

LILIAN COELHO DE FREITAS
(ORGANIZADORA)

Collection:

APPLIED COMPUTER ENGINEERING

Atena
Editora
Ano 2022

LILIAN COELHO DE FREITAS
(ORGANIZADORA)

Collection:

APPLIED COMPUTER ENGINEERING

Editora chefe

Profª Drª Antonella Carvalho de Oliveira

Editora executiva

Natalia Oliveira

Assistente editorial

Flávia Roberta Barão

Bibliotecária

Janaina Ramos

Projeto gráfico

Camila Alves de Cremo

Daphynny Pamplona

Gabriel Motomu Teshima

Luiza Alves Batista

Natália Sandrini de Azevedo

Imagens da capa

iStock

Edição de arte

Luiza Alves Batista

2022 by Atena Editora

Copyright © Atena Editora

Copyright do texto © 2022 Os autores

Copyright da edição © 2022 Atena Editora

Direitos para esta edição cedidos à Atena Editora pelos autores.

Open access publication by Atena Editora



Todo o conteúdo deste livro está licenciado sob uma Licença de Atribuição *Creative Commons*. Atribuição-Não-Comercial-Não-Derivativos 4.0 Internacional (CC BY-NC-ND 4.0).

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores, inclusive não representam necessariamente a posição oficial da Atena Editora. Permitido o *download* da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

Todos os manuscritos foram previamente submetidos à avaliação cega pelos pares, membros do Conselho Editorial desta Editora, tendo sido aprovados para a publicação com base em critérios de neutralidade e imparcialidade acadêmica.

A Atena Editora é comprometida em garantir a integridade editorial em todas as etapas do processo de publicação, evitando plágio, dados ou resultados fraudulentos e impedindo que interesses financeiros comprometam os padrões éticos da publicação. Situações suspeitas de má conduta científica serão investigadas sob o mais alto padrão de rigor acadêmico e ético.

Conselho Editorial**Ciências Exatas e da Terra e Engenharias**

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto

Profª Drª Alana Maria Cerqueira de Oliveira – Instituto Federal do Acre

Profª Drª Ana Grasielle Dionísio Corrêa – Universidade Presbiteriana Mackenzie

Profª Drª Ana Paula Florêncio Aires – Universidade de Trás-os-Montes e Alto Douro

Prof. Dr. Carlos Eduardo Sanches de Andrade – Universidade Federal de Goiás

Profª Drª Carmen Lúcia Voigt – Universidade Norte do Paraná



Prof. Dr. Cleiseano Emanuel da Silva Paniagua – Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Prof. Dr. Douglas Gonçalves da Silva – Universidade Estadual do Sudoeste da Bahia
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Profª Drª Érica de Melo Azevedo – Instituto Federal do Rio de Janeiro
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará
Profª Dra. Jéssica Verger Nardeli – Universidade Estadual Paulista Júlio de Mesquita Filho
Prof. Dr. Juliano Bitencourt Campos – Universidade do Extremo Sul Catarinense
Prof. Dr. Juliano Carlo Rufino de Freitas – Universidade Federal de Campina Grande
Profª Drª Luciana do Nascimento Mendes – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
Prof. Dr. Marcelo Marques – Universidade Estadual de Maringá
Prof. Dr. Marco Aurélio Kistemann Junior – Universidade Federal de Juiz de Fora
Prof. Dr. Miguel Adriano Inácio – Instituto Nacional de Pesquisas Espaciais
Profª Drª Neiva Maria de Almeida – Universidade Federal da Paraíba
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Profª Drª Priscila Tessmer Scaglioni – Universidade Federal de Pelotas
Prof. Dr. Sidney Gonçalo de Lima – Universidade Federal do Piauí
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista



Diagramação: Camila Alves de Cremo
Correção: Yaidy Paola Martinez
Indexação: Amanda Kelly da Costa Veiga
Revisão: Os autores
Organizadora: Lilian Coelho de Freitas

Dados Internacionais de Catalogação na Publicação (CIP)

C697 Collection: applied computer engineering / Organizadora Lilian Coelho de Freitas. – Ponta Grossa - PR: Atena, 2022.

Formato: PDF

Requisitos de sistema: Adobe Acrobat Reader

Modo de acesso: World Wide Web

Inclui bibliografia

ISBN 978-65-5983-859-2

DOI: <https://doi.org/10.22533/at.ed.592222801>

1. Computer engineering. I. Freitas, Lilian Coelho de (Organizadora). II. Título.

CDD 621.39

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora

Ponta Grossa – Paraná – Brasil

Telefone: +55 (42) 3323-5493

www.atenaeditora.com.br

contato@atenaeditora.com.br



DECLARAÇÃO DOS AUTORES

Os autores desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao artigo científico publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que os artigos científicos publicados estão completamente isentos de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autorizam a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.



DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação dos manuscritos publicados, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. Todos os e-book são *open access*, *desta forma* não os comercializa em seu site, sites parceiros, plataformas de *e-commerce*, ou qualquer outro meio virtual ou físico, portanto, está isenta de repasses de direitos autorais aos autores; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como nenhum outro dado dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.



APRESENTAÇÃO

Atena Editora is honored to present the e-book entitled “*Collection: Applied Computer Engineering*”. This volume presents 17 chapters about applications of computer engineering in industrial automation, robotics, data science, information security, neuromarketing, speech development in children, among others.

We want to take this moment to thank all of our authors for entrusting us with their discoveries. We are also grateful to the reviewers and readers who have contributed to the success of our books.

Enjoy your reading.

Lilian Coelho de Freitas

SUMÁRIO

CAPÍTULO 1..... 1

ALIMENTADOR AUTOMÁTICO DE PET UTILIZANDO A PLATAFORMA ARDUÍNO

Márcio Valério de Oliveira Favacho

Vivian da Silva Lobato

Raphael Saraiva de Sousa

Alberto Cauã Trindade da Silva

Denise Nascimento Cardoso

Jamilly da Silva Dias


Jéssica Ferreira e Ferreira

Pedro Afonso Alcântara Negrão

Rízia de Cássia da Fonseca Pereira

Ruam Melo dos Santos

Weliton Quaresma Ferreira

 <https://doi.org/10.22533/at.ed.5922228011>

CAPÍTULO 2..... 14


ANÁLISE DE AGRUPAMENTO PARA APRIMORAR A EXTRAÇÃO AUTOMÁTICA DE DEMONSTRATIVOS FINANCEIROS COM ESTUDO DE ESCALABILIDADE

Igor Raphael Magollo

Gabriel Olivato

Victor Vieira Ferraz

Murilo Coelho Naldi

 <https://doi.org/10.22533/at.ed.5922228012>


CAPÍTULO 3..... 32

AVALIANDO A USABILIDADE DE APLICAÇÕES VOLTADAS PARA A COMUNICAÇÃO DE CRIANÇAS COM TEA

Joêmia Leilane Gomes de Medeiros

Welliana Benevides Ramalho

Edinadja Mayara de Macedo

 <https://doi.org/10.22533/at.ed.5922228013>

CAPÍTULO 4..... 47

CONTROLE E MONITORAMENTO AUTOMATIZADO DOS FATORES LIMNOLÓGICOS IDEAIS PARA LARVICULTURA DO PTEROPHYLLUM SCALARE (ACARÁ BANDEIRA) UTILIZANDO TÉCNICAS DE INTELIGÊNCIA ARTIFICIAL


Raphael Saraiva de Sousa

Otávio Noura Teixeira

Augusto César Paes de Souza

Márcio Valério de Oliveira Favacho

Renato Hidaka Torres

 <https://doi.org/10.22533/at.ed.5922228014>

CAPÍTULO 5..... 63

GESTIÓN DE RIESGOS Y CONTINUIDAD DEL NEGOCIO SOBRE LA SEGURIDAD

INFORMÁTICA EN EL SECTOR RETAIL EN MÉXICO

José Eduardo Mendoza Macias

Emigdio Larios Gómez

 <https://doi.org/10.22533/at.ed.5922228015>

CAPÍTULO 6..... 73

IAÇÁ – OTIMIZAÇÃO DO PROCESSO DE EXTRAÇÃO DA POLPA DE AÇÁ UTILIZANDO A PLATAFORMA ARDUÍNO

Márcio Valério de Oliveira Favacho

Vivian da Silva Lobato

Adenildo da Conceição Silva da Silva

Ana Flavia Dias da Silva

Ian Castro Marinho da Silva

Leonan Gustavo Silva Rodrigues


Lilian Raquel de Campos Cardoso

Marily Luciene Pantoja Costa

Nayra Pereira Ferreira

Paulo Vitor Melo Amaral Ferreira

Rodrigo Figueiró Santana

 <https://doi.org/10.22533/at.ed.5922228016>

CAPÍTULO 7..... 84

LINGUAGEM DE DOMÍNIO ESPECÍFICO PARA A AUTORIA DE APLICAÇÕES PARA TV DIGITAL

Lucas de Macedo Terças

Daniel de Sousa Moraes

Carlos de Salles Soares Neto

 <https://doi.org/10.22533/at.ed.5922228017>

CAPÍTULO 8..... 95

NEUROMARKETING APLICADO AO EMOCIONAL BRANDING

Maiara Bettu

Vanessa Angélica Balestrin

 <https://doi.org/10.22533/at.ed.5922228018>

CAPÍTULO 9..... 111

PROPOSTA DE METAMODELOS DE GEOVISUALIZAÇÃO COM RECURSOS ADAPTÁVEIS

Ítalo Moreira Silva

Alexandre Carvalho Silva

Camilo de Lellis Barreto Junior

Diogo Aparecido Cavalcante de Lima


 <https://doi.org/10.22533/at.ed.5922228019>

CAPÍTULO 10..... 116

SISTEMA INTEGRAL AUTOMATIZADO DE SEGUIMIENTO DE EGRESADOS Y

EMPLEADORES

Leonor Angeles Hernández
Mónica Leticia Acosta Miranda
Daniel Domínguez Estudillo
Edi Ray Zavaleta Olea
José Arnulfo Corona Calvario

 <https://doi.org/10.22533/at.ed.59222280110>

CAPÍTULO 11..... 126

STRENGTH PREDICTION OF ADHESIVELY-BONDED JOINTS WITH COHESIVE LAWS ESTIMATED BY DIGITAL IMAGE CORRELATION


Ulisses Tiago Ferreira Carvalho
Raul Duarte Salgueiral Gomes Campilho

 <https://doi.org/10.22533/at.ed.59222280111>

CAPÍTULO 12..... 140

TAGARELAPP: PROTÓTIPO DE INTERFACE CENTRADO NA USABILIDADE PARA O DESENVOLVIMENTO DA FALA E COMUNICAÇÃO DE CRIANÇAS COM TEA


Joêmia Leilane Gomes de Medeiros
Welliana Benevides Ramalho
Edinadja Mayara de Macedo

 <https://doi.org/10.22533/at.ed.59222280112>

CAPÍTULO 13..... 152

ESTRATEGIA DE MIGRACIÓN DE UN SISTEMA LEGADO UTILIZANDO LA METODOLOGÍA “CHICKEN LITTLE” APLICADA AL SISTEMA DE BEDELÍAS DE LA UNIVERSIDAD DE LA REPÚBLICA DE URUGUAY

Cristina González
Mariela De León

 <https://doi.org/10.22533/at.ed.59222280113>

CAPÍTULO 14..... 169

INTRODUÇÃO A ANÁLISE FORENSE COMPUTACIONAL: DETECTANDO ROOTKITS EM AMBIENTE WINDOWS


Thiago Giroto Milani
Ricardo Slavov



 <https://doi.org/10.22533/at.ed.59222280114>

CAPÍTULO 15..... 191

USO DAS TICS COMO METODO PARA ELABORAR TRABALHO RECEPCIONAL E PLATAFORMA PARA A AUTOMATIZAÇÃO DE FORMATOS DE ESTADIAS

Eloína Herrera Rodríguez
Sonia López Rodríguez
Claudia Galicia Solís

 <https://doi.org/10.22533/at.ed.59222280115>

| | |
|---|------------|
| CAPÍTULO 16 | 209 |
| NARRATIVAS ACADÊMICAS EM PESQUISA: MÁQUINAS DE GUERRA VIRTUAIS | |
| Angeli Rose | |
|  https://doi.org/10.22533/at.ed.59222280116 | |
| CAPÍTULO 17 | 218 |
| OPTIMIZATION BASED OUTPUT FEEDBACK CONTROL DESIGN IN DESCRIPTOR SYSTEMS | |
| Elmer Rolando Llanos Villarreal | |
| Maxwell Cavalcante Jácome | |
| Edpo Rodrigues de Morais | |
| João Victor de Queiroz | |
| Walter Martins Rodrigues | |
|  https://doi.org/10.22533/at.ed.59222280117 | |
| SOBRE A ORGANIZADORA | 225 |
| ÍNDICE REMISSIVO | 226 |

GESTIÓN DE RIESGOS Y CONTINUIDAD DEL NEGOCIO SOBRE LA SEGURIDAD INFORMÁTICA EN EL SECTOR RETAIL EN MÉXICO

Data de aceite: 10/01/2022

José Eduardo Mendoza Macias

Project Manager Officer de Procesos y Sistemas en una de las compañías mexicanas líderes en el sector de alimentos en México desde 2016, México

Emigdio Larios Gómez

Profesor-Investigador en la Facultad de Administración de la Benemérita Universidad Autónoma de Puebla (BUAP) y Profesor invitado en IEU Universidad

RESUMEN: Esta investigación versa sobre el desarrollo e implementación de un modelo de Gestión de Riesgos y Continuidad del Negocio sobre la seguridad informática, específicamente en las empresas de Retail; Se ha realizado mediante la metodología de investigación y estándares oficiales como *ISO / IEC 27001: 2018 Information Technology - Security Techniques - Information Security Management Systems*, *ISO 22301 Business Continuity*, *ISO 31000: 2018 Risk Management*; El modelo que se utiliza en este contexto tiene como resultado final una matriz de riesgos propuesta y un documento de Plan de continuidad del negocio. Esta investigación propone y busca obtener un marco de trabajo base para que las empresas de este sector cuenten con un sistema de gestión preventivo y correctivo ligado a los estándares oficiales reconocidos mundialmente, con el fin de afrontar posibles ataques digitales en los procesos core y procesos de soporte ante una crisis de detención

de operaciones. Este artículo expone el proceso y el resultado documental de las propuestas de este modelo bajo la metodología y estándares previamente citadas.

PALABRAS CLAVE: Retail, Informática, Gestión de Riesgos, Seguridad Informática.

INTRODUCCIÓN

La pandemia mundial por el brote del SARS COV-2, también llamado Covid-19 inicia en la provincia de Hubei, China. Expertos afirman que el virus proviene del mercado Huanan, en donde se producía la venta y consumo de animales salvajes, pescados y mariscos. El virus del Covid-19 (SARS COV-2), fue transmitido al humano por el murciélago (*Rhinolopus ferrumequinum*). El día 31 de diciembre de 2019, las autoridades de la Organización Mundial de la Salud (OMS) advirtieron del brote que estaba siendo generado en China, como resultado la OMS activó su equipo de apoyo para la gestión de incidentes (IMST). Durante el inicio de este periodo y en continuación de la pandemia, algunas empresas del sector Retail, entre otras, fueron vulneradas por ataques informáticos a los procesos operacionales.

Uno de los temores de las empresas hoy en día, son los ataques informáticos. Aunque todo tipo de empresas tienen el riesgo de sufrir amenazas de seguridad cibernética, las empresas que no tienen un plan de Gestión de Riesgos acompañado de un plan de continuidad

de negocio son las más afectadas. (Timms, 2018). Un estudio de IDC Research sobre el mercado de la ciberseguridad revela que al día se producen en el mundo 350,000 ataques de malware. En este sentido, se espera que el mercado de la ciberseguridad crezca en México un 8.1% y que alcance los 1.324 millones de dólares.

Uno de los principales problemas de las empresas es que los hackers han automatizado sus ataques. Esto supone un problema añadido, pues se puede atacar a miles de empresas a la vez. Una empresa del sector Retail y de servicios no dedicados a la tecnología suele tener un nivel de seguridad menos estricto que el que podría tener una multinacional, los hackers lo saben y se aprovechan de ello y las empresas Retail se convierten, como ha ocurrido durante la COVID-19, en un blanco fácil, la pandemia aceleró determinados procesos digitales como el confinamiento ha obligado todo tipo de empresas a digitalizarse y muchas han creado páginas webs y han abierto una vía de comunicación con sus clientes a través de Internet, No obstante, el auge de las compras online y el teletrabajo ha supuesto un incremento en el número de ciberataques. Los hackers aprovechan las vulnerabilidades como consecuencia de las conexiones remotas, el uso de la nube o la mayor exposición de los usuarios a través de campañas de phishing.

De la misma manera, un informe reciente reveló que las empresas con menos de 500 empleados pierden una media de 2.5 millones de dólares por ataque. Perder esta cantidad de dinero en una violación cibernética es devastador para las pequeñas empresas, y eso sin mencionar el daño a la reputación que proviene de ser golpeado por un ataque cibernético. (Schätter, Hansen, Wiens, & Schultmann, 2019), Los ataques informáticos más comunes donde se podrá apreciar de mejor manera en la Tabla 1, basados estas categorías se buscó agrupar todos los tipos:

| Categoría | Descripción |
|-----------|---|
| Phishing | Es la amenaza más grande, dañina y extendida a la que se tienen que enfrentar las empresas de Retail. Se estima que este tipo de ciberataque representa el 90% de todas las infracciones a las que se enfrentan las organizaciones. Solo en el último año, el phishing ha crecido un 65% y ya supone unas pérdidas por valor superior a los 12 mil millones de dólares. (Kato & Charoenrat, 2018). Se trata de un ataque de suplantación de identidad. Para llevarlo a cabo, el atacante finge ser un contacto de confianza del usuario. Al hacerlo, le anima a hacer clic en un enlace malicioso o a dar datos personales. |
| Malware | la segunda gran amenaza a la que se enfrentan las empresas de Retail. Comprende una variedad de amenazas cibernéticas como son los troyanos y virus. Mediante un ataque de malware, los piratas informáticos obtienen acceso a las redes de las empresas. Emplean estos accesos para robar datos o destruir información de la compañía dicho esto, el malware generalmente proviene de descargas de sitios web maliciosos, correos electrónicos no deseados o al conectarse a otros dispositivos infectados. |

| | |
|---------------------|--|
| Contraseñas débiles | Parte de los ataques informáticos que entran a las empresas suceden debido a las contraseñas. Establecer contraseñas débiles o fáciles de adivinar es una amenaza más para las empresas y hay compañías que utilizan varios servicios basados en la nube, que requieren diferentes cuentas, es por ellos que estos servicios a menudo pueden contener datos confidenciales e información financiera. El uso de contraseñas fáciles de adivinar o el uso de las mismas contraseñas para varias cuentas puede hacer que estos datos se vean comprometidos. |
|---------------------|--|

Tabla 1. Descripción de categorías de riesgos y tipos de ataques informáticos.

Los tipos de virus informáticos que existen, que nadie debe dudar siempre son una amenaza latente para los equipos, las empresas de retail tienen la capacidad de proteger de la mejor manera cada uno de los dispositivos y activos de la organización. De eso pueden dar fe empresas y corporaciones de diferentes niveles, que en ocasiones disponen de un departamento dedicado a enfrentar la amenaza de sufrir un ataque de cualquier malware, pero no es el caso para la mayoría de los usuarios, que también pueden ser víctimas de un ataque que les causaría pérdida de datos, y en ocasiones hasta el daño total de los equipos.

Durante esta pandemia, existe un tipo de malware que ha afectado a las empresas con tendencia alcista. El Ransomware es un tipo de software malicioso o malware. Cifra los datos de una víctima, después de lo cual el atacante exige un rescate. Una vez que se paga el rescate, el atacante envía una clave de descifrado para restaurar el acceso a los datos de la víctima (Nicholson, 2014). El rescate puede variar desde unos pocos cientos de dólares hasta millones de dólares. Normalmente, el pago se exige en forma de criptomoneda, como bitcoins. Aunque el virus informático ha estado activo durante años, su problemática ha aumentado alarmantemente durante los últimos meses. Entre las consecuencias que comporta están las graves afectaciones a actividades y organismos críticos como hospitales, empresas o gobiernos.

DESCRIPCIÓN DEL MÉTODO

Análisis y evaluación de riesgos

Existen marcos y estándares de carácter mundial que permiten el desarrollo preventivo y correctivo de la Gestión de Riesgos y Seguridad Informática, complementado con la continuidad del negocio como se ven en la Tabla 2 que se muestra a continuación.

| Categoría | Descripción |
|---|--|
| ISO / IEC 27001: 2018 Information Technology - Security Techniques - Information Security Management Systems, | Es ampliamente conocido y proporciona requisitos para un sistema de gestión de seguridad de la información (SGSI); Su uso permite a las organizaciones de cualquier tipo gestionar la seguridad de activos como información financiera, propiedad intelectual, datos de empleados o información confiada por terceros. |
| ISO 31000: 2018 Risk Management | Un marco y un proceso para gestionar el riesgo. Puede ser utilizado por cualquier organización independientemente de su tamaño, actividad o sector; El uso de ISO 31000 puede ayudar a las organizaciones a aumentar la probabilidad de lograr los objetivos, mejorar la identificación de oportunidades y amenazas, así como asignar y utilizar de manera eficaz los recursos para el tratamiento de riesgos. |
| ISO 22301 – Business Continuity, Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio - Requisitos | El estándar internacional para implementar y mantener planes, sistemas y procesos de continuidad del negocio efectivos. |

Tabla 2. Descripción de categorías de los estándares basados en esta investigación.

El riesgo es la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. (Faertes, 2015), Es la vulnerabilidad o amenaza a que ocurra un evento y sus efectos sean negativos y que alguien o algo puedan verse afectados por él. Cuando se dice que un sujeto está en riesgo, es porque se considera se encuentra en desventaja frente a algo más, sea por su ubicación o posición; además de ser susceptible a recibir una amenaza sin importar cuál sea su índole. (Zeng & Zio, 2017). Los conceptos de apetito, tolerancia y capacidad ayudan a concretar y representar los criterios y niveles de riesgo, para así poder tomar las oportunas decisiones debidamente informadas. Por otro lado, clasificar es una actividad humana que realizamos a diario, de forma lúdica, profesional o simplemente para facilitar nuestra vida. (Icontec, 2020). Clasificar implica ordenar, agrupar por similitudes y de esta manera las clasificaciones son tantas y de tantos tipos como la imaginación o necesidad humana puedan limitar, también los criterios considerados para incluir o no un elemento en un grupo son ilimitados.

De acuerdo con Xing, Zeng, & Zio (2019), El riesgo es siempre una cuestión de creencias y preferencias, es decir, es siempre una combinación del grado de certeza que tenemos sobre la ocurrencia de eventos futuros, sus consecuencias y el daño / beneficio que dicha ocurrencia nos puede reportar. (García & Moret, 2015) Por tanto, hay tantas formas de ver cada riesgo como personas somos, dicho esto, se trata de que la evaluación de riesgos se convierta en un proceso de identificación, análisis y valoración que, aunque en cada caso sea diferente, contemple siempre las creencias y preferencias del que identifica, del que analiza, del que valora y especialmente del que decide, y que condicionan los resultados obtenidos, pues bien, la forma de considerar esas creencias y preferencias es mediante los siguientes grupos de conceptos:

- Los relacionados con los riesgos considerados y su caracterización: Apetito, tolerancia y capacidad.
- Los relacionados con la valoración y la decisión: Actitud, criterios y nivel de riesgo.

Madurez y Perfil de riesgo

Eventualmente se considera también como agregado de todos ellos el concepto de perfil de riesgo, el nivel en el que se centra la gestión del riesgo determinará el tipo de objetivo al que se enfrenta y, en consecuencia, la naturaleza de la incertidumbre con la que se debe trabajar. Habitualmente, como se avanza en el grado de complejidad de los diferentes niveles, más difícil es concretar el objetivo y, por tanto, con mayor incertidumbre deberemos trabajar. (Fani & Subriadi, 2019). Así, se determina los riesgos operacionales asociados, por ejemplo, a la calidad de la pieza que sale de una máquina de mecanizado, son más fáciles de identificar, analizar y valorar, que los riesgos reputacionales asociados a lo que pueda suceder casi en cualquier parte de la organización. (Von, Nielsen, Edwards, Hasson, Ipsen, Savage, Abildgaard, Richter, Lornudd, Mazzocato,, & Reed, 2020).

También es habitual que, cuanto mayor sea el nivel de agregación, mayor efecto del contexto externo y, como menor sea, mayor efecto del contexto interno. en un plano diferente, las empresas y organizaciones en general, estructuran su “comportamiento” también en diferentes niveles, esto puede apreciar en la figura 1 a continuación.



Figura 1. Del cumplimiento a la gobernanza, diferentes niveles de agregación.

Una buena forma de entender lo que es la madurez en este contexto, es partir de las siguientes dos definiciones:

- Medida para evaluar la capacidad de una organización respecto a una determinada disciplina. (Rosemann & De Bruin ,2005).

- Proceso evolutivo en la demostración de una habilidad específica. (Nicholson, 2014).

Niveles de modelo de madurez del riesgo

Y en términos de gestión de riesgos, como puede apreciarse, ambas son complementarias; La forma en la que se mide la capacidad en el caso de la primera definición y el grado de evolución en el segundo, es lo que vendrá a denominarse, Modelo de Madurez. (OIT, 2011). De esta manera, un modelo de madurez es un sistema de evaluación que acaba ofreciendo un indicador del grado en el que determinados criterios o condiciones se están considerando y la manera en que se obtienen los indicadores dependerá de un análisis basado en cuestionarios para los que la respuesta a cada pregunta devuelve un valor que, de forma agregada con el resto, acabará conformando ese “índice” de madurez buscado. La forma en la que se realizan las preguntas, la forma de agruparlas y la puntuación asignada a cada respuesta, determinarán la coherencia y utilidad del modelo de madurez.

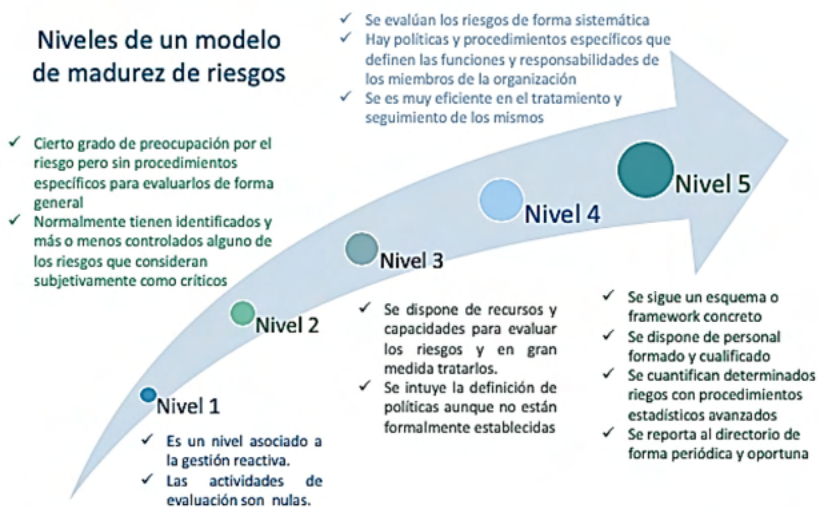


Figura 2. Propuesta de niveles de madurez, con una descripción no exhaustiva de cada nivel

En materia de gestión de riesgos, un excelente modelo integral es el desarrollado por G31000, que, aunque a fecha de febrero de 2020 solo está disponible en inglés es muy probable que no tarde en aparecer traducido al español. No obstante, la mejor forma de entender qué es un modelo de madurez es crear nuestro propio modelo, aunque solo sea a nivel de determinar las fases de madurez, las unidades sobre las que obtendremos los indicadores correspondientes, y el tipo de preguntas con los valores asociados que realizaríamos para calcular dichos indicadores.

Con base a Torabi, Rezae & Sahebjamnia (2014). Centrar ahora en las diferentes

técnicas de análisis que recoge la norma ISO 31010, fruto del trabajo de la Asociación de Profesionales de la Gestión del Riesgo y la incertidumbre en habla hispana (APEGRI). La norma indica los usos que, con carácter general y específico, se les puede dar a todas y cada una de las técnicas expuestas. Evidentemente, la relación de técnicas consideradas en la norma está pensada para dar opciones en cada una de las fases de la gestión del riesgo que contempla ISO 31000:2018. Una excelente forma de verlo, y que la norma ISO 31010:2019 incluye en la figura 3, se reproduce a continuación como adaptación de ésta.



Figura 3. Adaptación a la norma ISO 31010, mostrando todas las técnicas incluidas

COMENTARIOS FINALES

Resumen de resultados

Como se buscó en este artículo explicar el detalle entre la relación de las Normas y estándares más aceptados mundialmente en relación a la gestión de riesgos informáticos para las compañías de Retail, y se pudo abordar las diferentes técnicas y métodos para la gestión de riesgos referente al uso de este mindset. De acuerdo con los diversos autores la gestión de riesgo no es una implementación de normas, si no, una adopción de cultura organizacional para que este sea abordado a todos los niveles de la organización. De esta manera se propone una matriz de riesgos base que conlleva los siguientes puntos y su razón de ser de los mismos.

| Cabecero | Descripción |
|---------------------------------|---|
| ID | No. de Ítem en fila, típicamente este lleva un consecutivo, sin embargo, se deja a criterio del lector ocupar la secuencia a sus necesidades o código implementado por la Oficina de Gestión de Riesgos |
| Objetivo | Objetivo que se busca alcanzar dentro de la organización por lo que debería analizar el riesgo y este no interfiera con el cumplimiento del mismo. |
| Tipo de Riesgo | Categorización de riesgo por diferentes conceptos y detalle del mismo. |
| Fuente: | Motivante inicial por el que riesgo se puede materializar, típicamente este se considera en categoría generales (Externo / Interno), entrar al detalle es recomendable como departamento, categorías de procesos y supuestos de operaciones. |
| Consecuencia | Detalle del impacto que puede ocurrir si el riesgo es materializado, además de su descripción en la complejidad que el lector decida redactar. |
| Síntoma | Detalle de percepción del riesgo y criterios por los que se puede considerar como un riesgo latente a probabilidad media y máxima de materialización. |
| Impacto (Evaluación) | Según la escala de Licker este se puede considerar como Bajo, Bajo-Medio, Medio, Medio-Alto y Alto, al menos esta escala se toma como premisa de la evaluación. |
| Probabilidad (Evaluación) | De la misma manera como se evalúa el impacto, este debe ser considerado área evaluar la probabilidad de ocurrencia |
| Valor Obtenido | Según la relación de la Probabilidad y el impacto, este debe obtener una evaluación cuantitativa, típicamente se ocupa 1-9. |
| Nivel | De manera que la evaluación del valor obtenido da una calificación, esta debe ser evaluada con de manera cualitativa, típicamente se ocupa Bajo, Bajo-Medio, Medio, Medio-Alto y Alto. |
| Repuesta Preventiva | Plan de acción preventiva con el fin de relacionar los planes de ejecución antes de materializar un riesgo con el fin de cumplir con los objetivos previamente establecidos, este se puede desarrollar como texto o ligar un documento extenso. |
| Plan de Continuidad del Negocio | De la manera en cómo buscamos prevenir la ejecución de un riesgo, también se planteó un plan robusto de ejecución cuando este ya fue materializado, se plantea desarrollar un documento robusto que contenga los planes (típicamente 3) del como operar de manera que no afecte a los procesos core del negocio, este plantea y posibilita la opción de sacrificar, invertir y poner en riesgo otros procesos y/o activos |
| Responsable | Según una matriz RACI, se debe contemplar una solo persona responsable de la ejecución de la activación de los planes y análisis del riesgo para así darle mantenimiento de la gestión. |

Tabla 3. Documento final en cabeceros de Matriz de Gestión de Riesgos basados en esta investigación.

Conclusiones

Criterios, nivel, apetito, tolerancia, capacidad, actitud y perfil de riesgo son conceptos que forman parte del vocabulario habitual de todos los profesionales del riesgo. No obstante, en ocasiones se utilizan sin hacer referencia a su verdadero significado o tratándolos como sinónimos, dando lugar a verdaderos problemas de interpretación. Las clasificaciones son constructos artificiales que nos facilitan la vida. Por cada característica común que se ha tomado en algún momento como referencia para hacer una agrupación de elementos similares ha nacido una clasificación.

Los riesgos no son una excepción y, habitualmente, el nombre que toman las diferentes clasificaciones atiende a la necesidad de conocer eventos que puedan tener una misma característica en cuanto a su fuente u origen, o en cuanto al elemento que afecta. Todo proceso de gestión de riesgos comprende identificar, analizar, valorar y reportar para que se decida sobre cómo proceder (reporte interno al decisor) o cómo se ha procedido (reporte externo a partes interesadas).

Por otro lado, aunque la mejor clasificación es siempre la que nos sea más útil, en determinados sectores, normalmente fuertemente regulados, debemos considerar clasificaciones o taxonomías bien definidas y cerradas. El sector financiero, y las actividades con potencial impacto sobre la población en general, son buenos ejemplos de ello.

Como se puede apreciar en este análisis final, se propone estos cabeceros como documento base de la gestión de riesgos dentro de las empresas de Retail, este artículo busca motivar al lector a investigar más al detalle cada uno de los conceptos y marcos de referencia de esta materia corporativa de gestión con el fin de aprovechar y maximizar el potencial de los planes de acción preventivos y correctivos.

REFERENCIAS

Faertes, D. (2015). Reliability of Supply Chains and Business Continuity Management. *Procedia Computer Science*, 55, 1400-1409. <https://doi.org/10.1016/j.procs.2015.07.130>

Fani, S. V., & Subriadi, A. P. (2019). Business Continuity Plan: Examining of Multi-Usable Framework. *Procedia Computer Science*, 161, 275-282. <https://doi.org/10.1016/j.procs.2019.11.124>

Fresia Yanina Holguín García, Lohana Mariella Lema Moret, (2015) "Model for Measuring the Maturity of the Risk Analysis of Information Assets in the context of Shipping Companies". Universidad de Espiritu Santo (Ecuador)

Guía Técnica metodologías para el análisis de riesgos: Métodos cuantitativos. 1994. Dirección General de Protección Civil y Emergencias. Disponible de forma gratuita en internet

Icontec. (2020). GTC-ISO 22313. Seguridad y resiliencia. Sistemas de continuidad de negocio. Orientación sobre el uso de la NTC ISO 22301 (Icontec).

International Organization for Standardization. (2019). ISO 22301. Security and resilience. Business continuity management systems. Requirements. International Organization for Standardization.

International Organization for Standardization. (2018). ISO / IEC 27001: 2018. Information Technology - Security Techniques - Information Security Management System, International Organization for Standardization.

International Organization for Standardization. (2018)ISO 31000: 2018, Risk Management. International Organization for Standardization.

International Organization for Standardization. (2019) ISO 31010:2019. Risk Management –Risk assessment techniques, International Organization for Standardization.

Kato, M., & Charoenrat, T. (2018). Business continuity management of small and medium sized enterprises: Evidence from Thailand. *International Journal of Disaster Risk Reduction*, 27, 577-587. <https://doi.org/10.1016/j.ijdr.2017.10.002>

Nicholson Jhon (2012). La Comisión 9/11 y la NFPA1600, Nfpajla.org <https://www.nfpajla.org/archivos/exclusivos-online/manejo-de-emergencias-materiales-peligrosos/812-la-comision-9-11-y-la-nfpa-16001>

OIT. (2011). Multi-hazard business continuity management: Guide for small and medium enterprises. https://www.ilo.org/wcmsp5/groups/public/-ed_emp/documents/instructionalmaterial/wcms_187875.pdf

Rosemann, Michael; de Bruin, Tonia; and Hueffner, Tapio, "A Model for Business Process Management Maturity" (2004). ACIS 2004 Proceedings. 6. <http://aisel.aisnet.org/acis2004/6>

Schätter, F., Hansen, O., Wiens, M., & Schultmann, F. (2019). A decision support methodology for a disaster-caused business continuity management. *Decision Support Systems*, 118, 10-20. <https://doi.org/10.1016/j.dss.2018.12.006>

Timms, P. (2018). Business continuity and disaster recovery –advice for best practice. *Network Security*, 2018(11), 13-14. [https://doi.org/10.1016/S1353-4858\(18\)30113-2](https://doi.org/10.1016/S1353-4858(18)30113-2)

Torabi, S. A., Rezaei Soufi, H., & Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management (with a case study). *Safety Science*, 68, 309-323. <https://doi.org/10.1016/j.ssci.2014.04.017>

Von Thiele, U., Nielsen, K., Edwards, K., Hasson, H., Ipsen, C., Savage, C., Simonsen Abildgaard, J., Richter, A., Lornudd, C., Mazzocato, P., & Reed, J. E. (2020). How to design, implement and evaluate organizational interventions for maximum impact: The Sigtuna Principles. *European Journal of Work and Organizational Psychology*, 1-13. <https://doi.org/10.1080/1359432X.2020.1803960>

Xing, J., Zeng, Z., & Zio, E. (2019). Dynamic business continuity assessment using condition monitoring data. *International Journal of Disaster Risk Reduction*, 41, 101334. <https://doi.org/10.1016/j.ijdr.2019.101334>

Zeng, Z., & Zio, E. (2017). An integrated modeling framework for quantitative business continuity assessment. *Process Safety and Environmental Protection*, 106, 76-88. <https://doi.org/10.1016/j.psep.2016.12.002>

ÍNDICE REMISSIVO

A

- Acai berry* 74
- Accessibility* 2, 32, 140
- Adaptability* 112
- Adhesive joints* 126, 136, 138, 139
- Advertisement videos* 96
- Animals* 2
- Aquaculture reproduction* 48
- Arduino* 2, 4, 5, 12, 47, 49, 52, 57, 61, 74, 77, 80, 82
- Autistic spectrum disorder* 32, 140
- Automated monitoring* 47, 48
- Automation* 74, 191
- Automation software* 191

C

- Clustering* 14, 15, 29, 30, 31
- Cognition* 111, 112
- Cohesive zone models* 126, 138, 139
- Compilers* 84
- Cyber-crime* 169

D

- Data science* 15
- Digital image correlation* 126, 128, 130
- Digital TV* 84, 94

E

- Emotional branding* 95, 96, 99, 101, 102, 108
- Employers* 116

F

- Feature extraction* 15
- Final project report* 191
- Finite element method* 126, 127

G

Geovisualization 111, 112

Gestión de riesgos 63, 65, 68, 69, 70, 71

Gestión proyecto 152

Graduates 116

I

Informática 11, 30, 46, 63, 65, 77, 82, 94, 152, 169, 170, 171, 172, 187, 189

Information technologies 191

Innovation 74, 110

Interface 4, 32, 33, 35, 36, 38, 40, 45, 52, 76, 112, 114, 115, 128, 138, 140, 141, 143, 144, 145, 146, 149, 150, 175, 177, 178, 180, 185, 186

M

Machine learning technique 47, 48

Máquinas de guerra 209, 214, 215

Migración sistema legado 152

N

Narrativas académicas 209

Neuromarketing 95, 96, 98, 99, 101, 102, 107, 108, 109, 110

P

Panvel Pharmacy 96

PEG 84, 89

Prototype 2, 74, 140

R

Retail 63, 64, 65, 69, 71

Rootkit 169, 170, 180, 184, 185, 186, 188

S

Scouts 74

Seguridad informática 63, 65

Sistema bedelías 152

Sistema de gestión de la enseñanza 152

Sistema misión crítica 152

Structural adhesives 126, 127, 128

U

Usability assessment 32

V





Virtual learning space 191

 www.atenaeditora.com.br
 contato@atenaeditora.com.br
 [@atenaeditora](https://www.instagram.com/atenaeditora)
 www.facebook.com/atenaeditora.com.br

Collection:

APPLIED COMPUTER ENGINEERING


Ano 2022

 www.atenaeditora.com.br
 contato@atenaeditora.com.br
 [@atenaeditora](https://www.instagram.com/atenaeditora)
 www.facebook.com/atenaeditora.com.br

Collection:

APPLIED COMPUTER ENGINEERING


Ano 2022