Vol.7 No.4 (2023): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.7.4.2023.863-878

Security policy based on ISO 27002 standard controls to the help desk process. Case study: Catholic University of Cuenca

Política de seguridad basada en los controles del estándar ISO 27002 al proceso de mesa de ayuda. Caso de estudio: Universidad Católica de Cuenca

Autores:

Sigüenza-Cárdenas, Teresa de Jesús
Universidad Católica de Cuenca
Egresada de la Maestría de Ciberseguridad
Cuenca – Ecuador
tsigüenza@ucacue.edu.ec
https://orcid.org/0009-0007-8901-4933

Torres-Soto, Carlos Andrés
Universidad Católica de Cuenca
Docente Tutor de la Maestría de Ciberseguridad
Cuenca – Ecuador
atorres@ucacue.edu.ec
https://orcid.org/0009-0003-5893-6047

Saltos-Bernal, Ginger Viviana
Universidad Católica de Cuenca
Docente de la Maestría de Ciberseguridad
Cuenca – Ecuador
ginger.saltosb@ucacue.edu.ec
https://orcid.org/0000-0003-1140-1814

Fechas de recepción: 10-SEP-2023 aceptación: 10-OCT-2023 publicación: 15-DIC-2023
https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

A partir del año 2020, se estableció un servicio de asistencia técnica conocido como "mesa de ayuda". Este servicio permite a los solicitantes enviar comunicaciones por correo electrónico a una dirección designada con el propósito de acceder al soporte técnico de nivel inicial. La implementación de esta mesa de ayuda incluyó la creación de usuarios y la asignación de sus respectivos privilegios. Los profesionales técnicos que forman parte de la Jefatura de Tecnología Informática (JTI) en la Universidad Católica de Cuenca (UC) tienen acceso y roles específicos definidos de acuerdo a sus responsabilidades laborales.

Sin embargo, es importante destacar que hasta el momento no se han establecido requisitos de seguridad adecuados para el proceso de la mesa de ayuda. Estos requisitos son esenciales, debido a que la información que se recibe y procesa diariamente en la mesa de ayuda presenta un riesgo potencial para la integridad, confidencialidad y disponibilidad de dicha información. Por lo tanto, se hace imperativo abordar de manera adecuada las medidas de seguridad en este proceso con el propósito de mitigar posibles riesgos y salvaguardar la información de manera efectiva.

Palabras clave: riesgo, seguridad, control de seguridad, mesa de ayuda, gestión de incidentes, ISO 27002

Abstract

Beginning in 2020, a technical assistance service known as a "help desk" was established. This service allows requesters to send email communications to a designated address for the purpose of accessing entry-level technical support. The implementation of this help desk included the creation of users and the assignment of their respective privileges. The technical professionals that are part of the Information Technology Department (JTI) at the Catholic University of Cuenca (UC) have access and specific roles defined according to their job responsibilities.

However, it is important to note that adequate security requirements have not yet been established for the help desk process. These requirements are essential because the information received and processed daily at the help desk presents a potential risk to the integrity, confidentiality and availability of such information. Therefore, it is imperative to adequately address security measures in this process in order to mitigate potential risks and effectively safeguard information.

Keywords: risks, security, security controls, help desk, incident management, ISO 27002.

Introducción

En el contexto actual, las instituciones dependen en gran medida de la tecnología y sistemas de información para llevar a cabo sus operaciones diarias. Esta dependencia conlleva el riesgo de que ocurran fallos o incidentes, lo que hace necesario implementar un sistema de gestión de incidentes y requerimientos conocido como "help desk" o mesa de ayuda.

Como señalan algunos autores, el software de "help desk" o sistema de mesa de ayuda, actúa como un punto de contacto crucial entre el proveedor de tecnologías de la información y los usuarios finales (Juan Armando Rodriguez Gallardo, 2018). Este sistema requiere una colaboración intensa entre todos los usuarios y el equipo de soporte técnico, lo que implica la circulación de información que puede servir para el aprendizaje o la resolución de requerimientos e incidentes.

La mesa de ayuda es un componente de software utilizado en el servicio de soporte técnico, permitiendo a la JTI de la Universidad Católica de Cuenca gestionar eficazmente las incidencias y requerimientos de los usuarios, tanto de la comunidad universitaria como del público en general. Actualmente, se utiliza el módulo de mesa de ayuda de la herramienta GLPI (Gestionnaire libre de parc informatique / administrador libre de recursos informáticos) para centralizar y administrar las solicitudes de los usuarios mediante la creación de tickets o casos. Estos tickets son procesados mediante un conjunto de actividades que incluyen priorización, categorización, asignación de responsables, seguimiento y resolución (Project, 2021).

Los tickets se generan a través de tres canales, cada uno de los cuales debe contener información básica del solicitante, la ubicación y los detalles del caso a resolver: 1) envío de un correo electrónico a la dirección proporcionada por la universidad, 2) contacto telefónico y 3) atención presencial en la oficina de la JTI. La asignación del caso se realiza al técnico de soporte apropiado, y en caso necesario, los técnicos de primer nivel en el área de servicios y operaciones de la JTI resuelven el caso. Se establecen límites de tiempo para la resolución de los casos con el objetivo de brindar un servicio eficiente.

Si el ticket no es de competencia del área de tecnología, la aplicación proporciona plantillas de solución que contienen información sobre todas las jefaturas de la universidad y datos generales. Esto permite redirigir la solicitud al área o la persona adecuada para su resolución.

Considerando el procedimiento previamente expuesto, es crucial analizar y determinar los requisitos de seguridad necesarios para prevenir o mitigar los riesgos asociados con la información que fluye desde y hacia la mesa de ayuda. En este contexto, se vuelve fundamental tener en cuenta los parámetros y directrices establecidos por las normativas de la Organización Internacional de Normalización (ISO).

Con el propósito de evaluar los riesgos inherentes al proceso de atención de ayuda (help desk) en la institución universitaria, se ha efectuado una evaluación exhaustiva del proceso mismo, sus metas, funciones, responsabilidades, y las diversas categorías de solicitudes que son gestionadas a través de esta vía. A continuación, se procedió a la identificación de los activos de información pertinentes, seguido de un análisis detallado de las amenazas y vulnerabilidades asociadas. Como resultado de este análisis, se han determinado los riesgos a los cuales se encuentran expuestos tanto los activos como el proceso en su conjunto; estos riesgos serán objeto de tratamientos apropiados para su mitigación y gestión.

En el contexto de Ecuador, se ha observado un aumento significativo en los ataques cibernéticos, particularmente de ransomware, debido al desconocimiento generalizado sobre la seguridad de la información. En el año 2022, los ataques cibernéticos han experimentado un notable incremento en el país (Ecucert, 2022). Además, la reciente creación de la Ley Orgánica de Protección de Datos Personales, que entró en vigor en mayo de 2021 y que implementó su etapa sancionatoria a partir de mayo de 2023, subraya aún más la importancia de la seguridad de la información.

Ante las circunstancias descritas, la seguridad de la información se convierte en un aspecto fundamental dentro de la UC, y significativamente, en el proceso de mesa de ayuda. En consecuencia, es esencial implementar controles que prevengan y mitiguen los riesgos que pudieran incidir en la confidencialidad, integridad y disponibilidad de la información.

Material y métodos

La JTI comunica a la Comunidad Educativa Católica la disponibilidad de un catálogo de servicios que tiene como objetivo principal recopilar de manera integral, clara y transparente todos los servicios ofrecidos por esta jefatura, detallando sus procedimientos y condiciones. Así mismo, se pretende informar a los usuarios acerca del conjunto de servicios tecnológicos disponibles, facilitando su acceso y utilización mediante un sistema informático denominado

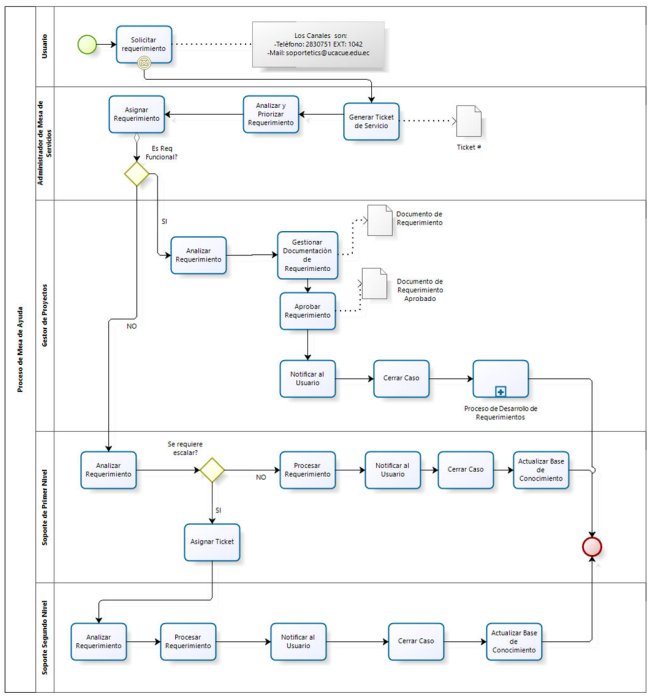
"mesa de ayuda". Este sistema registra las solicitudes de servicios y las soluciones proporcionadas por los técnicos o expertos en tecnología informática.

En este contexto, es relevante comprender el funcionamiento del proceso de la mesa de ayuda, el cual representa un componente esencial en el catálogo de servicios de la JTI de la UC.

Véase la Figura 1 para una representación visual del catálogo de servicios y su relación con la mesa de ayuda.

Figura 1

Proceso de mesa de ayuda de la JTI



FUENTE: Proceso de mesa de ayuda de la JTI (Universidad Católica de Cuenca, 2020)

A continuación, se presenta un resumen del proceso de mesa de ayuda:

Un usuario solicitante envía una solicitud por correo electrónico a la dirección designada por la UC.

Un usuario técnico de servicios de tecnología categoriza la solicitud y asigna el caso a un técnico de soporte utilizando la aplicación GLPI. Cabe mencionar que el técnico de gestión de tecnología también puede resolver directamente el caso si corresponde a soporte de primer nivel.

El técnico de soporte procede a resolver el caso o lo deriva a la entidad pertinente para su resolución. Se han establecido plazos de respuesta para cada tipo de solicitud.

Únicamente los usuarios técnicos registrados en la aplicación GLPI tienen acceso para interactuar en la misma, dependiendo del rol asignado.

Después de comprender el proceso de mesa de ayuda de la Universidad, se determinó que la metodología más adecuada para llevar a cabo el análisis de riesgos es Octave Allegro. Esta metodología, cuyas siglas traducen "Operational Critical, Threat, Asset, and Vulnerability Evaluation" (Evaluación Operativa Crítica, de Amenazas, de Activos y de Vulnerabilidad), se centra en aspectos de riesgos operativos y prácticas de seguridad (Excellence, Pmg-ssi, 2021).

En otras palabras, esta metodología permite a la UC tomar decisiones relacionadas con la protección de la información basadas en los riesgos asociados con la tríada de la información (Confidencialidad, Integridad y Disponibilidad) de los activos relacionados con el proceso y su información crítica. Esta metodología consta de ocho pasos para alcanzar su objetivo principal, según lo indicado por Torres-Solanot en 2019:

Primer paso: Establecer criterios de medición del riesgo. Para ello, fue necesario realizar un inventario de activos, analizar las vulnerabilidades y amenazas asociadas a cada uno de ellos, considerando su impacto en la tríada de la información (Confidencialidad, Integridad y Disponibilidad), así como los criterios cualitativos para la evaluación de riesgos, que se detallan en la siguiente tabla.

Tabla 1.

1.- Criterios riesgo

TIPO DE RIESGO	PRIORIDAD
Reputación / Confianza del cliente.	5
Financiera	2
Productividad	4
Seguridad/salud	3
Multas/penas legales	1
Área de impacto definida por el usuario	0

Fuente: Elaboración propia

Tabla 2.

2.- Criterios CID

CID	BAJO (1)	MEDIO (2,3)	ALTO (4,5)
CONFIDENCIALIDAD	No consecuencias	Consecuencias moderadas	Consecuencias graves
INTEGRIDAD	No consecuencias	Consecuencias moderadas	Consecuencias pérdidas económicas
DISPONIBILIDAD	8 horas o más sin consecuencias negativas	Máximo 4 horas consecuencias negativas	Máximo 1 hora consecuencias negativas, pérdidas económicas

Fuente: Elaboración propia.

En el inventario de activos es necesario identificar los tipos de activos de información, los cuales fueron establecidos como:

Tabla 3.

3.- Tipos AI

Tipo de activo (AI)	**Descripción**
Dato/Digital	Información del proceso.
Hardware	Equipos informáticos
Software	Virtualización, y aplicaciones
Servicio	Servicios que intervienen en el proceso
Físico	Espacio físico o instalaciones
Persona	Usuarios

Fuente: Elaboración propia

De acuerdo con los criterios presentados en las tablas previas, se llevó a cabo el análisis de un total de 20 activos de información, los mismo que fueron codificados mediante una nomenclatura secuencial que va desde (ACT-001) hasta (ACT-020). Posterior al análisis basado en la tríada CID, se determinó el valor correspondiente para cada activo.

Segundo paso: Desarrollar un perfil de activos de información. Durante esta fase del análisis, se procedió a describir los activos previamente identificados en el paso anterior. Además, se estableció la propiedad y la custodia de cada activo. El siguiente paso consistió en la identificación del tipo de activo y la aplicación de criterios de evaluación en relación con la tríada CID.

Tercer paso: Identificar contenedores de activos de información. En esta etapa, se identificaron los lugares donde se almacena la información, dado que estos sitios suelen ser los puntos críticos donde los riesgos se materializan con mayor frecuencia. Con base en la metodología empleada, los contenedores pueden clasificarse en tres tipos: técnicos, físicos y humanos. Esta categorización se fundamenta en la naturaleza en que la información puede existir, ya sea en formato digital, físico o como conocimiento tácito en las mentes de los empleados de la UC. Asimismo, se consideró el estado de la información, que puede ser almacenada, procesada o transmitida.

Cuarto paso: Identificar áreas de preocupación. El concepto de "área de preocupación" se refiere a una descripción que aborda una situación o área real que podría afectar a un activo de información específico. Cada activo identificado en el inventario realizado en el primer paso debe tener su propia área de preocupación definida. A partir del quinto paso, nos adentraremos en un análisis más profundo de los riesgos. En la siguiente tabla se presenta el tratamiento de los activos hasta el cuarto paso.

Tabla 4.

4.- Inventario Activos de Información

Código AI	TIPO AI	Tipo AI	Clasificación A.I.	Valor AI	Valor AI	Contenedor AI

ACT-001	Digital	Datos o información	Confidencial	4	ALTO	Técnico
ACT-002	Hardware	Equipos informáticos	Confidencial	4	ALTO	Físico
ACT-003	Servidor virtual	Aplicaciones de software	Confidencial	5	ALTO	Físico
ACT-004	Servicio	Datos o información	Confidencial	5	ALTO	Técnico
ACT-005	Servidor virtual	Equipos informáticos	Confidencial	4	ALTO	Técnico
ACT-006	Servicio	Aplicaciones de software	Confidencial	4	ALTO	Técnico
ACT-007	Servicio	Datos o información	Confidencial	5	ALTO	Técnico
ACT-008	Servicio	Servicio	Uso interno	3	MEDIO	Técnico
ACT-009	Servicio	Servicio	Uso interno	4	ALTO	Técnico
ACT-010	Aplicación	Aplicaciones de software	Uso interno	5	ALTO	Técnico
ACT-011	Persona	Personal	Uso interno	5	ALTO	Humano
ACT-012	Persona	Personal	Público	4	ALTO	Humano
ACT-013	Persona	Personal	Uso interno	5	ALTO	Humano
ACT-014	Persona	Personal	Uso interno	4	ALTO	Humano
ACT-015	Físico	Equipos informáticos	Confidencial	4	ALTO	Físico
ACT-016	Hardware	Redes y comunicación	Confidencial	4	ALTO	Físico
ACT-017	Software	Aplicaciones de software	Confidencial	4	ALTO	Físico
ACT-018	Físico	Equipos informáticos	Uso interno	3	MEDIO	Físico

ACT-019	Físico	Equipos informáticos	Público	4	ALTO	Físico
ACT-020	Físico	Equipos informáticos	Público	4	ALTO	Físico

Fuente: Elaboración propia

Tabla 5.

5. Valoración de los activos de información

Valor	DESCRIPCIÓN		
	C	**I**	**D**
Bajo (1)	Información no disponible 8 horas o más y no causa consecuencias negativas.	Información modificada sin autorización, no causa consecuencias negativas.	Conocimiento de la información que maneja el activo. No causa consecuencias negativas.
Medio (2,3)	Información no disponible 4 horas o más y no causa consecuencias negativas.	Información modificada sin autorización, no causa consecuencias moderadas.	Conocimiento de la información que maneja el activo. No causa consecuencias moderadas.
Alto (3,4)	Información no disponible 1 hora causa consecuencias negativas y económicas.	Información modificada sin autorización, no causa consecuencias graves.	Conocimiento de la información que maneja el activo. No causa consecuencias graves.

Fuente: Elaboración propia

Quinto paso: Identificar escenarios de amenaza. Durante esta fase, se procedió a identificar las amenazas y vulnerabilidades específicas en relación con cada activo de información. Se consideró el motivo o tipo de amenaza y se evaluó la vulnerabilidad existente en el activo que podría permitir que, en un momento dado, dicha amenaza se materialice.

Sexto paso: Identificar riesgos. Para llevar a cabo esta etapa, se empleó la siguiente ecuación:

Riesgo = Amenaza (condición) + Impacto (consecuencia)

Como resultado de esta evaluación, se obtuvo un total de 63 riesgos, los cuales fueron categorizados de la siguiente manera: 20 riesgos con un valor de 2, 19 riesgos con un valor de 4 y 24 riesgos con un valor de 5.

Séptimo paso: Analizar riesgos. Durante esta etapa, se procedió a analizar los riesgos identificados anteriormente. Los riesgos se categorizaron cualitativamente de acuerdo con el criterio establecido en el primer paso, que se relaciona con la seguridad. Para determinar el impacto de los riesgos, se utilizó la siguiente ecuación:

Impacto = Riesgo x Criterio de riesgo (seguridad)

El resultado de este análisis fue la identificación de un total de 63 riesgos, que se dividieron en tres categorías: 20 de nivel medio, 19 de nivel alto y 24 de nivel muy alto. Estos riesgos posteriormente fueron objeto de tratamiento y gestión.

Resultados

Octavo paso: Selección de un enfoque de mitigación. En esta etapa, se han determinado los controles de seguridad que deben ser implementados para reducir los riesgos identificados previamente en el estudio, los mismos que se han definido de acuerdo con los dominios de la norma ISO 27002:2013, que incluyen:

- A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN, control A.5.1.1.
- A.7 SEGURIDAD DE LOS RECURSOS HUMANOS, controles A.7.1.2 – A7.2.2 – A.7.3.1
- A.9 CONTROL DE ACCESO, controles A9.1.1 al A9.4.3
- A.11 SEGURIDAD FÍSICA Y DEL ENTORNO, controles A11.1.1 al A11.2.4
- A.12 SEGURIDAD DE LAS OPERACIONES, controles A12.2.1 al A12.6.1
- A.13 SEGURIDAD DE LAS COMUNICACIONES, controles A13.1.1 – A13.2.4
- A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, controles A14.2.2 al A14.2.4
- A.15 RELACIONES CON LOS PROVEEDORES, controles A15.1.1 – A15.2.1
- A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, controles A16.1.1 al A16.1.5

Análisis GAP: Es fundamental llevar a cabo un análisis GAP del proceso de mesa de ayuda, comparando la situación actual con los resultados esperados después de implementar las medidas de mitigación de riesgos sugeridas en los párrafos anteriores.

Situación actual del proceso de mesa de ayuda: Una vez que se han aplicado los criterios de la matriz de controles de la norma ISO 27002, se ha obtenido un nivel de madurez de los

dominios igual a 2 (dos) con un nivel de cumplimiento del 48.62%. Estos datos se presentan en la siguiente figura.

Figura 2

2.- Nivel de madurez de acuerdo a la norma ISO 27002, ejecutados inicialmente

Fuente: Elaboración propia

Figura 3

3.- Descripción del nivel de madurez actual cuyo valor es 2.

% de Cumplimiento	Definición
40%	Se desarrollan procesos dependientes de las personas y otras le siguen. No hay una comunicación ni entrenamiento formal y la responsabilidad recae sobre los individuos. Excesiva confianza en el conocimiento de los individuos, por tanto, los errores son comunes. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
2	
Control aplicado, pero no documentado	

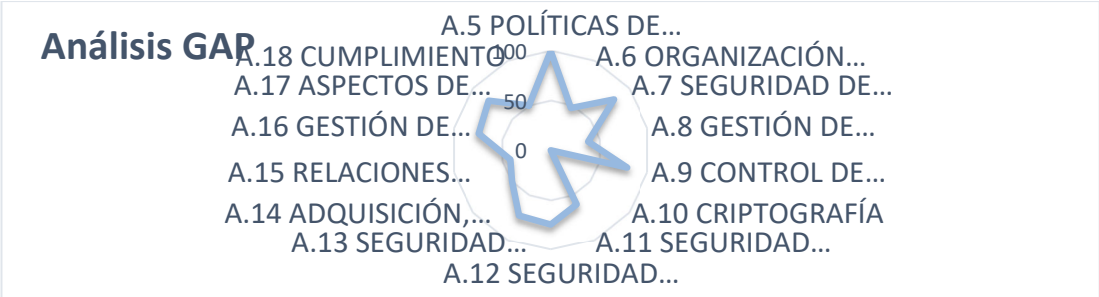
FUENTE: Tomado de la Guía de Evaluación de Controles Norma ISO 27001:20013, realizado por el Ministerio de Educación Nacional de Colombia.

Nivel de madurez esperado, luego de aplicar los controles de seguridad establecidos, así como, la política de seguridad para el proceso de mesa de ayuda de la JTI.

En la figura siguiente se ilustra el resultado del nivel de madurez esperado que asciende a 3 (tres) con un nivel de cumplimiento del 60,87%, esto, si se aplicaran los controles recomendados más la política de seguridad.

Figura 4

4.- Análisis GAP esperado, luego de aplicados los dominios de la norma ISO 27002



Fuente: Elaboración propia.

Figura 5.

5.- Definición del nivel de madurez esperado, luego del tratamiento de la brecha de seguridad inicial.

% de Cumplimiento	Definición
60%	Los procesos se definen, documentan y se comunican a través de entrenamiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de detectar desviaciones es alta. Los procedimientos por si mismos no son sofisticados pero se formalizan las prácticas existentes.
3	
Control formalizado, falta medición y monitoreo	

FUENTE: Tomado de la Guía de Evaluación de Controles Norma ISO 27001:20013, realizado por el Ministerio de Educación Nacional de Colombia.

Conclusiones

Tras llevar a cabo el análisis y tratamiento de los riesgos asociados al proceso de mesa de ayuda de la Jefatura de Tecnología Informática (JTI) de la Universidad Católica de Cuenca, se llega a las siguientes conclusiones de relevancia:

- Promover la conciencia de ciberseguridad entre los empleados de la JTI que utilizan activos de información es esencial para fomentar una cultura de seguridad en la

Universidad. Este enfoque contribuirá a la protección de la información y la prevención de riesgos cibernéticos.

- La evaluación y la identificación de amenazas y riesgos asociados a los activos de información deben realizarse en colaboración con los custodios de dichos activos. Esta colaboración garantiza que las valoraciones sean realistas y se basen en la experiencia del usuario administrador, lo que conduce a una toma de decisiones más informada.
- Se ha observado un cambio en el nivel de madurez del proceso, como se evidencia en la comparación entre el análisis GAP inicial y el esperado. Esta diferencia resalta la necesidad de abordar y mitigar los riesgos identificados y trabajar en el tratamiento de la brecha de seguridad de manera efectiva.
- La identificación de los controles de seguridad según la norma ISO 27002:2013 debe llevarse a cabo considerando las amenazas detectadas y en estrecha colaboración con los administradores y custodios de los activos afectados. Esto asegura que los controles sean precisos y eficaces en la mitigación de los riesgos identificados.
- La Universidad Católica de Cuenca ha logrado un destacado posicionamiento a nivel internacional, según los resultados de la rendición de cuentas en 2022. La implementación de la política de seguridad propuesta como anexo a este análisis contribuirá al avance continuo hacia la excelencia en el ámbito de la seguridad de la información y fortalecerá la posición de la UC en los rankings internacionales.

Referencias bibliográficas

Project, G. (02 de 03 de 2021). *GLPI Project*. El software de gestión de servicios de código abierto más completo. https://glpi-project.org/es/

Ecucert. (14 de 02 de 2022). Ecucert. Centro de respuesta a incidentes informáticos del Ecuador. https://www.ecucert.gob.ec/wp-content/uploads/2022/02/EC-2022-031_RANSOMWARE-ELBIE_V1.pdf

Excellence, I. (09 de 09 de 2021). Pmg-ssi. Metodología OCTAVE para el análisis de riesgos en SGSI

https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/

Excellence, I. (07 de 2021). Seguridad de la información. Activos en Seguridad de la Información. ¿Qué son y cómo definirlos? https://www.pmg-ssi.com/2021/07/activos-en-seguridad-de-la-informacion-que-son-y-como-definirlos/

Instituto Uruguayo de Normas Técnicas. (2014). Tecnología de la información – Técnicas de seguridad- Código de buenas prácticas para controles de seguridad de la información. https://www.unit.org.uy/normalizacion/normas/ics/35.040/

Juan Armando Rodriguez Gallardo, M. C. (2018). Estudio sobre la implementación del software Help Desk en una institution of higher education. Paakat: Revista de Tecnología y Sociedad, 20.
https://www.scielo.org.mx/scielo.php?pid=S2007-60720180002000003&script=sci_abstract

Torres-Solanot, A. M. (2019). El Análisis Riesgo de OCTAVE Allegro. antoniofpts, 6.
https://calidadengestiondeproyectos.com/2019/06/02/el-analisis-riesgo-de-octave-allegro/

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.