9 No.1 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.1.2025.e281

Baseline for Information Security in Project Management at M&M Asociados

Línea base para la seguridad de la información en la gestión de proyectos en la empresa M&M Asociados

Autores:

Guamán- León, Pablo Daniel
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Maestría en Administración de Empresas con Mención en Dirección y Gestión de Proyectos
Cuenca – Ecuador

pdguamanl13@est.ucacue.edu.ec

https://orcid.org/0009-0000-3510-2347

Erazo- Alvarez, Guido Olivier
UNIVERSIDAD CATÓLICA DE CUENCA
Docente de la Maestría en Administración de Empresas con Mención en Dirección y Gestión de Proyectos
Cuenca – Ecuador

oerazo@ucacue.edu.ec

https://orcid.org/0000-0002-2494-0967

Ortega- Castro, Juan Carlos
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Tutor de la Maestría en Administración de Empresas con Mención en Dirección y Gestión de Proyectos
Cuenca – Ecuador

jcortegac@ucacue.edu.ec

https://orcid.org/0000-0001-6496-4325

Fechas de recepción: 14-FEB-2025 aceptación: 14-MAR-2025 publicación: 15-MAR-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La evolución tecnológica ha impulsado la transformación digital en la gestión empresarial. Desde el precedente generado por la crisis causada por el COVID-19, el incremento en la adopción y uso de plataformas digitales coloco al sector empresarial en una posición de riesgo frente a múltiples métodos de ciberataques y la gestión de los datos manejados en entornos digitales. Bajo la situación actual del entorno es fundamental que las empresas desarrollen metodologías internas que permitan establecer directrices para la correcta gestión de sus datos, con la finalidad de evitar pérdidas, fugas e incumplimientos normativos en la gestión de la información. Para el análisis de caso se realizó un estudio en la empresa privada M&M Asociados, donde se ha podido evidenciar la falta de directrices o políticas que permitan establecer una línea base para la seguridad de su información. El factor de riesgo principal es la fuga y tratamiento correcto de datos, por ello es que bajo un enfoque cualitativo y descriptivo se ha realizado el análisis del estado actual de la empresa, que ha permitido realizar una propuesta de mejora en sus procesos internos, buscando eliminar los factores de riesgo identificados en visitas, entrevistas y encuestas realizadas, obteniendo una visión detallada de las principales oportunidades de mejora. La propuesta de la metodología busca alinearse a principios de normativas vigentes como la ISO/IEC 27001 y la Ley Orgánica de Protección de Datos Personales, mismas que controlan los estándares en seguridad de la información y manejo de datos personales respectivamente. Con este enfoque se busca que la empresa M&M Asociados consiga el fortalecimiento organizacional en la confidencialidad, disponibilidad y accesibilidad de sus datos críticos generados en cada uno de sus proyectos.

Palabras clave: Empresa privada; protección de datos; informática; política interna; método de evaluación

Abstract

Technological evolution has driven digital transformation in business management. Since the precedent created by the crisis caused by COVID-19, the increase in the adoption and use of digital platforms places the business sector in a position of risk against multiple methods of cyber-attacks and data management handled in digital environments. Given the current environment, it is essential that companies develop internal methodologies to establish guidelines for the proper management of their data, in order to avoid loss, leakage and regulatory non-compliance in the management of information. For the case analysis, a study was carried out in the private company M&M Asociados, where it has been possible to highlight the lack of guidelines or policies that allow establishing a baseline for the security of their information. The main risk factor is the leakage and correct processing of data; therefore, it is that under a qualitative and descriptive approach has been carried out the analysis of the current state of the company, which has made possible to make a proposal for improvement in its internal processes, seeking to eliminate the risk factors identified in visits, interviews and surveys conducted, obtaining a detailed view of the main opportunities for improvement. The proposed methodology seeks to align with the principles of current regulations such as ISO/IEC 27001 and the Organic Law on Personal Data Protection, which control standards in information security and personal data management respectively. With this approach the company M&M Asociados seeks to achieve organizational strengthening in confidentiality, availability and accessibility of its critical data generated in each of its projects.

Keywords: Private enterprise; data protection; informatics; internal policy; evaluation method; evaluation method

Introducción

La constante evolución tecnológica ha permitido que diferentes métodos tradicionales cambien al uso de herramientas de TICS pudiendo mejorar cualquier tipo de proceso, volviéndolos mucho más eficientes, prácticos y atractivos para el usuario. Para la administración de empresas y la gestión de negocios es importante que se desarrolle un concepto de transformación digital con la finalidad de expandir su participación en entornos digitales y poder de esta manera ganar posiciones en el mercado con sus productos o servicios ofertados (Rojas Valiente, 2024).

Cuando el mundo vivió la presencia del COVID-19, el concepto de digitalización sufrió una transformación importante, impactando para siempre la forma de hacer negocios y volviendo más familiar el concepto de E-Commerce y trabajo en plataformas digitales e incrementando el uso global del internet entre el 50% a 70% y con esto los términos ciberataques y ciberdelincuentes se volvieron más reconocidos (Gonzáles Macías & Urrutia de la Garza, 2021).

Si bien es cierto que a lo largo de la historia tecnológica se ha podido evidenciar ciberataques que han afectado a grandes compañías como Sony o a departamentos públicos en muchos países, se puede decir que los ciber atacantes han salido de ese enfoque y al día de hoy es muy sencillo encontrar un correo electrónico con links maliciosos que puedan hacerse con los datos de una cuenta o ataques de phishing que mediante métodos de ingeniera social consigan persuadir a una persona a enviar datos sensibles.

Esto para las PYMES (pequeñas y medianas empresas) pueden significar todo un problema considerando que estas enfrentan retos para implementar estrategias de seguridad principalmente por la falta de recursos, por lo que una persona que desconozca de herramientas y políticas que puedan ser aplicadas para el reconocimiento y tratamiento de estos riesgos es el blanco perfecto para ejecutar cualquier tipo de ataque (Alotaibi & Saini, 2021).

Ahora, si se considera lo antes mencionado y una empresa requiere implementar modelos digitales para la gestión de sus procesos en toda la cadena de valor, significa que, de una manera u otra debería generar una línea base para su gestión de seguridad informática,

cuidando principalmente para garantizar la protección de datos y la continuidad operativa (Liu & Zhou, 2023).

Para lo antes mencionado, se toma como caso de estudio a la empresa MYM Asociados, una empresa ecuatoriana fundada en el año 2014, dedicada a la importación y venta de zapatería y prendas de vestir, con su sede situada en la ciudad de Cuenca, provincia del Azuay.

En base a los resultados obtenidos en un acercamiento inicial, la presente investigación busca diseñar una línea base para la seguridad de la información que se estipule en un macroproceso que gestione los diferentes proyectos levantados, esto se traduce en procesos de desarrollo de productos, preventas, manejo de la cartera de clientes de la empresa, métodos de cobro, seguimiento de rutas de entrega del producto y la medición de la satisfacción al cliente. Con el caso busca proponer una metodología que pueda ser aplicada a empresas de similar índole y contrastar los resultados con estudios que guarden relación con el objetivo.

Material y métodos

Material

Enfoque del estudio

El trabajo de investigación tuvo un enfoque cualitativo considerando que existió una interacción con los individuos actores de los diferentes procesos y funciones dentro de la empresa, con la finalidad de obtener el detalle de sus actividades, medios y materiales utilizados para la ejecución de sus actividades, pues fue importante conocer e interpretar sus acciones para obtener una aproximación sobre la realidad de sus interacciones (Gonzáles Macías & Urrutia de la Garza, 2021). La aplicación de este enfoque buscó conseguir los resultados establecidos, en referencia a la falta de una línea base para la seguridad de la información, lo que puede ocasionar una pérdida de mercado y clientes.

Tipo de estudio

El tipo de estudio se denominó descriptivo, considerando que se enfocó en el análisis de las variables que se encontraron involucradas en la aplicación de la línea base de seguridad de la información y que su elaboración consideró como referencia las directrices de diferentes

normas existentes para este fin. Por otra parte, el estudio también empleó la investigación de campo considerando que la recolección de datos se realizó sobre la empresa, procesos y colaboradores para el análisis de su estado inicial y mapeo de propuesta.

Métodos

Técnicas de recolección de datos

Para la recolección de datos se consideró métodos de entrevistas, revisión de documentación, revisión de bases de datos y encuesta.

- Con estos métodos se consiguió realizar el análisis de estado inicial pudiendo recopilar información que revele como la falta de una línea base en la seguridad de los datos internos pueden afectar a la operación y crecimiento esperado por la empresa.
- Las encuestas buscaron mapear puntos de mejora en la calidad del talento humano referente al manejo adecuado de la información, además de recibir pautas que pudieron plasmarse en el desarrollo de la propuesta.

Población y muestra

Al haber direccionado el caso de estudio a la aplicabilidad de la línea base en la empresa MYM Asociados, se consideró una población finita compuesta por los trabajadores y gerencia de la misma, por lo que no se califica como relevante la toma de muestras en una población. Realizar el estudio sobre el total poblacional garantizó la obtención de buenos resultados ejecutando el análisis con las herramientas de datos y encuestas.

Resultados

Para los resultados obtenidos del acercamiento inicial, se realizó una entrevista al gerente propietario de la empresa, tomando en consideración las recomendaciones de la norma ISO 27001 respecto a las responsabilidades de la gerencia frente a la efectividad de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Tabla 1

Entrevista realizada a la gerencia de la empresa M&M Asociados.

Pregunta	Respuesta
¿Ha entregado recursos para para actividades que cuiden la seguridad de los datos de la empresa?	La empresa se limita a realizar los pagos de sueldos y viáticos.
¿Conoce acerca del SGSI y las herramientas necesarias para la implementación?	No considera, ni es consciente de la existencia de un riesgo.
¿Ha establecido políticas de mejora continua a cualquier nivel dentro de la empresa?	No existe ningún mecanismo de mejora en procesos.
¿Su empresa tiene implementada alguna política para la gestión de riesgos?	No existe ninguna metodología y/o política aplicada.
¿Conoce si su infraestructura tecnológica está segura de cualquier intento vulneración?	Los servicios tecnológicos se tercerizan, por lo que no se conoce el estado de seguridad.

Nota. Fuente: Autor.

De los resultados obtenidos en el acercamiento inicial, la gerencia no percibió la necesidad y la importancia de establecer metodologías para la gestión de riesgos y la seguridad de la información con la implementación de una línea base, desconoció los mecanismos que se pueden usar para la gestión de sus proyectos con un enfoque de protección a la información sensible que es utilizada para la venta y distribución de sus productos.

La gestión de la seguridad de la información en la actualidad es importante debido a la constante interacción digital y entrega masiva de datos, esto puede traer resultados como la

fuga de información y vulnerabilidades informáticas que en el caso de la empresa estudiada puede ser afectada principalmente por filtraciones de producto en desarrollo, pérdida de clientes por manipulación errónea de datos e incluso posibles incumplimientos legales por el mal manejo de datos personales (Calle Herencia, 2022).

Cabe mencionar que se debe cubrir la mayor cantidad de aristas de riesgo que puedan existir en una PYME, para lo cual se debe realizar una categorización de vulnerabilidades en las categorías: seguridad, dependencia, empleado, estratégico y legal, pudiendo utilizar un enfoque de análisis de valoración para construir la línea base dando prioridad a los puntos más críticos descubiertos (Liu y Zhou, 2023).

Tabla 2.

Resultados de encuesta a colaboradores.

Pregunta	Análisis de resultados
¿Cuenta con algún tipo de experiencia en el área de tecnología?	Directamente ningún colaborador ha trabajado en el área.
¿Conoce acerca de la seguridad de la información?	Ningún empleado considera que conoce del tema.
¿Usted considera que el sistema de información actual de la empresa es seguro?	El 70% considera que los sistemas de la empresa son seguros.
¿Está al tanto de las posibles amenazas cibernéticas como phishing, ransomware, etc.?	El 5% conoce que existen ataques informáticos de diferentes tipos.
¿Estaría usted dispuesto a participar en la formación de estos conceptos?	El 80% se muestra entusiasmado en participar en procesos de formación.

¿Alguna vez recibió capacitaciones referentes a la seguridad de la información?	El 100% nunca ha recibido capacitaciones del tema.

Nota. Fuente: Autor.

De los resultados obtenidos de la encuesta se pudo destacar que existen falencias significativas sobre la seguridad de la información que los colaboradores deben cuidar para la empresa, si bien consideraron que sus sistemas son seguros, la falta de conocimiento de significa que se transforman en una brecha de seguridad humano, por otra parte la predisposición para recibir capacitaciones puede ser considerado un elemento positivo en el levantamiento de la línea base, ya que se pudo evidenciar que el personal no se encuentra atado a una forma de trabajo estático.

Discusión

Propuesta.

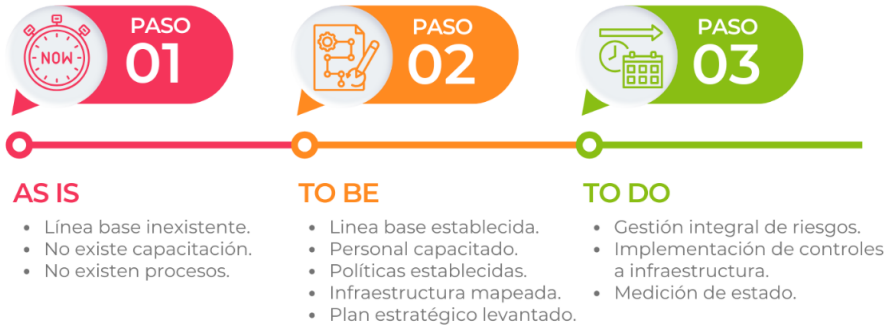
La implementación de la propuesta de línea base de seguridad informática que se encuentra asignada en el paso 2 de la Figura 1, busca establecer un enfoque integral y principalmente estratégico dadas las limitantes que la empresa puede poseer en niveles presupuestarios, de talento humano o de infraestructura tecnológica.

Esta propuesta estará alineada a estándares de seguridad de la información ISO/IEC 27001 Seguridad de la Información, Ciberseguridad y Protección de Privacidad y la Ley de Protección de Datos Personales, teniendo como objetivo principal minimizar las brechas de seguridad con soluciones prácticas que puedan ser ejecutadas a mediano plazo conforme se defina en la construcción del plan estratégico que acompañe a la gestión de proyectos empresariales. Este se encuentra mapeado en la misma etapa de implementación y sin embargo, también se busca crear mecanismos que respeten la ley vigente respecto del tratamiento de las bases de clientes y sus datos personales.

El cumplimiento de las etapas a su vez permitirá definir políticas a las cuales la empresa, el gerente y los colaboradores deberán responder.

Figura 1.

Etapas de implementación.



Objetivo de la propuesta.

Como indica Xu y Zhang (2021), la gestión de riesgos de seguridad de la información debe ser vista como una estrategia para fortalecer las capacidades organizaciones, por lo cual, la implementación busca que cualquier proyecto desarrollado llegue a término cumpliendo políticas internas que cuiden los intereses de la empresa, además de garantizar el correcto tratamiento de datos personales de los clientes.

Metodología.

El diseño de la línea base para la seguridad de la información considerará todos los elementos necesarios para que esta pueda ser aplicable con todos sus controles, políticas y métricas que se puedan establecer a nivel organizacional, con la finalidad de cuidar la integridad del desarrollo de proyectos de alto nivel.

Desarrollo.

Identificación de roles y categorización.

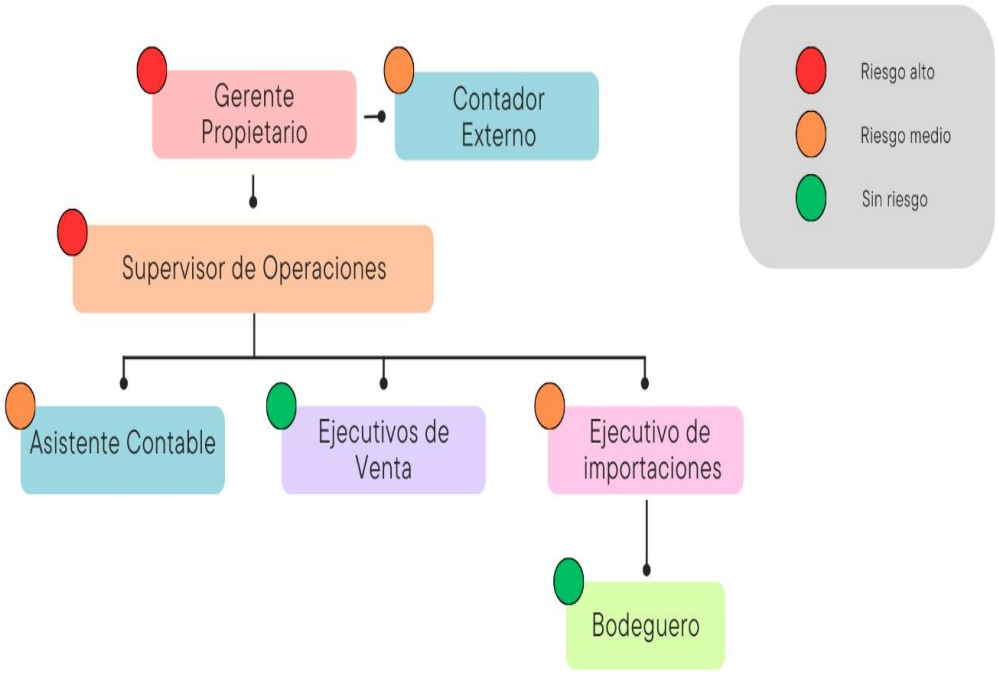
El diseño de la línea base para la seguridad de la información considerará todos los elementos necesarios para que esta pueda ser aplicable con todos sus controles, políticas y métricas que

se puedan establecer a nivel organizacional, con la finalidad de cuidar la integridad del desarrollo de proyectos de alto nivel.

La identificación de roles jugará un papel fundamental ya que permite a la empresa definir las responsabilidades y evaluar los riesgos de forma integral, lo cual complementado con la clasificación de riesgo por funciones desempeñadas en la operación permite delimitar políticas que puedan priorizar o dar tratamientos especiales a los procesos con directrices que deben ser cumplidas para garantizar que la información no se vea comprometida (Xu y Zhang, 2021).

Figura 2.

Organigrama con clasificación de riesgo.

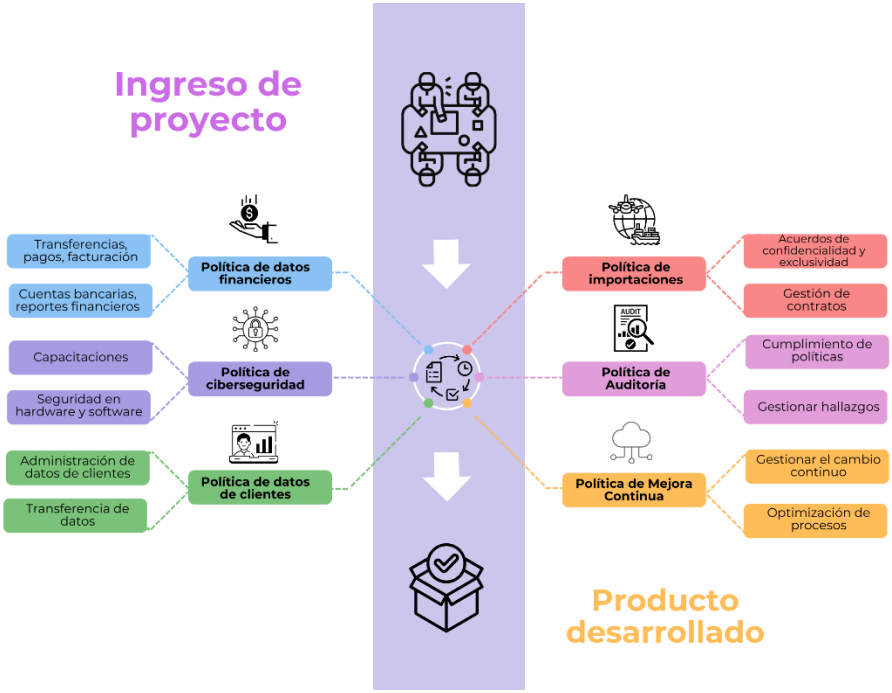


Macroproceso de línea base para la seguridad de la información.

En base a la identificación de roles y clasificación de riesgo se deben gestionar diferentes políticas que permitan gestionar la información de acuerdo a las buenas prácticas que la normativa aplicada pueda recomendar (Kumar & Yang, 2021).

Figura 3.

Mapa de línea base para la seguridad de la información.



El eje central de la línea base será la ejecución del proyecto, teniendo este que alinearse a cada una de las políticas estipuladas en la Figura 3, completando de esta forma la integración de la seguridad de la información en la estrategia empresarial.

Hay que ser enfáticos que el cuidado con la información garantiza procesos claros, robustos y controlables, todo esto con la finalidad de entregar un producto o servicio que se encuentre alineado a políticas que la empresa considere pertinentes.

Secciones de entrada y salida.

El ingreso del proyecto a ejecutar es el primer paso para obtener un producto desarrollado, en esta sección se colocan políticas clave como el manejo de datos financieros, ciberseguridad y datos de cliente, por otra parte, la sección de producto desarrollado busca completar la operación de desarrollo con prácticas que permitan identificar posibles hallazgos y gestionar la mejora continua con cada proceso ejecutado.

Política de datos financieros.

Declarar la política permitirá establecer directrices relacionadas con transacciones bancarias, facturación y reportes financieros de la empresa, por lo cual se deberá construir artículos que controlen:

- La confidencialidad generada por el usuario.
- Establecer directrices de cifrado de datos en el caso que aplique.
- Control de usuarios y contraseñas de entidades bancarias.

Política de datos ciberseguridad.

Declarar la política permitirá establecer directrices que controlen accesos en plataformas digitales, control de amenazas como malware o ataques de ingeniería social, considerando entre los más importantes:

- Esquemas de seguridad de proveedor de sistema ERP interno.
- Capacitaciones y simulaciones de eventos de riesgo.
- Control de acceso a páginas web.

Política de datos de cliente.

Declarar la política permitirá establecer directrices que controlen el mal uso o extracción de las bases de datos de clientes de los servidores de la empresa para usarlos en fines que no estuvieron considerados.

Política de importaciones.

Declarar la política permitirá establecer directrices que controlen el archivo y gestión de los diferentes contratos establecidos con proveedores con la finalidad de mantener la exclusividad de los productos adquiridos, garantizando la fiabilidad de las negociaciones ejecutadas en la etapa de proyecto.

Política de auditoría.

Declarar la política permitirá establecer directrices que controlen el cumplimiento de las diferentes políticas a establecer, además de generar observaciones en los diferentes proyectos

ejecutados con la finalidad de ejecutar acciones correctivas y mejorar la repuesta a la necesidad del desarrollo.

Política de mejora continua.

Declarar la política permitirá desarrollar acciones de optimización operacional y de riesgo para la obtención del producto.

Los hallazgos obtenidos a través de la metodología descrita demuestran que la empresa utilizada para el estudio carece de políticas y una línea base para la seguridad de la información, estos resultados se contrastan con mencionado por Miró Llinares (2021) siendo acertado el análisis realizado ya que menciona que el incremento en la digitalización ha traído también consecuencias, la falta de conciencia principalmente en las PYMES las vuelven el blanco perfecto de ataques o simplemente de una mala gestión de la seguridad.

Asimismo, Calle Herencia (2022) hace énfasis que esta transformación digital de la que somos parte dia con dia debe acompañarse de estrategias de gestión que se vinculen directamente con la visión estratégica de la empresa, por lo que la implementación de una línea base es una buena práctica que puede acompañar a la gestión de proyectos de forma eficiente y segura.

Conclusiones

El análisis realizado al personal y procesos de la empresa M&M Asociados permitió evidenciar que la falta de una línea base en la gestión de la seguridad de la información puede poner en riesgo a los datos generados en la gestión de sus proyectos, al no contar con políticas claras, además del desconocimiento de conceptos básicos de ciberseguridad y gestión de datos, vuelve vulnerable al entorno donde se desarrollen las actividades empresariales.

El diseño de la propuesta no solo permitió estructurar controles dentro de los diferentes procesos, sino permitió evidenciar cargos críticos y las diferentes políticas que se pueden generar para que velen por la seguridad de datos generados en los proyectos, además, la generación de políticas internas que soporten la línea base busca fortalecer la estructura

interna organizacional, lo que se puede traducir en mayor seguridad al momento de gestionar negocios con clientes y proveedores.

Los resultados obtenidos del análisis a los colaboradores es un indicador del valor agregado que genera el talento humano debidamente preparado frente a cualquier tipo de amenaza o efecto de vulnerabilidad a los datos internos, es necesario que cualquier política sea acompañada de la formación continua a todo nivel y de forma especial con los cargos críticos debidamente identificados por sus funciones.

Es importante que la línea base que se mapea dentro de una organización sea acompañada de procesos debidamente establecidos, además de una política integral y políticas satélites que cuiden cada eslabón dentro de la cadena de valor.

La mejora continua mediante mecanismos de identificación de problemáticas y capacitación continua pueden ser herramientas que vuelvan eficiente a un equipo y sus procesos, evitando fallas, perdidas de información o reprocesos, además de delimitar correctamente las responsabilidades en base a un proceso de levantamiento de criticidad de funciones.

Para finalizar la implementación de estos mecanismos debería considerarse dentro de una estrategia que tenga como objetivo la continuidad del negocio, la sostenibilidad de la empresa respecto del manejo de datos digitales y la confianza que se genere al entorno relacionado con esta.

Referencias bibliográficas

Alhazmi, A., & Kang, J. (2023). IoT security challenges and solutions: A review. Journal of Network and Computer Applications, 185, 103106. https://doi.org/10.1016/j.jnca.2021.103106

Alotaibi, H., & Renaud, K. (2022). Enhancing cybersecurity awareness through organizational culture: A framework for SMEs. Cybersecurity, 8(1), 1-11. https://doi.org/10.1186/s42400-022-00071-4

Calle Herencia, C. A. (2022). La transformación digital y su importancia en las pymes. Iberoamerican Business Journal, 5(2), 64-81.

https://doi.org/10.22451/5817.ibj2022.vol5.2.11059:contentReference[oaicite:0]{index=0}

Cao, J., & Zhang, T. (2022). Cybersecurity risk management in SMEs: A review of frameworks and strategies. Journal of Business Research, 145, 308-321. https://doi.org/10.1016/j.jbusres.2022.04.031

González Macías, C. J., & Urrutia de la Garza, J. A. (2021). Estudios cualitativos en la administración. En A. Y. Reyes-Escalante & D. A. Sandoval Chávez (Eds.), Metodologías, enfoques y estructuras de trabajos de investigación en las ciencias administrativas (pp. 437-439). El Colegio de Chihuahua. https://www.researchgate.net/publication/357046813:contentReference[oaicite:1]{index=1}

Huang, Y., & Zheng, M. (2021). Cybersecurity in SMEs: Risk management strategies and frameworks. Journal of Cybersecurity, 7(3), 345-358. https://doi.org/10.1093/cybsec/tyab028

Ibrahim, A., & Zhao, X. (2022). Addressing cybersecurity challenges in the healthcare sector: A review. Health Information Science and Systems, 10(1), 1-14. https://doi.org/10.1186/s13755-022-00450-w

Jones, D., & Smith, R. (2021). Mitigating cybersecurity risks in industrial systems. International Journal of Critical Infrastructure Protection, 33, 100428. https://doi.org/10.1016/j.ijcip.2021.100428

Kumar, P., & Saini, H. (2021). Cybersecurity frameworks and standards: A systematic review. Journal of Information Security and Applications, 59, 102897. https://doi.org/10.1016/j.jisa.2021.102897

Li, W., & Liu, J. (2022). Data security in cloud computing environments: Issues and solutions. Journal of Cloud Computing: Advances, Systems, and Applications, 11(1), 1-18. https://doi.org/10.1186/s13677-022-00308-9

Li, X., & Zhao, Y. (2023). Artificial intelligence for cybersecurity: Challenges and solutions. Computers & Security, 119, 102729. https://doi.org/10.1016/j.cose.2022.102729

Liao, C., & Lin, S. (2021). Privacy and security issues in big data: A systematic review. Big Data Research, 23, 100204. https://doi.org/10.1016/j.bdr.2021.100204

Liu, X., & Zhou, Y. (2023). A novel approach to cybersecurity risk analysis for small and medium enterprises (SMEs). Computers in Industry, 139, 103655. https://doi.org/10.1016/j.compind.2022.103655

Miró Llinares, F. (2021). Crimen, cibercrimen y COVID-19: Desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. Revista de los Estudios de Derecho y Ciencia Política, 32, 1-20. https://idp.uoc.edu:contentReference[oaicite:2]{index=2}

Rojas Valiente, M. J., Castillo Sarmiento, J. M. H., & Mendoza De Los Santos, A. C. (2023). Seguridad de la información en la prevención de pérdida de datos: Una revisión sistemática. Revista Innovación y Software, 4(2), 182-200. https://doi.org/10.48168/innosoft.s12.a92:contentReference[oaicite:3]{index=3}

Singh, M., & Patel, R. (2022). Analyzing cybersecurity trends in the banking sector. Journal of Financial Crime, 29(3), 631-642. https://doi.org/10.1108/JFC-01-2022-0011

Sun, J., & Lee, Y. (2021). Cybersecurity management in the digital transformation era: A survey. Journal of Computer Security, 29(4), 551-575. https://doi.org/10.3233/JCS-200773

Tan, J., & Huang, X. (2022). Cybersecurity strategies for SMEs in the digital economy. Journal of Digital Economy, 9(2), 45-60. https://doi.org/10.1016/j.jde.2022.04.004

Wang, L., & Liu, J. (2021). Security challenges in cloud computing: A survey. International Journal of Computer Applications, 175(1), 1-10. https://doi.org/10.5120/ijca202191658

Wang, Y., & Yang, Y. (2021). Cybersecurity risk assessment for industrial systems: A comprehensive review. Computers & Security, 103, 102191. https://doi.org/10.1016/j.cose.2021.102191

Xie, X., & Chen, X. (2021). Security-aware software engineering for cybersecurity risk management. Software: Practice and Experience, 51(6), 1195-1211. https://doi.org/10.1002/spe.2829

Xu, X., & Zhang, H. (2021). Cybersecurity risk management: A strategic approach. International Journal of Information Management, 58, 102313. https://doi.org/10.1016/j.ijinfomgt.2021.102313

Zhang, H., & Li, Z. (2022). Machine learning-based cybersecurity threat detection. IEEE Access, 10, 19050-19062. https://doi.org/10.1109/ACCESS.2022.3148477

Zhang, Z., & Wang, Y. (2022). Internet of Things security and privacy issues: A comprehensive survey. Sensors, 22(4), 1220. https://doi.org/10.3390/s22041220

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Nota:

El artículo no es producto de una publicación anterior.