conocer en qué situación se encuentra y cuales están en riesgo, es decir cuáles se deben mejorar para alcanzar el nivel óptimo logrando salvaguardar la seguridad de la información durante todo el proceso de contratación.

Palabras clave: seguridad de la información, ISO 27002, recursos humanos, análisis de riesgos.

Abstract

The process of hiring personnel for an institution or organization today is very important, because during this procedure it will be possible to know skills, capabilities and abilities, in order to understand whether a third person can contribute positively to an entity; considering in this case that the hired persons ensure information security by being instructed on their functions before, during and after the change or termination of the job. Prior to the application of the instrument for data collection, a bibliographic review is made on information security considering ISO 27002, then the triad of information security is conceptualized, ISO 27001/27002 and Annex A domain 7. In this research a quantitative methodology was used to analyze the risk of information security in the hiring process. The results obtained show that the analysis of the ISO 27002 controls allows to know in which situation the company is and which ones are at risk, that is, which ones should be improved to reach the optimum level, thus safeguarding the information security during the whole contracting process.

Keywords: information security, ISO 27002, human resources, risk analysis.

Introducción

Actualmente, la instituciones u organizaciones públicas o privadas utilizan diferentes tipos de activos tales como información, mobiliario, equipos de computación, sistemas de redes y comunicaciones, etc.; por tal motivo, es vital considerar que la información es un recurso valioso y por ello es necesario protegerla. Según Baca (2016) para una organización la información es lo más importante; no obstante, esta en riesgo de sufrir daños o ser objeto de robo, lo que podría llevar a la interrupción de sus funciones o actividades.

A nivel internacional, específicamente en España, el estudio realizado por la INTECO (Instituto Nacional de Tecnologías de la Comunicación) en cuanto a la seguridad de la información la INTECO (2012) expone que las organizaciones para garantizar en los dispositivos la seguridad de la información utilizan un paquete de soluciones tales como antivirus, antisepsias, cortafuegos, antispam, eliminación de archivos temporales, pin, contraseñas y cookies. Además, establece que aparte de poseer los recursos técnicos para la seguridad de la información, es importante contar con empleados que realicen una buena gestión de los recursos antes mencionados, con el objetivo de mantener y mejorar la seguridad de la información de las instituciones u organizaciones.

A nivel regional en Cuba, se llevó a cabo una investigación por Navarro y Reyes (2021) quienes afirman que los activos más importantes de toda entidad son la información y los sistemas y para salvaguardarlos se basan en la norma ISO (Organización Internacional de Normalización) específicamente en la 27001, ya que esta ayudará a evitar que las amenazas se materialicen sobre los bienes informáticos, también consideran al departamento de talento humano como imprescindible porque es el personal encargado desde antes de la contratación hasta la finalización del empleo, pues tienen el deber de hacer conocer a las personas sus responsabilidades y obligaciones en relación a la seguridad de la información. En Colombia se realizó una investigación por Cano y Almanza (2019), quienes argumentan que las instituciones realizan inversiones para la protección de la seguridad de la información enfocada en la tecnología, soporte y mantenimiento; así como la contratación de terceros o contratados, que deben estar capacitados para detectar y afrontar posibles amenazas, que sepan incorporar prácticas de gestión seguras de la información a todos los colaboradores de las organizaciones o instituciones pues son estos quienes deben generar confianza a los diferentes grupos de interés.

A nivel nacional, en una indagación realizada por Flores y Caiza (2017) se expone que para garantizar la seguridad de la información se debe asociar al recurso humano porque es el encargado de cumplir las políticas y los procedimientos, desde la contratación hasta que finalice el mismo proceso con la persona contratada y para ello toman como referencia la ISO 27002, debido a que en este framework se encuentran los controles dentro del anexo 7 para la seguridad de la información ligada a los recursos humanos. Cabe mencionar que,

mediante su uso, se crea la posibilidad de mantener al personal informado desde antes de su ingreso, durante y termino de contrato; lo que facultará evitar fraudes, robo de información y problemas legales.

Con base a los estudios presentados es necesario considerar que, en una era digital cada vez más interconectada, proteger la seguridad de la información se ha convertido en una prioridad esencial para las instituciones u organizaciones. Es importante considerar el área de Recursos Humanos por su complejidad en el manejo de datos confidenciales, por su responsabilidad en la contratación y gestión del personal. Consciente de esta importancia, la institución educativa superior ha reconocido la necesidad de fortalecer su sistema de seguridad de la información en el ámbito de los recursos humanos para la contratación de su personal. El presente trabajo de investigación se centra en abordar los desafíos de seguridad de información que afronta dicho departamento de la institución para garantizar la protección de sus activos y la integridad en los procesos de contratación y liquidación, en busca de implementar medidas preventivas para la gestión integral de riesgos. Siguiendo las directrices de la normativa ISO 27002, ampliamente reconocida como el estándar internacional para la gestión de la seguridad de la información, el Anexo A dominio 7 se presenta como la guía clave para llevar a cabo el análisis de riesgos. Este proceso resulta imprescindible para identificar vulnerabilidades, evaluar amenazas y comprender los posibles impactos en los activos y operaciones de la organización.

Conceptos relacionados

Seguridad de la información

De acuerdo a Valencia-Duque y Orozco-Alzate (2017) la seguridad de la información es un activo estratégico de cualquier entidad que tiene como objetivo mantener a salvo la información a través de una adecuada toma de decisiones para controlar y salvaguardar todos los datos que se manejen dentro de la organización. En la misma línea, Soriano (2014) menciona que la seguridad de la información es el proceso que garantiza la protección de datos confidenciales y los sistemas de información de un acceso, uso, divulgación, lectura, modificación, registro o destrucción no autorizada de datos y ante las posibles amenazas, dado que la seguridad de la información abarca servicios importantes como la confidencialidad, integridad y disponibilidad.

Tríada de la confidencialidad, integridad y disponibilidad

Según Soriano (2014) la seguridad de la información presenta tres pilares básicos a manera de servicios de seguridad siendo la confidencialidad, integridad y disponibilidad mismos que son conocidos como la tríada de la seguridad de la información cuyo objetivo es centrase en la seguridad de datos. Briceño (2021) expone que la confidencialidad es la capacidad de proteger los datos de terceros que no están autorizados para verlos; en cuanto a la integridad es la capacidad preservar que los datos se modifiquen o cambien de manera no autorizada; y la disponibilidad es la capacidad de acceder a los datos cuando lo requiera.

Figura 1

Triada de la seguridad de la información

Nota: La figura muestra los conceptos principales en seguridad de la información. Fuente: Soriano (2014).

ISO 27001

Monsalve et al. (2014) exponen que la ISO 27001 es una norma para implementar un sistema de gestión de seguridad de la información considerando las leyes y los reglamentos, así como la preocupación de la privacidad de datos, pues su rol es identificar las amenazas, el análisis de riesgo y razonamiento de seguridad. Además, la ISO 27001 es adaptable y altamente flexible logrando proporcionar estrategias, mecanismos y controles para implementar un adecuado sistema de seguridad de la información para cualquier organización o institución (Muyón et al., 2019).

ISO 27002

Calder (2017) manifiesta que la ISO 27002 de denomina Tecnología de la información - Técnica de seguridad - Código de prácticas para la gestión de la seguridad de la información, la cual ofrece buenas prácticas acerca del propósito e implementación de los diversos controles que se encuentran en el Anexo A, sin embargo, no es necesario utilizar todos, se puede usar el que más se acerque a la planificación de la organización. Por su parte, Valencia-Duque y Orozco-Alzate (2017) exponen que la ISO 27001 requiere del uso de la 27002 como fuente de orientación porque esta abarca el Anexo A con 114 controles, 35 objetivos de control y 14 dominios de seguridad de la información, de manera que puede contribuir a las organizaciones a seleccionarlos para implementar un sistema de seguridad de la información.

Anexo A: dominio 7 seguridad ligada a los recursos humanos

Navarro y Reyes (2021) sostienen que el objetivo del presente dominio es educar e informar a los empleados de una institución u organización desde su incorporación y de manera continua sobre las medidas de seguridad que puedan afectar al pleno desarrollo de sus

funciones y dificultar la confidencialidad. López (2023) argumenta que en el dominio 7 se puede evidenciar la Seguridad ligada a los recursos humanos, mismo que tiene tres objetivos de control. El primero se denomina antes de la contratación y contiene dos controles, el segundo se denomina durante la contratación y tiene tres controles y el tercero se llama cese o cambio del puesto de trabajo y presenta un control.

1. **Antes de la contratación:** es el objetivo que garantiza que todos los colaboradores de una institución u organización entiendan sus responsabilidades y para que puedan desarrollar sus funciones fortaleciendo la seguridad de la información. Dentro de este se encuentra el control sobre la *investigación de antecedentes*, en donde se debe verificar la información de los aspirantes en relación a las regulaciones, ética y leyes establecidas por la organización. Y el control de *términos y condiciones de contratación*, es un proceso que obliga a los colaboradores y a los contratistas a aceptar y firmar los términos y condiciones del trabajo (López, 2023).
2. **Durante la contratación:** es el objetivo que verifica que tanto los contratados como los contratistas cumplan sus responsabilidades con eficiencia garantizando la seguridad de la información. En el presente objetivo se evidencia el control de *responsabilidades de gestión*, en el cual el departamento encargado deberá exigir a todo el personal considerar las políticas y los procedimientos para mantener la información segura. El segundo control es la *concienciación, educación y capacitación en sí*, en el cual los empleados y contratistas requieren de una formación regular tomando en cuenta las políticas de la organización. Y el control sobre el *proceso disciplinario*, trata sobre la existencia de un comunicado formal a todo el personal para que promuevan la seguridad de los datos (López, 2023).
3. **Cese o cambio de puesto de trabajo**: este objetivo busca proteger los intereses de la entidad tras el cambio o la finalización del empleo. En este objetivo se presenta el control de *cese o cambio de puesto de trabajo*, el cual define con claridad las responsabilidades luego de la desvinculación del puesto de trabajo (López, 2023).

Material y métodos

La presente investigación se basó en la metodología cuantitativa, con un diseño descriptivo y como instrumento de medición se empleó una encuesta. Tal como lo menciona, Cárdenas (2018) la investigación cuantitativa ayuda a conocer de manera minuciosa la medición de la variable, ya que la información se puede obtener mediante diversas técnicas, de manera que esta al ser transformada en números permite al investigador responder a interrogantes. Por su parte, Guevara et al. (2020) manifiestan que una investigación al ser descriptiva proporciona características, análisis e interpretación de los datos, con la finalidad de proporcionar a los lectores información verídica, debido a que la información es observable y verificable. Para este estudio se utilizó una encuesta cerrada y de acuerdo a Hernández-Sampieri y Mendoza (2020) utilizarla facilita al investigador conocer la opinión del encuestado en relación a un tema determinado y sirve para recabar información, al estar previamente ya diseñada como

ventaja de la encuesta cerrada se menciona que la información puede ser cuantificable, además a los encuestados se les facilita entender y responder porque no tienen que verbalizar o escribir sus pensamientos. La encuesta constaba de 29 preguntas en total distribuidas en tres objetivos de control y cada uno de ellos subdividido en controles con preguntas específicas para evaluar diferentes aspectos de seguridad y para su desarrollo se contó con la partición del personal de recursos humanos, teniendo para ello una población de 12 personas y como muestra 8 personas.

Resultados

Tabla 1
Métricas de análisis de riesgo significado y valor

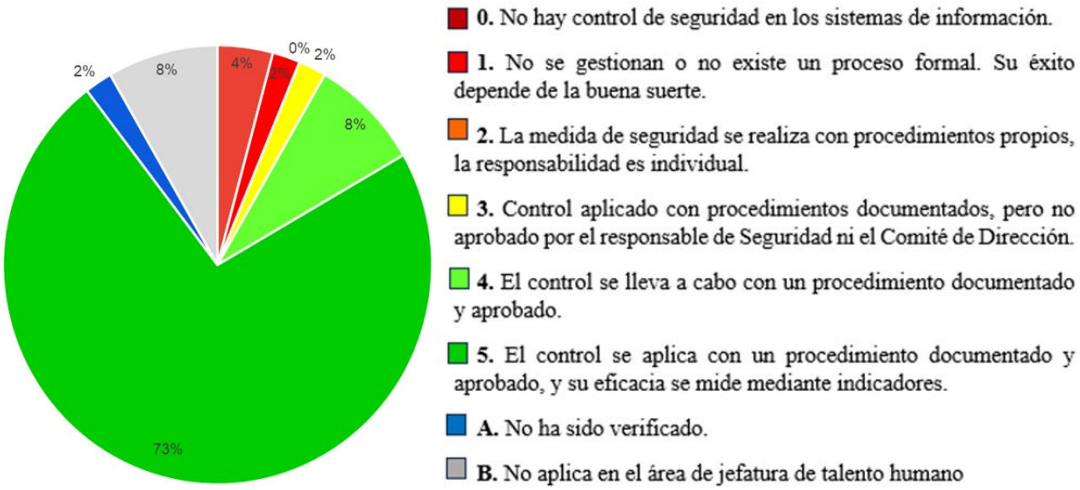
Estado	Significado	Valoración
Inexistente	No hay control de seguridad en los sistemas de información.	0
Inicial	No se gestiona o no existe un proceso formal. Su éxito depende de la buena suerte.	1
Repetible	La medida de seguridad se realiza con procedimientos propios, la responsabilidad es individual.	2
Definido	Control aplicado con procedimientos documentados, pero no aprobado por el comité de Seguridad ni el comité de dirección.	3
Administrado	El control se lleva acabo con un procedimiento documentado y aprobado.	4
Optimizado	El control se aplica con un procedimiento documentado y aprobado, y su eficiencia se mide mediante indicadores.	5
Desconocido	No ha sido verificado.	A
No aplicable	No aplica en el área de jefatura de talento humano.	B

Nota: Elaboración propia

La tabla 1 muestra los niveles de control conjuntamente con su significado y valoración de esta manera se podrá evaluar y analizar la seguridad de la información.

Figura 2

Control investigación de antecedentes



Nota: Elaboración propia

La figura 2 nos muestra que un porcentaje reducido (2%) refleja un estado inexistente, sin implementación de controles de seguridad. De la misma manera otro grupo (4%) considera el estado inicial, indicado una gestión no formalizada. Así mismo otro grupo (8%) opta por Administrado, señalando que la implementación de controles se lleva a cabo mediante procedimientos aprobados. Sin embargo, la opción preponderante es optimizado (73%), indicando una perspectiva mayoritariamente positiva sobre la eficiencia y gestión efectiva de la seguridad teniendo los procedimientos documentados y medición de indicadores. Un pequeño porcentaje (2%) describe como desconocido mientras otro (8%) indica que el controlo no son aplicables en el área de jefatura de talento humano.

Figura 3

Control términos y condiciones de contratación

Nota: Elaboración propia

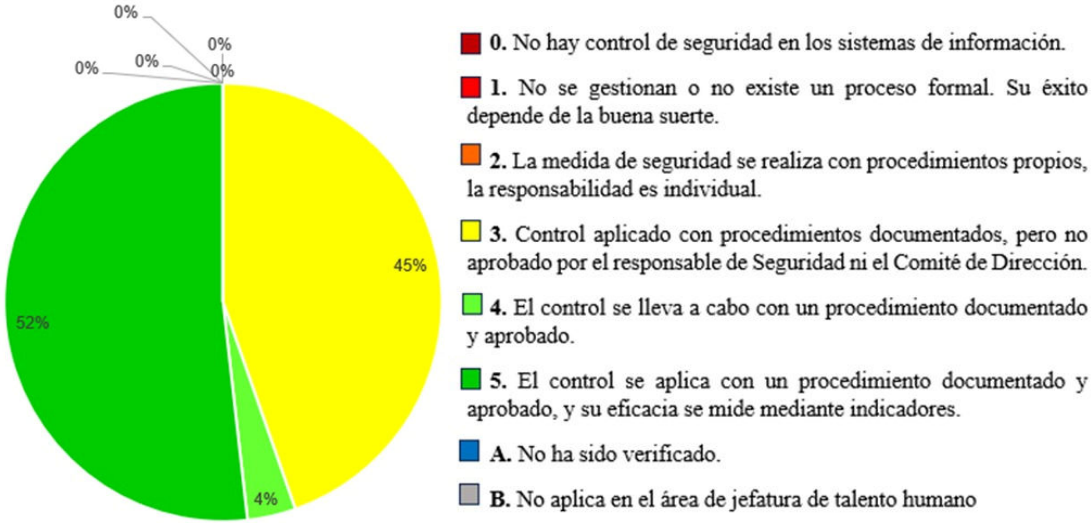
La figura 3 muestra que los estados Inexistentes, inicial, Definido, Administrado, Desconocido, No aplicable, no recibieron respuestas en la encuesta, representado un (0%) de selección en cada caso. Esto indica que estas categorías no fueron consideradas como opciones de respuesta. A diferencias el estado repetible obtuvo un (3%) de elección, mientras que el optimizado fue la opción preferida por (el 91%) de los encuestados. Esto refleja un conocimiento claro sobre el control llevado procedimientos documentados y medición de indicadores.

Figura 4
Control responsabilidades de gestión

Nota: Elaboración propia

La figura 4 ilustra que los estados inexistente, inicial, repetible, desconocido, no aplicable no obtuvieron respuestas en la encuesta representado un (0%), Por otro lado, el estado definido recibió un 3% de elección, mientras que administrado fue seleccionado por el (18%) de los encuestados. La opción más elegida fue optimizada con un (70%) de la respuesta, esto destaca una percepción mayoritariamente positiva sobre la eficiencia indicado que el control se lleva con procedimientos documentados y aprobados.

Figura 5
Control concienciación, educación y capacitación de SI.



Nota: Elaboración propia

La figura 5 muestra las únicas opciones de respuesta que fueron tomadas en cuenta son definido seleccionada por el (45%) de los encuestados indicando que un porcentaje considerable indica que el control aplica con procedimientos documentados, pero no aprobados. Por otro lado, la opción administrada obtuvo un (4%) de selección. Sin embargo, la opción más destacada fue optimizado elegida por un (52%), esto resalta que la mayoría del personal de jefatura de talento humano comprende el control de manera óptima.

Figura 6

Control proceso disciplinario

Nota: Elaboración propia

La figura 6 presenta entre las opciones e indica que la alternativa definida fue seleccionada por un (9%) de los encuestados, mientras que administrado obtuvo un (3%). Por otro lado, la opción optimizada destaco al ser elegida con un (47%) esto indica una percepción mayoritaria sobre la eficiencia de los procedimientos en este control. Además, la opción desconocida

obtuvo un (3%) mientras que no aplicable fue seleccionado con un (38%) por los encuestados, esto indica que para una parte significativa este control no se lleva a cabo en el área de jefatura de talento humano.

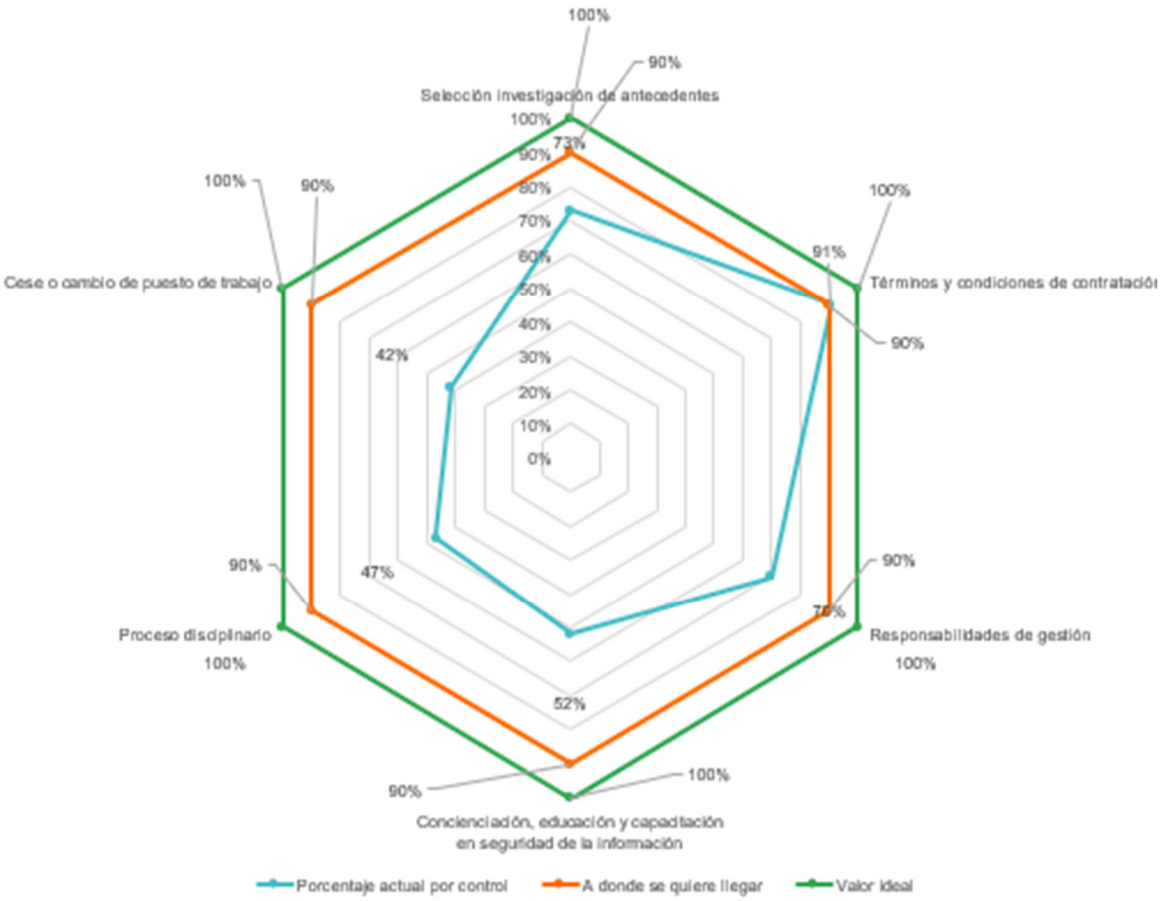
Figura 7
Control cese o cambio de puesto de trabajo

Nota: Elaboración propia

La figura 7 refleja que la opción Administrado es seleccionado por un 8% de los encuestados, y la opción optimizado elegida por un 42% de las personas. Además, la alternativa no aplicable fue seleccionado con un (52 %) esto indica que para la mitad de los de los encuestados el control no se aplica en el área de jefatura de talento humano

Análisis de los Resultados

Figura 8
Controles de la seguridad de información Anexo A dominio 7 – Seguridad ligada a los recursos humanos



Nota: Elaboración propia

La grafica presente indica el análisis de los datos sobre los controles de seguridad de la información en el área de recursos humanos reflejando un porcentaje actual y un objetivo aspirado en diferentes etapas. Se observa que, aunque ciertos controles, como términos y condiciones de contratación se encuentra en un nivel alto de cumplimiento (91%) existe controles como la concienciación, educación y capacitación en seguridad de la información (52%) y el proceso disciplinario (47%) que tienen margen para mejorar. La implementación actual de los controles varía, con porcentajes como (73%) en selección e investigación de antecedentes y (42%) en cese o cambio de puesto de trabajo. El objetivo ideal es alcázar el 100% de cumplimientos en todos los controles de esa manera se puede asegurar una gestión sólida y completa, salvaguardando la seguridad de la información durante todo el proceso.

Discusión

El análisis total de los resultados obtenidos en la evaluación de los controles de seguridad de la información en el marco de la jefatura de talento humano recalca tanto los logros alcanzados como las áreas con potencial para mejoras significativas. Los datos muestran que existe un éxito notable en diversos aspectos, como es el control de "Términos y condiciones

de contratación", donde se tiene un cumplimiento importante del 91%, lo que indica una efectiva implementación de medidas de seguridad. No obstante, este análisis también pone de manifiesto la necesidad de enfocar la atención en otros controles, como la "Concienciación, educación y capacitación en seguridad de la información" y el "Proceso disciplinario", donde los porcentajes de implementación son del 52% y 47% respectivamente. Estos hallazgos subrayan la importancia de abordar la seguridad de la información de manera integral y en todas las fases del ciclo de empleo. Al fijar metas aspiradas, como la obtención del 100% de cumplimiento en todas las áreas, debido a que se establece un compromiso sólido con la protección de la información y la consolidación de una cultura organizacional enfocada en la seguridad. En última instancia, esta discusión refleja la relevancia de un enfoque estratégico y holístico para garantizar la integridad, disponibilidad y confidencialidad de la información, de la institución al mismo tiempo que se resalta la necesidad de la mejora continua en todas las esferas de la jefatura de talento humano.

Conclusiones

El análisis de riesgo de seguridad de la información en el proceso de contratación del personal en la institución de educación superior en Ecuador utilizando la norma ISO 27002, los niveles de control antes de la contratación, durante la contratación y cese o cambio de puesto de trabajo en el ámbito de recursos humanos resalta la importancia de contar con procedimientos concretas para proteger la información sensible y los datos en el proceso de gestión del personal. La norma ISO 27002 se enfatiza como una guía valiosa en esta área, ya que ofrece un marco reconocido a nivel internacional para establecer y mejorar los controles de seguridad. En este caso específicamente, del Anexo A el dominio 7 de la ISO 27002, centrado en la seguridad de los recursos humanos, teniendo relevancia al considerar los aspectos críticos de selección, concienciación, educación y gestión del personal en relación a la seguridad de la información. Este análisis resalta la necesidad de adoptar y mejorar los controles de seguridad en cada etapa, desde la selección hasta el cese del empleo, asegurando que las medidas sean apropiadas y eficaces para minimizar los riesgos y salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas de información. En este contexto, la implementación e integración a la norma ISO 27002 se rige como un enfoque estratégico para fortalecer los controles y establecer una cultura solida de seguridad en el ámbito de recursos humanos.

Referencias bibliográficas

Baca, G. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria. https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=copyright#v=onepage&q&f=false

Briceño, E. (2021). *Seguridad de la información*. Editorial Área de innovación y desarrollo, S.L. https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Calder, A. (2017). *ISO27001/ISO27002: una Guía de Bolsillo.* IT Governance Publishing. https://www.proquest.com/legacydocview/EBC/5255172?accountid=61870.

Cano, J. y Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000–2018. *Revista Ibérica de sistemas e Tecnologías de Informação,* (27), 470-483. https://www.proquest.com/openview/91b5a2323f58400389c80c48e01aa42d/1?pq-origsite=gscholar&cbl=1006393

Cárdenas, J. (2018). Investigación cuantitativa. trAndeS – Programa de Posgrado en Desarrollo Sostenible y Desigualdades Sociales en la Región Andina. https://refubium.fu-berlin.de/bitstream/handle/fub188/22407/Manual_Cardenas_Investigaci%c3%b3n.pdf?sequence=5&isAllowed=y

Guevara, G., Verdesoto, A. y Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). RECIMUNDO, 4(3), 163-173. https://www.recimundo.com/index.php/es/article/view/860/1363

Hernández-Sampieri, R. y Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Mcgraw-hill. https://d1wqtxts1xzle7.cloudfront.net/64591365/Metodolog%C3%ADa_de_la_investigaci%C3%B3n._Rutas_cuantitativa__cualitativa_y_mixta-libre.pdf?1601784484=&response-content-disposition=inline%3B+filename%3DMETODOLOGIA_DE_LA_INVESTIGACION_LAS_RUTA.pdf&Expires=1692614045&Signature=QRrFd6jsxHYWU0mKRWskM~J9dYBHy

INTECO. (2012). *Estudio sobre seguridad de la información y continuidad de negocios en las empresas españolas.* Ministerio de Industria, Energía y Turismo. https://www.ismsforum.es/ficheros/descargas/estudioseguridadempresas1364380074.pdf

López, A. (2023). Anexo 7. *Iso2700.ES.* https://www.iso27000.es/iso27002_7.html

Monsalve-Pulido, J, A., Aponte-Novoa, F. A., y Chaves-Tamayo, D. F. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Revista Facultad de Ingeniería, 23* (37), 65-72. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007&lng=en&tlng=es

Muyón, C., Guarda, T., Vargas, G., y Quiña, G. N. (2019). Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. *Revista Ibérica de Sistemas e Tecnologias de Informação,* (18), 310-317.

https://www.proquest.com/openview/f4b193b46ccb16a251428b15a52d084a/1?pq-origsite=gscholar&cbl=1006393&fbclid=IwAR2fWazgmkeaQCr4THta3-zOrr3pUOOwGE97z54RJ83SzB3r8tr0JNw1DiE

Navarro, M. y Reyes, D. (2021). Procedimientos de seguridad informática relativos a los recursos humanos. *Serie Científica de la Universidad de las Ciencias Informáticas, 14*(7), 108-122. https://dialnet.unirioja.es/servlet/articulo?codigo=8590661

Soriano, M. (2014). *Seguridad en redes y seguridad de la información.* Improved. https://psm.fei.stuba.sk/pages/47/Seguridad_de_Red_e_Informacion.pdf

Flores, C. y Caiza, E. (2017). Concientización como factor crítico para la gestión de la seguridad de la información. *Revista Killkana Técnica, 1*(3), 1-8. https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/issue/view/12/pdf%20V1%20N3

Valencia Duque, F. y Orozco Alzate, M. (2017). Metodología para la implementación de la un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de sistemas e Tecnologías de Informação,* (22), 73-88. https://pdfs.semanticscholar.org/ff97/978e09c5bc3f1ca826017e9f34490d4e5c19.pdf

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.