UNIVERSIDAD ABIERTA PARA ADULTOS

UAPA

DIRECCIÓN ACADÉMICA DE POSGRADO

MAESTRÍA EN CIBERSEGURIDAD

PROPUESTA DE IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD PARA LA PREVENCIÓN DE CIBERATAQUES A LA BASE DE DATOS DE LA EMPRESA CLICK MÁS S.R.L. OCTUBRE – DICIEMBRE 2022

INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA OPTAR POR EL TÍTULO DE MAGISTER EN CIBERSEGURIDAD

POR:

Ing. Richard Emmanuel González de Jesús

Ing. José Misael Perdomo Pérez

ASESOR(A):

Carmen Luisa Aybar de Nicasio

Santiago de los Caballeros

República Dominicana

Marzo 2023

ÍNDICE GENERAL

RESUMEN

La presente investigación tiene como objetivo analizar la situación actual de la seguridad de la base de datos de la empresa Click Más S.R.L., con la finalidad de elaborar una propuesta de medidas de seguridad para la prevención de ciberataques. Esta investigación se ha realizado tomando en cuenta la importancia que representan las informaciones almacenadas en la base de datos, y la utilidad o necesidad de las mismas para poder realizar las labores diarias del negocio.

Las vulnerabilidades detectadas por la empresa y el equipo investigador están poniendo a la empresa en peligro de ciberataques. La falta de medidas de seguridad para la base de datos puede ocasionar ataques externos que impliquen la pérdida de información confidencial y crucial para el funcionamiento del negocio. En vista de esta situación nace la necesidad por parte de la empresa de contactar al equipo investigador para llevar a cabo una investigación técnica de la situación actual, con la finalidad de obtener los datos necesarios para elaborar una propuesta de medidas de seguridad que ayuden a solucionar los problemas y áreas de oportunidad detectados.

Esta es una investigación de campo tipo cualitativa, con un diseño no experimental realizada única y exclusivamente para la situación actual de la empresa Click Más S.R.L. La técnica de recolección utilizada en esta investigación fue la encuesta con el cuestionario como instrumento, el cual permitió tener una mejor perspectiva de los conocimientos actuales del personal que se encarga y maneja la base de datos de la empresa, así como la situación actual en la cual se manejan respecto a las tareas diarias y las diferentes situaciones que se presentan. Además del cuestionario se utilizaron algunas herramientas de software para realizar escaneos y auditorías de seguridad de la base de datos, las cuáles permitieron al equipo investigador analizar todos los factores necesarios para poder realizar la propuesta de medidas de seguridad de manera personalizada en base a la situación de la empresa y sus necesidades.

Dicho levantamiento de información llevó al equipo investigador a concluir que la empresa carece de procedimientos, políticas y medidas de seguridad básicas y/o esenciales para la protección de bases de datos a nivel empresarial. Esta situación, junto al hecho de que la empresa busca mejorar la seguridad de la base de datos sin cambiar o agregar más herramientas, da como resultado una propuesta de medidas de seguridad en la cual el equipo investigador propone las políticas, procedimientos y medidas a ejecutar para aplicar los niveles de seguridad básicos de bases de datos reconocidos por normas internacionales y las buenas prácticas del sector de las tecnologías de la información para la administración y protección de las bases de datos.

Tras la elaboración de la propuesta en base a las necesidades actuales de la empresa, el equipo investigador tomó la decisión de agregar algunas recomendaciones adicionales que pueden mejorar significativamente la seguridad de la base de datos mediante la creación de políticas y procedimientos organizacionales que permiten al encargado de la base de datos y la administración de la empresa tener un mejor control y seguimiento de todo lo que sucede en la misma. Dichas recomendaciones van desde políticas y procedimientos de revisión de control interno hasta la habilitación de registros de tipo log para auditorías y la inclusión de algunas herramientas de software que ayudarán a todo el equipo de TI a tener un mejor historial y entendimiento de todos los aspectos relacionados a la seguridad de la base de datos.

CONCLUSIONES

En base a los escaneos de vulnerabilidades y el levantamiento de información realizados por el equipo investigador, se puede concluir que en la actualidad la empresa no cuenta con ningún tipo de medida de protección o seguridad para la base de datos. Todas las configuraciones y contraseñas presentes son las que traen las herramientas por defecto, lo cual pone a la empresa en una posición sumamente vulnerable ante cualquier ciberataque a su base de datos. Otro detalle es que para todas las operaciones de la base de datos se está utilizando el usuario por defecto "**root**" y sin contraseña, lo cual deja expuesta una vulnerabilidad crítica que puede ser aprovechada incluso por intrusos sin mucha experiencia en penetración de bases de datos. Estas y otras faltas de protección, como la ausencia de copias de seguridad, hacen que los datos de la empresa estén totalmente desprotegidos no solo ante ciberataques, si no ante cualquier eventualidad interna o desastre natural que pueda incurrir en daños al servidor y por consiguiente las informaciones contenidas en la base de datos.

Las informaciones recolectadas por el equipo investigador permitieron la creación de una propuesta de medidas de seguridad personalizadas a la situación actual de la empresa, sus herramientas, y sus principales debilidades. En vista de la carencia de medidas básicas de seguridad el equipo investigador decidió tomar como base las recomendaciones presentes en las normas internacionales ISO/IEC 27001 e ISO/IEC 27002. Aparte de esto se plantearon recomendaciones en formato de políticas, procedimientos y otros elementos presentes en las buenas prácticas de TI y las sugerencias de algunas instituciones de seguridad reconocidas de manera internacional, que aplican a la situación de esta empresa en particular. El equipo investigador cuenta con los conocimientos y la experiencia necesarios para aplicar y recomendar otras medidas de seguridad presentes en marcos de referencia y otras normas internacionales, pero dada la situación de la empresa y su solicitud de trabajar en esta primera etapa con las herramientas que ya cuentan, se tomó la decisión de limitar los elementos a desarrollar para asegurar que todas las medidas y las recomendaciones propuestas sean aplicables y que la empresa pueda llevarlas a cabo sin la necesidad de expandir de manera exponencial su presupuesto para la seguridad de la base de datos.

Dicha propuesta se presentó a un especialista en el área el cuál validó que los procedimientos y controles establecidos en las medidas a trabajar y las recomendaciones propuestas van de la mano con los estándares internacionales, las buenas prácticas de TI y las normas internacionales que aplican y recomiendan establecer controles de acceso y medidas de seguridad para entornos de TI. Aparte de esto se desarrolló un cuestionario de validación, el cuál fue completado con el encargado de TI para asegurar que la empresa acepta las medidas propuestas por el equipo investigador, y que también entienden que las medidas de seguridad para bases de datos no se limitan a las presentadas en esta investigación, puesto que existen muchas otras vertientes y áreas de oportunidad sobre las cuáles la empresa puede seguir mejorando su seguridad. A todo esto la empresa afirma la necesidad presente de seguir mejorando en este sentido, y estarán evaluando la implementación de las recomendaciones establecidas por el equipo investigador, así como las presentes en otras normas internacionales que van de la mano con la seguridad y la administración de TI para los equipos y recursos que de alguna manera u otra contienen o manejan los datos necesarios para las labores de la empresa. La empresa también afirma que la propuesta realizada cumple con sus expectativas y las necesidades planteadas por la administración para cumplir con los objetivos organizacionales del departamento de tecnología a corto y largo plazo.

REFERENCIAS BIBLIOGRÁFICAS

Parra, R. (2021). Auge del teletrabajo en América Latina: políticas públicas y regulación tras la pandemia de Covid-19. DPL News. https://dplnews.com/auge-del-teletrabajo-en-america-latina-politicas-publicas-y-regulacion-tras-la-pandemia-de-covid-19/

INTERPOL (s.f.). Ciberamenazas relacionadas con la COVID-19. https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19

Moya, D. (2022). Crecimiento de ciberataques obligará a las empresas a fortalecer la cultura interna e invertir más a 2023. DFSUB. https://dfsud.com/america/crecimiento-de-ciberataques-obligara-a-las-empresas-a-fortalecer-la

CNN (2021). Los ciberataques a objetivos gubernamentales y empresariales en EE.UU. https://cnnespanol.cnn.com/2021/08/12/10-ciberataques-empresas-gobierno-estados-unidos-orix/

Kaspersky (2022). Las PyMEs de América Latina enfrentan un creciente número de ciberataques. https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/

Holgado, R. (2022). Las PYMES, las grandes perjudicadas en los ciberataques: un 44% de ellas sufrió uno en España el año pasado. 20minutos. https://www.20minutos.es/tecnologia/ciberseguridad/las-pymes-las-grandes-perjudicadas-en-los-ciberataques-un-44-de-ellas-sufrio-uno-en-espana-el-ano-pasado-5020792/

IBM (2019). Seguridad de las bases de datos. https://www.ibm.com/es-es/cloud/learn/database-security

Oracle (s.f.). ¿Qué es una base de datos? https://www.oracle.com/mx/database/what-is-database/

Vásquez, Y. (2019). Estructura y Base de Datos. Universidad Nacional de Educación. https://repositorio.une.edu.pe/bitstream/handle/20.500.14039/5113/Vasquez%20Lozano%2c%20Yimmy%20Yester.pdf?sequence=1&isAllowed=y

Beal, V. (2021). Base de Datos en la Nube. Webopedia. https://www.webopedia.com/definitions/cloud-database/

Rivas, J. (2016). Bases de Datos en La Nube. TABD. https://jprivascanio.wordpress.com/2016/06/01/bases-de-datos-en-la-nube/

CEPAL (2020). Uso de contraseñas seguras. https://biblioguias.cepal.org/c.php?g=495473&p=4398100

ACENS (2015). Bases de datos y sus vulnerabilidades más comunes. https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

Izquierdo, J. y Tafur, T. (2017). Mecanismos de seguridad para contrarrestar ataques informáticos en servidores web y base de datos. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/4062/TESIS_IzquierdoCabrera_TafurCallirgos.pdf

CISCO (s.f.). ¿Qué es la seguridad de red? https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

TRENDMICRO (s.f.). ¿Cuáles son las medidas de la seguridad de red? https://www.trendmicro.com/es_es/what-is/network-security/network-security-measures.html

INFASE (2017). Motores de Bases de Datos. https://infase.net/motores-de-bases-de-datos/

Gil, M. (s.f.). La base de datos. Importancia y aplicación en educación. Instituto de Investigaciones sobre la Universidad y la Educación Distrito Federal, México. https://www.redalyc.org/pdf/132/13206506.pdf

García, J. (2022). Manejadores de base de datos (DBMS): Gestores de bases de datos (SGBD) relacionales. EWEBIK. https://ewebik.com/base-de-datos/sgbd

GEEKFLARE (2022). Las amenazas de bases de datos más peligrosas y cómo prevenirlas. https://geekflare.com/es/database-threats-and-prevention-tools/

IBM (s.f.). ¿Qué es el cifrado? Definición de cifrado de datos. https://www.ibm.com/es-es/topics/encryption

Capacho, J. y Nieto, W. (2017). Diseño de base de datos. Universidad del Norte. https://books.google.es/books?hl=es&lr=&id=TLBJDwAAQBAJ&oi=fnd&pg=PP1&dq=Roles+en+bases+de+datos&ots=I4DysFBAsF&sig=oZ4DJwcNHyf1I77eeVoLrqnEEDs#v=onepage&q=Roles%20en%20bases%20de%20datos&f=false

IBM (2021). Grupos de usuarios y usuarios de base de datos de Netezza. https://www.ibm.com/docs/es/psfa/7.1.0?topic=control-netezza-database-users-user-groups

IBM (2021). Roles de base de datos. https://www.ibm.com/docs/es/data-studio/4.1.1?topic=management-database-roles

Salesforce (s.f.). Permisos de usuario. https://help.salesforce.com/s/articleView?id=sf.admin_userperms.htm&type=5

Roque, R. y Juárez, C. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. Universidad de Guadalajara. https://www.scielo.org.mx/pdf/prts/v8n14/2007-3607-prts-8-14-00005.pdf

Motadata (s.f.). Monitoreo de bases de datos. https://www.motadata.com/es/database-monitoring/

Manage Engine (s.f.). Auditoría de bases de datos. https://www.manageengine.com/latam/eventlog/auditoria-de-bases-de-datos.html

Coronel, D. (2018). Enmascaramiento en la base de datos oracle para resguardar la información financiera y personal en la cooperativa de ahorro y crédito de la pequeña empresa de Cotopaxi. Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/bitstream/123456789/28313/1/Tesis_t1438si.pdf

GESLOPD (2020). La importancia de cambiar las contraseñas de tus cuentas con frecuencia. https://www.geslopd.es/cambiar-contrasenas/

Giménez, J. (2019). Buenas prácticas en el diseño de bases de datos. Universidad Tecnológica Intercontinental. https://www.utic.edu.py/revista.ojs/revistas/6/html/9.html

MINTIC (2016). Seguridad y privacidad de la información. https://gobiernodigital.mintic.gov.co/692/articles-150518_G12_Seguridad_Nube.pdf

Rinaldi, P. (2017). ¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético. Le VPN. https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Sánchez, S. (2017). Más de 5 mil millones de documentos y 229 empresas afectadas: así han sido los mayores robos de datos de la historia. XATAKA. https://www.xataka.com/privacidad/mas-de-5-mil-millones-de-documentos-y-229-empresas-afectadas-asi-han-sido-los-mayores-robos-de-datos-de-la-historia

Tidy, J. (2021). Scraping: "Robé los datos de 700 millones de usuarios de LinkedIn por diversión". BBC. https://www.bbc.com/mundo/noticias-57835205

CNN (2021). Los ciberataques a objetivos gubernamentales y empresariales en EE.UU. https://cnnespanol.cnn.com/2021/08/12/10-ciberataques-empresas-gobierno-estados-unidos-orix/

IBM (s.f.). ¿Qué es la ciberseguridad? https://www.ibm.com/es-es/topics/cybersecurity

Arreola, A. (2019). Ciberseguridad: ¿Por qué es importante para todos? Grupo Editorial Siglo Veintiuno.

https://books.google.es/books?id=ZqHDDwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Reinares, D. (2020). Origen e importancia de la ciberseguridad. https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/

Arias, M. (2021). Evolución de la ciberseguridad en la era digital. https://www.pwc.com/co/es/pwc-insights/evolucion-ciberseguridad.html

KIO (s.f.). La importancia de la ciberseguridad y la ciberdefensa para los países. https://www.kionetworks.com/blog/ciberseguridad/importancia-de-ciberseguridad-y-ciberdefensa-para-los-paises

Universidad Internacional de Valencia (2021). Por qué es importante la ciberseguridad. https://www.universidadviu.com/pe/actualidad/nuestros-expertos/por-que-es-importante-la-ciberseguridad

Bustamante, G. y Cano, J. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Cuaderno Activa. https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206

Cloudflare (s.f.). ¿Qué es la privacidad de los datos? https://www.cloudflare.com/es-es/learning/privacy/what-is-data-privacy/

Calero, R. (2013). Modelo de seguridad para mitigar los problemas derivados de las vulnerabilidades en dispositivos moviles android con respecto a los principios de integridad, confidencialidad y disponibilidad. Pontificia Universidad Javeriana. https://repository.javeriana.edu.co/bitstream/handle/10554/12667/CaleroAsenciosRaul2013.pdf?sequence=3&isAllowed=y

Mejía, M. (2019). Implementación de técnicas de seguridad informática para garantizar los principios de integridad, confidencialidad y disponibilidad de la información a un sistema de radiolocalización híbrido. Universidad Pontificia Bolivariana. https://repository.upb.edu.co/bitstream/handle/20.500.11912/4682/Implementaci%C3%B3n%20

de%20t%C3%A9cnicas%20de%20seguridad%20inform%C3%A1tica%20para%20garantizar.pdf?sequence=1&isAllowed=y

INCIBE (2020). Las 7 fases de un ciberataque. ¿Las conoces? https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

Chávez, C. (2021). Hacking ético: qué es, fases, informes y análisis. SEGURILATAM. https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/hacking-etico-que-es-fases-informes-y-analisis_20210729.html

Hurtado, M. (2016). Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado. Escuela Politécnica Nacional. https://biblioteca.epn.edu.ec/cgi-bin/koha/opac-detail.pl?biblionumber=45144&shelfbrowse_itemnumber=63531

IBERDROLA (2020). Ataques cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos? https://www.iberdrola.com/innovacion/ciberataques

Alcántara, B. (2018). El primer ciberataque de la historia de la humanidad ocurrió hace casi 200 años. Urbantecno. https://www.mundodeportivo.com/urbantecno/tecnologia/primer-ciberataque-historia

Holgado, R. (2022). La evolución de la ciberdelincuencia: ¿qué ataques tradicionales siguen funcionando y cuáles están cambiando? 20bits. https://www.20minutos.es/tecnologia/ciberseguridad/la-evolucion-de-la-ciberdelincuencia-que-ataques-tradicionales-siguen-funcionando-y-cuales-estan-cambiando-5040671/

Márquez, J. (2017). Armas cibernéticas. Malware inteligente para ataques dirigidos. Ingenierías USBMed. http://revistas.usbbog.edu.co/index.php/IngUSBmed/article/view/2955

Rivera, R. (2018). Dirección y clasificación de malware con el sistema de análisis de malware Cuckoo. Universidad Internacional de La Rioja. https://reunir.unir.net/bitstream/handle/123456789/7444/RIVERA%20GUEVARA%2cRICHARD%20PAUL.pdf?sequence=1&isAllowed=y

Marciá, G. (2007). Ataques de denegación de servicio a baja tasa contra servidores. Universidad de Granada. https://digibug.ugr.es/bitstream/handle/10481/1543/16714763.pdf?sequence=1

Kaspersky (s.f.). ¿Qué es un ataque de fuerza bruta? https://latam.kaspersky.com/resource-center/definitions/brute-force-attack

Chicaiza, G., Ponce, L. y Velásquez, G. (2016). Inyección de SQL, caso de estudio Owasp. Universidad de las Fuerzas Armadas ESPE.

Belcic, I. (2022). Guía esencial del phishing: cómo funciona y cómo defenderse. Avast. https://www.avast.com/es-es/c-phishing

Benedini, I. (2013). Ataque de man in the middle para protocolo sip mediante análisis de caja negra. Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0816_BenediniI.pdf

Panda (2022). ¿Qué es un ataque Man-in-the-Middle (MITM)? Definición y prevención. https://www.pandasecurity.com/es/mediacenter/seguridad/ataque-man-in-the-middle/

Baranda, J. (2020). Integración de bases de datos para la detección de ataques mediante spoofing. Universidad del País Vasco. https://addi.ehu.es/bitstream/handle/10810/47019/document.pdf?sequence=1&isAllowed=y

Comisión Federal de Comunicaciones (2022). Suplantación de Identidad Telefónica (Spoofing) y Cómo Evitarla. https://www.fcc.gov/consumers/guides/suplantacion-de-identidad-telefonica-spoofing-y-como-evitarla

OWASP (s.f.). Cross Site Scripting (XSS). https://owasp.org/www-community/attacks/xss/

Klusaitė, L. (2021). ¿Qué es el cross-site scripting (XSS)? NordVPN. https://nordvpn.com/es/blog/ataque-xss/

Dustyn, Z., Anthony, T., Puris, A. y Zhuma, R. (2020). Análisis y técnicas de prevención ante ataques ransomware. Revista Tecnológica Ciencia y Educación Edwards Deming. https://revista-edwardsdeming.com/index.php/es/article/view/73

Martínez, H. y Chuc, L. (2016). Hidden Tear: Análisis del primer Ransomware Open Source. Instituto Tecnológico Superior Progreso.

IBM (2019). Seguridad de las bases de datos. https://www.ibm.com/es-es/cloud/learn/database-security

Infogram (s.f.). Normas y Estándares de seguridad base de datos. https://infogram.com/normas-y-estandares-de-seguridad-base-de-datos-1hzj4o0ykdmd4pw

Villamizar, C. (2022). ¿Qué es COBIT y para qué sirve? GlobalSuite. https://www.globalsuitesolutions.com/es/que-es-cobit/

Cruz, E., Velázquez, J. y Briones, A. (2019). Formas, enfoques y tipos de investigación. Universidad Autónoma del Estado de Hidalgo https://www.uaeh.edu.mx/docencia/P_Presentaciones/icea/asignatura/turismo/2020/formas-tipos-investigacion.pdf

Universidad Veracruzana (s.f.). Tipos de investigación. https://www.uv.mx/apps/bdh/investigacion/unidad1/investigacion-tipos.html

EUROINNOVA (s.f.). ¿Qué es el método en una investigación? https://www.euroinnova.edu.es/blog/que-es-el-metodo-en-una-investigacion#:~:text=A%20los%20m%C3%A9todos%20de,y%20cu%C3%A1l%20es%20el%20resultado.

Diaz, M. (s.f.). Técnicas e instrumentos de investigación. Universidad de la Costa. https://eduvirtual.cuc.edu.co/moodle/pluginfile.php/618544/mod_resource/content/1/T%C3%A9cnicas%20y%20m%C3%A9todos%20inv.pdf

Diaz, N. (s.f.). Población y muestra. Universidad Autónoma del Estado de México. https://core.ac.uk/download/pdf/80531608.pdf

David, G. (2018). La importancia de proteger las Bases de Datos en una organización. Licencias Online. https://www.licenciasonline.com/ec/es/noticias/importancia-proteger-bases-de-datos

Constitución de la República Dominicana, Actualizada, Presidencia de la República, 10 de julio del año 2015, (República Dominicana). https://presidencia.gob.do/sites/default/files/statics/transparencia/base-legal/Constitucion-de-la-Republica-Dominicana-2015-actualizada.pdf

Ley 172-13 sobre Protección de los Datos Personales, Congreso Nacional, 15 de diciembre del año 2013, (República Dominicana). https://www.tribunalconstitucional.gob.do/transparencia/marco-legal/leyes/ley-172-13/

Domínguez, J. (2015). Principios Básicos de Seguridad en Bases de Datos. Universidad Politécnica Territorial del estado Aragua.

NQA (s.f.). ISO 27001: Sistemas de gestión de seguridad de la información. https://www.nqa.com/es-mx/certification/standards/iso-27001

ISOTools (2013). Norma ISO 27002: El dominio política de seguridad. https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Manrique, A. (2021). ¿Qué es el análisis de factibilidad? Testamarketing. https://testamarketing.com/blog/articulos/que-es-el-analisis-de-factibilidad

Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, Congreso Nacional, 23 de abril del año 2007, (Republica Dominicana). https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

OpenSSL (s.f.). OpenSSL 1.1.1 Series Release Notes. https://www.openssl.org/news/openssl-1.1.1-notes.html

Apache (s.f.). Overview of new features in Apache HTTP Server 2.4. https://httpd.apache.org/docs/2.4/new_features_2_4.html

OnaSystem (s.f.). Seguridad de bases de datos es afectada por vulnerabilidades. https://www.onasystems.net/seguridad-de-bases-de-datos-es-afectada-por-vulnerabilidades/

Php (s.f.). PHP 8 ChangeLog. https://www.php.net/ChangeLog-8.php#PHP_8_2

Herrera, D. (2023). HTTP vs HTTPS: Comparación, pros y contras, y más. Hostinger. https://www.hostinger.es/tutoriales/http-vs-https

Zanotti, L. (2022). Logs o archivos de registro (log): qué utilidad tienen y cómo analizarlos. Networkdigital360. https://www.innovaciondigital360.com/cyber-security/data-security/que-son-los-archivos-de-registro-log-y-por-que-no-hay-seguridad-sin-gestion-de-registros/

SCC (s.f.). La importancia de contar con una solución de backup. https://www.sccenlared.es/la-importancia-de-contar-con-una-solucion-de-backup/

MIT (s.f.). Red Hat Enterprise Linux 4: Introducción a la administración de sistemas. https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/ch-acctsgrps.html

Agencia Nacional de Investigación y Desarrollo (2023). La importancia del cambio de contraseña. https://ayuda.anid.cl/hc/es/articles/4411632424596-La-importancia-del-cambio-de-contrase%C3%B1a

IBM (2021). Modelos lógicos de datos. https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/es/ida/9.1.2?topic=modeling-logical-data-models

Universidad de América Latina (s.f.). Análisis de sistemas mediante diccionarios de datos. http://ual.dyndns.org/Biblioteca/Dise%F1os_Sistemas_Informacion/Pdf/08%20Capitulo%2008_Analisis%20de%20sistemas%20mediante%20diccionarios%20de%20datos.pdf

Aguilera, D. (2019). Por qué deberías usar un entorno de desarrollo/pruebas en tus proyectos. NELIO. https://neliosoftware.com/es/blog/por-que-deberias-usar-un-entorno-de-desarrollo-pruebas-en-tus-proyectos/

INCIBE (2019). La importancia de proteger la información mediante acuerdos de confidencialidad. https://www.incibe.es/protege-tu-empresa/blog/importancia-proteger-informacion-mediante-acuerdos-confidencialidad

Paris, J. (2022). El usuario administrador sin control puede ser tu peor pesadilla. Linkedin. https://es.linkedin.com/pulse/el-usuario-administrador-sin-control-puede-ser-tu-paris-balleza

CONTPAQI (s.f.). La importancia de asignar usuarios para proteger la información de tu empresa. https://www.contpaqi.com/publicaciones/transformacion-digital/la-importancia-de-asignar-usuarios-para-proteger-la-informacion-de-tu-empresa#:~:text=Concede%20derechos%20de%20acceso%20a,pol%C3%ADtica%20de%20uso%20de%20datos.

AIMETIS (s.f.). Concepto de grupos de usuarios. https://www.aimetis.com/webhelp/Symphony/6.13/es/Concepto_de_grupos_de_usuarios.htm#:~:text=La%20pertenencia%20a%20grupos%20facilita,los%20privilegios%20de%20cada%20usuario.&text=Si%20se%20aplica%20una%20restricci%C3%B3n,los%20miembros%20de%20ese%20grupo.

MySQL (s.f.). Configuración del formato de registro binario. https://dev.mysql.com/doc/refman/8.0/en/binary-log-setting.html

Poston, H. (2019). Protocolo de transferencia de hipertexto (HTTP) con Wireshark. INFOSEC. https://resources.infosecinstitute.com/topic/hypertext-transfer-protocol-http-with-wireshark/#:~:text=HTTP%20in%20Wireshark,%2C%20ACK%20and%20so%20on

LESATH (s.f.). Documentación Interna de la Empresa. https://lesath.mx/documentacion-interna-de-la-empresa/

Microsoft (2023). Vigencia máxima de la contraseña. https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/maximum-password-age

Tibco (s.f.). ¿Qué es un modelo de datos lógico? https://www.tibco.com/es/reference-center/what-is-a-logical-data-model

Erwin (s.f.). Modelador de datos Erwin. https://www.erwin.com/products/erwin-data-modeler/#:~:text=erwin%20Data%20Modeler%20by%20Quest,high%2Dquality%20enterprise%20data%20assets.

ALMER (2022). ¿Por qué es importante realizar auditorías periódicas? https://www.almer.com.mx/articulo/49-por-que-es-importante-realizar-auditorias-periodicas#:~:text=En%20especial%2C%20cuando%20las%20auditor%C3%ADas,para%20los%20retos%20log%C3%ADsticos%20futuros.

INFOBAE (2022). Tras la pandemia, el 83 por ciento de los jóvenes cambió su modalidad de trabajo. https://www.infobae.com/economia/2022/12/28/tras-la-pandemia-el-83-por-ciento-de-los-jovenes-cambio-su-modalidad-de-trabajo/

Diarioti (2022). Trabajo remoto, una tendencia en aumento; crecen vacantes a distancia. https://diarioti.com/trabajo-remoto-una-tendencia-en-aumento-crecen-vacantes-a-distancia/119965

INCIBE (s.f.). Copias de seguridad: una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

CIS (2022). CIS Controls v8 Mapping to ISO/IEC 27002:2022. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec2-27002-2022

ISO (2013). Estándar internacional ISO / IEC 27001.

INSTRUCCIONES PARA LA CONSULTA DEL TEXTO COMPLETO:

Para consultar a texto completo esta tesis solicite en este formulario (https://forms.gle/vx5iLzv1pAMyN3d59 como hipervínculo) o dirigirse a la Sala Digital del Departamento de Biblioteca de la Universidad Abierta para Adultos, UAPA.

Dirección

Biblioteca de la Sede – Santiago

Av. Hispanoamericana #100, Thomén, Santiago, República Dominicana

809-724-0266, ext. 276; biblioteca@uapa.edu.do

Biblioteca del Recinto Santo Domingo Oriental

Calle 5-W Esq. 2W, Urbanización Lucerna, Santo Domingo Este, República Dominicana.

Tel.: 809-483-0100, ext. 245. biblioteca@uapa.edu.do

Biblioteca del Recinto Cibao Oriental, Nagua

Calle 1ra, Urb Alfonso Alonso, Nagua, República Dominicana.

809-584-7021, ext. 230. biblioteca@uapa.edu.do