Revista Conectividad
Enero - junio 2023 *ISSN:2806-5875*
pp. 38-49 *Correo: revista@ister.edu.ec*
Volumen 4, Número 1

Evaluación del nivel de seguridad informática desplegado en los institutos de educación superior de la red RIT II

Evaluation of the level of IT security deployed in the higher education institutes of the RIT II network.

Gerardo Cajamarca Mendez[1], Mario Giovanny Ron Gavi[2], Patricio Tomas Chamorro Ruiz[3], Carlos Andrés Genovez Tobar[4]

[1]Instituto Tecnológico Universitario Rumiñahui, gerardo.cajamarca@ister.edu.ec, Sangolquí, Ecuador.
[2]Instituto Tecnológico Universitario Rumiñahui, mario.ron@ister.edu.ec, Sangolquí, Ecuador.
[3]Instituto Tecnológico Universitario Rumiñahui, patricio.chamorro@ister.edu.ec, Sangolquí, Ecuador.
[4] Instituto Tecnológico Universitario Rumiñahui, carlos.genovez@ister.edu.ec, Sangolquí, Ecuador.

Autor para correspondencia: gerardo.cajamarca@ister.edu.ec

Fecha de recepción: octubre 2022 ***Fecha de aceptación:*** diciembre 2022

RESUMEN

El objetivo de la presente investigación es determinar una línea base sobre la realidad de la seguridad de la información (SI) en los institutos de educación superior de la red RIT II, para lo cual se analizó la información obtenida mediante la aplicación de una evaluación basada en buenas prácticas relacionadas al nivel de seguridad de la información. El objetivo es identificar las vulnerabilidades que presentan los institutos y categorizarlas de acuerdo a su nivel de riesgo, de esta manera poder establecer una adecuada gestión y posterior tratamiento con la elaboración de políticas y controles que permitan minimizar el impacto en caso de producirse un evento de seguridad. Se aplicó el método deductivo y la investigación de exploración para examinar la información obtenida de las encuestas generadas utilizando el marco de referencia ISO / IEC 27001:2013 – 27002:2013. Este análisis pudo determinar las vulnerabilidades más críticas a las que se encuentran expuestas las instituciones educativas objeto del presente estudio, evidenciado que el índice de seguridad de las instituciones analizadas es medianamente aceptable en sus objetivos de seguridad, así como la falta adopción de marcos de seguridad referenciales, elevando el riesgo de afectación de los incidentes de seguridad.

Palabras clave: Seguridad tecnológica, políticas de seguridad, institutos tecnológicos superiores de Ecuador, identificación de vulnerabilidades, análisis de riesgo.

ABSTRACT

The objective of this investigation is to determine a baseline on the reality of information security (SI) in the institutes of higher education of the RIT II network, for which the information obtained through the application of an evaluation based on good practices related to the level of information security was analyzed. The objective is to identify the vulnerabilities presented by the institutes and categorize them according to their level of risk, in order to establish an adequate management and subsequent treatment with the development of policies and controls to minimize the impact in case of a security event. The deductive method and exploratory research were applied to examine the information obtained from the surveys generated using the ISO/IEC 27001:2013 – 27002:2013 framework. This analysis was able to determine the most critical vulnerabilities to which the educational institutions under study are exposed, evidencing that the security index of the analyzed institutions is moderately acceptable in their security objectives, as well as the lack of appropriation of referential security frameworks, raising the risk of security incidents.

Key words: Technological security, security policies, higher technological institutes of Ecuador, identification of vulnerabilities, risk analysis.

INTRODUCCIÓN

Las posibilidades de acceso al conocimiento el día de hoy, no quedan limitadas a los ámbitos locales donde las personas habitan, sino que su alcance se expande al mundo gracias al Internet(Suárez and Najar 2014), en este contexto las tecnologías de las información y telecomunicaciones (TIC) juegan un rol importante en la educación gracias al aporte de recursos que facilitan la interacción de los involucrados en el ecosistema educativo (alumnos y docentes), generando un valor agregando en cuanto a usabilidad y pedagogía en este entorno. (Suárez and Najar 2014).

De igual manera el aporte de la TIC ha permitido el desarrollo los recursos educativos en los últimos años de manera acelerada. Puntualmente el inicio de la pandemia del COVID 19 hizo que la evolución de todos los recursos “en línea” estén disponibles en los hogares tanto para la generación de teletrabajo más aún para el ámbito educativo llegando a niveles nunca antes vistos en cuanto a concurrencia de usuarios y uso de herramientas tecnológicas a distancia (Topuz et al. 2022).

En virtud de lo antes mencionado se hace imprescindible hablar de niveles adecuados de seguridad informática como parte de la evolución tecnológica que se ha suscitado en la actualidad ya que se debe garantizar el acceso a las plataformas y recursos de educación, así como de la información que las mismas generan y almacenan en sus infraestructuras informáticas (Xolani and Kelebogile 2022).

Adicionalmente al hablar de políticas públicas vemos con mucha expectativa la aplicación de artículos parte de las leyes y reglamentos nacionales que garantizan el derecho de los ciudadanos al acceso a la información y protección de la misma, lo que obliga a las instituciones a fomentar políticas de seguridad para el cumplimento de estos mandatos(Información 2021).

Se ha considerado en todo el mundo que la SI es uno de los activos principales para las organizaciones públicas y privadas. Solo la gestión correcta de la seguridad evitará que las organizaciones se vean afectadas por temas como transferencias bancarias sin autorización, ataques terroristas, robos de información, manipulación de procesos, acceso a información confidencial, secuestros de información, violaciones e incidentes de seguridad, entre otros. Existe un gran impacto sobre SI y las tecnologías de la información y comunicación, ante la administración deficiente del riesgo (Toapanta Toapanta, S. M., & Mafla Gallegos 2019).
La ciberseguridad radica en la protección de ataques digitales, robo de información, violación de la privacidad hacia infraestructuras críticas, donde se encuentran inmersos los derechos y las libertades de las personas en el ciberespacio. Las amenazas no solo provienen de ciberdelincuentes, terroristas, activistas, sino también de actores y terceros cuyas esferas buscan obtener influencia y control económico y político. El internet es donde se realizan ejercicios de dominación de las estructuras económicas, tecnológicas y culturales (Posincovich et al. 2020).

El crecimiento de las tecnologías de la información y comunicación ha introducido herramientas para actividades en distintas áreas como finanzas, educación, sociales, recreativas, entre otras. Este crecimiento atrae la atención de los ciberdelincuentes que se aprovechan de las vulnerabilidades para comprometer los sistemas informáticos y cometer acciones ilegales(Cedeño Villacis 2022).

El 43% de la población del Ecuador tiene acceso a internet, la falta de medidas de protección y prevención de las amenazas y peligros que incluye su uso, es debido al desconocimiento de temas informáticos, convirtiéndolos en víctimas de los ciberataques. Se observa la misma deficiencia en aplicar políticas de seguridad en el entorno empresarial (Alvarado-Chang 2020).

MATERIALES Y MÉTODOS

Una de las herramientas para la implementación de políticas y controles en TIC de mayor aceptación a nivel mundial es la norma internacional para la SI ISO/IEC 27001 aprobado por la International Organization for Standardization y por la International Electrotechnical Commission, misma que detalla los objetivos de control y controles que permite el aseguramiento, la confidencialidad e integridad de los datos y la información, así como los sistemas que intervienen(Anon n.d.) Permitiendo generar insumos basados en sus objetivos de control y dominios como encuestas, check list, etc. , a fin de evaluar y analizar el estatus de las organizaciones.

El consejo superior de administración electrónica de España elaboro **MAGERIT**, que es una metodología de gestión de riesgos, posibilita analizar riesgos derivados del uso de las TIC. Consta de tres partes claves en su desarrollo. a) Modelo de gestión de riesgos; b) Identificación y valuación de activos, lista las amenazas y sus respectivos controles; c) Una guía habitualmente utilizada en el análisis de riesgos (Digital) n.d.)

“COBIT (Control Objectives for Information and related Technology) este sistema incluye mejores prácticas para la administración de un sistema de información, como objetivos planeta lo siguiente: a) Suministrar normas basadas en buenas prácticas para el control de la información y la tecnología de la información; b) Proveer a los usuarios de una base sólida para administrar la TI y obtener garantías; c) Brindar a los auditores para las tareas de evaluación y auditoria; d) Respaldar los esfuerzos conjuntos de la gerencia, los responsables de procesos de negocio y los auditores a fin de propiciar el mejor gobierno de TI” (ISACA n.d.)

Muchos profesionales mencionan que para establecer políticas de SI se debe centrar en decisiones de riesgos ya que las amenazas están en constante cambio. Al hablar de SI no es de extrañarse que se mencione gestión de riesgos, evaluación de riesgos o análisis de riesgos (Vacca n.d.).

La seguridad se ha visto vulnerada en diferentes ámbitos sobre todo los tecnológicos se puede mostrar como ejemplo un caso sucedido en Atwerp de Bélgica que se vieron afectados por un ataque perpetrado por un narcotraficante que trataba de afectar los sistemas informáticos de la entidad puertearía que se encargaba de revisar los contenedores que entraban, también se puede mencionar un caso de la naviera MAERSK que tuvieron un ataque de virus conocido como ramsomware que provoco la pérdida de $264 millones, finalmente se puede mencionar un caso registrado en Barcelona España por un ataque de ramsomware hacia el sistema administrativo que hasta el momento no se tiene registros del daño (Fidler 2020).

Los riesgos que se presentan en la seguridad informática se deben clasificar en los que amenazan los bienes sociales y los que representen menor impacto. Podemos agrupar los riesgos que son gran amenaza como los que ponen en riesgo la vida, la salud, dañen el medio ambiente sin dejar a un lado también los efectos por la naturaleza como huracanes, terremotos, inundaciones, todos estos riesgos mediante una gestión adecuado y planes preventivos se logra minimizar los daños. Los riesgos son algo común en la vida, pero la mitigación de los riesgos mejora la calidad de vida (Umbrasas 2011), afectando a la continuidad del negocio.

La metodología de investigación a utilizar para alcanzar los objetivos del presente proyecto es la mixta, ya que se va a realizar la exploración directa a través de preguntas cerradas o abiertas para los departamentos de TI de las instituciones educativas. La metodología deductiva se utilizará en la elaboración de análisis de riesgo con la finalidad de conocer:

¿Cómo se ha desarrollado hasta la actualidad el control de los riesgos informáticos en la Institución Educativa?

¿Disponen de manuales de políticas de SI?

¿Disponen de planes de continuidad del negocio?, entre otras interrogantes.

Con la finalidad de realizar la investigación de manera eficiente vamos a distribuirla en las siguientes fases:

Primera Fase: Establecer el marco de control a utilizar en la investigación.

Luego de haber realizado un análisis de la declaración aplicabilidad de la norma ISO 27001:2013, se obtiene una guía de referencia con la cual se identifica que controles se pueden implementar para establecer políticas de seguridad informática para las instituciones de educación superior.

Segunda Fase: Análisis de los objetivos de control que se aplican en la evaluación de los institutos de educación superior.

A continuación, se detallan los objetivos de control de la norma ISO 27001:2013 que se consideraron necesarios valorarlos para determinar la línea base.

Tabla 1. Dominios y objetivos de control ISO 27001:2013 seleccionados

Nº	*DOMINIO – OBJETIVO DE CONTROL*	
A5	**POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN**	
	A5.1	¿Se ha definido un documento con las políticas de seguridad de la información?
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
	A6.1	¿Se han definido las roles y responsabilidades en seguridad de la información?
	A6.2	¿Aplica medidas de seguridad en la utilización de dispositivos móviles del personal docente y administrativo?
A7	**SEGURIDAD RELATIVA A LOS RECURSOS**	
	A7.1	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la Institución Educativa?
	A7.2	¿Realiza un proceso de inducción al personal y proveedores sobre manejo de la información?
	A7.3	¿Realiza seguimientos de los cumplimientos de las cláusulas de confidencialidad de contratos con empleados y proveedores?
A8	**GESTIÓN DE ACTIVOS**	
	A8.1	¿Dispone de un inventario de actualizado de activos?
	A8.2	¿Se ha clasificado en términos de importancia a la información?
	A8.3	¿La Institución Educativa, ha implementado el proceso para evitar la revelación, la modificación, eliminación o destrucción no autorizada de la información almacenada en soportes?
A9	**CONTROL DE ACCESO**	
	A9.1	¿Limita el acceso a los recursos de tratamiento de información y, a la información?
	A9.2	¿Garantiza el acceso de usuarios autorizados y evita el acceso no autorizado a los sistemas y servicios?
	A9.3	¿Los usuarios siguen buenas prácticas para el uso de información secretas?
	A9.4	¿Sus usuarios disponen de controles de acceso a sistemas y aplicaciones?

A10	**CRIPTOGRAFIA**	
	A10.1	¿Su institución dispone de procedimientos y políticas para uso de controles criptográficos?
A11	**SEGURIDAD FÍSICA Y DEL ENTORNO**	
	A11.1	¿Su institución dispone de controles físicos para áreas restringidas, centros de cómputo y/o puertos de acceso?
	A11.2	¿Los equipos que manejan datos sensibles, se encuentran ubicados en donde se reduzca el riesgo de acceso no autorizado?
A12	**SEGURIDAD DE LAS OPERACIONES**	
	A12.1	¿Su institución dispone de procedimientos en donde se establezca el tratamiento y manipulación de la información, tanto automatizada como manual?
	A12.2	¿Su institución cuenta con políticas en donde se prohíbe el uso de software no autorizado?
	A12.3	¿Su institución dispone de políticas de respaldo de la información?
	A12.4	¿Su institución dispone de registro y seguimiento de eventos (syslog)?
	A12.5	¿Su institución dispone de controles de integridad del software en producción?
	A12.6	¿Su institución dispone de controles de vulnerabilidades técnicas (exploits, zeroday)?
	A12.7	¿Su institución dispone de políticas de auditoría en los sistemas de información?
A13	**SEGURIDAD DE LAS COMUNICACIONES**	
	A13.1	¿Su institución dispone de políticas y procedimientos para asegurar la infraestructura de red?
	A13.2	¿Se dispone de políticas de seguridad de la información para transferir información entre personal de la institución y terceros?
A14	**ADQUISICIÓN DESARROLLO Y MANTENIENDO DE SISTEMAS**	
	A14.1	¿Uno de los requisitos para implementar o mejorar un sistema es la seguridad de la información?
	A14.2	¿Cuentan con reglas definidas para el desarrollo seguro de aplicaciones y sistemas?
	A14.3	¿Los datos utilizados en prueba son seleccionados cuidadosamente, protegidos y controlados?
A15	**RELACIONES CON LOS PROVEEDORES**	
	A15.1	¿Cuentan con controles de seguridad para el acceso a los activos por parte de los proveedores?
	A15.2	¿La institución controla, revisa o audita regularmente la provisión de servicios del proveedor?
A16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.**	
	A16.1	¿Se ha definido las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información?
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**	
	A17.1	¿Cuenta con un plan de la continuidad del negocio?
	A17.2	¿Cuenta con arquitecturas redundantes?
	A18.1	¿Se ha creado procedimientos para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales?
	A.18.2	¿Se realiza revisiones para garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización?

Tercera Fase: Determinación del instrumento para realizar el levantamiento del estado actual de los institutos de educación superior.

El instrumento utilizado para levantar la información fue un cuestionario, el cual constaba de preguntas relacionadas a los controles listados en la segunda fase. El objetivo de las preguntas

es establecer el porcentaje de cumplimiento de las instituciones educativas en temas de seguridad informática. La escala utilizada para la evaluación se indica en la Tabla 2 a continuación.

Tabla 2. Escala para valoración del nivel de seguridad.

VALORACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA IMPLEMENTADO		
Cuantitativo	**Cualitativo**	**Descripción**
0 - 25%	Baja	Los niveles de seguridad son mínimos por lo que se considera que están expuestos a incidentes de seguridad.
26% - 50%	Moderada	Los niveles de seguridad son moderados por ende están expuestos a incidentes de seguridad.
51% - 75%	Importante	Los niveles de seguridad son importantes por cuanto no se encuentran muy expuesto a incidentes de seguridad.
76% - 100%	Alta	Los niveles de seguridad son altos sin embargos se encuentran expuestos a incidentes de seguridad mínimos.

Cuarta fase: Recolección de datos de acuerdo al instrumento planteado

La recolección de datos se la realizo a través de un formulario, el mismo que fue aplicado a los institutos de educación superior de la red RIT II con la finalidad de medir el nivel de seguridad informática con la que cuentan; y fue estructurado con la herramienta Forms de Google, para esto se logró la colaboración del 4 de los 10 institutos que conforman la red RIT II, misma que se encuentra posicionada en las ciudades de Quito, Guayaquil, Cuenca e Ibarra.

Quinta fase: Análisis de resultados

El análisis de los resultados de la recolección de los datos se la realizo a través del Alfa de Cronbach utilizando la Tabla 3 y la Fig.1.

Tabla 3. Escala confiabilidad alfa de Cronbach

RANGO	*CONFIABILIDAD*
0.53 a menos	Confiabilidad nula
0.54 a 0.59	Confiabilidad baja
0.60 a 0.65	Confiable
0.66 a 0.71	Muy confiable
0.72 a 0.99	Excelente confiabilidad
1	Confiabilidad perfecta

Revista Conectividad
Enero - junio 2023
pp. 38-49
Volumen 4, Número 1

ISSN:2806-5875
Correo: revista@ister.edu.ec

Fig. 1. Alfa de Cronbach

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum {S_i}^2}{{S_T}^2}\right]$$

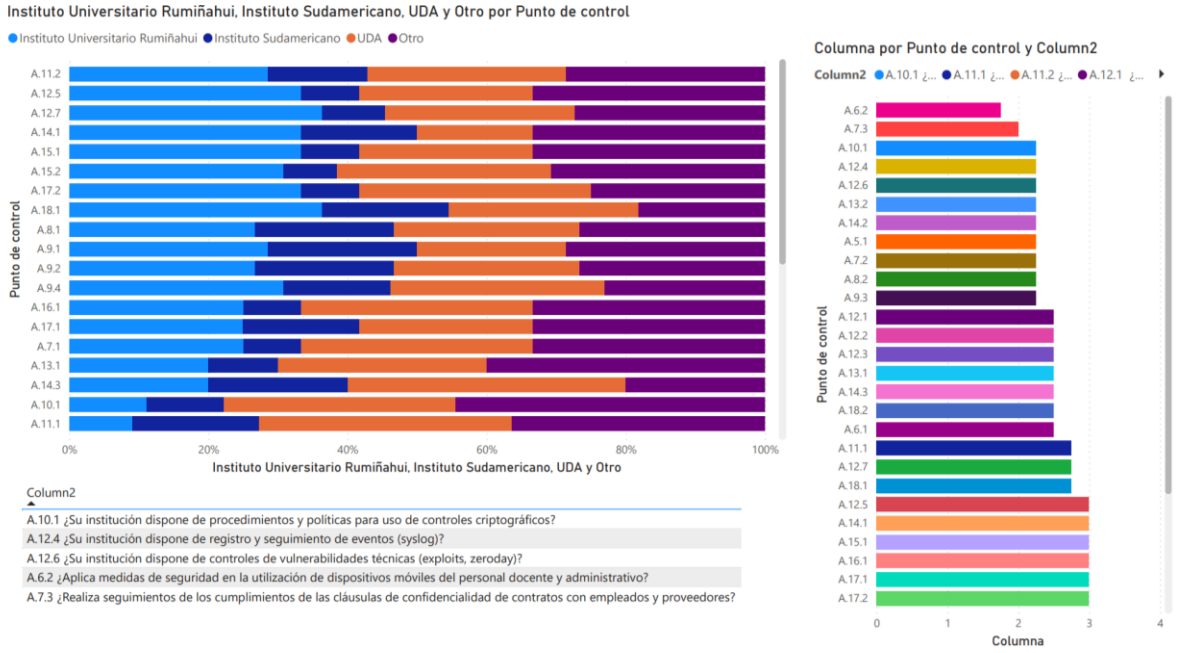
α: Coeficiente de confiabilidad del cuestionario → 0.97
k: Número de ítems del instrumento → 35
$\sum_{i=1}^{k} S_i^2$: Sumatoria de las varianzas de los ítems. → 41.000
S_t^2: Varianza total del instrumento. → 676.250

Del análisis realizado a los institutos utilizando 35 ítems se desprende que el instrumento de evaluación tiene una confiabilidad del **0.97 referencia.**

RESULTADOS Y DISCUSIÓN

Los resultados que se detallan a continuación nos ayudan establecer una línea base general actualizada del estado de la SI en los institutos de educación superior pertenecientes a la red, los mismos que por motivos de SI son anonimizados para mantener la confidencialidad, y servirá para que los niveles estratégicos de las instituciones puedan tomar decisiones acertadas sobre el aseguramiento de la información y que además sirva de insumo a tomarse en cuenta al inicio de la implementación del proyecto CSIRT (Equipo de Respuesta a Incidentes de Seguridad de Información), Fig. 2.

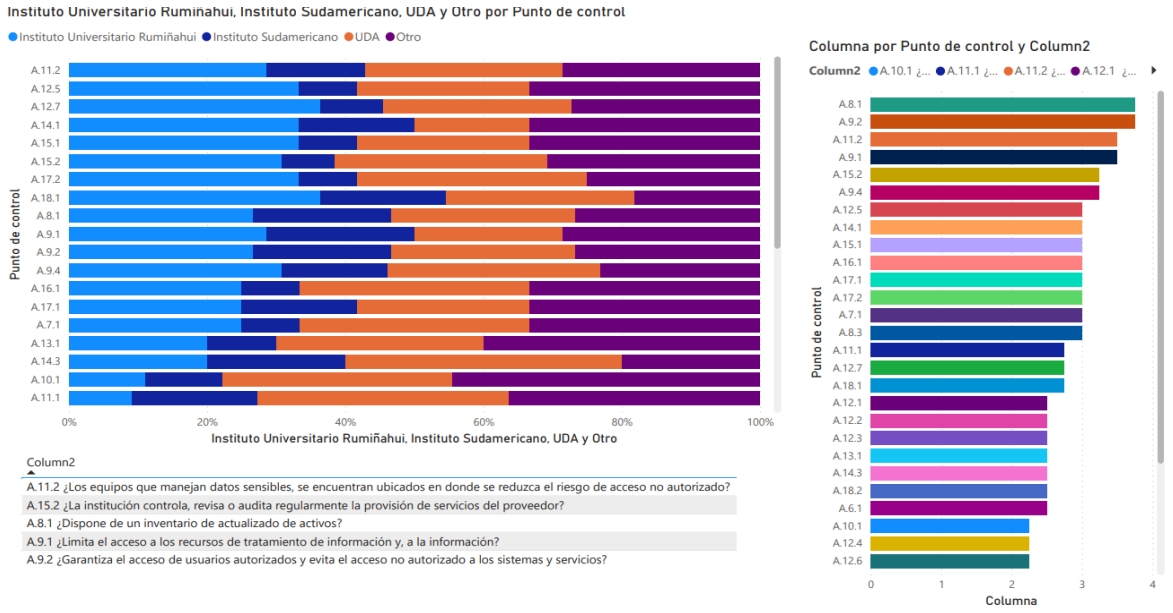
Fig. 2. Objetivos de control evaluados e identificados con menor cumplimiento.



ISSN:2806-5875
Correo: revista@ister.edu.ec

Con relación a los controles A.6.2 "¿Aplica medidas de seguridad en la utilización de dispositivos móviles del personal docente y administrativo?" y A.7.3 "¿Realiza seguimientos de los cumplimientos de las cláusulas de confidencialidad de contratos con empleados y proveedores?" se puede determinar que son los puntos más débiles en cuanto al aseguramiento de la información y que debería aprovechar esté análisis para determinar un procedimiento para mejorar esta percepción ya que son puntos clave en la gestión de TI, Fig. 3.

Fig. 3. Objetivos de control evaluados e identificados con mayor cumplimiento.



Con relación a los controles A.8.1 "¿Dispone de un inventario de actualizado de activos?" y A.9.2 "¿Garantiza el acceso de usuarios autorizados y evita el acceso no autorizado a los sistemas y servicios?" se puede observar que son los controles con más aseguramiento de los que se puede tener una tranquilidad al momento de gestionar los activos de TI así como los accesos a sus recursos, Fig. 3.

Con relación al objetivo "*POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN*", se puede determinar que el interés por generar directrices para el manejo de la SI es de un alto interés por los altos mandos de las instituciones educativas evaluadas.

CONCLUSIONES

El estudio realizado será de vital importancia en futuros análisis para proyectos de SI, concretamente apuntando a la implementación del proyecto de CSIRT en el Instituto Tecnológico Universitario Rumiñahui.

Adicionalmente se debería organizar una mesa de análisis para determinar el nivel de riesgo que se va a asumir con relación a los demás controles a fin de estimar la línea de acción para mejorar el aseguramiento de la información.

REFERENCIAS

Alvarado-Chang, Jorge. 2020. "Análisis De Ataques Cibernéticos Hacia El Ecuador." *Revista Científica Aristas* 2(1):18–27.

Anon. n.d. "Iso 27000." Retrieved (https://www.iso27000.es/).

Cedeño Villacis, R. P. 2022. "Ciberseguridad y Ciberdefensa: Perspectiva de La Situación Actual En El Ecuador." *Revista Tecnológica Ciencia y Educación Edwards Deming* 50–62. doi: 10.37957/rfd.v6i1.88.

Digital), Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación. n.d. "MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información." Retrieved (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html).

Fidler, David P. 2020. "Cybersecurity in the Time of COVID-19." *Council on Foreign Relations* (2020):7–9.

Información, Ministerio de Yelecomunicaciones y de la Sociedad de la. 2021. *Política de Ciberseguridad*. Vol. 15.

ISACA. n.d. "COBIT 2019."

Posincovich, Ayelén, Aylen Facco, Marco Gaiero, Pilar Fregona, Franco Bergero, and Marco Iazzetta. 2020. "Seguridad y Derechos Humanos:" *Perspectivas Revista de Ciencias Sociales* 19(9):147–54. doi: 10.35305/prcs.v0i9.154.

Suárez, Nubia Esperanza Suárez, and José Custodio Najar. 2014. "Evolución De Las Tecnologías De Información Y Comunicación En El Proceso De Enseñanzaaprendizaje." *Vínculos* 11(1):209–20.

Toapanta Toapanta, S. M., & Mafla Gallegos, L. E. 2019. "An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador."

Topuz, Arif Cem, Eda Saka, Ömer Faruk Fatsa, and Engin Kurşun. 2022. "Emerging Trends

of Online Assessment Systems in the Emergency Remote Teaching Period." *Smart Learning Environments* 9(1). doi: 10.1186/s40561-022-00199-6.

Umbrasas, Vytautas. 2011. "Journal of Security and Sustainability Issues." *Journal of Security and Sustainability Issues* 1(2).

Vacca, John. n.d. "Managing Information Security." 2nd Editio:372.

Xolani, Moffat, and Patience Kelebogile. 2022. "Lecturers' Experiences of Administering Online Examinations at a South African Open Distance e-Learning University During the COVID-19." *International Journal of Educational Methodology* 8(2):275–83. doi: 10.12973/ijem.8.2.275.