TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

GESTIÓN DE RIESGOS EN LAS TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Yaneisy Onelia Massó Agramonte

Empresa de Aplicaciones Informáticas, DESOFT, Cuba
yaneisyonelia@nauta.cu

RESUMEN

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) han tenido un gran impacto en las organizaciones. El aumento de una serie de amenazas que atentan contra la seguridad y disponibilidad de la información, le han dado una gran importancia a la gestión de riesgos. El siguiente trabajo se basó en la gestión de riesgos principalmente en las tecnologías de la información. Se expuso de manera general el objetivo de la gestión de riesgos y su importancia para los organismos, además de las buenas prácticas de su aplicación y las fases en las que se agrupa. También se trataron algunos estándares relacionados con los riesgos y la gestión de estos, que indican requerimientos para una gestión adecuada, y los beneficios de su implementación en los organismos, además de actividades correspondientes para llevar a cabo una apropiada ejecución de la gestión de riesgos, así como la utilización de las TIC para ello.

PALABRAS CLAVE: Gestión de riesgos, riesgos, seguridad, información

RISK MANAGEMENT IN INFORMATION TECHNOLOGY

SUMMARY

Due to the development of Information and Communication Technologies (ICT) and their significant impact on organizations, a series of threats have increased that threaten the authenticity, confidentiality, security, and availability of information. This attaches great importance to risk management. The following work was based on risk management, mainly in information technologies. The objective of risk management and its priority for organizations were explained in a general way, as well as the good practices of its application and the phases in which it is grouped. Some standards related to risks and their management were also discussed, which indicate requirements for adequate management and the benefits of its implementation in organizations, as well as related activities to carry out an appropriate execution of risk management, as well as the use of ICT for it.

KEY WORDS: Risk management, risks, security, information

1. INTRODUCCIÓN

Al surgir las tecnologías de la información (TI), también surge la necesidad de garantizar la confidencialidad, integridad y disponibilidad de los sistemas de procesamiento de datos y su almacenamiento. La información es un elemento muy importante debido a que apoya a la organización y su misión. Una organización se enfrenta regularmente a una serie de factores internos y externos que pueden afectar a su actividad o no permitirle alcanzar sus objetivos, dependiendo de la capacidad que tenga para enfrentar estas amenazas podrá sostener las operaciones.

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización y permite determinar la naturaleza, el costo y la protección que tiene un sistema. Al implantar este plan se debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la dirección de la organización. El riesgo se puede estimar mediante el producto entre la probabilidad de que ocurra y el impacto que causa dicho riesgo. [1]

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

La realización de un análisis de riesgos en el entorno de las Tecnologías de la Información y las Comunicaciones (TIC) proporciona a las organizaciones una visión de la situación, tanto por lo que hace a nivel de protección de sus sistemas de información, como por la relación entre estos niveles y el coste que representa para la organización. De esta forma, la gestión del riesgo se constituye como uno de los pilares fundamentales que permite conocer de manera detallada la infraestructura y su funcionamiento interno, así como las consecuencias de una eventual vulnerabilidad o pérdida de servicio.

Riesgo es "la probabilidad de que una amenaza determinada se materialice, explotando las vulnerabilidades de un activo o grupo de activos y por lo tanto causar daño o pérdidas a la organización", "ISO/Guide.". [2]

Según la ISO 31000, el riesgo es el efecto de la incertidumbre sobre los objetivos. La definición de riesgo es común a pesar de la gran variedad de autores y temas que lo tratan. Al ser la seguridad de la información la protección de la misma contra la transferencia, modificación, divulgación o destrucción no autorizada de forma voluntaria o accidental; es fundamental la gestión de riesgos de forma eficiente y responsable. El riesgo a la seguridad de la información tiene varios componentes que influyen enormemente. Cuando un agente de amenaza ya sea humano o no, explota una vulnerabilidad, tiene consecuencias con resultados no deseados, un impacto. Por lo que:

Activos de Información: Hacen referencia a cualquier elemento que contenga información. Según el estándar ISO/IEC 27002:2013, los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.[3]

Vulnerabilidades: Son las debilidades o fallos de un activo o sistema de información que puede comprometer su seguridad. Deben ser expresadas en una escala numérica para posteriormente cuantificar su impacto, se sugiere que éstas sean identificadas y valoradas individualmente.

Amenazas: Son los actos intencionados o no que aprovechan las vulnerabilidades existentes de un activo y que pueden dañar o alterar la información de una u otra forma, las amenazas se pueden clasificar en varios tipos: de origen natural, del entorno, por defecto de aplicaciones, causadas por personas de forma accidental o de forma deliberada.

Impacto: Es un indicador de lo que puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza de materializarse sobre un activo.

El riesgo en informática es un problema de vital importancia para las empresas tecnológicas, el objetivo de la gestión de riesgos en estas empresas es el de proteger a las personas los equipos y trabajos vinculados con la actividad informática, Basado en la afirmación anterior se pueden diferenciar varios tipos de amenazas respecto a:

Los equipos o hardware: Pueden ser Interrupciones, temporales o no, en la capacidad de funcionamiento del dispositivo. Causados por desastres naturales, perdida de energía eléctrica, fallas, incendios y otros.

Los programas: fraudes con la información afectando los activos de la empresa, robo de programas, falta de respaldo o backup, modificaciones no autorizadas imprudenciales o no, entre otras.

Los trabajos: ineficiencias en la realización de proyectos informáticos, destrucción de los soportes voluntaria o involuntaria que contienen la información lo que genera la desaparición de los datos, divulgación de información confidencial, errores en la concepción de las aplicaciones, y otras

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

Las personas: están ligados a la protección contra las amenazas anteriores e incluyen simultáneamente una acción de sensibilización, formación y control.

Para contrarrestar las amenazas y minimizar los riesgos a las TI, las empresas pueden implementar estrategias reactivas y/o preventivas. Las estrategias reactivas evalúan las consecuencias una vez que ha ocurrido el incidente, es un enfoque basado en la respuesta y depende de las valoraciones de incidentes anteriores. El Enfoque de las estrategias preventivas está dirigido hacia la prevención, se realiza una evaluación previa y sistemática para identificar amenazas potenciales, y a la vez se elaboran medidas preventivas para mitigarlo o eliminarlos y se conforman planes de contingencias para evitar y minimizar el impacto de estas. Además tiende a la capacitación y a la formación de los empleados.

2. GESTIÓN DE RIESGOS

La ISO Guide 73:2009, define gestión de riesgos como: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo [4]. La gestión de riesgos, tiene como objetivo minimizar que un evento negativo o adverso ocurra, realizando la detección, evaluación, corrección, monitoreo y control de los riesgos. Las actividades principales consisten en identificar y clasificar los riesgos de seguridad informática de la organización en este caso: evaluación de riesgos, e identificar estrategias apropiadas para mitigar los riesgos. En general, la gestión de riesgos de TI puede considerarse fundamentalmente un requisito previo para tomar decisiones de inversión en seguridad. [5]

Se puede decir que la gestión de riesgo permite analizar procesos para obtener una visión global de la organización y muestra la necesidad de proteger y gestionar procesos críticos que afecten de forma drástica a la organización. Así mismo, la gestión del riesgo de la seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos y sus vulnerabilidades, y su impacto en la información, los sistemas de información y organizaciones que dependen de la información para sus operaciones. Una aproximación sistemática, basada en la valoración de las amenazas y las vulnerabilidades, para la determinación de las medidas necesarias para la protección de la información y/o los servicios y recursos que la soportan.

Estándares de Gestión de riesgo

Debido a que la gestión de riesgos es de gran importancia para las organizaciones, se han desarrollado estándares que tratan sobre riesgos generales y específicos. Algunos ejemplos son, ISO 27000 sobre seguridad de la información, ISO 27001 certifica la selección de las medidas adecuadas de seguridad que salvaguardan los activos referentes a información, ISO/IEC 27005:2018 indica las directrices para la gestión de riesgos, PMBOK para riesgos en proyectos, ISO 31000 para la gestión de riesgos. En el caso de la ISO 31000 es aplicable para la gestión de cualquier tipo de riesgo, y a cualquier tipo de organización ya que propone un sistema para la gestión de cualquier riesgo empresarial, conocido como ERM, (Enterprise Risk Management). Este estándar internacional, recoge las prácticas para gestionar el riesgo de forma eficiente en cualquier organización, pública o privada. La normativa ayuda a poder identificar, analizar, evaluar y disminuir los riesgos que puedan afectarla. La implantación de ISO 31000 en una organización tiene gran ventaja debido a que mejorará su eficiencia operativa, tendrá mejor gobernabilidad interna aumentando la confianza de partes externas. Además, mejora el rendimiento, sostenibilidad y acentúa su calidad, a la vez que reduce los costos y disminuye o desaparece los incidentes inesperados. En un proyecto que implemente la ISO 31000 se desarrollarían las siguientes actividades:

Establecer el contexto estratégico. Se definen los parámetros básicos para la gestión del riesgo, así como el alcance y los criterios para el resto de los procesos, algo que se debe hacer de manera ineludible desde el conocimiento de todos los aspectos que se engloban en la actividad llevada a cabo por la organización.

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

Identificar los riesgos. Se identifican de forma sistémica los riesgos, las causas de estos y los posibles efectos que tendría su materialización.

Analizar el riesgo. Se establece la probabilidad de que suceda un riesgo y el impacto que generan sus consecuencias, mediante su calificación y su evaluación, con el fin de que se establezca, de la manera más eficiente posible, el nivel de riesgo y por lo tanto las acciones correctoras que se deben llevar a cabo.

Valoración de los riesgos. Se confrontan los resultados obtenidos a raíz del análisis del riesgo, con las medidas de control que han sido identificadas, para establecer prioridades en el tratamiento de los riesgos y poder fijar las políticas de gestión que sean más adecuadas.

Políticas de administración de riesgos. Una vez identificados, clasificados y valorados los riesgos, se establecen las políticas de gestión de riesgo, que se encuentran articuladas en cuatro ejes diferentes: transferencia del riesgo, retención del riesgo, reducción del riesgo o evitar dicho riesgo.

Monitorización y revisión. Debido a que es muy difícil que los riesgos detectados dejen de suponer una amenaza para la organización, se deben establecer indicadores de seguimiento sobre las medidas definidas para la gestión de riesgos. [6]

Fases de la Gestión de riesgo

La gestión de riesgo se agrupa fundamentalmente en 4 fases: análisis, clasificación, reducción y control, como se muestra en la fig. 1.

Figura 1. Fases de la gestión de riesgo.

En el *análisis de riesgo* se determinan los componentes de un sistema que requieren protección, las vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. En este se encuentra la *clasificación y flujo de la información*. Donde la clasificación de datos garantiza la protección de datos y define, los diferentes niveles de autorización de acceso a los datos e informaciones. La clasificación y análisis de los datos es muy importante pues influye directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección.

Existe variedad de métodos para valorar un riesgo y todos tienen variables difíciles de precisar, en su mayoría, estimaciones. Y todos obtienen casi los mismos resultados. En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo.

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

$$R = P \times M \quad (1)$$

Donde:

R: Riesgo
P: Probabilidad de Amenaza
M: Magnitud de Daño

En el proceso de analizar un riesgo también es importante reconocer que cada riesgo tiene sus características:

Puede ser dinámico y cambiante (Interacción de Amenazas y Vulnerabilidad)

Puede ser diferenciado, o con diferentes caracteres (caracteres de Vulnerabilidad)

No siempre es percibido de igual manera entre los miembros de una institución que tal vez puede terminar en resultados inadecuados y por tanto es importante que participen los especialistas de los diferentes elementos del sistema (Coordinación, Administración financiera, Técnicos, Soporte técnico externo etc.), entre más alta la probabilidad de amenaza y magnitud de daño, más grande es el riesgo y el peligro al sistema, lo que significa que es necesario implementar medidas de protección.

El impacto es el alcance del daño o las consecuencias causadas a un activo, de materializarse una amenaza a la seguridad de la información. Aunque se conozca bien el impacto de una amenaza, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto donde se maneja la información. Un punto esencial en el análisis de estas consecuencias es la diferenciación entre los dos propósitos de protección de la Seguridad Informática, la Seguridad de la Información y la Protección de datos, porque permite determinar, quien va a sufrir las consecuencias del impacto.

Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros. La magnitud de daño se puede definir como baja, media, alta. Se puede decir que la magnitud es baja cuando es un daño aislado, que no perjudica ningún componente de la organización. La magnitud es mediana cuando provoca desarticulación de un componente de la organización, incluso puede ser a largo plazo. Y la magnitud de daño es alta cuando en corto plazo desmoviliza o desarticula la organización.

El riesgo en cuanto al posible impacto se puede medir como:

1- Insignificante: cuando las consecuencias o efectos son mínimos sobre la entidad.
2- Menor: Cuando es bajo el impacto o efecto sobre la entidad.
3- Moderado: Cuando son moderadas las consecuencias o efectos sobre la entidad.
4- Mayor: Serian altas las consecuencias o efectos sobre la entidad.
5- Catastrófico: tendría desastrosas consecuencias o efectos sobre la entidad. [7]

El objetivo de la *clasificación de riesgo* es determinar hasta qué grado es factible el tratamiento a los riesgos encontrados. La factibilidad depende de la voluntad y posibilidad económica de una organización, también del entorno donde se ubique. Para manejar los riesgos a que puede estar sometido un activo se utilizan las técnicas siguientes:

- Evitar: aplicar acciones y controles adecuados en los procesos para impedir el riesgo.
- Reducir: optimizar los procedimientos y la implementación de controles para reducir un riesgo inevitable hasta el nivel más bajo posible.
- Transferir: compartir el riesgo con otra entidad, para transferirlo de un lugar a otro o mantenerlo a un nivel mínimo.

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

- Retener: Cuando se reduce el impacto de los riesgos pueden aparecer riesgos residuales. Dentro de las estrategias de gestión de riesgos de la entidad se debe plantear como manejarlos para mantenerlos en un nivel mínimo [8].

Sobre esta última técnica se quiere argumentar que, los riesgos residuales deben ser aceptados. Estos riesgos pueden verse de dos maneras, por un lado, están las amenazas que, a pesar de tener implementadas medidas para evitar o mitigar los riesgos, si el ataque ocurre con una magnitud superior a lo esperado, siempre pueden afectar. Por otro lado, cuando se acepta conscientemente el posible impacto y sus consecuencias, después de realizar el análisis de riesgo y la definición de las medidas de protección.

La *reducción de riesgo* se logra a través de la implementación de medidas de protección, que se basa en los resultados del análisis y de la clasificación de riesgo. Las medidas de protección están divididas en medidas físicas, técnicas y organizativas. Las medidas de protección aumentan la capacidad física, técnica, personal y organizativa, reduciendo así las vulnerabilidades que están expuestas a las amenazas que se enfrentan. Se debe evitar la escasez de protección porque queda el peligro que puede causar daño, y el exceso de medidas y procesos de protección pueden fácilmente paralizar los procesos operativos e impedir el cumplimiento de la misión del organismo. La Implementación de estas medidas implica realizar inversiones, en general económicas. El desafío en definir las medidas de protección está en encontrar un buen equilibrio entre su funcionalidad y el esfuerzo económico que se debe hacer para la implementación y el manejo de estas.

La fuerza y el alcance de las medidas de protección dependen del nivel de riesgo, que puede ser alto o medio. El alto riesgo son las medidas que deben evitar el impacto y sus consecuencias. Y las de medio riesgo son las medidas que solo mitigan las consecuencias, pero no evitan el impacto. Debido a esto las medidas para la prevención de riesgos son mucho más costosas y complejas. Las medidas deben estar respaldadas y aprobadas, sino pierden su credibilidad. Para que sean exitosas, es importante que se verifique que técnicamente funcionen y cumplen su propósito. Además, deben ser diseñadas de tal forma que no obstaculicen los procesos operativos institucionales.

El propósito del *control de riesgo* es analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias. Las actividades del proceso tienen que estar integradas en el plan operativo institucional, donde se define los momentos de las intervenciones y los responsables de ejecución.

Medir el cumplimiento y la efectividad de las medidas de protección requiere que se lleven constantemente registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados. Estos deben ser analizados frecuentemente. Dependiendo de la gravedad, el incumplimiento y el sobrepasar de las normas y reglas, requieren sanciones institucionales para los funcionarios. Se puede decir que todo el proceso está basado en políticas de seguridad, normas y reglas institucionales, con el propósito de potenciar las capacidades de la organización, reduciendo así, la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo, orientando el funcionamiento organizativo y funcional, además de garantizar el comportamiento homogéneo y la corrección de conductas o prácticas que nos crean vulnerabilidad y también conducir a la coherencia entre lo que se piensa, se dice y se hace.

Utilización de las Tecnologías de la informatización en la Gestión del Riesgo

Las TIC, posibilitan, de manera más efectiva, la atención a las diferentes ramas de los procesos empresariales. La efectividad del uso y explotación de una herramienta informática dentro de la gestión directiva solo puede ser evaluada y medida por el análisis exhaustivo de una amplia variedad de factores que incluyen desde la necesidad e importancia que produzca para la empresa la implantación de la misma, hasta la organización de los datos a evaluar.

La gestión de riesgos ofrece muchos beneficios, algunos de ellos son la colaboración en la implementación de sistemas de control interno apoyados de un software de última tecnología, el aumento en la probabilidad de logro de los objetivos de la organización y la identificación e intercambio de

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

Revista Telemática. Vol. 22 No. 3, Julio-Septiembre, 2023, p. 35-42 ISSN 1729-3804

conocimientos sobre riesgos cruzados. Además, permite una mayor comprensión de los riesgos claves y sus implicaciones. También, mejora la gestión de proyectos y la estructura de gobierno corporativo, de igual forma, existe mayor disponibilidad de información a nivel estratégico y operativo para la toma de decisiones. Al mismo tiempo, actualiza los conocimientos por parte de los profesionales en temas de gestión por procesos, control interno, indicadores y riesgos.

Las mejores prácticas de gestión de riesgos de seguridad en las Tecnologías de la Información y usando como guía los estándares de la industria se incluyen:

- Un conocimiento integral de los entornos TI de la organización.
- Conocer los riesgos de seguridad.
- Saber qué riesgos de seguridad son los más pertinentes.
- Desarrollar planes para responder a un evento de seguridad.
- Capacitar a todo el personal de la organización en prácticas de seguridad.

En general, las organizaciones, para que les sea posible implementar y mantener la gestión de riesgos para con sus activos deben tener siempre presentes que su objetivo es preservar la confidencialidad, la integridad la disponibilidad y la autenticidad de la información y que cada uno tiene un rol diferente dentro de la organización, que exigen acciones precisas para conseguir definir y mantener la protección de todo el sistema corporativo. Una buena Gestión de riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios. [9] La aplicación de mejores prácticas para la gestión de los riesgos proporcionará beneficios tangibles de negocios; por ejemplo, un menor número de eventos inesperados y fracasos, el aumento de la calidad de la información, una mayor confianza de las partes interesadas, menos preocupaciones de carácter regulatorio y nuevas iniciativas para el negocio apoyadas por aplicaciones innovadoras. [10]

3. CONCLUSIONES

La gestión del riesgo de seguridad de la información permite a una organización evaluar lo que está tratando de proteger, y por qué, como elemento de apoyo a la decisión en la identificación de medidas de seguridad. Una evaluación integral del riesgo de seguridad de la información debería permitir a una organización evaluar sus necesidades y riesgos de seguridad en el contexto de sus necesidades empresariales y organizativas. El marco de referencia de la norma 31000 integra la gestión del riesgo en todas sus actividades y funciones significativas. Requiere el apoyo de las partes interesadas, particularmente de la alta dirección de la organización para lograr una mejor integración, diseño, implementación, valoración y mejora de la gestión del riesgo. Se puede concluir que la gestión de riesgos es de suma importancia para evitar problemas internos, problemas con clientes o pérdidas innecesarias. No sólo optimizar los procesos internos de una organización, también el desarrollo de las actividades comerciales que afectan a la economía de un país.

4. REFERENCIAS BIBLIOGRÁFICAS

[1] Grupo de autores, “Las Tics como herramienta para lagestión de riesgos”, [Online].Disponible en: http://recimundo.com/index.php/es/article/view/793. Recimundo, Vol 4, No. 1, 2020.
[2] “ISO Guide 73:2009(en) Risk management”,[Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:guide:73:ed-1:v1:en. [Accessed Oct., 2021].
[3] ISO, “ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.” [Online]. Available: https://www.iso.org/standard/54533.html, [Accessed Oct., 2021].
[4]“Gestión de riesgo en softwares”, [Online]. Disponible en: https://www.ecured.cu/Gestión_de_riesgo_en_ softwares. [Accedido Oct., 2021].
[5] W. A. Bailón-Lourido,“Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó”, Polo del Conocimiento, Vol 4, No.8, pp 165-189, 2019.

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

[6]"ISO 31000. Análisis y gestión de riesgos", [Online]. Disponible en: https://www.encolaboracion.net/continuidadde-negocio/iso-31000/. [Accedido Oct., 2021].
[7] Grupo de autores, "Procedimiento de gestión de riesgos como apoyo a la toma de decisiones", Ingeniería Industrial, Vol XLI, No. 1, 2020
[8]Colectivo de autores, "Modelo de gestión de riesgos de ti que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú", Tesis,Universidad Católica Santo Toribio de Mogrovejo, Perú, 2018.
[9]"Gestión de Riesgo en la Seguridad Informática", [Online]. Disponible en: https://protejete.wordpress.com/gdr_principal. [Accedido Oct., 2021].
[10]"Gestión del riesgo en seguridad. Métodos y herramientas. Manejo de la información", [Online]. Disponible en: https://blog.siete24.com/gestion-del-riesgoen-seguridad-metodos-y-herramientasmanejo-de-la-informacion.[Accedido Oct., 2021].

5. SOBRE LOS AUTORES

Graduada de Ingeniería informática en laUniversidad Tecnológica de la Habana, José Antonio Echeverría en 2008. Especialista en informática de la empresa DESOFT habiendo realizado tareas de desarrollo de aplicaciones y gestión de contenidos. Actualmente especialista en Calidad de software con habilidades en pruebas manuales y automatizadas. Cursados posgrados de informática, recientemente relacionados a la Calidad de Software. Identificador ORCID: https://orcid.org/0000-0003-0023-0079

CONFLICTO DE INTERESES

No existe conflicto de intereses de los autores o de las instituciones a las cuales pertenecen en relación al contenido del artículo aquí reflejado.

CONTRIBUCIONES DE LOS AUTORES

La autora realizó la conceptualización, preparación, creación y desarrollo del artículo.

Manuscrito recibido: 31-08-2022, aceptado: 24-04-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele