Seguridad informática: Mejores prácticas en las organizaciones

Computer security: Best practices in organizations

Autores: Palau Delgado Sandro Antonio, Cajape Bravo Jesús Stefano, Quijije Vera Carlos Pierre, Aura Dolores Zambrano Rendón.

sandro.palau@espam.edu.ec,
jesus.cajape@espam.edu.ec,
carlos.quijije@espam.edu.ec,
azambrano@espam.edu.ec.

Resumen

La seguridad informática es una disciplina vital para la protección de datos y recursos en todas las empresas y organizaciones. A menudo se realizan análisis estadísticos para determinar qué prácticas de seguridad son las mejores para implementar, y el presente artículo pretende recopilar esta información mediante una revisión sistemática para su posterior análisis, que se divide en un conteo de tendencias, clasificación de prácticas, y la posterior identificación de ventajas y desventajas de las prácticas de seguridad informática establecidas como las más utilizadas. Las mejores prácticas para la seguridad informática en las empresas y organizaciones según este estudio, giran en torno a la implantación de políticas y procedimientos adecuados, el uso de herramientas de seguridad eficaces y el establecimiento de una cultura de seguridad sólida. De acuerdo con esto, se identificaron cinco categorías en las que una práctica de seguridad informática se puede clasificar: Gestión de riesgos, ciberseguridad, privacidad de datos, recuperación de desastres y educación/concientización.

Palabras clave: Protección de datos; vulnerabilidades; ciberseguridad; buenas prácticas.

Abstract

Computer security is a vital discipline for the protection of data and resources in all companies and organizations. Statistical analyzes are often performed to determine which security practices are the best to implement, and this article aims to collect this information through a systematic review for further analysis, which is broken down into trend count, practice ranking, and subsequent identification of advantages and disadvantages of computer security practices established as the most efficient. The best practices for computer security in companies and organizations, according to this study, revolve around the implementation of adequate policies and procedures, the use of effective security tools and the establishment of a solid security culture. Based on this, five categories were identified into which an IT security practice can be classified: Risk Management, Cybersecurity, Data Privacy, Disaster Recovery, and Education/Awareness.

Keywords: Data Protection; vulnerabilities; cybersecurity; techniques

1. Introducción

“La sociedad actual está desarrollando un sentido de responsabilidad y seguridad corporativas que debe ser cumplido estrictamente por las organizaciones, el cual busca un enfoque innovador y especial, que disponga de un conjunto de servicios avanzados de consultoría para alcanzar la seguridad corporativa completa. Al respecto, algunos expertos manifiestan que la seguridad no es solamente implementar usuarios y contraseñas, sino también poner en funcionamiento políticas que garanticen la seguridad tanto física como lógica de la información” (Vianey and Gutiérrez 2020).

Las mejores prácticas de seguridad informática son un conjunto de normas y recomendaciones que ayudan a proteger los sistemas y la información de una organización. Las buenas prácticas de seguridad deben adaptarse a las necesidades específicas de cada organización, pero algunos elementos clave incluyen la protección de los datos, la seguridad de los equipos y la gestión de los riesgos.

Entonces, para que una organizacón pueda protegerse de cualquier ataque informatico exiten cienco categorías de seguridad informatica, tales

como: Gestión de riesgos, ciberseguridad, privacidad de datos, recuperación de desastres y educación/concientización, estás mismas son fundamentales para una buena práctica de seguridad informática porque permiten establecer un marco general para la protección de la información y los sistemas de información (Romero et al. 2018)

De acuerdo con Tellez Carbajal (2018), la protección de los datos es esencial para cualquier organización que trate información confidencial o sensible. Los datos deben almacenarse de forma segura y protegidos contra accesos no autorizados. La seguridad de los equipos es otro aspecto crucial de la seguridad informática. Los ordenadores y otros dispositivos deben estar protegidos contra virus y ataques externos, y los sistemas deben ser regularmente actualizados. La gestión de los riesgos es un elemento importante de las mejores prácticas de seguridad informática. Las organizaciones deben identificar y evaluar los riesgos a los que están expuestos, y tomar medidas para minimizar el impacto de los riesgos.

En este propósito, este artículo hace una revisión bibliográfica sobre la seguridad informática en las organizaciones y que técnicas de seguridad deben utilizar las mismas para garantizar la integridad de su información en cualquier momento y lugar, teniendo en cuenta que dentro del entorno de la red se debe asegurar la confidencialidad, integridad y disponibilidad de la información sin dejar de protegerla, para prevenir las operaciones de daños ya sean no intencionados o deliberados.

2. Materiales y Métodos

Para obtener el objetivo planteado se empleó la metodología de revisión sistemática (Carrizo y Moller, 2018) que consta de tres etapas: definición de la búsqueda, ejecución de la búsqueda y discusión de los resultados.

2.1 Definición para la búsqueda

Se revisó bibliografía específica de artículos científicos en distintas bibliotecas y repositorios digitales relacionados con “Seguridad informática: Las mejores prácticas para empresas y organizaciones”, y se identificaron alrededor de 30 artículos, de los cuales se implementan una o más prácticas específicas de seguridad informática. De forma más detallada, se tomaron en cuenta artículos desde el 2017, además se realizó una búsqueda más personalizada con las siguientes palabras clave: Seguridad informática, vulnerabilidades, ciberseguridad, buenas prácticas. en repositorios de bases de datos confiables como ScienceDirect, IEEExplore, Scielo, Dialnet, Redalyc, SpringerLink, eLibro, Google (Académico).

2.2 Ejecución de la búsqueda

A continuación, se distribuyeron los campos específicos para el proceso de extracción de información de los artículos investigados. En la Tabla 1 se detalla una referencia sobre la formulación de los campos necesarios para realizar la recopilación de información propuesta en la revisión bibliográfica.

Tabla 1 – Campos que se consideraron en la recopilación de información.

Campos	**Descripción**
Año	Año en el que se aprobó y publicó el artículo científico. Solo se investigaron artículos con al menos de 5 años de antigüedad.
Título	Nombre con el que se identifica el artículo.
Autor(es)	Aquellos que participaron en la elaboración de los artículos investigados.
Prácticas	Prácticas específicas de seguridad informática que adoptan distintas organizaciones para proteger sus sistemas y la integridad de sus datos.

2.3 Discusión de los resultados

En la última etapa, se realizaron pruebas estadísticas específicas con los artículos científicos que se consideraron relevantes de acuerdo con las palabras claves, y tomando en cuenta como punto crítico la descripción de una práctica de seguridad informática específica como parte de los resultados. De esta forma, se realizaron dos pruebas respectivamente, que involucran actividades de conteo, medidas de tendencia central y dispersión respectivamente:

Análisis de descripción de prácticas de seguridad informática- Funciona como un punto de partida del estudio, con el objetivo de indicar cuál es la tendencia de aplicación de consideración en este tipo de problemas.

Demostrar cuáles son las prácticas de seguridad informáticas más eficientes. - De acuerdo a la descripción de tendencias propuesta previamente, se pretende aislar a aquellas prácticas más populares, y de estas, analizar las ventajas y desventajas. En el caso de que la distribución de las prácticas presente varias técnicas, se crearán etiquetas específicas para categorizar a las mismas (de 3 a 5 categorías). Estos criterios de clasificación se implementaron para llegar a la primera aproximación de los resultados de forma sencilla.

3. Resultados y Discusión

En base a la revisión bibliográfica clasificada, se lograron obtener resultados basados en las buenas prácticas de ciberseguridad en organizaciones y empresas. Se analizaron 30 artículos, de diferentes autores, los cuales usaron o promueven algunas de estas prácticas.

Para la clasificación de estas prácticas, se incluyeron las siguientes categorías: Gestión de riesgos, ciberseguridad, privacidad de datos, recuperación de desastres y educación/concientización como se observa en la tabla 2.

Tabla 2. Clasificación de prácticas.

Prácticas de SI	**Categoría**
Ley de Evaluación de la Fuerza Laboral de Ciberseguridad (Mishra et al. 2022)	Ciberseguridad
Evitar prácticas de ISKS dentro de la organización (Hassandoust, Subasinghage, and Johnston 2022)	Educación/concientización
Análisis de ciberseguridad cognitiva (Jiang and Atif 2021)	Ciberseguridad
Análisis de riesgos y ciberseguridad (Razikin and Soewito 2022).	Gestión de riesgos
Proceso con gestión de riesgos cibernéticos (Senarak 2021).	Gestión de riesgos
Política de seguridad específica para el usuario (AlQadheeb, Bhattacharyya, and Perl 2022).	Privacidad de datos
Política de seguridad de la información (Bhaharin et al. 2019)	Privacidad de datos
Sistema de Gestión de la Seguridad de la Información (GERARDO AYALA GONZÁLEZ JULIÁN ALBERTO GÓMEZ ISAZA 2011).	Privacidad de datos
SNORT en un entorno de detección de intrusos para la prevención de incidentes de ciberseguridad (MEDINA 2020).	Ciberseguridad

Aplicación de la seguridad informática en los sistemas contables (Hernández et al. 2019).	Gestión de riesgos
ISO 27001 (Ahmad et al. 2021).	Educación/concientización
Tecnologías de la Información (Vianey and Gutiérrez 2020).	Educación/concientización
Seguridad de información en el seminario de actualización profesional (Bogantes 2020).	Privacidad de datos
Técnicas de prevención ciberseguridad (Cando-Segovia and Medina-Chicaiza 2021).	Ciberseguridad
Las Tecnologías de la Información y la Comunicación (Landum, Moura, and Reis 2020).	Educación/concientización
Establecer políticas y lineamientos sobre los cuales se debe direccionar el desarrollo de la seguridad de la información (Susanti et al. 2017).	Educación/concientización
Política propia sobre seguridad TIC (Urruchi and Seprose 2021).	Educación/concientización
Estrategias de los sistemas de información (Sisti 2019).	Gestión de riesgos
Análisis de la Eficacia de los Controles de Seguridad de la Información (Sun et al. 2020).	Gestión de riesgos
Método de acuerdo con los requisitos de seguridad de la información que se compone de un marco tecnológico (Wang, Yao, and Yu 2018).	Gestión de riesgos
La seguridad de la información corporativos o personales (González López and Ramírez Mesa 2020).	Privacidad de datos
ISO 27000 (R. D. Cárdenas 2020).	Educación/concientización
ISO 27002 (Díaz 2018)	Educación/concientización
Implementación de Políticas y Estrategias para entidades públicas (Tim May, Malcolm Williams, Richard Wiggins 2021).	Educación/concientización
Implementación de políticas y controles por medio de SGSI – Auditoría (Torres 2019).	Gestión de riesgos
ISO 27000 (Galarza Jojoa 2019).	Educación/concientización
Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 (Tonysé de la Rosa Martín 2021).	Educación/concientización
ISO 27002 (Pérez 2021).	Educación/concientización

Políticas de Ciberseguridad para los Dispositivos de Conmutación de Red en el Centro de Datos Hospitalario (Case et al. 2022).	Ciberseguridad
Mecanismos de ciberseguridad en dispositivos de teletrabajo para una institución financiera (Guevara 2022).	Ciberseguridad

De los resultados obtenidos se tabularon los datos según la clasificación categórica establecida, y se clasificaron como se observa en la tabla 3.

Tabla 3. Promedio de datos

Categoría	F	Fr
Ciberseguridad	6	0,2
Educación/concientización	12	0,4
Gestión de riesgos	7	0,233
Privacidad de datos	5	1,166
Recuperación de desastres	0	0
Total	30	1

En base a ello se lograron obtener los siguientes resultados, en la tabla 3 se aprecia que de las prácticas más comunes realizadas por las organizaciones, están las educación/ concientización, esto quiere decir que las empresas y organizaciones se preocupan por que sus empleados tengan claras algunas normas de seguridad informática, para evitar este tipo de incidentes dentro de as organizaciones.

4. Conclusiones

Tras la realización del detallado análisis al que se sometió el presente estudio, y tomando en consideración los artículos recopilados sobre las buenas prácticas de seguridad informática en las organizaciones, se definen los siguientes puntos como conclusión:

- De los resultados obtenidos se puede concluir que las organizaciones y empresas, se preocupan por qué sus empleados tengan conocimientos básicos de seguridad informática para evitar algún tipo de ataque a estas mismas entidades.

- Las empresas deben considerar la seguridad informática como una inversión, y no como un costo, y deben implementar las mejores prácticas de seguridad para proteger sus sistemas y datos.

- De igual manera, las organizaciones deben adoptar buenas prácticas de seguridad informática para protegerse contra amenazas cibernéticas. La seguridad informática es esencial para la protección de los datos, la infraestructura y los activos de las empresas. Las buenas prácticas de seguridad informática pueden ayudar a las organizaciones a protegerse contra ataques cibernéticos, robos de información y otras amenazas, lo que generalmente contribuye a recuperar la confianza de los clientes y la reputación de la organización.

- El nivel de impacto de las prácticas y estándares de seguridad informática es una responsabilidad compartida entre todos los miembros de una organización o empresa. Todos deben colaborar para proteger los sistemas y la información de la organización.

5. Referencias

Ahmad, Atif, Sean B. Maynard, Kevin C. Desouza, James Kotsias, Monica T. Whitty, and Richard L. Baskerville. 2021. "How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice." Computers and Security 101:102122. doi: 10.1016/j.cose.2020.102122.

AlQadheeb, Arwa, Siddhartha Bhattacharyya, and Samuel Perl. 2022. "Enhancing Cybersecurity by Generating User-Specific Security Policy through the Formal Modeling of User Behavior." Array 14(April):100146. doi: 10.1016/j.array.2022.100146.

Bhaharin, Surayahani Hasnul, Umi Asma Mokhtar, Rossilawati Sulaiman, and Maryati Mohd Yusof. 2019. "Issues and Trends in Information Security Policy Compliance." International Conference on Research and Innovation in Information Systems, ICRIIS December-2019. doi: 10.1109/ICRIIS48246.2019.9073645.

Bogantes, Alejandro. 2020. "El Rol de La Seguridad Informática En El Ámbito Académico y Los Sistemas de Información Asociados." CICIC 2020 - Decima Conferencia Iberoamericana de Complejidad, Informatica y Cibernetica, Memorias 1:57–62.

Cando-Segovia, Mauricio Rodrigo, and Patricio Medina-Chicaiza. 2021. "Prevención En Ciberseguridad: Enfocada a Los Procesos de Infraestructura Tecnológica." 3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC 10(1):17–41. doi: 10.17993/3ctic.2021.101.17-41.

Case, Centers A., Study Políticas, De Ciberseguridad, Conmutación De Red, and Miriam Avila. 2022. "Cybersecurity Policies for Network Switching Devices in Hospital Data Cybersecurity Policies for Network Switching Devices in Hospital Data Centers : A Case Study Políticas de Ciberseguridad Para Los Disposi- Tivos de Conmutación de Red En El Centro de Da." (June). doi: 10.18502/espoch.v2i2.11413.

Díaz, Giner. 2018. "Facultad de Ingeniería Facultad de Ingeniería." Ucv 0–89.

Galarza Jojoa, Jenny Paola. 2019. Evaluación Del Sistema de Control Interno a Los Procesos de Ciberseguridad En La Empresa Ecuatran S.A.

GERARDO AYALA GONZÁLEZ JULIÁN ALBERTO GÓMEZ ISAZA. 2011. "GUÍA DE BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN CONTEXTOS DE MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS DE LA REGIÓN. GERARDO." (July).

González López, Juan Camilo, and Cristián Ramírez Mesa. 2020. "Guía de Controles y Buenas Prácticas de Ciberseguridad Para MiPymes."

Guevara, Paúl Sebastián Silva. 2022. "MECANISMOS DE CIBERSEGURIDAD EN DISPOSITIVOS DE TELETRABAJO PARA UNA INSTITUCIÓN FINANCIERA." *הארץ* (8.5.2017):2003–5.

Hassandoust, Farkhondeh, Maduka Subasinghage, and Allen C. Johnston. 2022. "A Neo-Institutional Perspective on the Establishment of Information Security Knowledge Sharing Practices." Information and Management 59(1):103574. doi: 10.1016/j.im.2021.103574.

Hernández, Muñoz, Zapata Cantero, Laura Giseth, Requena Vidal, and Dina Marcela. 2019. "Riesgos Informáticos y Alternativas Para La Seguridad Informática En Sistemas Contables En Colombia." Revista Venezolana de Gerencia 2. doi: 10.37960/revista.v24i2.31508.

Jiang, Yuning, and Yacine Atif. 2021. "A Selective Ensemble Model for Cognitive Cybersecurity Analysis." Journal of Network and Computer Applications 193(August):103210. doi: 10.1016/j.jnca.2021.103210.

Landum, Manuel, M. M. M. Moura, and Leonilde Reis. 2020. "ICT Good Practices in Alignment with Green IT." Iberian Conference on Information Systems and Technologies, CISTI 2020-June(June):24–27. doi: 10.23919/CISTI49556.2020.9141166.

MEDINA, JHON ALEXANDER MARTÍNEZ ROMERO LEIDY XIOMARA BLANCO. 2020. "RECOMENDACIONES DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN PYMES PARA LA GENERACIÓN DE SOLUCIONES DE DETECCIÓN DE INTRUSOS USANDO SNORT."

Mishra, Alok, Yehia Ibrahim, Memoona Javeria, and Asif Qumer. 2022. "Computers & Security Attributes Impacting Cybersecurity Policy Development : An Evidence from Seven Nations." Computers & Security 120:102820. doi: 10.1016/j.cose.2022.102820.

Pérez, Jose. 2021. “Modelo De Ciberseguridad Para La Universidad De Cartagena.” 9.

R. D. Cárdenas. 2020. “Gestión Tecnológica y Buenas Prácticas En Cooporecal R.” MetalINNOva (3):32.

Razikin, Khairur, and Benfano Soewito. 2022. “Cybersecurity Decision Support Model to Designing Information Technology Security System Based on Risk Analysis and Cybersecurity Framework.” Egyptian Informatics Journal (xxxx). doi: 10.1016/j.eij.2022.03.001.

Romero, Martha Irene, Grace Liliana Figueroa, Denisse Soraya Vera, José Efraín Álava, Galo Roberto Parrales, Christian José Álava, Ángel Leonardo Murillo, and Miriam Adriana Castillo. 2018. Mecanismo Correctivos En Seguridad Informática.

Senarak, Chalermpong. 2021. “Cybersecurity Knowledge and Skills for Port Facility Security Officers of International Seaports: Perspectives of IT and Security Personnel.” Asian Journal of Shipping and Logistics 37(4):345–60. doi: 10.1016/j.ajsl.2021.10.002.

Sisti, María. 2019. “Seguridad Informática: La Protección de La Información En Una Empresa Vitivícola de Mendoza 2019.” 1–86.

Sun, Zhe, Jinkun Zhang, Hongqing Yang, and Jun Li. 2020. “Research on the Effectiveness Analysis of Information Security Controls.” Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020 (Itnec):894–97. doi: 10.1109/ITNEC48623.2020.9084809.

Susanti, Henny Dwi, Revi Arfamaini, Maria Sylvia, Angelina Vianne, Yusniar Hanani D, Hanan Lanang D, Muslimah muslimah Muslimah, Lorena Saletti-cuesta, Charles Abraham, Paschal Sheeran, Wignyo Adiyoso, Wilopo Wilopo, Dominique Brossard, Wendy Wood, Robert Cialdini, Robert M. Groves, Derwin K. C. Chan, Chun Qing Zhang, Karin Weman Josefsson, Liliana Cori, Fabrizio Bianchi, Ennio Cadum, Carmen Anthonj, NIH Office of Behavioral and Social Sciences, Edward L. Deci, Richard M. Ryan, MPOC, Nicolás Brunet, Sarah Dryhurst, Claudia R. Schneider, John Kerr, Alexandra L. J. Freeman, Gabriel Recchia, Anne Marthe van der Bles, David Spiegelhalter, Sander van der Linden, Hendrik Godbersen, Laura Anna Hofmann, Susana Ruiz-Fernández, Tojo Naoko, Kogg Beatrice, Kiørboe Nikola, Aalto Kristiina, Kjær Birgitte, Council Nordic, Lorena Saletti, Natalia Tumas, Silvina Berra, Cecilia Johnson, A. Carbonetti, Gabriel Horn Iwaya, Janaína Gularte Cardoso, João Henriques de Sousa Júnior, Andrea Valéria Steil, Piyapong Janmaimool, Recommended Introduction, F. O. R. Surveys, Modules With, Recommended Order, Starting Fall, Student Feedback, Student Feedback, Ahmed Elzainy, Abir El Sadik, Waleed Al Abdulmonem, Johns Hopkins Bloomberg School of Public Health, Sara Haghighi, Caterina Lucarelli, Camilla Mazzoli, Sabrina Severini, Peter D. Lunn, Cameron A. Belton, Ciarán Lavin, Féidhlim P. McGowan, Shane Timmons, Deirdre A. Robertson, John P. Joyce, Richard G. Pfau, Ira J. Berman, Robert T. Sataloff, Michael M. Johns, Karen M. Kost, Benjamin J. Cowling, Sheikh Taslim Ali, Tiffany W. Y. Ng, Tim K. Tsang, Julian C. M. Li, Min Whui Fong, Qiuyan Liao, Mike YW Kwan, So Lun Lee, Susan S. Chiu, Joseph T. Wu, Peng Wu, Gabriel M. Leung, Talya Porat, Rune Nyrup, Rafael A. Calvo, Priya Paudyal, Elizabeth Ford, Yogi Tri Prasetyo, Allysa Mae Castillo, Louie John Salonga, John Allen Sia, Joshua Adam Seneta, Muhd Najib Abdul Kadir, Abdul Rahim Ridzuan, M. I. A. .. Kashim, Mohd Noor, Syaidatun Nazirah Abu Zahrin, Ahmad Fakhrurrazi Mohammed, Sarah Dryhurst, Claudia R. Schneider, John Kerr, Alexandra L. J. Freeman, Gabriel Recchia, Anne Marthe van der Bles, David Spiegelhalter, Sander van der Linden, Council Isbn, This Pdf, National Academies Press, National Academy, Society Panel, Engineering Interactions, With Society, Council Isbn, This Pdf, National Academies Press, National Academy, Fernando Filgueira, Fabricio Carneiro, Antonio Matas, Jay J. Va. Bavel, Katherine Baicker, Paulo S. Boggio, Valerio Capraro, Aleksandra Cichocka, Mina Cikara, Molly J. Crockett, Alia J. Crum, Karen M. Douglas, James N. Druckman, John Drury, Oeindrila Dube, Naomi Ellemers, Eli J. Finkel, James H. Fowler, Michele Gelfand, Shihui Han, S. Alexander Haslam, Jolanda Jetten, Shinobu Kitayama, Dean Mobbs, Lucy E. Napper, Dominic J. Packer, Gordon Pennycook, Ellen Peters, Richard E. Petty, David G. Rand, Stephen D. Reicher, Simone Schnall, Azim Shariff, Linda J. Skitka, Sandra Susan Smith, Cass R. Sunstein, Nassim Tabri, Joshua A. Tucker, Sander van der Linden, Paul van Lange, Kim A. Weeden, Michael J. A. Wohl, Jamil Zaki, Sean R. Zion, Robb Willer, Robert West, Susan Michie, G. James Rubin, Richard Amlôt, Dale Weston, Athena Ip, Richard Amlôt, Master P. D. F. Editor, Demo Version, Master P. D. F. Editor, Demo Version, Anonymous, IOTC, and I. R. Aryanta. 2017. “MANUAL DE BUENAS PRACTICAS SOBRE LA SEGURIDAD DE LA

INFORMACIÓN SENSIBLE DE LA ENTIDAD DEL DANE." Jurnal Keperawatan. Universitas Muhammadya Malang 4(1):724–32.

Tellez Carbajal, Evelyn. 2018. "TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS TECHNOLOGIES, INFORMATIC SECURITY AND HUMAN RIGHTS." IUS Et. Scientia 4:19–39.

Tim May, Malcolm Williams, Richard Wiggins, and Prof. Alan Bryman. 2021. "IMPORTANCIA DE LAS BUENAS PRÁCTICAS EN CIBERSEGURIDAD EN EL TRABAJO REMOTO DE ENTIDADES PÚBLICAS DE COLOMBIA EN ÉPOCA DE PANDEMIA." (1996):6.

Tonysé de la Rosa Martín. 2021. "AUTOMATIZACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001." 3(March):6.

Torres, Beduit Jorge. 2019. "Desafíos , Oportunidades y Buenas Prácticas de La Seguridad de La Información En Las Empresas , El Futuro Es Ahora." Universidad Piloto de Colombia 7.

Urruchi, Coronel Humberto, and Jefe D. E. L. Seprose. 2021. "UltraSync : La Nube Cibersegura."

Vianey, Geiver, and Ríos Gutiérrez. 2020. "Seguridad de La Información En Las Organizaciones." (July).

Wang, Yubin, Jinyu Yao, and Xiaoxue Yu. 2018. "Information Security Protection in Software Testing." Proceedings - 14th International Conference on Computational Intelligence and Security, CIS 2018 449–52. doi: 10.1109/CIS2018.2018.00106.