07-001

DIGITAL TRANSFORMATION AND RISK MANAGEMENT IN PROJECTS

Alvarez Toro-Moreno, Alejandro [(1)]

[(1)] Universidad de las Américas

At a global level, one of the main tools to measure the success and failure of Information Technology (IT) projects consists of the Chaos Report, possibly the report with the greatest reference and credibility regarding the implementation of IT systems. Every two years, this report highlights factors that explain the failure of IT projects that allow the digital transformation in the organizations. Taking this information as a reference, it is important to classify those risks that consider the presence of problems in the implementation of computer systems. Additionally, risks must be addressed, not with the purpose of eliminating them totally, but rather to mitigate their effects within an acceptable margin of tolerance. In this way, before a potential occurrence of said risk, the organization will have effective tools for its control, being essential a correct risk management for these projects and the identification of threats. The purpose of this work is to present the types of risks faced by organizations that choose for digital transformation through technological projects, in addition to describing tools for the correct management those identified risks.

Keywords: digital transformation; information systems; risk management; projects

LA TRANSFORMACIÓN DIGITAL Y LA GESTIÓN DE RIESGOS EN LOS PROYECTOS

A nivel global, una de las principales herramientas de medición en cuanto a los éxitos y fracasos de los proyectos informáticos consiste en el Reporte Chaos, posiblemente el informe con mayor referencia y credibilidad en cuanto a la implementación de sistemas de información. Cada dos años, este reporte destaca ciertos factores que explican los fracasos de proyectos de tecnologías informáticas que permiten la transformación digital de las organizaciones. Tomando como referencia esta información, es importante clasificar aquellos riesgos que consideran la presencia de inconvenientes en la implementación de sistemas. Adicionalmente, los riesgos deben ser atendidos, no con el propósito de eliminarlos en su totalidad, sino para mitigar sus efectos dentro de un margen aceptable de tolerancia. De esta manera, ante una potencial ocurrencia de dicho riesgo, la organización contará con efectivas herramientas para su control, siendo imprescindible una correcta gestión de los riesgos para estos proyectos y la identificación de amenazas. El propósito de esta exposición es presentar cuáles son los tipos de riesgos a los que se enfrentan comúnmente las organizaciones que opten por la transformación digital a través de proyectos tecnológicos, junto con la descripción de herramientas para la correcta administración de dichos riesgos.

Palabras clave: transformación digital; sistemas de información; gestión de riesgos; proyectos

1. Introducción

No cabe duda de que los consumidores cada día están más informados, debido al acceso en las plataformas digitales y multicanales que apoyan la toma de decisiones en relación con la adquisición de productos. La tecnología en los negocios ha generado una transformación en la actividad de los sectores económicos y uno de los más beneficiados es la logística, siendo clave la optimización de sus procesos, lo cual permite apoyar la cadena de suministro, en el que uno de sus resultados es la satisfacción de los clientes que se han vuelto cada vez más exigentes al adquirir un bien o requerir un servicio.

La digitalización ha permitido que los procesos industriales se destaquen en términos de eficacia y rapidez, traduciéndose en la ejecución de tareas y actividades en menos tiempo (Entel Ocean, 2022). Con un proceso de digitalización adecuado, las organizaciones pueden obtener diversos beneficios, destacándose la disminución en los costos, control de los riesgos, incremento de la rentabilidad y gestión de inventarios en tiempo real.

El próximo paso en este proceso es la transformación digital, que toma un lugar importante en la transformación organizacional, implicando una reestructuración de múltiples procesos existentes en la empresa. Esto conlleva a generar un verdadero cambio cultural, cuyo resultado debe ser el incremento sustancial de la productividad.

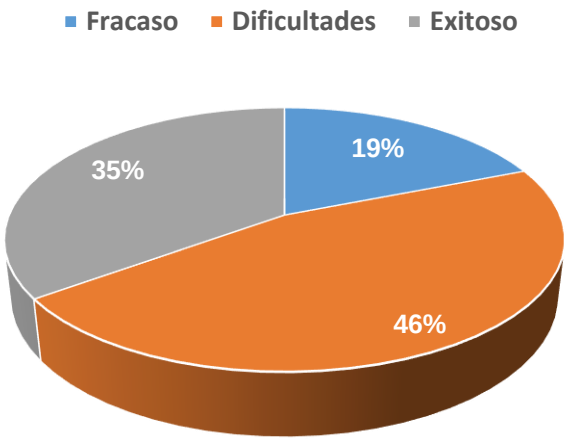
Diversos autores se han referido acerca de la transformación digital, entendiéndose como tal al “proceso que tiene como objetivo mejorar una entidad, generando cambios significativos en sus propiedades mediante combinación de tecnologías de la información, computación, comunicación y conectividad” (Vial, 2019). La transformación digital no debe entenderse como una simple digitalización de procesos (Llorens, 2020), lo que se complementa y refuerza con el concepto de que la transformación digital requiere de las personas y es para las personas (Fonseca, García-Peñalvo & Camba, 2020).

Fuentes bibliográficas adicionales describen los múltiples beneficios que las organizaciones obtienen con la implementación de la transformación digital. Un estudio desarrollado por Frendiana y Soediantono (2022) muestra los efectos y recomendaciones de la transformación digital aplicadas a la industria de la defensa, mientras que las investigaciones de Pramanik, Kirtania y Pani (2019) concluyen que la adopción de tecnología digital genera beneficios de tipo comercial, operativo, de crecimiento, mejor calidad social, entre otros, los que se materializan en los beneficios visibles para instituciones bancarias.

Lo expresado en los párrafos anteriores explica las ventajas de la implementación de la transformación digital en las organizaciones, sin embargo, los proyectos de transformación digital no responden al mismo interés. Algunas de las razones consisten en que no hay acuerdo de objetivos o se visualiza un involucramiento muy escaso de los empleados de la organización (Hernández D. , 2019). Para explorar las estadísticas de éxitos y fracasos de los proyectos informáticos, se dispone del reporte Chaos presentado por Johnson (2022), una de las referencias bibliográficas de mayor credibilidad en cuanto a reportes relacionados con la implementación de los sistemas informáticos.

Si se realiza una comparación de datos del Reporte Chaos, el año 1994 presentaba un nivel global de proyectos exitosos de un 16% aproximadamente. Para el período comprendido entre los años 2015 y 2020, el porcentaje de proyectos exitosos llega solo a un 35%. De hecho, este porcentaje resulta ser menor si se compara con el período 2010 a 2014, en que la tasa de proyectos exitosos llega a un 38%. La sección restante en el período 2015 a 2020 se divide en proyectos que presentan dificultades (46%) o que han resultado en fracasos (19%).

Figura 1: Resultados Reporte CHAOS 2015-2020



Fuente: Chaos Report: Beyond Infinity – The Standish Group – 2022

Existen causas que explican los fracasos o inconvenientes en los proyectos de TI, como la falta de vinculación entre los proyectos y prioridades de estrategia de las organizaciones, junto con un escaso conocimiento de la industria de las tecnologías de la información y sus proveedores (García, 2015).

En consecuencia, los riesgos deben atenderse para disminuir al máximo el impacto negativo de sus efectos dentro de un margen de tolerancia aceptable, por lo que, si se declara un riesgo, la empresa dispondrá de herramientas que permitan su control y correcta gestión.

La identificación de los potenciales riesgos es primordial para que la gestión de los riesgos sea un instrumento eficaz que impulse la proactividad, incremente las posibilidades de alcanzar los objetivos y favorezca la identificación de las amenazas. El propósito de este documento es dar a conocer cuáles son los riesgos a los que se enfrentan las organizaciones que opten a proyectos tecnológicos que permitan la transformación digital y cómo gestionar estos riesgos identificados.

2. Desarrollo

Ningún proyecto está exento de riesgos, por lo que es crucial que la organización sea capaz de controlar sus efectos, con el propósito de disminuir la incertidumbre. Existen metodologías que evalúan y controlan los efectos de los riesgos. El trabajo realizado por Pulido-Rojano, Ruiz-Lázaro y Ortiz-Ospino (2020) propone la importancia de identificar y evaluar aquellos eventos clasificados como no deseados, a través de la unión de la utilización de ciertas herramientas estadísticas, en conjunto con la norma ISO 31000, que hace referencia a los principios y las directrices existentes para la correcta gestión de los riesgos.

Una aproximación de clasificación de riesgos para los proyectos de tecnologías de información está representada por el riesgo tecnológico, consistente en aquella potencial avería en el software que perjudica el panorama de sistemas dentro de una organización. Es la “amenaza de un fallo en la tecnología de gestión que podría comprometer la seguridad cibernética y la inteligencia empresarial” (Henderson, 2021).

Si bien los riesgos tecnológicos deben controlarse, el solo preocuparse de este tipo de riesgo resulta una visión acotada de los potenciales efectos, puesto que no se incluyen otros eventos como la administración de los datos. Por esta razón, se necesita de un concepto más amplio, lo que se conoce como riesgo de TI, entendiéndose como aquel daño “cuando una amenaza

se aprovecha de una vulnerabilidad en los recursos informáticos de una organización" (Acronis Cyber Protect Cloud, 2021).

Para una correcta gestión del riesgo en los proyectos de tecnologías de información, se necesita identificar cuáles son los posibles tipos de eventualidades a los que se enfrenta una organización. A criterio del autor, las potenciales eventualidades que pueden presentarse son:

2.1 Riesgos tecnológicos

Se relacionan con fallas tecnológicas. Ante este tipo de inconvenientes, existe la posibilidad de que se produzca un impacto en los propios sistemas de información, las personas y el capital humano. Algunos ejemplos de estos riesgos son problemas de software y hardware, inconvenientes con la integración de las diferentes partes del proyecto que se han desarrollado en paralelo, entre otros (De Aza, 2011).

Cuando la empresa adopta un sistema tecnológico como apoyo para el cambio cultural de la organización y la definición de estrategias para el éxito de un determinado negocio, la tecnología para a ser una efectiva herramienta para gestionar las organizaciones, presentando diversos beneficios, siendo destacados por Chablé (2020): simplificación y automatización de las actividades, mejora en los procesos empresariales, control de los procesos en tiempo real. Es importante indicar que esto es posible, siempre y cuando en conjunto con la tecnología, exista un proceso para su desarrollo y mantenimiento. De lo contrario, el solo hecho de contar con una herramienta que no se actualice en el tiempo evidenciará que no aportará con la continuidad del negocio de la empresa y, finalmente, se obtengan costos innecesarios por mantención reactiva.

Para evitar estos riesgos, se requiere de una correcta gestión a nivel interno y externo, pero, sobre todo, clasificar los riesgos (Escuela Europea de Excelencia, 2016), de manera que este control mantenga intactos tanto la información como la comunicación. Esto requiere de diferentes análisis, como la evaluación de contar con una solución On-Promise o Cloud, así como buscar proveedores que se especialicen en diversas áreas de la tecnología. Para ello, es prioritario poseer un sistema de evaluación de riesgos, puesto que, de esta manera, se controlan correctamente los peligros potenciales.

2.2 Riesgos del Ciberespacio

Este tipo de riesgos hace referencia a aquellos accesos no autorizados por la organización, por lo que, en este caso, todo lo que se relacione con la confidencialidad e integridad de los sistemas tecnológicos son elementos cruciales en esta era de la globalización, en el que se han incrementado los ataques cibernéticos, los robos de información y los ciberdelincuentes (Universidad Europea, 2021). La siguiente tabla, proporcionada por el Ministerio del Interior del Gobierno de Chile (2022), presenta información histórica acerca de los incidentes reportados y que afectan los sistemas de las organizaciones en la nación chilena:

Tabla 1: Distribución de Tickets reportados en mayo de 2022

Número	Tipo de Ticket	Código	Mayo 2022
1	Vulnerabilidad	9V00	1989
2	Disponibilidad	6D00	257
3	Otros	11O00	134
4	Código Malicioso	2C00	103
5	Fraude	8F00	74
6	Información de seguridad de contenidos	7S00	36

7	Intentos de intrusión	4I00	6
8	Intrusión	4I00	2
9	Recopilación de información	5I00	1
10	Contenido abusivo	1A00	0

Fuente: Informe de Gestión de Seguridad Cibernética – Ministerio del Interior – Chile

Tal como se muestra en la Tabla 1, la importancia de controlar estos riesgos ha llevado a que, dentro de los tipos de ticket reportados, se encuentra la vulnerabilidad del ciberespacio como el incidente con mayor cantidad de reportes, lo que se confirma en Red Seguridad (2022), llegando al mismo nivel de las campañas de desinformación y efectos del cambio climático, clasificados como riesgos que, a largo plazo, provocan un mayor deterioro.

Por lo tanto, para hacer frente a estos ataques y amenazas del ciberespacio, se requiere una estrategia de prevención. Algunas acciones que forman parte de estas estrategias son las siguientes: gestión adecuada de incidentes, capacidad de recuperación del sistema y gestión de los cambios.

2.3 Riesgos por fuga de datos

Existe una fuga de datos cuando información confidencial de una organización es expuesta de forma accidental o intencional por Internet u otras formas, de acuerdo con lo que señala Tyas (2023). En la actualidad, se visualiza dentro de las organizaciones y población en general un incremento en el uso de dispositivos móviles, lo que hace crecer las probabilidades de riesgos en cuanto a la fuga de información confidencial con la que se trabaja.

Diversos autores han investigado acerca de las razones por las que ocurre una fuga de datos en las organizaciones. Posiblemente lo que más se destaca en dichas investigaciones es la utilización de aplicaciones móviles. De hecho, Cordero (2016) recalca que aproximadamente un 97% de las aplicaciones cuentan con un portillo que permite la fuga de datos, lo que se complementa con los estudios de Zuo, Lin y Zhang (2019), quienes analizaron múltiples aplicaciones proporcionadas por proveedores como Google Play, Amazon y Microsoft, descubriendo que más de 15000 servidores de aplicaciones presentan un potencial riesgo de ataque por fuga de datos.

Frente a este tipo de vulnerabilidades, las empresas y colaboradores pueden realizar acciones concretas para evitar la aparición de estos riesgos en las organizaciones. Algunas acciones son: una adecuada **simplificación de los permisos de acceso**, puesto que es fundamental para la ciberseguridad una eficiente gestión del acceso privilegiado. Una segunda solución para la fuga de datos es la encriptación de estos, lo que De Groot (2022) define como la traducción de datos en otro tipo de código, permitiendo que solamente usuarios con una clave específica de cifrado puedan leer dicha información, dificultando a los delincuentes en el ciberespacio obtener la información privilegiada. Por lo tanto, para que la estrategia de prevención en cuanto a la fuga de datos sea eficaz, es preciso un enfoque dirigido a la “amenaza de seguridad más importante para una organización: el error humano” (Kost, 2023).

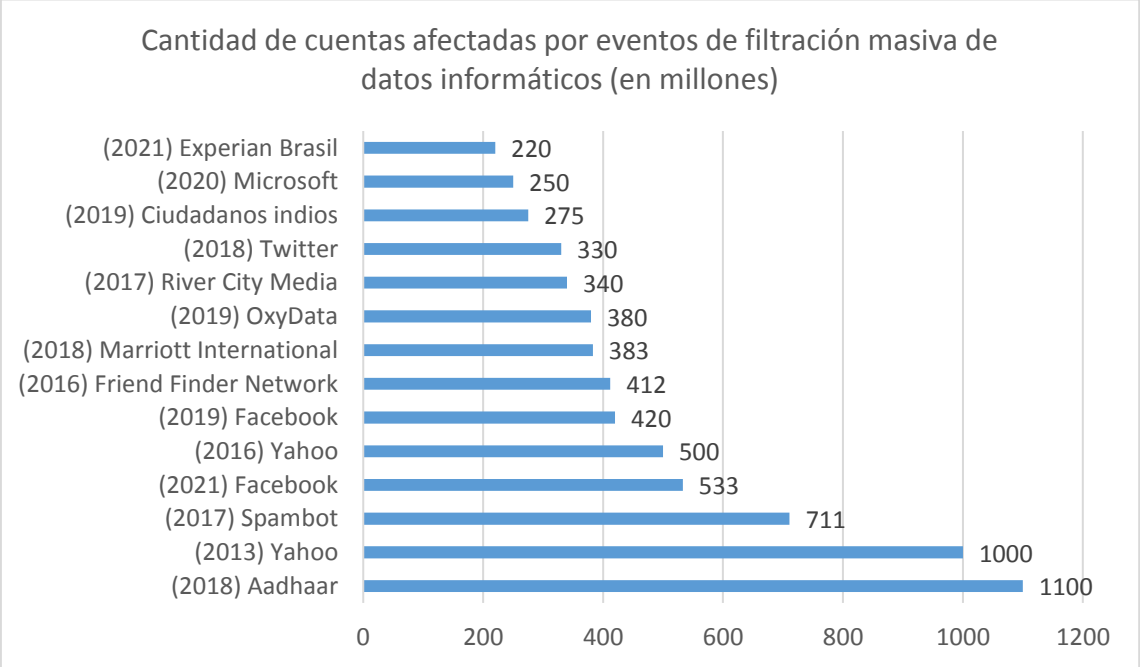
2.4 Riesgos de privacidad

Es importante diferenciar entre los riesgos de fuga de datos y los riesgos de privacidad. Si el riesgo de fuga de datos es la pérdida de confidencialidad de la información provocando con ello la pérdida de control por parte de la organización (Mellado, 2020), el riesgo de privacidad hace referencia a la información confidencial del empleado o cliente, en otros términos, a la privacidad del individuo.

Esta situación se ha presentado con más notoriedad en los tiempos de pandemia en que el teletrabajo fue la modalidad principal para la operatividad de las instituciones, lo que ha abierto nuevos caminos para la comunicación en ambientes virtuales, pero a su vez ha incrementado la probabilidad de una pérdida de control de datos personales. Las investigaciones desarrolladas por Rodríguez (2021) muestran una evidencia acerca de cómo la pandemia ha incrementado la importancia en cuanto a la protección de los datos personales, bajo el escenario de que una nación se encuentre en un estado excepcional de emergencia dado por una crisis sanitaria.

Si no existe protección de datos, los factores de riesgo son múltiples, por nombrar algunos: suplantación de la identidad, información confidencial utilizada por terceras personas, pérdida de autoridad sobre la información confidencial, pérdida de la información personal. El problema que se visualiza en la actualidad es que esta realidad sigue en crecimiento y las consecuencias pueden ser graves, tal como lo ejemplifica Rojas (2017) en el que, por un simple clic en un vínculo sospechoso por una cuenta de Facebook, un criminal consigue controlar el dispositivo de una persona. La siguiente gráfica proporcionada por Chevalier (2021) presenta las mayores filtraciones de datos a nivel mundial hasta el 07 de abril de 2021:

Figura 2: Resultados Reporte CHAOS 2015-2020



Fuente: Statista - 2021

Para evitar este tipo de riesgos simples recomendaciones permiten mantener los datos protegidos de ciberataques como los siguientes: configurar la privacidad al momento de utilizar navegadores de internet como Microsoft Edge, Google Chrome o Mozilla Firefox; establecer contraseñas seguras, tanto a nivel de intranet como internet, conocer todas las medidas de seguridad ofrecidas por una plataforma Wifi gratuita, evitando acceder a sitios con información privilegiada como bancos o redes sociales, entre otros.

2.5 Riesgos por el no cumplimiento de regulaciones obligatorias

Las clasificaciones de riesgos indicadas en las páginas anteriores se relacionan con las atenciones que la propia organización a nivel interno debe realizar para que los proyectos de tecnologías de información se lleven a cabo correctamente, con sus alcances, tiempos y recursos establecidos. Sin embargo, puede ocurrir que las regulaciones internas incumplan las legislaciones a nivel gubernamental enfocadas a la correcta gestión y auditoría de los sistemas de información.

Puesto que existe una clara dependencia de la información que se administre dentro de la sociedad, las organizaciones requieren de sistemas que sean capaces de procesar la información con una tasa de rapidez a lo menos igual al crecimiento de los datos. Sin embargo, se corre el riesgo de que parte de esta información se pierda, debido a la rapidez en las transferencias de datos. Por esta razón, los gobiernos publican normativas cuyo objetivo es la protección de la información gestionada, de acuerdo con lo que menciona Olsen (2019). El mismo autor indica que la ética debe llevar a las empresas a ofrecer garantías para el aseguramiento de confidencialidad para los datos de sus clientes lo que, mediante normativas, se exige a las organizaciones que cumplan con este cometido.

En este sentido, es posible visualizar la gran diferencia existente entre países que cuentan con potentes legislaciones en materia de ciberseguridad y aquellos que no lo poseen o su legislación es muy débil. Una publicación presentada por Hernández M. (2020), presenta una tabla de los países con mejor ciberseguridad y aquéllos que son menos ciberseguros:

Tabla 2: Ranking 2020 de países con mayor cantidad de ciberataques

Número	País	Puntaje 2020	% computadores con malware	% ataques de malware financiero	Países mejor preparados para ciberataques	Países con mejor legislación de ciberseguridad
1	Argelia	48,99	19,75	0,5	0,262	1
2	Tayikistán	48,54	8,12	1,4	0,263	2
3	Turkmenistán	48,39	5,84	1,1	0,115	2
4	Siria	44,51	13,99	1,2	0,237	1
5	Irán	43,48	7,21	0,8	0,641	2
72	Japón	9,46	9,17	0,2	0,880	6
73	Irlanda	9,40	4,51	0,1	0,784	5
74	Alemania	9,39	9,29	0,5	0,849	7
75	Suecia	8,40	4,03	0,1	0,810	5
76	Dinamarca	6,72	3,15	0,1	0,852	5

Fuente: Investigación efectuada por Comparitech del Reino Unido, año 2020

En esta investigación, se analizaron 76 países en cuanto a su nivel de ciberseguridad, siendo la posición 1 el país menos ciberseguro, mientras que el valor 76 resulta ser el país más ciberseguro. Los países que ocupan los últimos lugares de la tabla presentan legislaciones que no solo se enfocan a la protección de los datos, sino a establecer leyes que se preocupan del contenido de las páginas de Internet, además del delito en ciberseguridad.

Esto implica que los países se enfrentan constantemente a la problemática de mejorar la legislación de la seguridad en Internet, frente a una sociedad en que la comunicación a distancia va en aumento permanente, desafíos que deben sortear dos tipos de amenazas (Ibarra & Nieves, 2016). La primera es la ilegal, a través de la expresión cibernética del

terrorismo. En segundo lugar, está la amenaza del sector privado, que posee un mayor dominio del Internet y, en consecuencia, tienen más posibilidades de transformarse en dueños de la información disponible.

Por lo tanto, es importante contar con una legislación eficiente en sistemas de información para garantizar la disminución de los potenciales impactos. Uruguay, por ejemplo, ha implementado diferentes medidas como la creación de un Centro nacional de Respuesta a Incidentes de Seguridad Informática CERTuy, mientras que en Chile su homólogo es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT, organismos encargados del fortalecimiento de las buenas prácticas, leyes y estándares relacionados con la ciberseguridad, de manera que “el proceso de transformación digital de cara a los ciudadanos se consolide con la mayor seguridad posible” (CSIRT, 2021). En este punto, “las normas o estándares ISO, pueden ser un buen punto de partida a la hora de establecer un sistema de gestión en la información en la empresa” (Canteli, 2018).

2.6 Riesgos de tipo estratégico

Cualquier proyecto de sistema de información que busque la transformación digital, debe responder a las siguientes preguntas: ¿qué se espera conseguir con la implementación? ¿La empresa se encuentra preparada para un cambio tan importante? Esto implica definir objetivos y analizar si el personal está dispuesto a asumir una nueva cultura digital.

Para esto, es importante considerar cuáles son las clases de riesgos estratégicos que pueden visualizarse dentro de las organizaciones. Arrarte (2021) plantea que este tipo de riesgos se observa por medio de una tipología de riesgos estratégicos, cuyas características son:

- Los riesgos no son los mismos para diferentes organizaciones. Considerando que cada empresa cuenta con su propia estructura organizacional, así como sus procesos de negocios y operaciones específicos para cada organización, los riesgos estratégicos se caracterizan por no ser idénticos entre entidades.
- Son fáciles de ignorar, debido a que erróneamente se presentan como riesgos de alta improbabilidad de ocurrencia, lo que puede llevar a la empresa a confiar en que dichas eventualidades están descartadas, siendo que realmente ocurre lo contrario.
- No son fáciles de controlar, si se ocupan herramientas tradicionales relacionadas con la administración de los riesgos empresariales.

Diversos estudios muestran que, si las empresas se enfocan a controlar los riesgos de tipo financiero, de seguridad y operacionales, no necesariamente prestarán atención a los posibles riesgos estratégicos que pueden presentarse en las organizaciones. El impacto que posiblemente ocurra en estos últimos riesgos es la destrucción a gran escala del valor generado, razón por la que se agrega en Deloitte (2016) la importancia en colocar atención e inyectar recursos a este tipo de riesgos. Por lo tanto, es primordial tratar estos riesgos correctamente.

En una implementación de Tecnologías de Información, las empresas se ven enfrentadas tanto a amenazas como a vulnerabilidades, siendo crucial la gestión, ya que permite la administración de la exposición al riesgo de la mejor manera posible, minimizando con ello las pérdidas frente a hechos potenciales de ocurrencia (Lavell, 2001), siempre y cuando la gestión se relacione directamente con la seguridad física y lógica de los sistemas de información.

Sin embargo, este punto no es suficiente, de no incorporarse otros elementos como una adecuada normativa interna que oriente las tecnologías de información hacia el cumplimiento de los objetivos trazados por las organizaciones, una adecuada capacitación de los usuarios hacia una nueva cultura digital y las amenazas provenientes del exterior.

Si bien los párrafos anteriores proporcionan herramientas válidas para una consecución exitosa de la gestión de riesgos para este tipo de proyectos, esto carece de validez si la

organización no conoce su modelo de negocio. Dicho modelo permite a la empresa conocer sus limitaciones, lo que representa el primer perfil en las necesidades primarias de cumplimiento por parte de la firma. Esto, en consecuencia, permitirá definir la mejor manera de implementar un sistema de información en cuanto al avance hacia la transformación digital.

Una vez identificada la forma de implementación de un proyecto tecnológico, es importante definir las necesidades de personal y tecnológicas que se ajusten a los requerimientos del negocio. Todos estos tópicos otorgan como elemento resultante una línea base de cumplimiento. De acuerdo con Todd (2022), si la línea base representa el resultado esperado, se requiere evaluar la efectividad del sistema (o proyecto) para el control de los riesgos e identificar si se cumplen con los estándares establecidos por la organización.

Finalmente, es imposible descartar la participación de terceros para los procesos de negocio. Esto, debido a que las organizaciones normalmente subcontratan servicios de tecnologías de información a proveedores de TI, quienes cuentan con la experiencia en la implementación de estos sistemas. De esa forma, es posible potenciar los procesos operativos y empresariales, siendo crucial la gestión adecuada de las terceras partes puesto que, de lo contrario, se incrementan los riesgos. Como indica Descalzo (2017) esto se traduce en incumplimientos contractuales con los clientes o vulnerabilidades en cuanto a la tecnología utilizada.

3. Conclusiones

Los riesgos estarán presentes en cualquier tipo de proyecto, incluyendo los que se relacionan con la transformación digital de las organizaciones, por lo que es clave su gestión para, de esta manera, mitigar los efectos negativos como consecuencia de una fallida implementación.

La conectividad máxima, la potencia informática extrema y la gran automatización forman parte de la Industria 4.0, una evolución de las revoluciones industriales anteriores que ha permitido el incremento de la productividad en las empresas y en el flujo de información. Sin embargo, este vertiginoso avance implica el nacimiento de nuevas eventualidades.

En cuanto a los proyectos de transformación digital, se han identificado diversos tipos de riesgos dentro del trabajo de investigación, como la fuga de datos, privacidad, riesgos tecnológicos y riesgos del ciberespacio. Una correcta gestión de los riesgos permite que su exposición sea administrada de la mejor manera posible.

Para ello, es clave considerar ciertos factores que se traducen en una disminución drástica en cuanto a la incertidumbre, así como la seguridad de los sistemas de información, capacitación de los usuarios para la cultura digital de las organizaciones, definición y establecimiento de procesos adecuados y coherentes. A esto se suma el conocimiento del modelo de negocio, puesto que los proyectos relacionados con tecnologías de información implican el establecimiento de objetivos que consideran las necesidades primarias de cumplimiento.

La adecuada implementación del proyecto tecnológico y la correcta determinación de necesidades tecnológicas y de personal, considerando la línea base de cumplimiento, permite la consecución de una administración eficiente de los recursos.

Referencias Bibliográficas

Acronis Cyber Protect Cloud. (2021, Junio 24). *¿Qué es la gestión de riesgo de TI?* Mensaje publicado en https://www.acronis.com/es-mx/blog/posts/it-risk-management/

Arrarte, R. (2021, Diciembre 21). *9 riesgos estratégicos y cómo enfrentarse a ellos de manera efectiva*. Mensaje publicado en: https://www.diligent.com/es/9-riesgos-estrategicos-y-como-enfrentarse-a-ellos-de-manera-efectiva/

Canteli, A. (2018, Junio 8). *Cumplimiento de requisitos legales en la gestión de la información.* Mensaje publicado en https://www.openkm.com/es/blog/cumplimiento-de-requisitos-legales-en-la-gestion-de-la-informacion.html

Chablé, V. (2020, Mayo 18). *Ventajas de la tecnología de la información*. Obtenido el 10 de marzo de 2023, de LinkedIn: https://www.linkedin.com/pulse/ventajas-de-la-tecnolog%C3%ADa-informaci%C3%B3n-v%C3%ADctor-chabl%C3%A9/?originalSubdomain=es

Chevalier, S. (2021, Abril 8). *Las mayores filtraciones de datos del mundo*. Obtenido de Statista: https://es.statista.com/grafico/5986/las-mayores-filtraciones-de-datos-personales/

Cordero, C. (2016, Marzo 31). 97% de las apps tienen portillos que facilitan fuga de datos de usuarios. *El Financiero*. Obtenido de https://www.elfinancierocr.com/tecnologia/97-de-las-apps-tienen-portillos-que-facilitan-fuga-de-datos-de-usuarios/JGYS4OLPDJAHVEDVS34JSYOXKU/story/

CSIRT. (2021). *Quiénes Somos*. Obtenido el 15 de Marzo de 2023, de CSIRT - Ministerio del Interior - Gobierno de Chile: https://www.csirt.gob.cl/quienes-somos/

De Aza, E. (2011, diciembre 18). *Análisis de Riesgo de un Proyecto.* Mensaje publicado en Escuela de Organización Industrial: https://www.eoi.es/blogs/estefanykaryelindeaza/2011/12/18/analisis-de-riesgo-de-un-proyecto/

De Groot, J. (2022, Noviembre 7). *What is Data Encryption? Definition, Best Practices & More*. Obtenido de Digital Guardian: https://www.digitalguardian.com/blog/what-data-encryption

Deloitte. (2016). *Riesgo estratégico: La piedra angular para la transformación del riesgo.* Obtenido de Deloitte IAS Plus: https://www.iasplus.com/en/publications/colombia/other/riesgo-estrategico/at_download/file/Riesgo%20estrategico.pdf

Descalzo, F. (2017, Julio 3). *Integración de Riesgos de IT y Riesgos Operacionales.* Obtenido de LinkedIn: https://es.linkedin.com/pulse/integracion-de-riesgos-y-operacionales-fabi%C3%A1n-descalzo

Entel Ocean. (2022, Septiembre 29). *¿Cómo la transformación digital optimiza los procesos industriales?* Obtenido de Entel Ocean: https://entelocean.com/blog/como-la-transformacion-digital-optimiza-los-procesos-industriales#:~:text=Gracias%20a%20la%20digitalizaci%C3%B3n%2C%20los,empresa%20a%20ser%20m%C3%A1s%20competitiva

Escuela Europea de Excelencia. (2016, Julio 4). *Proceso de gestión de riesgo*. Obtenido de Escuela Europea de Excelencia: https://www.escuelaeuropeaexcelencia.com/2016/07/proceso-gestion-de-riesgo/

Fonseca, D., García-Peñalvo, F. J., & Camba, J. D. (2020, Octubre 26). New methods and technologies for enhancing usability and accessibility of educational data. *Universal Access in the Information Society, 20*, 421-427. DOI: https://doi.org/10.1007/s10209-020-00765-0

Frendiana, M. L., & Soediantono, D. (2022, Febrero 19). Benefits of Diigital Transformation and Implementation Proposition in the Defense Industry: A Literature review. *International Journal of Social and Management Studies*, *3*(4), 1-12. Obtenido de http://download.garuda.kemdikbud.go.id/article.php?article=2496301&val=20406&title=Benefits%20of%20Digital%20Transformation%20and%20Implementation%20Proposition%20in%20the%20Defense%20Industry%20A%20Literature%20Review

García, G. (2015, Diciembre 3). *Por qué fracasan los Proyectos de T.I.* Mensaje publicado en Naps Tecnología y Educación: https://naps.com.mx/blog/por-que-fracasan-los-proyectos-de-t-i/

Henderson, C. (2021, Marzo 12). *¿Qué es el riesgo tecnológico? Cómo administrar las amenazas empresariales.* Obtenido de AnyConnector: https://anyconnector.com/es/digital-transformation-strategy/technology-risk.html

Hernández, D. (2019, Octubre 21). ¿Por qué fracasan los proyectos de transformación digital? *Repositorio Comillas*. Obtenido de http://hdl.handle.net/11531/52295

Hernández, M. (2020, Marzo 5). *Selección Forbes 2020 - Estos son los países más ciberseguros del mundo*. Obtenido de Forbes México: https://www.forbes.com.mx/radiografia-cuales-son-los-paises-mas-ciberseguros-del-mundo/

Ibarra, V., & Nieves, M. (2016, Noviembre 23). La seguridad internacional determinada por un mundo On-line: el Estado ante el desafío del terrirismo y la ciberseguridad. *VIII Congreso de Relaciones Internacionales.* La Plata: Instituto de Relaciones Internacionales - Universidad Nacional de La Plata. Obtenido de http://sedici.unlp.edu.ar/handle/10915/58156

Johnson, J. (2022). *Chaos Report: Beyond Infinity.* Centerville, MA: The Standish Group International Inc.

Kost, E. (2023, Marzo 2). *6 Most Common Causes of Data Leakes in 2023*. Obtenido el 14 de Marzo de 2023 de UpGuard: https://www.upguard.com/blog/common-data-leak-causes

Lavell, A. (2001). *Sobre la Gestiòn del Riesgo: Apuntes hacia una Definición.* Obtenido de http://cidbimena.desastres.hn/docum/crid/Mayo2004/pdf/spa/doc15036/doc15036-contenido.pdf

Llorens, F. (2020, Enero 13). *Transformación digital versus digitalización*. Mensaje publicado en Universídad: https://www.universidadsi.es/transformacion-digital-versus-digitalizacion/

Mellado, L. (2020, Enero 28). *Fuga de Información, el terror de las empresas*. Obtenido el 15 de Marzo de 2023 de Smart HC: https://www.smarthc.com/index.php/fuga-de-informacion/

Ministerio del Interior - Gobierno de Chile. (2022, Mayo). Informe de Gestión de Seguridad Cibernética. Obtenido de Ministerio del Interior - Gobierno de Chile: https://www.ciberseguridad.gob.cl/media/2022/06/IGM-CSIRT-2022-Mayo.pdf

Olsen, O. C. (02 de noviembre de 2019). *La importancia del cumplimiento de regulaciones en la seguridad de información*. Obtenido el 16 de Marzo de 2023 de Kriptos:

https://www.kriptos.io/es-post/la-importancia-del-cumplimiento-de-regulaciones-en-la-seguridad-de-informacion

Pramanik, H. S., Kirtania, M., & Pani, A. K. (2019, Junio). Essence of digital transformation - Manifestations at large financial institutions from North America. *Future Generation Computer Systems, 95*, 323-343. DOI: https://doi.org/10.1016/j.future.2018.12.003

Pulido-Rojano, A. D., Ruiz-Lázaro, A., & Ortiz-Ospino, L. E. (2020, Marzo). Mejora de procesos de producción a través de la gestión de riesgos y herramientas estadísticas. *Ingeniare, Revista chilena de ingeniería, 28*(1). DOI: http://dx.doi.org/10.4067/S0718-33052020000100056

Red Seguridad. (2022, Abril 20). La vulnerabilidad del ciberespacio, entre los principales riesgos para la Seguridad Nacional. *Red Seguridad*. Obtenido de https://www.redseguridad.com/actualidad/la-vulnerabilidad-del-ciberespacio-entre-los-principales-riesgos-para-la-seguridad-nacional_20220420.html

Rodríguez, J. F. (2021, Marzo 20). Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos. *Revista de Derecho Político*(110), 299-318. DOI: https://doi.org/10.5944/rdp.110.2021.30337

Rojas, J. C. (2017, Marzo 13). La pesadilla de Angélica por un "hackeo" que empezó con un clic. *El Tiempo*. Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/historia-de-una-mujer-que-fue-hackeada-66604

Todd, B. (2022, Junio 22). *Everything about a Baseline Risk Assessment.* Publicado de Makrosafe: https://www.makrosafe.co.za/blog/baseline-risk-assessment

Tyas, A. (2023, Marzo 02). *What is Data Leak? Stop Giving Cybercriminals Free Access*. Mensaje publicado de UpGuard: https://www.upguard.com/blog/data-leak

Universidad Europea. (2021, Abril 27). ¿Cuáles son las principales amenazas y riesgos del ciberespacio? *Universidad Europea*. Obenido de https://universidadeuropea.com/noticias/cuales-son-las-principales-amenazas-y-riesgos-del-ciberespacio/

Vial, G. (2019, Junio). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118-144. DOI: https://doi.org/10.1016/j.jsis.2019.01.003

Zuo, C., Lin, Z., & Zhang, Y. (2019). Why does your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps. *2019 IEEE Symposium on Security and Privacy*. San Francisco, CA: IEEE. DOI: https://doi.org/10.1109/SP.2019.00009

Comunicación alineada con los Objetivos de Desarrollo Sostenible