Journal **TechInnovation**
Volumen 2, Número 1, 2023
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO DE REVISIÓN

Seguridad de información en el mundo de los negocios digitales

Information security in the world of digital businesses

https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.85-91

Recibido: 19-01-2023 **Aceptado:** 24-04-2023 **Publicado:** 01-06-2023

Mario Javier Marcillo Merino[1]*
https://orcid.org/0000-0001-5818-367X

Jandry Nicolas Cantos Plúa[2]
https://orcid.org/0000-0002-2511-2776

Jean Carlos Holguín Anchundia[3]
https://orcid.org/0000-0001-5439-9166

Josefa Aracely Vera Gutiérrez[4]
https://orcid.org/0000-0001-7405-8713

1. Máster en Docencia Universitaria e Investigación Educativa; Ingeniero en Sistemas; Docente de la Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
2. Estudiante de Tecnologías de la Información, Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
3. Estudiante de Tecnologías de la Información, Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
4. Estudiante de Tecnologías de la Información, Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.

Volumen: 2
Número: 1
Año: 2023
Paginación: 85-91
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/41
***Correspondencia autor:** mario.marcillo@unesum.edu.ec

RESUMEN

Las problemáticas en el mundo de los sistemas digitales hoy en día son cada vez más frecuentes, la bases que tradicionalmente se han manejado es la Tecnología. La estabilidad digital es un criterio que ha entrado en diversos puntos de nuestra vida y, sin duda, es de enorme relevancia en el trabajo, los negocios, el descanso y muchísimo más. El objetivo de este presente trabajo es reconocer el mayor nivel de vulnerabilidad de la información en el mundo de los negocios digitales. La ciberseguridad es un punto clave para las empresas, debido a que los ataques que evita no solo están afectando a los individuos y a las organizaciones económicamente, sino que además están afectando la confianza que el público tiene sobre la organización. La tecnología ha ayudado a las empresas a automatizar sus procesos y apresurar las labores, empero con ello por igual se han abierto las puertas para que terceros con malas intenciones intenten hurtar sus datos o entren a sus sistemas para sacar beneficio ilícito.

Palabras clave: ataques; ciberseguridad; vulnerabilidad; personas.

ABSTRACT

The problems in the world of digital systems today are increasingly frequent, since the bases that have traditionally been handled is Technology. Digital stability is a criterion that has entered at various points of our life and, without a doubt, it is of enormous relevance at work, business, leisure and much more. The objective of this present work is to recognize the highest level of information vulnerability in the world of digital business. Cybersecurity is a key point for companies, because the attacks it prevents are not only affecting individuals and organizations financially, but they are also affecting the trust that the public has in the organization. Technology has helped companies automate their processes and speed up work, but with this, the doors have also been opened for third parties with bad intentions to try to steal their data or enter their systems to obtain illegal benefits.

Keywords: ttacks; cybersecurity; vulnerability; people.

Introducción

En el mundo actual de los negocios digitales, la seguridad de la información es una preocupación creciente para las empresas. Las empresas enfrentan desafíos al tratar de implementar medidas de seguridad de información adecuadas para proteger sus sistemas y datos valiosos. Este artículo discutirá las dificultades que las empresas enfrentan al aplicar la seguridad de información en el mundo de los negocios digitales y cómo pueden superar estas dificultades.

Desde el comienzo de la pandemia, se ha visto a las empresas tomar caminos digitales no tradicionales, la mayoría de ellas trabajan cara a cara en un edificio u oficina. Por ello, en los últimos meses se ha visto el poder que ha comenzado a tomar la ciberseguridad en la sociedad actual a la hora de poder crear entornos digitales seguros para empleados y empleadores, estén donde estén, con la ayuda de este servicio. Tenga esto en cuenta, una de las amenazas de ciberseguridad más comunes implica la instalación ilegal de software de terceros. Esto se debe a que intentan hacer que los programas pagos sean gratuitos mediante el uso de métodos de instalación de software pirateado para dar acceso a los ciberdelincuentes a la información en nuestros dispositivos.

Investigación sobre las dificultades al momento de utilizar alguna seguridad que se encuentran inmersas dentro del mundo digital, por ende, los indicios para este desarrollo será un gran aval para saber con exactitud las posibles dificultades en el tema. Sabemos que la tecnología avanza y hoy en la actualidad tenemos varias especificaciones como lo son los negocios digitales.

Dificultades de seguridad de la informacion

Según Iso Told Existen una gran cantidad de diferentes fallos en la seguridad de la información que suceden a diario (Iso TOOLS s.f.).

Para segmentarlos, podemos clasificarlos en tres categorías: fallos de seguridad de la información malintencionados, intencionados o delictivos, seguidos de los fallos del sistema y en tercer lugar los fallos provocados por errores humanos.

Según el estudio realizado por IBM, el 49% de los fallos de seguridad de la información se producen de forma intencionada, el 23% se debe a problemas técnicos del propio sistema y el 20% se debe a errores humanos.

Echemos un vistazo más de cerca a cada una de estas tres categorías de violaciones de la seguridad de la información.

Principales causas de los fallos en la seguridad de la información

1.- Fallos en la seguridad de la información de carácter malicioso, intencional o criminal:

Esta falla en la seguridad de la información fue premeditada y el objetivo era tener un impacto negativo en el negocio.

Entre este tipo de fallas en la seguridad de la información se encuentran el fraude, el fraude, la piratería, el robo de propiedad intelectual, los delitos informáticos, la introducción de virus o el desvío de fondos.

Para evitar este tipo de problemas, las organizaciones implementan sistemas de seguridad que les permiten proteger la información almacenada en ellos, evitando que sea robada.

En este sentido y con el objetivo de garantizar la seguridad de sus sitios, las operaciones comerciales de comercio electrónico son sometidas periódicamente a diversas pruebas.

2.- Errores técnicos del propio sistema

Para este problema es difícil detectar la razón por la que está sucediendo. Sucedió inesperadamente. Serían, por ejemplo, cuando un día operamos el equipo con total normalidad y al día siguiente al reactivar el

pedido simplemente no funciona, no hace nada.

Por lo general, estos problemas se resuelven con relativa rapidez y puede volver al trabajo.

La solución para evitar que este tipo de problemas vuelvan a ocurrir es investigar, solucionar y hacer el seguimiento correspondiente.

3.- Fallos en la seguridad de la información debido al error humano

Entre los ejemplos más comunes de este tipo de error, destacamos cosas como cuando los empleados pierden archivos o teléfonos de la empresa, cuando se comparten contraseñas que no deberían compartirse, cuando se registra información incorrecta en un sitio web en un momento inapropiado.

Ante esta falla en la Seguridad de la Información, muchas organizaciones se comprometen a implementar un Sistema de Seguridad de la Información, que trabaja para mantener la confidencialidad e integridad de sus datos y los sistemas encargados de procesarlos (Campos 2021).

Software ISO 27001

ISOTools Excelle ayuda a las organizaciones a implementar el Sistema de Gestión de Seguridad de la Información automáticamente. Las diferentes funcionalidades combinadas hacen de la plataforma una pieza de software flexible para las especificidades de diferentes organizaciones, lo que le permite aumentar el nivel de seguridad de su información y aumentar la eficiencia y eficacia en su gestión.

Seguridad de la información en el mundo digital

La seguridad digital es un concepto que ha entrado en varios aspectos de nuestra vida y, sin lugar a duda, es de gran relevancia en el trabajo, los negocios, el ocio y mucho más (DocuSing 2021).

Cuando nos referimos a la seguridad digital, este concepto engloba una gran cantidad de técnicas y procedimientos para llevar a cabo dicha protección. Gracias a las herramientas disponibles se puede evitar el hurto o hurto de información valiosa o cualquier ciberataque.

La ciberseguridad es un punto clave para las organizaciones, pues los ataques que previene no solo afectan financieramente a personas y empresas, sino que también afectan la confianza del público en la institución.

La tecnología ha ayudado a las organizaciones a automatizar sus procesos y agilizar tareas, pero con esto también se abre la puerta a que terceros con malas intenciones intenten robar sus datos o ingresar a sus sistemas para sacar provecho ilegal.

Los pilares de la seguridad de la información

Disponibilidad

Esto implica que las personas autorizadas puedan acceder a los datos cuando lo necesiten, lo que se traduce en las funciones necesarias de los sistemas informáticos y bases de datos.

Esta disponibilidad o accesibilidad debe coexistir con la inaccesibilidad de quienes no están autorizados a acceder a la información, lo que implica la adopción de medidas que restrinjan el acceso.

Confidencialidad

Esto significa que sólo podrán acceder a la información quienes estén expresamente autorizados para ello. Además, quienes conocen la información deben mantenerla confidencial.

Para hacer posible la confidencialidad, se definen diferentes medidas de control de acceso a los datos. Por ejemplo, solicitando la identificación del usuario y acreditando esa identidad a través de una contraseña que sólo debe conocer el titular.

Autenticación

Esto está muy relacionado con el tema anterior. El sistema debe poder verificar que el usuario es quien dice ser. Para ello no solo se utiliza un sistema de contraseñas, existen muchas más medidas de seguridad.

Por ejemplo, algunos softwares envían notificaciones al responsable del fichero de datos si detectan que un usuario registrado se está comportando de forma extraña o si el acceso se produce desde una ubicación o dispositivo diferente al habitual.

Integridad

La información debe protegerse de terceros no autorizados, así como de errores humanos. La manipulación de datos puede tener consecuencias nefastas para las empresas, por lo que se debe garantizar su integridad.

Para lograrlo, sólo se permiten cambios en los datos si se autorizan previamente y son realizados por personas con la debida acreditación.

La seguridad de la información es un tema complejo, pero muy importante. Datos de empresas, gobiernos, etc. Son de gran valor en el mercado y debes tratar de protegerlos de la mejor manera posible. A su vez, se debe asegurar que puedan ser utilizados por las personas autorizadas para ello.

Negocios digitales

Los negocios digitales son aquellos que utilizan Internet y la tecnología para comercializar productos o servicios (Sydle 2021).

Es un modelo de negocio en constante crecimiento que ofrece innumerables oportunidades y excelentes resultados siempre que se gestione bien. Descubra ahora cuáles son los tipos de negocios digitales más importantes, cuál es la mejor manera de administrarlos y otros valiosos consejos sobre el tema.

Tipos de negocios digitales:

- E-commerce: una plataforma de negocios donde ofreces tus productos y los clientes compran en una experiencia 100% virtual;
- Marketplace: Sitios web que intermedian las ventas por usted y ganan una comisión. Es el caso de Amazon, entre otros.
- Productos de información: son productos digitales como libros electrónicos, aplicaciones, tutoriales, etc. Pueden comercializarse u ofrecerse de forma gratuita con el fin de atraer clientes.
- Blog de Contenido: Es donde se ofrece información y curiosidades sobre un tema, servicio o producto.
- Portal de cursos: Son plataformas de cursos virtuales. Las clases se llevan a cabo a través de Internet y existe la oportunidad de que los estudiantes se comuniquen con la persona que imparte los cursos, ya sea a través de mensajes, transmisiones en vivo o foros.
- Servicios en línea: servicios como redacción, desarrollo de sitios web, revisión, traducción, análisis de SEO, redes sociales, etc.

¿Cuáles son las principales características de los negocios digitales?

En un negocio digital, es imperativo que la empresa cuente con profesionales que entiendan el tema, tecnologías apropiadas y una cultura compatible.

Porque es necesario:

- Estar siempre conectado.
- Seguimiento de las tendencias del mercado y fomento de la actualización constante.
- Aplicar marketing continuo y estratégico
- Llevar a cabo una transformación digital en la empresa.
- Implementar sistemas de control inteligente.
- Ser competitivo.
- Sepa cómo mostrar sus diferenciadores como punto de venta.

Metodología

Existen diferentes metodologías las cuales se emplearon para dar un concepto detallado, partiendo con la metodología empírico y analítico, como base para llegar a la cuestión del problema y brindar el análisis de fuentes bibliográficas para concretar conceptos sobre seguridad, el análisis de seguridad busca superar estas dificultades, y por ende las empresas deben implementar medidas de seguridad de información efectivas y estar al día en las últimas tecnologías y estrategias de seguridad.

Se utilizo el método explicativo para abarcar un concepto en referencia a seguridad de la información, la capacitación y educación en seguridad de información para los empleados también son esenciales. Las empresas deben desarrollar programas de capacitación que sean efectivos y accesibles para todos los empleados. Las pruebas regulares de penetración también son importantes para detectar vulnerabilidades y brechas de seguridad en los sistemas y mejorar la seguridad en general.

Resultados y Discusión

Se encontraron muchas vulnerabilidades y amenazas informáticas a las que están expuestas las empresas en la actualidad, como; amenazas de Malware, virus, vulnerabilidades del sistema, vulnerabilidades producidas por contraseñas, existen muchas otras amenazas informáticas que afectan a las empresas. Los ciberdelincuentes no descansan y siempre buscan nuevas formas de atacar, infectar y robar información de las empresas.

Referente a lo presentado anteriormente, se puede combatir la delincuencia en medios digitales mediante la formulación de políticas públicas y estrategias de ciberseguridad y de protección de infraestructuras críticas e implementar medidas para garantizar la seguridad de la información.

La autora Sáinz Peña (2016) asume que: durante los últimos años, la aparición de noticias sobre amenazas a la privacidad en Internet, que afectan tanto a empresas como a personas, ha despertado la conciencia en una parte muy amplia de la sociedad respecto a la importancia que tiene proteger la información en un mundo digital. Esto para considerar el proceso de digitalización.

Por otra parte, la autora Galiana (2022) de la página IEBS indicas que, en las últimas décadas, la tecnología se ha convertido en parte integral del lugar de trabajo. Por ende, este mundo tecnológico es una ventaja para el ecosistema empresarial, pero también nos expone al riesgo de pérdida de información en tanto en negocios digitales o en cualquier ámbito.

Mientras tanto los autores Henríquez y Frez (2022). Directores en magister de negocios digitales en FAE y UDP afirman que, el negocio digital puede concebirse como un método de gestión empresarial que utiliza las nuevas tecnologías; es una nueva revolución en la que se necesita iniciativa innovadora para gestionar distintos tipos de tecnologías en un entorno empresaria especifico.

Básicamente, el negocio digital se refiere, entre otras cosas, a aprovechar las nuevas oportunidades que existen en torno a las últimas tecnologías accesibles, buscando así otras formas de interactuar, ganar nuevos consumidores, conquistar mercados, intercambiar datos entre productos, proveedores y socios comerciales.

Conclusiones

En conclusión, la seguridad de la información es un tema crítico en el mundo de los negocios digitales. Las empresas enfrentan dificultades al tratar de aplicar medidas de seguridad de información efectivas para proteger sus sistemas y datos valiosos. Las tecnologías y sistemas complejos, la necesidad de equilibrar la seguridad con la facilidad de uso y accesibilidad, y la falta de conciencia y capacitación en seguridad de los empleados son solo algunas de las dificultades que las empresas deben enfrentar. Sin embargo, a través de la implementación de políticas de seguridad claras, la educación y capacitación de los empleados, y una actitud proactiva hacia la seguridad de la información, las empresas pueden superar estos desafíos y proteger sus sistemas y datos valiosos. Es esencial que las empresas estén al día en las últimas tecnologías y estrategias de seguridad y que trabajen diligentemente para mantener un alto nivel de seguridad de información en el mundo de los negocios digitales.

Bibliografía

Campos. «KIO Networks.» 2021. https://info.kionetworks.com/ciberseguridad_transformacion_digital?_ga=2.222797469.763238614.1622472333-396401740.1613062521 (último acceso: 27 de Diciembre de 2022).

DocuSing. «DocuSing.» Entiende el concepto de seguridad digital. 01 de Noviembre de 2021. https://www.docusign.mx/blog/seguridad-digital (último acceso: 27 de Diciembre de 2022).

Galiana, Patricia . «iebschool.» Qué es la Ciberseguridad, por qué es importante y como convertirte en experto. 22 de Agosto de 2022. https://www.iebschool.com/blog/que-es-ciberseguridad-tecnologia/ (último acceso: 02 de Marzo de 2023).

Henríquez, Pablo, y Jonathan Frez. «UDP Facultad de administración y economía.» LOS NEGOCIOS DIGITALES Y SU IMPORTANCIA EN LA ACTUALIDAD, POR PABLO HENRÍQUEZ Y JONATHAN FREZ. 20 de Julio de 2022. https://administracionyeconomia.udp.cl/2022/07/20/los-negocios-digitales-y-su-importancia-en-la-actualidad-por-pablo-henriquez-y-jonathan-frez/ (último acceso: 02 de Marzo de 2023).

Iso TOOLS. «PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA.» Principales causas de los fallos en la seguridad de la información. s.f. https://www.isotools.cl/principales-causas-los-fallos-la-seguridad-la-informacion/#:~:text=Entre%20este%20tipo%20de%20fallos,virus%20o%20desv%C3%ADo%20de%20fondos. (último acceso: 27 de Diciembre de 2022).

Sáinz Peña, Rosa María. «fundaciontelefonica.» Ciberseguridad, la protección de la información en un mundo digital. 2016. https://telos.fundaciontelefonica.com/archivo/numero105/ciberseguridad-la-proteccion-de-la-informacion-en-un-mundo-digital/ (último acceso: 02 de Marzo de 2023).

Sydle. «Sydle.» Negocios digitales: ¿qué son y cómo gestionarlos? 03 de Noviembre de 2021. https://www.sydle.com/es/blog/negocios-digitales-6182d1bd3885651fa241cb66/ (último acceso: 27 de Diciembre de 2022).

Cómo citar: Marcillo Merino, M. J., Cantos Plúa, J. N., Holguín Anchundia, J. C., & Vera Gutiérrez , J. A. (2023). Seguridad de información en el mundo de los negocios digitales. Journal TechInnovation, 2(1), 85–91. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.85-91