PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE LETRAS Y CIENCIAS HUMANAS

Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones

Trabajo de Suficiencia Profesional para obtener el título profesional de Licenciado en Ciencias de la Información que presenta:

Marco Antonio Bermudez Torres

Asesora:

Maria del Pilar Acha Albujar

Lima, 2024

Informe de Similitud

Yo, Maria del Pilar Acha Albujar, docente de la Facultad de Letras y Ciencias Humanas de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de suficiencia profesional titulado:

...Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones

del autor/ de los(as) autores(as)

MARCO ANTONIO BERMUDEZ TORRES,

dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 31 %. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 28/02/2024.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 28 de febrero de 2024

Apellidos y nombres del asesor / de la asesora: Acha Albujar, Maria del Pilar	
DNI: 08811199	Firma
ORCID: 0009-0004-0668-4666	

DEDICATORIA

Dedico esta tesina a mi familia, padres, hermano y esposa, pero especialmente a mi hija Nathalie Abigail y a mi hijo Esteban Ludwig, esperando que este trabajo los inspire a reconocer la importancia de las Ciencias de la Información y la ciberseguridad en sus futuros roles profesionales. En un mundo cada vez más interconectado, donde las amenazas como la ciberdelincuencia y la ciberguerra son omnipresentes, y donde tecnologías complejas y emergentes como la inteligencia artificial y la computación cuántica plantean nuevos desafíos y una amplia gama de oportunidades.

AGRADECIMIENTO

Expreso mi sincero agradecimiento a mi asesora, la profesora María del Pilar Acha Albujar, por su invaluable orientación durante todo el proceso de esta investigación. Agradezco también a la profesora Ana María Talavera Ibarra, coordinadora académica del curso de titulación, y a los profesores de la especialidad de Ciencias de la Información encargados de dictar el curso, cuyo compromiso y dedicación fueron fundamentales para mi desarrollo académico.

Asimismo, reconozco la contribución de las profesoras Ela Villa Rojas y Patricia Naka Shimabukuro, quienes como miembros del jurado brindaron su tiempo y valiosas recomendaciones para enriquecer este trabajo.

Agradezco a la Facultad de Letras y Ciencias Humanas de la PUCP por permitirme lograr este nuevo hito académico.

Además, deseo expresar mi profundo agradecimiento a la organización que me brindó la autorización para exponer de manera genérica mi experiencia profesional en la implementación de estándares de ciberseguridad en su empresa. Su apertura y confianza en compartir este conocimiento sin vulnerar la confidencialidad de sus datos han sido fundamentales para enriquecer este trabajo. Su colaboración ha sido un ejemplo de compromiso con el desarrollo académico y profesional, y estoy sinceramente agradecido por su generosidad.

Por último, mi reconocimiento a los profesionales cuyos conocimientos y documentos fueron fuentes esenciales para esta investigación.

RESUMEN

En la actualidad, el Estado peruano participa activamente en la sociedad de la información y del conocimiento. De igual manera, con la participación de la Secretaría de Gobierno y Transformación Digital, que forma parte de la Presidencia del Consejo de Ministros (PCM), se está promoviendo el despliegue de la Transformación y Gobierno Digital en el Estado peruano. Como resultado, se están llevando a cabo diversas actividades dirigidas a la gestión, administración, ejecución, implementación y divulgación de la seguridad de la información y la ciberseguridad, entre otros temas relevantes. Además, tenemos los esfuerzos del Instituto Nacional de Calidad (INACAL), que basándose en los criterios internacionales de los estándares de la Organización Internacional de Normalización (ISO) aprobaron las Normas Técnicas Peruanas, referidas a las temáticas de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), gestión de riesgos de ciberseguridad y seguridad de la información, y ciberseguridad en general, que son usadas por el Estado Peruano y organizaciones privadas como referencia para implementar su SGSI o implementar controles de seguridad de la información y de ciberseguridad. En este contexto la aplicación de estándares de ciberseguridad resulta de vital importancia en las organizaciones para gestionar sus riesgos, proteger sus datos e información, y para apoyar la continuidad de sus operaciones. En esta perspectiva, el objetivo general de este trabajo de suficiencia profesional es: Analizar la importancia de la ciberseguridad en las organizaciones, considerando estándares internacionales, normas peruanas y mi experiencia profesional, además evaluar la relevancia de su incorporación en la formación de los futuros profesionales de Ciencias de la Información, y por objetivos específicos: i) Explicar la importancia de la ciberseguridad en las organizaciones, abordando los principales estándares y normativas peruanas pertinentes., ii) Evaluar la relevancia de incorporar temáticas de seguridad de la información y ciberseguridad en la formación académica de los futuros profesionales de Ciencias de la Información, iii) Describir mi experiencia como profesional de las Ciencias de la Información en la implementación de estándares de ciberseguridad en una organización; y, iv) Presentar los resultados beneficiosos

obtenidos en la aplicación de estándares de ciberseguridad en un caso real. En cuanto a la metodología empleada, se ha adoptado un enfoque cualitativo, empleando el método de investigación documental; complementándose con la descripción de mi experiencia profesional en una organización sobre la implementación de controles de ciberseguridad, basados en estándares internacionales.

Palabras clave: Ciencias de la Información, seguridad de la información, ciberseguridad, información, Sistema de Gestión de Seguridad de la Información y organización.

ABSTRACT

Currently, the Peruvian State actively participates in the information and knowledge society. Likewise, with the participation of the Secretariat of Government and Digital Transformation, which is part of the Presidency of the Council of Ministers (PCM), the deployment of Digital Transformation and Government in the Peruvian State is being promoted. As a result, various activities are being carried out aimed at the management, administration, execution, implementation and dissemination of information security and cybersecurity, among other relevant topics. In addition, we have the efforts of the National Quality Institute (INACAL), which based on the international criteria of the standards of the International Organization for Standardization (ISO) approved the Peruvian Technical Standards, referring to the issues of implementation of a Quality Management System. Information Security (ISMS), cybersecurity risk management and information security, and cybersecurity in general, which are used by the Peruvian State and private organizations as a reference to implement their ISMS or implement information security controls and cybersecurity. In this context, the application of cybersecurity standards is of vital importance for organizations to manage their risks, protect their data and information, and to support the continuity of their operations. From this perspective, the general objective of this professional proficiency work is: Analyze the importance of cybersecurity in organizations, considering international standards, Peruvian norms and my professional experience, and also evaluate the relevance of its incorporation in the training of future professionals. of Information Sciences, and for specific objectives: i) Explain the importance of cybersecurity in organizations, addressing the main relevant Peruvian standards and regulations., ii) Evaluate the relevance of incorporating information security and cybersecurity topics in the academic training of future Information Sciences professionals, iii) Describe my experience as an Information Sciences professional in the implementation of cybersecurity standards in an organization; and, iv) Present the beneficial results obtained in the application of cybersecurity standards in a real case. Regarding the methodology used, a qualitative approach has been adopted, using the documentary research method;

complemented by the description of my professional experience in an organization on the implementation of cybersecurity controls, based on international standards.

Keywords: Information Sciences, information security, cybersecurity, information, Information Security Management System and organization.

ÍNDICE

Introducción ……..…….. 10

1. Capítulo 1: Aspectos generales ……..…….. 14

1.1. Consideraciones metodológicas …… 14

1.2. Objetivos …… 14

1.2.1. Objetivos generales ……..… 15

1.2.2. Objetivos específicos ……..…… 15

1.3. Marco general sobre la ciberseguridad ……..….. 15

1.3.1. La ciberseguridad y las organizaciones ……. 15

1.3.2. Relevancia de la ciberseguridad en las Ciencias de la Información …… 25

1.3.3. Estándares de ciberseguridad y su importancia en las organizaciones …..... 32

1.3.4. Normas peruanas relacionadas con ciberseguridad ……... 39

2. Capítulo 2: Experiencia profesional de implementación de estándares de ciberseguridad en una organización ……..…… 47

2.1. Aspectos generales de la empresa ……... …… 48

2.2. Requisitos de Protección de Datos para proveedores de Microsoft 48

2.3. Actividades desarrolladas …….. 49

3. Capítulo 3: Resultados obtenidos ……... 55

3.1. Documentos de ciberseguridad implementados ……. 55

3.2. Aspectos técnicos de ciberseguridad implementados ……... 61

3.3. Capacitación y sensibilización en temas de seguridad de la información y ciberseguridad ……...… 63

3.4. Beneficios obtenidos ……... 66

4. Conclusiones ……..…….. 70

5. Recomendaciones ……..……. 73

Referencias ……..……... 77

Anexo A: Curriculum Vitae resumido ……..……. 84

Anexo B: Requisitos de Protección de Datos para proveedores de Microsoft ……. 85

INTRODUCCIÓN

La sociedad actual se encuentra inmersa en la era de la información y del conocimiento, donde las organizaciones operan diariamente en entornos digitales. En estos escenarios, la globalización y la innovación tecnológica son fuerzas influyentes que moldean sus actividades. Vivimos en un mundo digitalizado y altamente interconectado, donde la seguridad de la información y la ciberseguridad se establecen como pilares fundamentales para el funcionamiento seguro y eficiente de las organizaciones. La adopción de estándares internacionales, como la ISO/IEC 27001:2022 y su equivalente nacional la Norma Técnica Peruana NTP-ISO/IEC 27001:2022, se presentan como un marco estructurado que permite gestionar y proteger la información de manera efectiva. Esta implementación, respaldada por normativas específicas como la ISO/IEC 27002-2022 y su equivalente peruana NTP-ISO/IEC 27002-2022, no solo contribuye a salvaguardar la confidencialidad, integridad y disponibilidad de los datos e información, sino que también permite mitigar riesgos y amenazas, promoviendo prácticas consistentes de ciberseguridad. Además, es importante mencionar al Marco de Ciberseguridad NIST (CSF) 2.0, que emerge como un estándar vital ofreciendo una orientación inestimable a las organizaciones en la gestión de los riesgos de ciberseguridad, publicado el 26 de febrero de 2024, destaca por ser una guía crucial para las organizaciones en la gestión de riesgos de ciberseguridad..

Como parte de la iniciativa de transformación digital liderada por el Estado peruano, diversas normativas, como la Ley de Gobierno Digital y el Decreto de Urgencia que da inicio al Sistema Nacional de Transformación Digital, reconocen la ciberseguridad como un pilar fundamental para preservar la confianza digital. Estas normativas establecen la obligación de gestionar (implementar, auditar y mantener) un Sistema de Gestión de Seguridad de la Información (SGSI), destacando la necesidad de gestionar proactivamente los riesgos e incidentes de seguridad y ciberseguridad. Este abordaje integral no solo considera aspectos técnicos de seguridad informática y ciberseguridad, adicionalmente también contempla cuestiones éticas, legales y de gobernanza digital en el ámbito peruano.

Tomando en cuenta este preámbulo, el propósito de este trabajo es explorar la importancia de la ciberseguridad en las organizaciones. En este sentido, la presente investigación plantea el objetivo general de: Analizar la importancia de la ciberseguridad en las organizaciones, considerando estándares internacionales, normas peruanas y mi experiencia profesional, además evaluar la relevancia de su incorporación en la formación de los futuros profesionales de Ciencias de la Información, y por objetivos específicos: i) Explicar la importancia de la ciberseguridad en las organizaciones, abordando los principales estándares y normativas peruanas pertinentes., ii) Evaluar la relevancia de incorporar temáticas de seguridad de la información y ciberseguridad en la formación académica de los futuros profesionales de Ciencias de la Información, iii) Describir mi experiencia como profesional de las Ciencias de la Información en la implementación de estándares de ciberseguridad en una organización; y, iv) Presentar los resultados beneficiosos obtenidos en la aplicación de estándares de ciberseguridad en un caso real.

Se optó por un enfoque cualitativo en la metodología, utilizando el metodo de investigación documental, lo que ha facilitado una comprensión y aproximación de la materia abordada. Este enfoque se respaldó mediante el uso de diversas fuentes documentales tanto nacionales como internacionales en formato digital, y se llevó a cabo un análisis exhaustivo de dichos documentos. Por otro lado, se incorporó una explicación detallada de mi experiencia como profesional de las Ciencias de la Información con un caso real sobre la implementación de estándares de ciberseguridad en una organización.

Este trabajo de suficiencia profesional fue elaborado en su totalidad por el investigador, conforme a las directrices establecidas en el Reglamento del Comité de Ética de la Investigación de la Pontificia Universidad Católica del Perú (2011), teniendo como referente los principios éticos de integridad científica; así mismo, durante el desarrollo de este trabajo, se realizó una comunicación gradual del análisis. Además, se realizó un riguroso apego a los estándares académicos, asegurando la correcta atribución de los documentos empleados, utilizando el formato de escritura APA 7ª.

El tema de la ciberseguridad en las organizaciones es el enfoque principal de la investigación o campo de estudio, el cual se ubica en el área de seguridad de la información en las organizaciones. En tres capítulos, junto con las conclusiones y referencias, se organiza esta investigación. El primer capítulo aborda la explicación de los aspectos generales, como consideraciones metodológicas, objetivos y el marco general de ciberseguridad, este último se subdivide en: La ciberseguridad y las organizaciones, la relevancia de la ciberseguridad en las Ciencias de la Información, los estándares de ciberseguridad y su importancia en las organizaciones, y sobre las normas peruanas relacionadas con ciberseguridad. El segundo capítulo trata sobre mi experiencia como profesional de las Ciencias de la Información en la implementación de estándares de ciberseguridad en una organización. Y por último en el tercer capítulo se explican los resultados obtenidos en mi experiencia de implementación de estándares de ciberseguridad referida en el capítulo anterior.

Como resultado de este trabajo, se concluye que la implementación de estándares de seguridad de la información y ciberseguridad, son esenciales para la gestión y resguardo eficaz de los datos e información en las organizaciones. Esto se traduce en un fortalecimiento de la confidencialidad, integridad y disponibilidad de la información. Además la importancia de la seguridad en toda la cadena de suministro es enfatizada específicamente por algunos estándares reconociendo la ciberseguridad como un elemento crucial para el éxito organizacional en el contexto digital actual. En el contexto de la transformación digital en Perú, normativas como la Ley de Gobierno Digital reconocen la ciberseguridad como fundamental para la confianza digital. La necesidad de implementar y gestionar un Sistema de Gestión de Seguridad de la Información (SGSI) resalta la importancia de abordar proactivamente los riesgos e incidentes, considerando aspectos técnicos, éticos y legales. Emergiendo como una prioridad para las organizaciones, la efectiva implementación y gestión de medidas de seguridad de la información, favoreciendo al avance social y económico del Estado peruano en la era digital.

Así mismo, se concluye que resulta crucial para los futuros profesionales de Ciencias de la Información desarrollar competencias y capacidades en seguridad de la información y ciberseguridad, no solo para adaptarse a los rápidos cambios

tecnológicos, sino también para proteger los datos, la información y los sistemas, además para cumplir con su responsabilidad ética de preservar la privacidad y seguridad en un entorno digital en constante evolución.

Por último, se muestra los resultados de la implementación exitosa de estándares de ciberseguridad en una organización, focalizada en dar cumplimiento con los "Requisitos de Protección de Datos para proveedores de Microsoft", destaca la necesidad de adaptabilidad y respuesta proactiva de las organizaciones ante los desafíos dinámicos en ciberseguridad. Esta iniciativa no solo cumplió con éxito los requisitos señalados, sino que también fortaleció la postura de seguridad de los datos e información de la empresa.

Los beneficios resultantes abarcan desde el cumplimiento de estándares hasta mejoras en la respuesta ante incidentes, gestión de derechos de acceso y eficiencia operativa, consolidando a la empresa como un referente comprometido con el resguardo de datos en un ecosistema corporativo en constante cambio.

CAPÍTULO 1
ASPECTOS GENERALES

1.1. Consideraciones metodológicas

Se optó por un enfoque cualitativo como metodología, utilizando el método de investigación documental. Esto ha posibilitado un acercamiento y conocimiento de la temática estudiada, respaldada por la utilización de diversas fuentes documentales nacionales e internacionales en formato digital. Se llevó a cabo un análisis de varios tipos de documentos nacionales e internacionales, como artículos académicos, normativas legales y técnicas peruanas, así como estándares internacionales. Cabe precisar, que Revilla (2020), argumenta que en la investigación cualitativa, el método principal es la investigación documental, el cual permite al investigador aproximarse indirectamente a la realidad estudiada. Esto se logra mediante el uso de fuentes secundarias, accediendo a su contenido sin realizar cambios o modificaciones.

Por otro lado, en la elaboración del presente trabajo de suficiencia profesional, como parte de la metodología se incorporó una explicación detallada de mi experiencia como profesional de las Ciencias de la Información con un caso real que abordó la implementación de estándares de ciberseguridad en una organización. Este enfoque permitió contextualizar con situaciones concretas vividas en el ámbito profesional lo desarrollado mediante el método de investigación documental señalado en el párrafo precedente. La integración de mi experiencia práctica en el análisis de resultados añadió un componente significativo al trabajo, proporcionando una perspectiva más completa y aplicada, y contribuyendo a la solidez y relevancia de las conclusiones alcanzadas en el contexto del presente trabajo.

1.2. Objetivos

A continuación, se muestran los objetivos del presente trabajo de suficiencia profesional:

1.2.1 Objetivo general:

- Analizar la importancia de la ciberseguridad en las organizaciones, considerando estándares internacionales, normas peruanas y mi experiencia profesional, además evaluar la relevancia de su incorporación en la formación de los futuros profesionales de Ciencias de la Información.

1.2.2. Objetivos específicos:

- Explicar la importancia de la ciberseguridad en las organizaciones, abordando los principales estándares y normativas peruanas pertinentes.
- Evaluar la relevancia de incorporar temáticas de seguridad de la información y ciberseguridad en la formación académica de los futuros profesionales de Ciencias de la Información.
- Describir mi experiencia como profesional de las Ciencias de la Información en la implementación de estándares de ciberseguridad en una organización.
- Presentar los resultados beneficiosos obtenidos en la aplicación de estándares de ciberseguridad en un caso real.

1.3. Marco general sobre la ciberseguridad

1.3.1. La ciberseguridad y las organizaciones

En el mundo actual, digitalizado, es crucial comprender que la información se ha vuelto un recurso de gran valor para las organizaciones, la ciberseguridad se ha vuelto una preocupación fundamental. La interconexión global y la dependencia de la tecnología han expuesto a las empresas a una variedad de amenazas internas y externas que podrían vulnerar la integridad, confidencialidad y disponibilidad de los datos e información. En este contexto, es crucial comprender el papel de la ciberseguridad en las organizaciones, así

como las medidas necesarias para protegerse contra las crecientes nuevas amenazas.

En este sentido, según el estudio de Rodríguez, Fernández y Fernández (2023), se destacó la importancia crucial de implementar y mantener un sistema de gestión de la seguridad de la información en las empresas, lo que requiere una inversión considerable de tiempo y recursos para proteger los datos de los riesgos a los que suelen estar expuestos. Los principales desafíos identificados tanto para los proveedores como para los consumidores de las empresas incluyen las transacciones, la privacidad y la seguridad del sistema en el que se llevan a cabo estas operaciones, así como las vulnerabilidades asociadas (Rodríguez et al., 2023). Esta cita resalta la importancia crítica de la seguridad de la información en los procesos de las organizaciones, subrayando los desafíos clave que enfrentan en la protección de los datos y la mitigación de riesgos de ciberseguridad. Estos hallazgos respaldan la necesidad de una gestión efectiva de la seguridad de la información en las organizaciones para garantizar la integridad, confidencialidad y disponibilidad de los datos e información en un entorno digital cada vez más complejo.

Según García Forero (2020), la seguridad de la información se define como "La disciplina que nos presenta la información, sus riesgos, sus amenazas, cómo analizar, reaccionar y prever escenarios de riesgo, las buenas prácticas en los procesos integran una organización y también nos habla de que existen esquemas normativos que son herramientas para las organizaciones pueden implementar para reducir el riesgo hasta un nivel aceptable" (p. 2).

Asimismo, García Forero (2020) señala que la seguridad informática y la seguridad de la información no son conceptos similares, y que tienen objetivos y alcances diferentes. Argumenta que "Usualmente los conceptos de seguridad informática y de seguridad de la información suelen confundirse debido a que son muy simulares, sin embargo, tienen objetivos y alcances diferentes, si se considerara la seguridad de la información como un libro

entonces la seguridad informática es un capítulo que pertenece a él. La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información" (p. 2).

Enmarcado en lo anterior, García Forero (2020) discute el concepto de ciberseguridad, destacando que "La ciberseguridad es una parte de la seguridad informática con un alcance diferente, esta se centra en el ciberespacio, según la RAE este es un ámbito virtual creado por medios informáticos. Es decir que la ciberseguridad busca a la reducción de los riesgos a los que está expuesta la información en un medio digital, desde las redes hasta los sistemas de información en los siguientes estados de la misma en sistemas interconectados: 1) Procesamiento 2) Almacenamiento, y 3) Transporte" (p. 2).

En el contexto, detallado anteriormente, según García Forero (2020), “La información puede encontrarse de diferentes maneras, ya sea en formato digital (a través de archivos en medios electrónicos u ópticos), en forma física (como documentos escritos o impresos en papel) o incluso de manera no representada, como las ideas o el conocimiento de las personas. Esta diversidad de formas en las que la información puede presentarse implica que los activos de información pueden adoptar distintos formatos. Además, la información puede ser almacenada, procesada o transmitida de diversas maneras, ya sea en formato electrónico, verbal o a través de mensajes escritos o impresos. Esto significa que la información puede existir en diferentes estados. Por lo tanto, independientemente de su forma o estado, la información requiere medidas de protección adecuadas según su importancia y criticidad. Es en este contexto que la seguridad de la información desempeña un papel fundamental, garantizando la protección y seguridad de la información en todas sus formas y estados” (p. 2).

Los conceptos esenciales de seguridad de la información, ciberseguridad y seguridad informática, tal como se exponen por García Forero

(2020), nos revelan la complejidad y la interrelación entre estas disciplinas. Desde la definición integral de la seguridad de la información hasta la distinción entre seguridad informática y seguridad de la información, y finalmente, la explicación detallada sobre la ciberseguridad, se pone de manifiesto la importancia de proteger la información en todas sus formas y estados. Estos conceptos proporcionan un marco sólido para comprender cómo las organizaciones pueden gestionar eficazmente los riesgos y las amenazas en un entorno digital en constante evolución.

Por otro lado, Carrillo (2015) plantea que "El ciberespacio es un dominio caracterizado por su artificialidad, relativa inmaterialidad y permeabilidad, capilaridad o transversalidad. Esos caracteres, junto con lo que se ha denominado su esencia, esto es, su capacidad para alterar el resto de las realidades, hacen que la seguridad en el ciberespacio o la ciberseguridad sean un problema, asimismo, como el propio ciberespacio, capilar y transversal, pero que dista mucho de ser un problema artificial o inmaterial" (p. 25).

Asimismo, sostiene que "La ciberseguridad no es sólo la seguridad del ciberespacio entendido como un espacio más y, en consecuencia, no puede comprenderse como tal mediante una extrapolación mecánica de los parámetros tradicionales que han operado en los otros dominios como la seguridad territorial, marítima, aérea o medioambiental. La ciberseguridad implica un nuevo paradigma de seguridad global, inclusiva y comprehensiva de la totalidad de los escenarios que se van a ver afectados por la impronta que introduce la existencia y la utilización del ciberespacio" (Carrillo, 2015, p. 25).

Los párrafos de Carrillo (2015) resaltan la singularidad del ciberespacio y la ciberseguridad como un desafío complejo que requiere un enfoque global y no simplemente una extrapolación de paradigmas de seguridad tradicionales. Sugiere que la ciberseguridad implica un nuevo paradigma que abarca todos los escenarios afectados por la existencia y uso del ciberespacio.

Por otro lado, según la investigación de Rodriguez Baca y sus colegas (2020). Señalan que la implementación y mantenimiento de un Sistema de

Gestión de Seguridad de la Información bajo el estándar ISO 27001 en las organizaciones influyen en los atributos de la confidencialidad, integridad y disponibilidad de los datos e información. Respecto a la confidencialidad, indican que tiene la finalidad de garantizar que la información solo fuera accesible para usuarios autorizados, considerando sus roles o cargos en la empresa. En cuanto a la integridad de los datos e información, indican que está relacionada con la protección de la información contra modificaciones no autorizadas. Por último, respecto a la disponibilidad de la información, señalan que es importante su disponibilidad permanente para respaldar las correctas decisiones de los usuarios de la organización (Rodríguez Baca et al., 2020, p. 9). En el párrafo precedente, se brinda los conceptos de la confidencialidad, integridad y disponibilidad de la información y se destaca que son aspectos fundamentales que deben ser abordados para garantizar la protección efectiva de los datos en un entorno empresarial cada vez más digitalizado.

Así mismo, de acuerdo con Cano (2011), es esencial tener en cuenta las medidas fundamentales en ciberseguridad que un país implementa para proteger de manera coherente, sistemática y sistémica los recursos de información críticos distribuidos en toda su infraestructura, y cómo estas medidas influyen en el funcionamiento del Estado (p. 4). Esta perspectiva resalta la importancia crítica de la ciberseguridad y por lo tanto de la seguridad de la información en las organizaciones, ya que la protección efectiva de los activos de información no solo garantiza la integridad y disponibilidad de los datos, sino que también asegura la continuidad y estabilidad de las operaciones empresariales en un entorno cada vez más digitalizado y sujeto a amenazas cibernéticas en constante evolución.

El National Institute of Standards and Technology (NIST) explica que el adiestramiento en asuntos relativos a la seguridad de la información, seguridad digital, protección de datos e información, está dirigido a cultivar competencias que capaciten a un individuo para llevar a cabo tareas específicas, habilidades que se desarrollan empleando principios, teorías y mejores prácticas en seguridad digital, ciberseguridad, protección de datos e información (NIST, 2015). Este párrafo resalta la importancia del adiestramiento en seguridad de

la información según el NIST, es decir basado en estándares internacionales, subrayando cómo este desarrollo de habilidades específicas es esencial para enfrentar los desafíos de la seguridad digital y protección de datos en la era actual, lo que demuestra su vigencia e importancia para las organizaciones.

Un estándar de suma importancia es el Marco de Ciberseguridad NIST (CSF) 2.0, el cual proporciona orientación a la industria, agencias gubernamentales y otras organizaciones para gestionar los riesgos de ciberseguridad. Ofrece una taxonomía, clasificación o tipología de resultados de ciberseguridad de alto nivel que pueden ser utilizados por cualquier organización, independientemente de su tamaño, sector o madurez, para comprender mejor, evaluar, priorizar y comunicar sus esfuerzos en ciberseguridad. El CSF no determina cómo deben lograrse los resultados. En su lugar, enlaza a recursos en línea que proporcionan orientaciones complementarias sobre buenas prácticas y controles que podrían utilizarse para alcanzar esos resultados. (NIST, 2024). El Marco de Ciberseguridad NIST (CSF) 2.0, siendo un documento vigente de febrero de 2024, destaca por ser una guía crucial para las organizaciones en la gestión de riesgos de ciberseguridad. Su relevancia radica en su capacidad para adaptarse a las necesidades actuales del entorno digital en constante evolución.

Por otro lado, el tratado sobre la ciberdelincuencia, conocido como el Convenio de Budapest, adoptado en 2001 y en vigor desde 2004, destaca la relevancia para individuos y organizaciones digitales de poseer competencia en seguridad de la información y ciberseguridad. Este acuerdo internacional aborda diversos aspectos de la ciberseguridad, incluyendo actividades dirigidas a sistemas informáticos y datos, la falsificación y fraudes informáticos, el uso indebido de tecnología computacional para la pornografía infantil y la infracción de la propiedad intelectual. Asimismo, insta a los Estados a establecer legislaciones que faciliten la preservación y producción de evidencia electrónica, la búsqueda legal de sistemas informáticos y la recolección de datos de tráfico y contenido. Además, promueve el intercambio de información y la asistencia en investigaciones de ciberdelitos (Gálvez Reyes & Gálvez Pacheco, 2020).

La importancia de considerar los diversos aspectos de la ciberseguridad para las organizaciones se destaca en el párrafo anterior. Como se mencionó previamente, se enfatiza que la ciberseguridad y la seguridad de la información son conceptos distintos. Es crucial entender que la seguridad de la información adopta una perspectiva integral, mientras que la ciberseguridad se centra en proteger sistemas y datos digitales contra amenazas como ataques y acceso no autorizado. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información en ambientes digitales mediante la implementación de medidas preventivas y prácticas seguras en línea. Por otro lado, la seguridad de la información también abarca aspectos orales y escritos. Sin embargo, cuando nos referimos a ciberseguridad, nos concentramos principalmente en proteger la información en formato digital y los sistemas interconectados que la manejan. En términos generales, la seguridad de la información comprende políticas, esquemas de seguridad, directrices, métodos de gestión de riesgos, capacitación, concientización, buenas prácticas y técnicas utilizadas para proteger los recursos empresariales (Mario & Correa, 2018).

En el Manual de Tallin 2.0, producido por el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN en Tallin, Estonia, se proporciona un argumento clave sobre la importancia de la ciberseguridad en las organizaciones. Esta versión 2.0 del año 2017 se centra en el derecho internacional aplicable a las operaciones y seguridad cibernética en el ciberespacio. A diferencia del Convenio de Budapest, este manual no tiene fuerza legal obligatoria para los Estados, pero ofrece la doctrina consensuada por expertos líderes a nivel mundial. Su objetivo es avanzar en el desarrollo del derecho internacional en relación con las operaciones y seguridad cibernética, brindando orientación legal a los asesores legales de los Estados sobre diversos temas relevantes para la legislación en estas áreas dentro de sus propios países (Gálvez Reyes & Gálvez Pacheco, 2020). Lo citado, aborda el derecho internacional aplicable a las operaciones y seguridad cibernética. Aunque no tiene fuerza legal obligatoria, proporciona una guía consensuada por expertos a nivel mundial, lo que subraya la importancia de protegerse contra amenazas cibernéticas y de tener una comprensión sólida del marco legal en

este ámbito. Esto destaca la necesidad crucial para las organizaciones de estar preparadas y tener políticas de ciberseguridad sólidas para protegerse en el entorno digital actual.

En el ámbito peruano, varios argumentos resaltan la necesidad de la ciberseguridad en las organizaciones. Por ejemplo, se destaca que el Perú ha establecido el Sistema Nacional de Transformación Digital a inicios del año 2020 a través del Decreto de Urgencia Nº 006-2020, seguido por el Marco de Confianza Digital establecido por el Decreto de Urgencia Nº 007-2020. Este último tiene como objetivo incrementar la confianza de los ciudadanos cuando usan los servicios digitales puestos a disposición por entidades privadas y públicas. Estos aspectos subrayan la necesidad urgente de incluir la seguridad de la información y la ciberseguridad en una estrategia integral y visionaria en el país. Es crucial considerar la ciberseguridad enfocada en la protección de la infraestructura crítica, la prevención del ciberdelito y el fortalecimiento de la competencia en seguridad de la información como parte del día a día de las organizaciones (Pacheco Araoz, 2020). El descrito destaca la importancia de la ciberseguridad para las organizaciones en el contexto peruano, señalando la creación del Sistema Nacional de Transformación Digital y el Marco de Confianza Digital como ejemplos de iniciativas gubernamentales para fortalecer la seguridad digital. Esto subraya la necesidad urgente de incorporar medidas de ciberseguridad en las estrategias organizativas, con un enfoque en la protección de la infraestructura crítica y la prevención del ciberdelito. En resumen, resalta cómo la ciberseguridad es esencial para garantizar la confianza y la protección de los servicios digitales ofrecidos tanto por entidades públicas como privadas en el país.

En el ecosistema peruano, comprender la ciberseguridad y su función actual en las organizaciones para optimizar la seguridad digital, protección de datos e información implica primeramente entender lo que abarca un Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI proporciona la mirada fundamental para todas las áreas de ciberseguridad, seguridad digital y protección de datos e información en cualquier tipo de empresa a nivel global, entre ellas las entidades peruanas. Es importante tener en cuenta que todos

estos conceptos teóricos están estandarizados en los diversos documentos internacionales de la familia ISO 27000, que normalizan estos espacios de conocimiento a nivel mundial. Por consiguiente, se requiere que un SGSI incluya: políticas tanto generales como específicas, procedimientos del SGSI y salvaguardas o controles de ciberseguridad, protección de datos e información, aspectos que contribuyan con la gestión de la información, y esté dirigida para: asegurar la confidencialidad, integridad y disponibilidad de los datos e información de las entidades peruanas. Se destaca que la confidencialidad implica restringir el acceso a la información exclusivamente a los que correspondan estar autorizados, la integridad implica mantener la exactitud y la información completa, y la disponibilidad se refiere a asegurar el acceso a la información por parte de los usuarios autorizados cuando lo necesiten (Organización Internacional de Normalización, 2022). En este sentido, de lo referido la ciberseguridad es crucial para las organizaciones en Perú. Un SGSI proporciona un marco esencial para proteger los datos e información, cumpliendo con estándares internacionales de la familia ISO 27000. Orientando el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, lo que es vital para el éxito de las empresas en el mundo digital actual.

Dentro de este enfoque, el SGSI aborda de manera holística tanto a la organización como a los procesos que impactan su seguridad digital, ciberseguridad y protección de datos e información. Su objetivo primordial es comprender, gestionar y reducir al mínimo los posibles riesgos que puedan amenazar la seguridad de la información desde una perspectiva global, lo que otorga confianza a las organizaciones de que se cumplirán los requisitos de seguridad (Organización Internacional de Normalización, 2018).
El SGSI aborda la seguridad digital y la protección de datos de manera integral, orientándose a que las organizaciones cumplan con implementar controles, con la finalidad de proteger sus activos de información y buscando garantizar el correcto funcionamiento empresarial.

Es importante considerar que la información es un recurso valioso para las empresas, ya que es esencial para todos sus procesos y decisiones,

lo que afecta su funcionamiento y rentabilidad. Por lo tanto, garantizar la integridad, confidencialidad y disponibilidad de la información es crucial. La seguridad digital, ciberseguridad y protección de datos implican salvaguardar los activos de información más significativos de las entidades. Es relevante tener en cuenta que cada día enfrentamos riesgos que amenazan la integridad, confidencialidad y disponibilidad de la información, y estos riesgos pueden originarse tanto fuera como dentro de las organizaciones (Organización Internacional de Normalización, 2017). De lo anterior, se rescata que la ciberseguridad es esencial para garantizar la protección de los recursos digitales de una organización y su funcionamiento continuo en un entorno con amenazas nuevas siempre presentes.

Para salvaguardar a las empresas de las constantes amenazas presentes en los entornos globales, es esencial considerar estas amenazas en primer lugar. Luego, se debe abordarlas de la manera más óptima y eficiente posible. En consecuencia, las organizaciones deben establecer protocolos y aplicar medidas integrales de seguridad de la información y ciberseguridad, las cuales deben estar respaldadas por una evaluación exhaustiva de los riesgos de seguridad de la información y ciberseguridad, cómo también de una evaluación continua de su eficacia (Organización Internacional de Normalización, 2022). Se resalta la importancia de la ciberseguridad en las organizaciones, subrayando la necesidad de implementar medidas integrales de protección y evaluar constantemente estas medidas implementadas para hacer frente a las amenazas digitales en constante evolución y para garantizar la continuidad de las operaciones empresariales.

Por lo descrito previamente, se evidencia que la vital importancia de la ciberseguridad para las organizaciones se comprende desde diversas perspectivas. Así mismo, es relevante señalar que los estándares internacionales aludidos previamente son válidos en el Estado Peruano y, por ende, pueden ser usados por las entidades peruanas, como se demuestra a través de la existencia de una Norma Técnica Peruana equivalente a los principales estándares de la ISO. Estos documentos se presentan y comentan

en el rubro estándares de ciberseguridad y su importancia en las organizaciones.

1.3.2. Relevancia de la ciberseguridad en las Ciencias de la Información

Para comenzar, es crucial reconocer que, en la actualidad, la sociedad peruana está inmersa en la era de la información y del conocimiento. Esto implica que estamos viviendo en un período caracterizado por un continuo avance tecnológico y una rápida transformación digital. En este contexto, el Perú se encuentra inmerso en una dinámica de cambio constante, impulsada tanto por el desarrollo tecnológico como por la implementación de políticas de gobierno digital. En este escenario de evolución tecnológica, las temáticas de seguridad de la información, ciberseguridad y Ciencias de la Información adquieren una relevancia sin precedentes. La protección de datos, la seguridad de la información y la gestión de riesgos cibernéticos se convierten en elementos fundamentales para conseguir la integridad, confidencialidad y disponibilidad de los datos e información y de los sistemas de información en un ambiente digital en constante cambio. Por lo tanto, es imprescindible que los próximos profesionales de las Ciencias de la Información adquieran competencias en estas áreas para hacer frente a los desafíos y amenazas emergentes en el ámbito de la seguridad cibernética.

En concordancia con lo expuesto anteriormente, adquirir nuevas competencias tiene un rol general en la sociedad del conocimiento, dado que, en su conjunto, las competencias están interconectadas. Es decir, los elementos de una habilidad clave respaldan otras competencias, desde las esenciales como la capacidad lingüística, la comprensión lectora, la escritura fluida, las matemáticas y el cálculo, hasta los aspectos tecnológicos que sustentan diversas plataformas de información y comunicación, proporcionando así el respaldo necesario para el continuo proceso de aprendizaje en el que están inmersos los estudiantes. Sin embargo, estas competencias se sustentan en la habilidad de aprender de manera continua y constante. Entender primero el rol de las habilidades esenciales en el

aprendizaje perene en la sociedad admite apreciar su importancia en el desarrollo de estas capacidades en los alumnos de manera complementaria. Además, aspectos como la innovación, la creación de servicios avanzados y la adopción de nuevas formas de trabajo y procesos, junto con la generación de nuevos modelos empresariales y enfoques de vida, son elementos relevantes para el año 2030. Estas habilidades emergentes se basan en la creatividad, la adaptación, la curiosidad y una mentalidad abierta, según indica la OECD (2018). Adquirir competencias en general y también de ciberseguridad es esencial en la sociedad del conocimiento, donde las habilidades están interconectadas y respaldan el aprendizaje continuo. Estas competencias, basadas en la creatividad y la adaptación, son cruciales para enfrentar los desafíos de seguridad de la información en un mundo cada vez más digitalizado.

En relación a las habilidades requeridas en las competencias digitales, estas abarcan la capacidad de buscar, recopilar o adquirir información, así como de analizarla de manera crítica considerando los riesgos asociados a la seguridad digital y la protección de datos. Es crucial que los estudiantes sean capaces de utilizar diversas tecnologías que respalden la comunicación e intercambio de información, además de tener la habilidad de crear, presentar y comprender información compleja. Todo esto les permitirá tener acceso y poder emplear estos servicios digitales usando Internet y las nuevas tecnologías de información de manera efectiva (Comisión Europea, 2007). Se explica la importancia de las competencias digitales, considerando la seguridad digital y la protección de datos, las cuales son importantes para el uso de las tecnologías de información y comunicación. En el ámbito empresarial, la ciberseguridad se vuelve esencial para proteger los datos e información de la organización.

Para fomentar la adquisición de estos aspectos por parte de los estudiantes, es esencial dirigir la educación hacia el desarrollo de nuevas competencias. Por lo tanto, es importante aclarar que, según la Comisión Europea, las competencias no se limitan a un único tipo de conocimiento, habilidad o actitud, sino que abarcan una combinación de estos aspectos, adaptados a un ambiente particular. Estas competencias, conocidas como

esenciales, son indispensables tanto para la sociedad como para los individuos, ya que les proporcionan los medios necesarios para su construcción personal, desarrollo, integración en la sociedad y progreso global, así como para implicarse activamente en la vida ciudadana, lo que facilita su inclusión social y acceso al empleo (Comisión Europea, 2007). Es crucial reconocer que, junto con las competencias esenciales mencionadas, el desarrollo de habilidades en ciberseguridad es cada vez más trascendente para los futuros profesionales en Ciencias de la Información. En un mundo donde la información y los sistemas digitales son imprescindibles, la capacidad para protegerlos contra amenazas cibernéticas se convierte en un componente indispensable de su formación académica. Por lo tanto, el énfasis en el desarrollo de competencias en ciberseguridad es fundamental para preparar a los futuros profesionales de las Ciencias de la Información para enfrentar con éxito los retos del mundo digital en constante evolución.

El Marco de Competencias Digitales para la Ciudadanía (DigComp 2.2) abarca una amplia gama de competencias digitales que se extienden por diversos campos, como ciencia, ingeniería y matemáticas, tecnología, alfabetización, lenguaje, conciencia cultural, expresión, habilidades civiles, emprendimiento, temas sociales y de aprendizaje. La competencia digital general se desglosa en cinco áreas principales: búsqueda y gestión de información y datos; comunicación y colaboración; creación de contenido en entornos digitales; seguridad digital y protección de datos; y resolución de problemas (Vuorikari, 2022). El desarrollo de competencias de ciberseguridad es fundamental para los futuros profesionales de Ciencias de la Información, ya que les permite abordar los desafíos emergentes en un entorno digital cada vez más complejo. Es crucial que estos profesionales adquieran habilidades en seguridad digital, protección de datos e información, especialmente en áreas como búsqueda y gestión de información, comunicación y colaboración, así como creación de contenido en entornos digitales. Esto les permitirá enfrentar de manera efectiva los riesgos y amenazas cibernéticas, protegiendo la integridad de la información y contribuyendo al desarrollo seguro de la sociedad digital.

En relación con la preeminencia de las competencias digitales en seguridad del DigComp 2.2 en el ámbito de los ciudadanos digitales y la protección de sus datos e información en el Perú, se destaca la necesidad de cultivar estas habilidades digitales. Esto se debe a su potencial contribución en diversos aspectos de la ciberseguridad y la protección de datos requeridos por el Estado peruano, particularmente en el contexto de la digitalización y la implementación del gobierno digital. En estas circunstancias, se están llevando a cabo diversas actividades relacionadas con la seguridad de los datos y ciberseguridad, particularmente en la implementación de los Sistemas de Gestión de Seguridad de la Información (SGSI) conforme a estándares internacionales basadas en la línea de la ISO 27000 y las demás ISO que las conforman, tanto en organizaciones privadas como en entidades públicas del Estado peruano. Para llevar a cabo la implementación de los SGSI, se requieren aptitudes digitales de ciberseguridad, especialmente durante la evaluación de riesgos de seguridad de la información y de ciberseguridad, que implica la identificación de amenazas, el análisis de amenazas y la identificación de las vulnerabilidades a los activos de información. Además, luego de estudiar las principales normativas legales del Estado peruano, se concluye que es esencial que los estudiantes adquieran y estudien competencias digitales de seguridad desde etapas tempranas de su educación para formar ciudadanos digitales competentes en una extensa variedad de asuntos vinculados con la seguridad en línea digital y contribuir así a la protección de datos y la seguridad de la información en el país (Bermúdez Torres, 2022). La importancia de desarrollar competencias de ciberseguridad en los futuros profesionales de Ciencias de la Información radica en su capacidad para enfrentar los desafíos de seguridad digital que se presentan en la era actual. Al adquirir estas habilidades los estudiantes no solo estarán mejor preparados para proteger la información, sino que también contribuirán a fortalecer la infraestructura digital y a salvaguardar la integridad de los sistemas de información en la sociedad en general.

El National Institute of Standards and Technology (NIST) describe que el propósito de adquirir competencias en seguridad digital y ciberseguridad es desarrollar habilidades que capaciten a las personas para llevar a cabo tareas

concretas. Estas habilidades se adquieren mediante la aplicación de aspectos teóricos, y mejores prácticas de seguridad digital y ciberseguridad (NIST, 2015). La ciberseguridad es fundamental para las Ciencias de la Información, ya que permite desarrollar habilidades específicas para llevar a cabo tareas concretas y proteger la información mediante la aplicación de conceptos y buenas prácticas de ciberseguridad, en un contexto cada vez más digitalizado y expuesto a riesgos cibernéticos.

Además de lo indicado previamente, el National Institute of Standards and Technology ha lanzado la más reciente edición del bien conocido Marco de Ciberseguridad “NIST CSF”. Esta versión 2.0 fue desarrollada con el propósito de asistir a organizaciones de todas las dimensiones y ámbitos, incluyendo industrias, entidades gubernamentales, centros académicos y entidades sin fines de lucro, en la gestión y reducción de sus riesgos relacionados con la ciberseguridad. Esta actualización, caracterizada por una estructura más sucinta que abarca 6 funciones, 22 categorías y 106 subcategorías, denota una evolución hacia un enfoque más amplio en la administración de riesgos y la gobernanza de la ciberseguridad. En resumen, el CSF 2.0 emerge como una herramienta indispensable para aquellas entidades que buscan reforzar su posición en materia de ciberseguridad y adaptarse eficientemente a un entorno digital en continua transformación (NIST, 2024). El lanzamiento reciente del citado Marco de Ciberseguridad marca un hito importante en la gestión de riesgos, ofreciendo una guía esencial para organizaciones de todas las dimensiones y sectores. Esta versión actualizada, con una estructura más concisa pero ampliada, refleja la creciente relevancia de la ciberseguridad en un entorno digital dinámico, por lo que es fundamental que los futuros profesionales de Ciencias de la Información comprendan y estudien esta temática, ya que la protección de la información se vuelve cada vez más crítica en nuestra sociedad digital. Con el aumento de estas nuevas amenazas la capacitación en este campo no solo ofrece oportunidades laborales amplias y variadas, sino que también permite contribuir activamente a la seguridad y estabilidad de las organizaciones en un mundo interconectado y en constante evolución.

Por otro lado, a pesar de la importancia de la capacitación en ciberseguridad apoyada en competencias para ciudadanos no relacionados con las tecnologías de la información y la comunicación (TIC), su nivel de madurez es considerablemente bajo. Aunque existe una amplia gama de investigaciones en este espacio para el personal TIC, el uso de marcos de competencias asociados a roles laborales para el personal no TIC, actualmente no está muy desarrollado (Mendivil Caldentey, Sanz Urquijo, & Gutierrez Almazor, 2022). La falta de capacitación en ciberseguridad para el personal no especializado en tecnologías de la información y la comunicación (TIC) crea una oportunidad valiosa para que los próximos profesionales de Ciencias de la Información se capaciten en este campo. Esta capacitación contribuiría significativamente a fortalecer la protección de la información y a mitigar los riesgos cibernéticos en diversos entornos laborales.

Por último, la visión prospectiva de la seguridad de la información y ciberseguridad para la próxima década deberá integrar elementos como la flexibilidad cognitiva, la gestión estratégica de la incertidumbre y la desinformación, la adaptación a una cultura caracterizada por la discontinuidad y la desconexión, así como las tensiones geopolíticas entre las naciones. Asimismo, se considerará la omnipresencia de los dispositivos inteligentes. Igualmente, se deberá abordar el desafío del uso indebido e ilegal de tecnologías emergentes como los libros contables distribuidos y las herramientas de inteligencia y monitorización sin autorización (Cano, 2020).

La importancia del conocimiento en seguridad de datos e información y ciberseguridad para los futuros profesionales de Ciencias de la Información radica en diversos factores cruciales en el contexto actual y futuro de la sociedad digital. En primer lugar, la rápida evolución tecnológica implica la constante aparición de nuevas amenazas y vulnerabilidades que pueden comprometer la integridad, confidencialidad y disponibilidad de la información. Por lo tanto, es imperativo que los profesionales de Ciencias de la Información estén al tanto de esta temática para poder anticipar y mitigar posibles riesgos.

Además, en un entorno cada vez más interrelacionado, donde la información fluye a través de redes globales, la seguridad de la información y ciberseguridad se convierte en un aspecto crucial para garantizar la integridad, confidencialidad y disponibilidad de los sistemas de información. Los profesionales de Ciencias de la Información deben comprender los conceptos fundamentales de estos temas para su adecuado desempeño laboral.

La responsabilidad ética también juega un papel fundamental en el ámbito de la seguridad de los datos e información y ciberseguridad. Los profesionales de Ciencias de la Información tienen la responsabilidad de proteger la privacidad y los derechos de los usuarios, así como de garantizar la confidencialidad de la información sensible. Esto implica no solo el cumplimiento de las regulaciones y normativas de seguridad, sino también la adopción de prácticas y políticas éticas que promuevan la transparencia y la confianza en el manejo de la información.

En resumen, el desarrollo de competencias en seguridad de los datos e información y ciberseguridad es esencial para los profesionales de Ciencias de la Información no solo para adaptarse a los rápidos cambios tecnológicos, sino también para proteger datos y sistemas, y cumplir con su responsabilidad ética de preservar la privacidad y seguridad en un entorno digital en constante evolución. Así mismo, la relación entre las Ciencias de la Información y la Ciberseguridad es importante en el entorno actual, en primera instancia las Ciencias de la Información se ocupan del estudio y la gestión de la información en sus diversas formas, incluyendo su creación, procesamiento, almacenamiento, recuperación y uso. Por otro lado, la Ciberseguridad se centra en proteger la información y los sistemas de información en el entorno digital, abordando amenazas como el acceso no autorizado, el robo de datos, la interrupción del servicio y el sabotaje de sistemas. Ambos campos están estrechamente interconectados debido a la creciente dependencia de la tecnología de la información y las comunicaciones en todas las áreas de la sociedad. La información se transmite y almacena principalmente en entornos digitales, lo que aumenta la vulnerabilidad a diversas amenazas. Por lo tanto, las Ciencias de la Información y la ciberseguridad pueden colaborar

profundamente para desarrollar estrategias y herramientas que protejan la integridad, confidencialidad y disponibilidad de la información en el mundo digital.

1.3.3. Estándares de ciberseguridad y su importancia en las organizaciones

El Comité N° 21 "Codificación e Intercambio Electrónico de Datos" del Instituto Nacional de Calidad (INACAL) de Perú, basándose en normas globales de la Organización Internacional de Estandarización (ISO), revisó, analizó, adoptó y aprobó diversas Normas Técnicas Peruanas que son aplicadas por las entidades públicas y empresas privadas como parte de su camino a la transformación digital y gobierno electrónico. Las siguientes normas son las principales relacionadas con la seguridad de la información, ciberseguridad y gestión de riesgos de estas temáticas, así como, respecto a la implementación de un SGSI. Cabe precisar que el suscrito participó como miembro experto de dicho comité en la elaboración de todas las Normas Técnicas Peruanas señaladas a continuación:

En primer lugar, se discutirá la Norma Técnica Peruana NTP-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos, en su tercera edición del 29 de diciembre de 2022, que corresponde a la ISO/IEC 27001:2022. Este estándar es el pilar central de la familia ISO/IEC 27000 y establece los requisitos esenciales para implementar y gestionar un SGSI. En su Anexo A, proporciona una relación de objetivos de control y una lista de controles de seguridad de la información y ciberseguridad que corresponden ser aplicados (Norma Técnica Peruana, 2022).

Fundamentalmente aborda las consideraciones esenciales y requisitos necesarios para que cualquier empresa o institución, independientemente de su tamaño o ubicación geográfica, pueda implementar con éxito su SGSI. Dichos requisitos se toman como referencia las principales prácticas internacionales en materia de seguridad de la información y ciberseguridad. Los

requisitos más destacados son: comprender la empresa y su ecosistema lo cual implica alinear los objetivos de seguridad de la información y ciberseguridad con la estrategia holística de la organización considerando su entorno; requisitos relacionados al liderazgo también son importantes y se refiere al compromiso incesante de los líderes de la empresa con la implementación del citado sistema de gestión y el fomento de una cultura de integral de seguridad y riesgos; también tenemos la gestión de riesgos de seguridad de la información, ciberseguridad y protección de la privacidad, que incluye la identificación de activos de información, de sus vulnerabilidades y amenazas, así como, la evaluación de riesgos de los referidos activos de información (identificación, análisis y valoración del riesgo) y el plan de tratamiento de riesgos (el cual incluirá la estrategia de tratamiento de riesgos y los controles aplicables del total de controles del Anexo A); por último, en cuanto a las supervisiones continuas del funcionamiento del SGSI, se citan requisitos relacionados con auditorías internas y revisiones por parte de la dirección.

Lo manifestado en los párrafos precedentes, muestra que es importante que las organizaciones implementen un SGSI ya que les proporciona un marco estructurado para gestionar y resguardar la información, garantizando la confidencialidad, integridad y disponibilidad de sus datos. Además, el SGSI ayuda a mitigar riesgos y amenazas, promoviendo la ciberseguridad. Así mismo, al establecer procesos y controles de ciberseguridad y seguridad de la información, el SGSI fortalece la resistencia de la organización ante incidentes de seguridad, contribuyendo a mantener la confianza de clientes, socios y partes interesadas. En un contexto mundial donde la información es un activo crítico, la implementación de un SGSI es esencial para garantizar la continuidad de las operaciones de las organizaciones y preservar su reputación en un entorno digital muy cambiante, lo señalado anteriormente se enmarca en lo establecido por la NTP-ISO/IEC 27001:2022 e ISO/IEC 27001:2022.

Así mismo, la Norma Técnica Peruana NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información, en su segunda edición del 29 de

diciembre de 2022, equiparable a la ISO/IEC 27002:2022, funciona como una pauta de mejores experiencias que ofrece recomendaciones para la cumplir con los objetivos, directrices y los controles de ciberseguridad y seguridad de la información detallados en el Anexo A de la NTP-ISO/IEC 27001:2022 (Norma Técnica Peruana, 2022).

En el año 2022, fue publicada la mencionada norma siendo esta su versión más actualizada, la cual abarca un total de 93 controles, distribuidos en 4 clausulados, que se dividen en 37 para aspectos organizativos, 8 relacionados con el factor humano, 14 para temas físicos y 34 tecnológicos. Estas directrices abarcan una amplia variedad de áreas temáticas, que comprenden aspectos como gobernanza de la seguridad de la información, gestión o administración de activos, salvaguarda de datos e información, seguridad física, protección de redes y sistemas, seguridad de aplicaciones, configuraciones seguras, gestión de identidades, gestión de accesos, gestión de vulnerabilidades y amenazas, continuidad operativa del negocio, interrelaciones con proveedores seguras, cumplimiento normativo, gestión de eventos de seguridad de la información y aseguramiento de la información, con un enfoque especial en aspectos relacionados con la ciberseguridad. La lista de contenidos señalados provee evidencias que su implementación en las organizaciones a nivel mundial es esencial debido a su papel fundamental en fortalecer la ciberseguridad y la seguridad de la información. Estos controles ofrecen un marco integral que aborda aspectos clave de la ciberseguridad, la gestión de riesgos y protección de datos. Al seguir los lineamientos de la NTP-ISO/IEC 27002:2022 e ISO/IEC 27002:2022 las organizaciones pueden establecer medidas efectivas para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Además, la adopción de estos controles ayuda a cumplir con requisitos normativos, mejora la resiliencia ante amenazas, promueve prácticas de seguridad consistentes y contribuye a la construcción de la confianza tanto interna como externamente.

Del mismo modo, con fecha 18 de diciembre del 2019 tenemos la Norma Técnica Peruana NTP-ISO/IEC 27003:2019. Tecnología de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la

Información. Orientación, la cual tiene como estándar internacional equivalente la ISO/IEC 27003:2017, proporcionando orientaciones complementarias referidas a los requisitos establecidos en un SGSI, establecidas en la NTP-ISO/IEC 27001:2014 (Norma Técnica Peruana, 2019).

Lo anterior detalla los requisitos y exigencias para la implementación y gestión de un SGSI, ofreciendo pautas sobre cómo precisar el alcance y lograr el consentimiento del SGSI, así mismo establece directrices sobre las demarcaciones o límites y las políticas del sistema. Un punto importante señalado en esta norma es la inclusión de la evaluación y el plan de tratamiento de riesgos de forma exhaustiva durante la implementación de un SGSI. Estas disposiciones, tanto de la NTP-ISO/IEC 27003:2019 como de la ISO/IEC 27003:2017, enfatizan la importancia de los controles de seguridad de la información y ciberseguridad para proteger la información de las organizaciones y brindar la continuidad de sus operaciones.

Respecto a la Norma Técnica Peruana NTP-ISO/IEC 27004:2018. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación, 2° Edición, de fecha 28 de diciembre del 2018, cuya norma tomada como referencia es la ISO/IEC 27004:2016, el referido estándar suministra orientación sobre el seguimiento, medición, análisis y evaluación, en relación a la implementación de un SGSI, de acuerdo a lo establecido por la NTP-ISO/IEC 27001:2014 (Norma Técnica Peruana, 2018).

En cuanto al párrafo anterior, esta ISO proporciona directrices para el seguimiento, medición, análisis y evaluación de un SGSI. Es útil a las organizaciones porque les ayuda a establecer procesos eficientes para evaluar la efectividad de sus controles de ciberseguridad y seguridad de la información, también para identificar áreas de mejora y realizar un seguimiento continuo de su desempeño en términos de confidencialidad, integridad y disponibilidad de los datos e información de las organizaciones, lo señalado anteriormente se enmarca en los requisitos de la NTP-ISO/IEC 27004:2018 e ISO/IEC 27004:2014.

Al examinar las regulaciones previas, se resalta la importancia fundamental del proceso de gestión de riesgos de seguridad de la información y de ciberseguridad durante la implementación de un SGSI. En este contexto, la Norma Técnica Peruana NTP-ISO/IEC 27005:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información, 3° Edición, desempeña un papel crucial. Emitida el 29 de diciembre de 2022 y equivalente a la ISO/IEC 27005:2022, esta norma proporciona directrices sobre la gestión de riesgos para facilitar el cumplimiento de los requisitos concretos establecidos en la NTP-ISO/IEC 27001:2022. Es importante destacar que la ISO mencionada permite la aplicación de diversos enfoques o metodologías en la gestión del riesgo (Norma Técnica Peruana, 2022).

Una primera observación relevante acerca de la NTP-ISO/IEC 27005:2022 es que se vincula y se ajusta a la Norma Técnica Peruana NTP-ISO/IEC 31000:2018. Gestión del riesgo. Directrices, de 27 de junio del 2018, equivalente a la ISO 31000:2018. Ofrece directrices y define términos clave, principios fundamentales y un marco detallado para la implementación efectiva del proceso de gestión del riesgo en las empresas. Destaca la importancia de la comunicación, consulta, monitoreo y revisión para garantizar la eficacia del sistema de gestión (Norma Técnica Peruana, 2018). La Norma Técnica Peruana NTP-ISO/IEC 27005:2022 se relaciona con la Norma Técnica Peruana NTP-ISO/IEC 31000:2018 al proporcionar directrices específicas para la gestión de riesgos de seguridad de la información y ciberseguridad, mientras que la segunda establece principios generales para la gestión de riesgos en cualquier ámbito organizacional. En conjunto, ambas normas permiten una gestión completa y coherente de los riesgos, abordando tanto los riesgos generales como los específicos de la seguridad de la información y ciberseguridad. Estos estándares abarcan desde establecer el contexto hasta realizar la evaluación del riesgo (identificar, analizar y valorar el riesgo), contemplando también el tratamiento, la comunicación y el seguimiento de los riesgos. En cuanto a la identificación y análisis de riesgos de seguridad de la información y ciberseguridad, se requiere identificar amenazas, vulnerabilidades y sus riesgos relacionados a los activos de información.

La ISO/IEC 27005:2022, identifica múltiples amenazas y vulnerabilidades, como: (a) Amenazas: compromiso de información, fallas técnicas, acciones no autorizadas y compromiso de funciones, entre otras; (b) Vulnerabilidades: en hardware y software, incluyendo problemas de mantenimiento, sensibilidad a factores externos, falta de control de configuración, problemas de seguridad en el software, y deficiencias en la gestión de contraseñas y acceso, etc.

Las amenazas y vulnerabilidades son relevantes para ser analizadas durante la gestión integral de riesgos de seguridad de la información y ciberseguridad, según lo establecido en la NTP-ISO/IEC 27005:2022 y en la ISO/IEC 27005:2022. Este análisis es parte esencial de la implementación de un SGSI en las organizaciones, de acuerdo a lo indicado en la ISO/IEC 27001:2022 y la NTP-ISO/IEC 27001:2022. Así mismo, se debe tener en cuenta lo indicado en los documentos siguientes: NTP-ISO/IEC 27001:2022, ISO/IEC 27001:2022, NTP-ISO/IEC 27002:2022, ISO/IEC 27002:2022, NTP-ISO/IEC 27003:2019 e ISO/IEC 27003:2017, así como la NTP-ISO/IEC 27004:2018 e ISO/IEC 27004:2014. Documentos que destacan la importancia crítica de implementar controles de seguridad de la información y ciberseguridad para proteger dispositivos digitales, datos personales, privacidad de datos y en general buscando la protección de los datos e información de las organizaciones de cualquier tipo a nivel mundial.

Otro estándar relevante es la Norma Técnica Peruana NTP-ISO/IEC 27007:2020. Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información, 3° Edición, que ofrece pautas y criterios para auditar un SGSI, fue emitida el 28 de diciembre de 2018 y es equivalente a la ISO/IEC 27007:2020 (Norma Técnica Peruana, 2020). Respecto a esta ISO desempeña un papel fundamental para las organizaciones al proporcionar directrices específicas para la auditoría de los SGSI, son útiles para evaluar la eficacia del cumplimiento de los requisitos y planteamientos de la NTP-ISO/IEC 27001:2022 e ISO/IEC 27001:2022, ayudando a identificar posibles debilidades en los controles de seguridad de la información y ciberseguridad

implementados en las organizaciones, sino que también contribuye al perfeccionamiento continuo de los procesos de gestión de la seguridad de la información y ciberseguridad, lo señalado anteriormente se enmarca en la NTP-ISO/IEC 27004:2018 e ISO/IEC 27004:2014.

Por otro lado, la Norma Técnica Peruana NTP-ISO/IEC 27036-1:2022. Ciberseguridad. Relaciones con Proveedores. Parte 1: Visión general y conceptos, 1° Edición, de 29 de diciembre del 2022, equivalente a la ISO/IEC 27036-1:2021, la cual aborda la seguridad de la información en el contexto de las relaciones con proveedores, que se especifican en la NTP-ISO/IEC 27036-1:2022 (Norma Técnica Peruana, 2022).

Finalmente, tenemos el Marco de Ciberseguridad NIST (CSF) 2.0, publicado el 26 de febrero de 2024, el cual proporciona orientación a una amplia gama de organizaciones, que incluyen industrias y entidades gubernamentales, para abordar los riesgos relacionados con la ciberseguridad. Respecto a los Perfiles y Niveles del CSF, se establece que los Perfiles describen la posición actual o futura de una organización en términos de los resultados fundamentales del Marco de Ciberseguridad NIST y se emplean para entender, adaptar, evaluar, priorizar y comunicar los resultados del referido marco, teniendo en cuenta los objetivos de la misión de la organización, las expectativas de las partes interesadas, el panorama de amenazas y los requisitos. Cada perfil organizativo incluye uno o ambos de los siguientes elementos: un perfil actual, que especifica los resultados del marco que una organización está logrando o intentando alcanzar en la actualidad, y describe cómo o en qué medida se están logrando; y un perfil deseado, que establece los resultados deseados que una organización ha seleccionado y priorizado para cumplir con sus objetivos de gestión de riesgos de ciberseguridad, considerando cambios anticipados en la postura de ciberseguridad, como nuevos requisitos, adopción de tecnologías y tendencias de inteligencia de amenazas (NIST, 2024). El Marco de Ciberseguridad NIST (CSF) es una herramienta esencial para las organizaciones, ya que proporciona orientación para abordar los riesgos cibernéticos. La importancia de la ciberseguridad radica en proteger los activos digitales de las organizaciones contra amenazas

y ataques, lo que garantiza su competitividad y éxito en un entorno empresarial cada vez más digitalizado.

Esta ISO es crucial para las organizaciones, ya que proporciona un marco reconocido para gestionar la seguridad de la información y ciberseguridad, en las relaciones con proveedores, permitiendo brindar conformidad con regulaciones referidas a proveedores, fortalecer la seguridad de la información a lo largo de la cadena de suministro, aumenta la confianza de los clientes y mejora la eficiencia operativa, lo señalado anteriormente se enmarca en los requisitos de la NTP-ISO/IEC 27036-1:2022 e ISO/IEC 27036-1:2021. Esta norma aborda específicamente la ciberseguridad y establece pautas para garantizar la seguridad de la información cuando se interactúa con proveedores externos.

1.3.4. Normas peruanas relacionadas con ciberseguridad

Se debe tener en cuenta, que el gobierno peruano está promoviendo activamente el avance de la transformación digital, la digitalización, el gobierno digital y la protección de la información a través de impulsar la implementación de los SGSI en las organizaciones. En este contexto, se han establecido diversas regulaciones relacionadas con la ciberseguridad, abarcando leyes, decretos legislativos, decretos supremos, decretos de urgencia y otros documentos. Estas normativas abordan de manera integral la importancia de garantizar la ciberseguridad, la seguridad digital, la protección de datos y la gestión de la información en las organizaciones. A continuación, se mencionan algunas de estas normativas relevantes.

En primer lugar, resulta relevante mencionar la Ley de Gobierno Digital, la cual fue aprobada mediante el Decreto Legislativo N° 1412 el 12 de setiembre de 2018 a través de la Presidencia del Consejo de Ministros (PCM). Un aspecto sobresaliente de esta legislación es la establecimiento del Marco de Seguridad Digital del Estado peruano, que abarca una serie de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares destinados a asegurar la confidencialidad, integridad y disponibilidad de los datos e

información en el entorno digital y dentro del marco de la ciberseguridad. Además, se hace hincapié en las diferencias esenciales entre seguridad digital o seguridad informática y seguridad de la información, detallando que la seguridad digital se enfoca únicamente en el ámbito informático en entornos digitales mientras que la seguridad de la información cubre la totalidad de la información en sus distintas formas (información física, oral y digital). Por otro lado, esta ley establece el Marco General del Gobierno Digital, el cual aborda aspectos como la gestión de la identidad digital, los servicios digitales, la arquitectura digital, la interoperabilidad, la seguridad digital y la seguridad de datos, elementos cruciales relacionados con la ciberseguridad en las empresas y organizaciones. Es relevante subrayar que esta ley instituye la obligación para las entidades públicas peruanas de implementar y gestionar un SGSI (PCM, 2018).

Otra normativa legal de relevancia es el Reglamento de la Ley de Gobierno Digital, que fue aprobado por la PCM el 18 de febrero de 2021 mediante el Decreto Supremo N° 029-2021-PCM. Este reglamento establece las directrices específicas para las actividades contempladas en la Ley de Gobierno Digital. Además, presenta el Modelo de Identidad Digital del Estado, el cual incluye aspectos como los atributos de identidad digital y las credenciales de autenticación. Es importante destacar que este modelo incorpora elementos de ciberseguridad orientados hacia el ciudadano digital y la protección de la información en las organizaciones en ambientes digitales. Específicamente en lo que respecta a la ciberseguridad, esta regulación define la seguridad digital como el grado de confianza que las organizaciones tienen en el entorno digital, resultado de la implementación de controles de seguridad de la información y ciberseguridad, tanto de manera proactiva como reactiva ante los riesgos que puedan afectar la seguridad de los datos e información de las organizaciones. Asimismo, el reglamento hace referencia al Marco de Seguridad Digital del Estado Peruano, el cual abarca, entre otros aspectos, modelos, políticas, roles, procesos y estándares destinados a proteger la confidencialidad, integridad y disponibilidad de los datos e información, contribuyendo así a la ciberseguridad de las organizaciones. Adicionalmente, señala que el Modelo de Seguridad Digital está integrado por responsables de

los diferentes ámbitos del Marco de Seguridad Digital, como el Centro Nacional de Seguridad Digital, las Redes de Confianza en Seguridad Digital, el Oficial de Seguridad Digital, entre otros actores relevantes (PCM, 2021).

Una tercera norma legal a considerar, es el Decreto de Urgencia N° 0006-2020, aprobado por la PCM el 8 de enero de 2020, el cual establece la creación del Sistema Nacional de Transformación Digital. Este sistema tiene como finalidad principal fomentar la transformación digital en las organizaciones en general tanto públicas como privadas, promoviendo buenas prácticas de ciberseguridad y alentando el uso de tecnologías y servicios digitales entre los ciudadanos. Además, el Sistema Nacional de Transformación Digital fomenta el uso de herramientas de ciberseguridad tanto en entidades públicas como en organizaciones del sector privado, con el fin de reforzar la confianza en el entorno digital. Por otro lado, busca robustecer la participación de la ciudadanía digital, apoyando la seguridad de la información, transparencia de la información, protección de datos personales, siempre bajo la perspectiva de la ética en la gestión de las organizaciones. En este sentido, la transformación digital requiere el fortalecimiento de competencias digitales así como el desarrollo de servicios digitales, seguridad digital y aspectos de ciberseguridad (PCM, 2020).

El Estado peruano complementa la normativa anterior con el Reglamento del Sistema Nacional de Transformación Digital, aprobado mediante el Decreto Supremo N° 157-2021-PCM el 24 de setiembre de 2021. Este documento detalla las regulaciones del Sistema Nacional de Transformación Digital, abarcando una amplia gama de temas que incluyen desde el gobierno digital, la conectividad digital, la educación digital, los servicios digitales, la confianza digital, la ciberseguridad, entre otros. Se destaca que las organizaciones pueden usar estándares sobre gestión de riesgos de seguridad de la información y ciberseguridad; y otras normas aplicables. Además, se indica que el SGSI, se adapta a los objetivos estratégicos y a cada organización en particular, consiste básicamente en políticas, procedimientos, actividades para proteger los activos de información, entre otros aspectos, donde la gestión de riesgos de seguridad de la

información y ciberseguridad juega un papel importante, y cuyo resultado deriva en la implementación de controles de seguridad con la finalidad de salvaguardar la información y los datos procesados, almacenados y compartidos de las empresas (PCM, 2021).

Otra regulación relevante en este estudio es el Decreto Supremo N° 050-2018-PCM, aprobado por la PCM el 14 de mayo de 2018. Este decreto define la seguridad digital en el Estado peruano como el estado o nivel de confianza o seguridad que los ciudadanos tienen en los entornos o ambientes digitales. Cabe resaltar, que este estado de confianza se obtiene como resultado de un proceso exhaustivo de gestión de riesgos, que incluye la evaluación de riesgos de seguridad de la información y ciberseguridad. Donde la evaluación de riesgos incluye la identificación, análisis y valoración de riesgos (PCM, 2018).

Por otra parte, el Decreto de Urgencia 007-2020, aprobado por la PCM el 8 de enero de 2020, instituye el marco para la confianza digital y prescribe lineamientos para fortalecerla. Su fin es brindar actividades que generen confianza en los ciudadanos al utilizar los servicios que funcionan en entornos digitales. En relación con el concepto de confianza digital, este juega un rol vital en la transformación digital contemplando temáticas como la protección de datos personales, la ética, la transparencia, la ciberseguridad, entre otros. Cabe mencionar, que la confianza digital resulta del nivel de seguridad logrado luego de que el ciudadano hizo uso de los servicios digitales. Por otro lado, el entorno o ambiente digital se define como el espacio donde las tecnologías de información y comunicación, y los servicios digitales funcionan e interactuan. Cabe precisar, que esta norma respecto al concepto de ciberseguridad señala que es la capacidad de los recursos tecnológicos de brindar un correcto trabajo de las redes informáticas, activos de informáticos y sistemas o aplicativos informáticos, para resguardarlos frente a amenazas y vulnerabilidades en el entorno o ambiente digital ya mencionado anteriormente (PCM, 2020).

También debemos considerar la Ley N° 3099, aprobada por la PCM el 09 de agosto de 2019, que aprueba la Ley de Ciberdefensa, así como su

Reglamento aprobado el 13 de febrero de 2024. Estas normativas, en relación a la definición de ciberdefensa, definen esta como la destreza militar del Estado peruano para enfrentar amenazas o ataques en el ciberespacio que puedan perturbar la seguridad de la nación. En este contexto, se requiere que tanto las entidades públicas como las organizaciones privadas implementen controles de ciberseguridad y seguridad de la información. Esto complementa las disposiciones normativas destinadas a preservar la seguridad nacional al ayudar a proteger los activos digitales y mejorar la resiliencia ante amenazas cibernéticas, beneficiando a las organizaciones y a los usuarios finales. Además, estas normativas subrayan la relevancia de incorporar cursos sobre seguridad digital, incluyendo el tema de ciberdefensa en las instituciones de educación superior universitaria (PCM, 2019-2024).

Adicionalmente, se dispone de la Resolución N° 003-2023-PCM/SGTD, aprobada el 6 de septiembre de 2023 por la PCM, que aprueba la Directiva Nº 001-2023-PCM/SGTD, detallando el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital para las entidades públicas. En esta disposición, se brinda el concepto de ciberseguridad como la habilidad o pericia tecnológica de asegurar el funcionamiento adecuado de las redes informáticas, activos de información y sistemas o aplicativos informáticos, protegiéndolos contra amenazas y vulnerabilidades en el entorno o ambiente digital. Así mismo, se define el SGSI como la agrupación de políticas, lineamientos, procedimientos, recursos, entre otras actividades, que son gestionadas por una organización o entidad pública, con la finalidad de salvaguardar sus activos de información. La normativa también refiere que el SGSI abarca la gestión de riesgos e incidentes de seguridad de la información y ciberseguridad, así como la implementación de controles en beneficio de las organizaciones (PCM, 2023).

Igualmente, la referida Resolución N° 003-2023-PCM/SGTD, también aborda consideraciones sobre la implementación del SGSI en las entidades públicas. En este sentido, establece el uso de la Norma Técnica Peruana NTP ISO/IEC 27001 vigente, que a la fecha de redacción de la presente investigación corresponde la del 29 de diciembre de 2022, destacándose que el alcance del SGSI debe incluir los procesos misionales o esenciales y los

relevantes para la operatividad de la organización. En cuanto a los objetivos del SGSI, subraya la importancia de mantener la confidencialidad, integridad y disponibilidad de los datos e información. También diferencia entre seguridad de la información y seguridad digital, explicando de manera similar a como se explicó anteriormente, que la primera abarca cualquier tipo de información, independientemente de su formato, mientras que la segunda se centra en las medidas de seguridad aplicadas a la información en entornos digitales, ya sea en su procesamiento, transmisión, almacenamiento o contenido (PCM, 2023).

En relación con la Circular N° G-140-2009 aprobado el 2 de abril de 2009 por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS), se destaca que esta normativa enfatiza en que la seguridad de la información y ciberseguridad en las empresas se logra mediante la correcta implementación de políticas, procedimientos y una estructura organizacional adecuada, respaldada por herramientas informáticas especializadas con los controles de ciberseguridad correctos. El objetivo principal es garantizar que la información empresarial cumpla con los criterios fundamentales de confidencialidad, integridad y disponibilidad. Se aclara que, según esta norma, la confidencialidad implica que solo las personas autorizadas tengan acceso a la información, la integridad se refiere a que la información debe ser precisa y completa, mientras que la disponibilidad indica que la información debe estar accesible para los usuarios autorizados cuando sea necesario. Además, se establece que las empresas deben implementar, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI), que incluya como mínimo una política de seguridad de la información, una metodología para gestionar los riesgos de seguridad de la información y ciberseguridad, que se conserven los registros que permitan verificar el cumplimiento de las normas, estándares, políticas y procedimientos, y que la organización preserve las pistas de auditoría de sus sistemas o aplicativos informáticos (SBS, 2009).

La penúltima norma legal, revisada es el Circular N° G-167-2012 aprobado el 5 de noviembre de 2012 por la SBS, para la cual información se entiende como cualquier tipo de registro electrónico, óptico, magnético u otro

que pueda ser procesado, distribuido y almacenado en las organizaciones (SBS, 2012).

Por último, tenemos la Resolución S.B.S. Nº 504-2021 mediante la cual la SBS aprobó el 19 de febrero de 2021 el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, este documento respecto al concepto de ciberseguridad, refiere que debe entenderse como el resguardo de los activos de información de las organizaciones a través de la prevención, detección, respuesta y recuperación ante incidentes que afecten la disponibilidad, confidencialidad o integridad de dicha información en el ciberespacio; definiendo ciberespacio como un sistema complejo que no tiene existencia física, pero si interactúan personas, así como, dispositivos y sistemas informáticos, así mismo, en cuanto al término información se refiere a los datos de las organizaciones que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso o en otro formato. Un tema importante que contempla esta norma es sobre el Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C), definiéndolo como la agrupación de políticas, procesos, procedimientos, roles y responsabilidades, creados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación de la información ante incidentes de ciberseguridad que se presenten en las organizaciones, teniendo el SGSI-C como objetivos proteger la confidencialidad, es decir que la información esté disponible para entidades o procesos autorizados, la disponibilidad, para asegurar el acceso y uso en el momento requerido, y la integridad referida a evitar su modificación o destrucción no autorizada, un aspecto importante de esta norma dice que las organizaciones deben contar con un equipo multidisciplinario que gestionen los incidentes de ciberseguridad (SBS, 2021).

Finalmente, después de revisar detenidamente las principales regulaciones legales del Estado peruano relacionadas con la ciberseguridad, se hace evidente su vital importancia para las organizaciones. Las citadas normas resaltan la necesidad de gestionar la ciberseguridad, reconociéndola como un pilar esencial para preservar la confidencialidad, integridad y

disponibilidad de los datos e información en entornos o ambientes digitales. Estas regulaciones no solo abordan la gestión de la identidad digital y servicios digitales, sino que también enfocan la atención en la importancia de proteger activos de información y los activos tecnológicos, redes de comunicación y sistemas o aplicativos informáticos ante amenazas y vulnerabilidades en el ciberespacio, destacando la necesidad de implementar controles de ciberseguridad y de seguridad de la información en las organizaciones públicas y privadas. En conjunto, estas normas forman un marco integral que busca garantizar la confianza digital, proteger datos personales y fomentar prácticas éticas en el uso de tecnologías digitales en el ámbito peruano en el marco del proceso de transformación digital y del gobierno digital en el cual nos encontramos.

CAPÍTULO 2
EXPERIENCIA PROFESIONAL DE IMPLEMENTACIÓN DE ESTÁNDARES DE CIBERSEGURIDAD EN UNA ORGANIZACIÓN

En el siguiente capítulo, resguardando la confidencialidad y privacidad de los datos e información de la empresa y con la aprobación formal por escrito de su Gerencia General de LHH DBM Perú, se detalla mi experiencia de manera general como profesional de las Ciencias de la Información en la implementación de estándares de ciberseguridad, cabe precisar que la citada empresa se dedica a brindar soluciones integrales en procesos de reubicación profesional, desarrollo de liderazgo y capacitación. En el año 2023, se analizaron medidas o controles en relación a los "Requisitos de Protección de Datos para proveedores de Microsoft", lo cual condujo a la implementación de controles de seguridad de la información y ciberseguridad.

Mi participación en esta consultoría abarcó el desarrollo e implementación de documentos, la incorporación de aspectos técnicos de seguridad informática y la realización de capacitaciones en seguridad de la información y ciberseguridad, siguiendo las mejores prácticas establecidas en los estándares ISO de la familia ISO/IEC 27000, como la ISO/IEC 27001:2022, ISO/IEC-27002:2022, ISO/IEC 27003:2017, ISO/IEC 27004:2014, ISO/IEC 27005:2022, ISO/IEC 27036-1:2022, ISO/IEC 27007:2020, entre otros estándares. También se consideraron las normas peruanas, en el escenario actual que el Estado peruano se encuentra inmerso en la temática de transformación digital y gobierno digital. Cabe precisar que estos documentos fueron analizados y comentados en el capítulo precedente.

Se hizo énfasis en considerar las buenas prácticas más relevantes referidas a la protección de datos y la seguridad de la información y ciberseguridad en el entorno empresarial. Este capítulo aborda las actividades llevadas a cabo para cumplir con los cincuenta y dos (52) requisitos de Microsoft y fortalecer la postura de seguridad de la empresa.

2.1. Aspectos generales de la empresa.

En el dinámico panorama empresarial actual, caracterizado por cambios constantes tanto internos como externos, las empresas de todos los sectores se enfrentan a la necesidad de adaptarse rápidamente. Estos cambios pueden implicar la reubicación de personal que ya no encaja en la estructura organizativa o la redefinición de roles para empleados clave. Desde el año 1993, LHH DBM Perú se ha destacado por ofrecer soluciones integrales a gerentes, ejecutivos, profesionales y personal administrativo, entre otros. Su enfoque abarca desde la reubicación profesional hasta el desarrollo de liderazgo y la capacitación, brindando un apoyo crucial tanto a individuos como a organizaciones en este entorno de cambios continuos.

Busca acompañar integralmente a las empresas y profesionales en todo su proceso de cambio, a través de sus programas de renovación de competencias. Para lo cual, cuenta con programas que ayudan a los profesionales a lograr en forma efectiva y productiva a través de herramientas y recursos tecnológicos innovadores, que permitan una transición rápida y productiva, estos programas incluyen mejorar las competencias para mejorar su carrera profesional, buscando que sea exitosa en el futuro.

En resumen, algunas de sus actividades principales son las siguientes:

- Ayudar a desarrollar mejores carreras profesionales, mejores líderes y mejores organizaciones en este entorno cambiante.
- Diagnosticar la situación actual de las empresas y proponer soluciones integrales, proponiendo estrategias de talento que estén alineadas con las estrategias corporativas.

2.2. Requisitos de Protección de Datos para proveedores de Microsoft.

Los “Requisitos de Protección de Datos para proveedores de Microsoft”, son requisitos que Microsoft demanda a sus proveedores cuando estén involucrados en el tratamiento de datos personales o datos confidenciales

de Microsoft en relación con la actividad de dicho proveedor en el marco de los términos de su contrato con Microsoft, este documento en su versión 9 del mes octubre de 2023, cuenta con cincuenta y dos (52) requisitos, describiendo por cada requisito su prueba de cumplimiento, los mismos que se detallan integralmente en el Anexo B de este documento.

Para cumplir LHH DBM Perú con los requisitos señalados por Microsoft para ser su proveedor de diversos servicios, requirió en el año 2023 implementar controles de seguridad de la información y ciberseguridad, sobre los referidos requisitos, es en este contexto que tuve la oportunidad de participar como parte de una consultoría que me permitió desarrollar y proponer diversas políticas, planes, programas y procedimientos de seguridad de la información y ciberseguridad los cuales fueron implementados y aprobados en esta empresa, también se logró implementar aspectos técnicos de ciberseguridad y por último capacitar y sensibilizar en temas de seguridad de la información y ciberseguridad.

2.3. Actividades desarrolladas.

A continuación, se describen de manera general, resguardando la confidencialidad y privacidad de los datos e información de la empresa, las actividades realizadas como parte de mi experiencia como profesional de las Ciencias de la Información en el año 2023, para elaborar e implementar los controles de seguridad de la información y ciberseguridad, sobre los cincuenta y dos (52) "Requisitos de Protección de Datos para Proveedores de Microsoft" que fueron implementados por la referida organización.

Las actividades que se desarrollaron fueron de tres (3) tipos, el primer grupo tienen que ver con: “El desarrollo e implementación de documentos de ciberseguridad”, el segundo grupo está relacionado a: “La implementación de aspectos técnicos de ciberseguridad”, mientras que el tercer tema se refiere a: “Capacitación y sensibilización en temas de seguridad de la información y ciberseguridad” actividades que se explican a continuación:

a) Desarrollo e implementación de documentos de ciberseguridad.

Durante el proceso de consultoría, para el desarrollo e implementación de los documentos de ciberseguridad se realizaron las siguientes actividades:

- ✓ **Levantamiento de Información.**

  Se realizó un análisis del ecosistema de ciberseguridad, de la infraestructura de seguridad informática existente, de los procesos internos de la empresa, de los sistemas informáticos utilizados y de la documentación referida a ciberseguridad con la que cuenta la empresa, a fin de identificar las brechas de los controles de seguridad de la información y ciberseguridad con que cuenta la empresa frente a los cincuenta y dos (52) requisitos establecidos por Microsoft.

- ✓ **Entrevistas y reuniones.**

  Se llevaron a cabo entrevistas y reuniones con personal de la organización, las cuales proporcionaron una comprensión de la situación actual de la empresa, sus necesidades específicas y sus desafíos en el contexto de la seguridad de la información y ciberseguridad.

- ✓ **Mapeo de los "Requisitos de Protección de Datos para proveedores de Microsoft".**

  Se realizó un mapeo de los cincuenta y dos (52) requisitos establecidos por Microsoft, a fin de garantizar que cada uno de ellos fuera abordado con los controles o salvaguardas de seguridad de la información y ciberseguridad necesarios. Este proceso permitió asegurar la conformidad y aprobación de la empresa con las brechas existente y con el cumplimiento de los requisitos de Microsoft.

- ✓ **Análisis de los estándares ISO vigentes referidos a ciberseguridad.**

  Se analizaron prioritariamente los tres (3) estándares siguientes en sus últimas versiones del año 2022.

  - ISO/IEC 27001:2022, “Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos”.
  - ISO/IEC 27002:2022, “Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información”.
  - ISO/IEC 27005:2022, “Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información”.

  También se consideró, complementariamente a lo anterior las buenas prácticas de las ISO siguientes: ISO/IEC 27003:2017, ISO/IEC 27004:2014, ISO/IEC 27036-1:2022 e ISO/IEC 27007:2020; y los aspectos más relevantes de las normas peruanas en el escenario actual que el Estado peruano se encuentra inmerso en la temática de transformación digital y gobierno digital.

  Lo cual permitió incorporar las últimas actualizaciones y mejores prácticas en el marco de ciberseguridad para los controles de seguridad de la información y ciberseguridad necesarios para cumplir con los cincuenta y dos (52) requisitos establecidos por Microsoft.

- ✓ **Elaboración de documentos de ciberseguridad.**

  Los documentos de ciberseguridad, incluyendo las políticas, planes y procedimientos, fueron elaborados tomando en cuenta las buenas prácticas establecidas principalmente en los tres (3) estándares ISO: ISO/IEC 27001:2022, ISO/IEC 27002:2022 e ISO/IEC 27005:2022. También se consideró, complementariamente a lo anterior las buenas

prácticas de las ISO siguientes: ISO/IEC 27003:2017, ISO/IEC 27004:2014, ISO/IEC 27036-1:2022 e ISO/IEC 27007:2020.

Antes de la aprobación de estos documentos por parte de la empresa fueron revisados conjuntamente, realizándose los ajustes necesarios para garantizar su alineación con las necesidades operativas y estratégicas de la organización.

b) Implementación de aspectos técnicos de ciberseguridad.

Sobre este aspecto, se implementaron en la empresa medidas técnicas de ciberseguridad, a fin de cubrir conjuntamente con los documentos de ciberseguridad mencionados en el literal a) con el cumplimiento de los "Requisitos de Protección de Datos para Proveedores de Microsoft", cabe precisar, que durante la implementación de los aspectos técnicos se consideraron principalmente las mejores prácticas de los tres (3) estándares ISO siguientes: ISO/IEC 27001:2022, ISO/IEC 27002:2022 e ISO/IEC 27005:2022, así como las normas peruanas que correspondan. Los aspectos técnicos implementados abarcaron los temas siguientes:

1. Gestión de incidentes y cambios.- Incluyó la implementación de un Sistema ITSM (Information Technology Service Management), el cual comprendió un conjunto de buenas prácticas y procesos diseñados para gestionar la respuesta a incidentes y cambios en la organización.

2.- Sistema de inventario de activos.- Se enfocó en la implementación de un mecanismo centralizado para rastrear la ubicación y el estado de los dispositivos de cómputo, integrándolo con la gestión de cambios para mantener registros precisos y actualizados.

3.- Medidas específicas de seguridad técnica.- Se implementan políticas de contraseñas robustas y la encriptación de las laptops mediante BitLocker, lo cual es un proceso de seguridad que utiliza el software

de cifrado BitLocker, desarrollado por Microsoft, para proteger la información almacenada en las unidades de disco de las laptops.

c) Capacitación y sensibilización en temas de seguridad de la información y ciberseguridad.

Se realizaron capacitaciones virtuales en temas de seguridad de la información y ciberseguridad, con el objetivo de sensibilizar al personal de la empresa y fortalecer su postura de seguridad en la protección de la información sensible. Durante estas sesiones, se abordaron diversos temas fundamentales, como la concienciación sobre amenazas cibernéticas, prácticas seguras de navegación en internet, gestión de contraseñas robustas, identificación y prevención de ataques de phishing, seguridad en el manejo de datos personales y empresariales, así como el uso seguro de dispositivos móviles y redes Wi-Fi públicas.

Estas capacitaciones proporcionaron a los empleados las herramientas necesarias para adoptar medidas proactivas y mitigar los riesgos asociados a la seguridad informática en su entorno laboral y personal. Para el contenido de estas capacitaciones se consideró como referencia lo señalado en los estándares ISO ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27003:2017, ISO/IEC 27004:2014, ISO/IEC 27005:2022, ISO/IEC 27036-1:2022 e ISO/IEC 27007:2020.

Cabe precisar, que la implementación de estos controles de seguridad de la información y ciberseguridad contribuyó con él fortalecimiento de la seguridad de la información de la empresa, así como con el cumplimiento de los cincuenta y dos (52) "Requisitos de Protección de Datos para proveedores de Microsoft".

En este sentido, la implementación de controles de seguridad de la información y ciberseguridad en LHH DBM Perú, que permitió cumplir con los requisitos de protección de datos de Microsoft, se alinea con las teorías de los autores citados previamente. Rodríguez, Fernández y Fernández (2023) resaltan la importancia de tales controles para proteger los datos de riesgos comunes. De

manera similar, Rodríguez Baca y sus colegas (2020) destacan la influencia de un Sistema de Gestión de Seguridad de la Información en aspectos clave como la confidencialidad y disponibilidad de la información. Cano (2011) subraya la necesidad de acciones básicas en ciberseguridad para proteger activos de información crítica.

Además, la implementación de controles de seguridad de la información y ciberseguridad en LHH DBM Perú, se enmarca en las directrices de la Organización Internacional de Normalización, las cuales respaldan la implementación de medidas integrales de seguridad para el caso de Perú basadas en las Normas Técnicas Peruanas NTP-ISO/IEC 27001:2022, NTP-ISO/IEC 27002:2022, junto con otras normas técnicas peruanas complementarias, las cuales brindan una estructura y guía específica para fortalecer la seguridad de la información y ciberseguridad, en consonancia con los estándares internacionales, garantizando el cumplimiento de requisitos obligatorios y buenas prácticas en la organización.

CAPÍTULO 3
RESULTADOS OBTENIDOS

En este capítulo, como se indicó anteriormente resguardando la confidencialidad y privacidad de los datos e información de la empresa y con la aprobación formal por escrito de su Gerencia General de LHH DBM Perú, se resaltan los beneficios derivados de la implementación de controles de seguridad de la información y ciberseguridad en la empresa, en cumplimiento de los cincuenta y dos (52) "Requisitos de Protección de Datos para proveedores de Microsoft". Estos beneficios reflejan una visión completa de los logros alcanzados, abarcando desde el cumplimiento de estándares hasta la protección de datos sensibles, así como la instauración de una cultura organizacional orientada hacia la conciencia y responsabilidad en materia de seguridad de la información. Dichos resultados fueron posibles gracias a mi experiencia y conocimientos en seguridad de la información y ciberseguridad, así como a la aplicación de mis competencias como profesional en Ciencias de la Información. Estos logros no solo consolidan la posición de la empresa en términos de seguridad de la información y ciberseguridad, sino que también la posicionan como una organización confiable y comprometida con la protección de los datos personales y de la información en un entorno empresarial en constante evolución.

3.1. Documentos de ciberseguridad implementados.

A continuación, se indican a alto nivel y de manera genérica, las políticas, planes, programas y procedimientos de seguridad de ciberseguridad implementados y aprobados en la empresa en el año 2023, como resultado de la consultoría realizada.

Políticas.

- **Política de seguridad de la información.**

Es una declaración de compromiso con la gestión de la seguridad de la información de la empresa. La política, incluyendo los estándares,

procesos y procedimientos, y cualquier política relacionada serán los documentos que rigen para definir los requerimientos mínimos acerca de la gestión de la seguridad de la información. Esta, tiene como objetivo establecer las directrices y medidas para proteger la confidencialidad, integridad y disponibilidad de los datos e información utilizada en los procesos y otras actividades relacionadas.

- **Política de ciberseguridad.**

  Es una declaración de compromiso con la gestión del programa de ciberseguridad de la empresa. La política, incluyendo los estándares, procesos y procedimientos, y cualquier política relacionada serán los documentos que rigen para definir los requerimientos mínimos acerca de la ciberseguridad. Aprovecha el marco de seguridad cibernética de la industria, aborda los requisitos reglamentarios de acuerdo con la legislación vigente, y protege las funciones comerciales, la información de la empresa y los activos al aplicar un enfoque equilibrado de negocio versus riesgo.

- **Política de conservación de documentos.**

  Es una declaración de compromiso con el establecimiento de las pautas y procedimientos para la gestión adecuada de los documentos generados y recibidos por la empresa en el desarrollo de sus procesos. La política de conservación de documentos tiene como objetivo que la conservación adecuada de los documentos es esencial para garantizar el cumplimiento normativo, la protección de la privacidad y la confidencialidad de la información, y para mantener una eficiente operación interna.

- **Política de borrado seguro de información y gestión de soportes.**

  Es una declaración de compromiso que establece las directrices y prácticas necesarias para la eliminación segura y efectiva de información

almacenada en diversos medios y soportes. Esta política tiene como objetivo salvaguardar la privacidad y la confidencialidad de la información al establecer procedimientos para la eliminación de los datos.

- **Política de contraseñas seguras.**

  Es una declaración de compromiso que tiene el propósito de garantizar que en la empresa se utilice credenciales de acceso robustas y adecuadas, minimizando así el riesgo de brechas de seguridad y protegiendo la integridad, confidencialidad y disponibilidad de los datos, información y sistemas de información.

- **Política de protección de datos de terceros.**

  Es una declaración de compromiso que tiene el propósito de asegurar que los datos de terceros estén protegidos adecuadamente por la empresa, respetando la privacidad y los derechos de las personas, y cumpliendo con las normativas pertinentes.

- **Política de copias de seguridad.**

  Es una declaración de compromiso que tiene el propósito de realizar periódicamente copias de seguridad de datos e información, a fin de salvaguardar la integridad, accesibilidad y continuidad de los datos importantes de la empresa.

- **Política de dispositivos móviles.**

  Es una declaración de compromiso que tiene el propósito de garantizar el uso seguro y efectivo de los dispositivos móviles en la empresa, a fin de proteger la información empresarial.

Planes y Programas.

- **Plan de respuesta a incidentes de seguridad de la información.**

  Busca contar con actividades planificadas ante amenazas a la integridad, confidencialidad y disponibilidad de los activos empresariales, promoviendo una postura de comunicación transparente y un compromiso de mejora permanente.

- **Plan de gestión de derechos de acceso.**

  Orientado a asegurar la integridad, confidencialidad y disponibilidad de la información y sistemas informáticos de la empresa. Valorando la privacidad, seguridad y transparencia, se busca establecer controles robustos y consistentes que permitan a los usuarios acceder solo a los recursos que necesitan.

- **Plan de recuperación de desastres.**

  El propósito de este plan es asegurar la supervivencia y la capacidad de funcionamiento de la empresa en situaciones de interrupción o desastres que afecten dramáticamente el normal desarrollo de la organización.

- **Programa de prevención de pérdida de datos.**

  El propósito de este programa es contribuir con la integridad, confidencialidad y disponibilidad de la información de la empresa, buscando establecer políticas, procedimientos y soluciones técnicas para prevenir, detectar y responder a posibles pérdidas de datos, ya sean accidentales o maliciosas.

- **Programa de capacitación en materia de seguridad de la información y ciberseguridad.**

  El propósito de este programa es proporcionar a los participantes los conocimientos y habilidades necesarios para proteger la información y datos de la empresa contra amenazas cibernéticas, Incluye una variedad de temas, como los conceptos fundamentales de seguridad de la información, la identificación de amenazas y vulnerabilidades, uso seguro de contraseñas, reconocimiento de ataques de ingeniería social, la prevención de malware y el phishing, y la respuesta adecuada a incidentes de seguridad. La finalidad principal es fortalecer la postura de seguridad de la información de la empresa mediante la formación y sensibilización de su personal en relación con los riesgos y las mejores prácticas en el ámbito de la seguridad cibernética. Este programa se adapta a las necesidades concretas de la organización y proporciona a los participantes las herramientas necesarias para enfrentar de manera efectiva las amenazas emergentes en el entorno digital actual.

Procedimientos.

- **Procedimiento para validar los datos personales.**

  Tiene como objetivo garantizar la exactitud, integridad y confiabilidad de los datos personales en la empresa desde su recopilación hasta su actualización, protegiendo la privacidad y confianza de las personas implicadas.

- **Procedimiento de gestión de parches.**

  Tiene como objetivo proteger contra vulnerabilidades los sistemas informáticos, aplicaciones y dispositivos de la empresa.

- **Procedimiento para comunicar los resultados de la investigación de la respuesta a incidentes.**

  Tiene como objetivo garantizar una comunicación transparente, oportuna y efectiva de los resultados derivados de la investigación de respuestas a incidentes, permitiendo una acción informada y coordinada en toda la empresa.

- **Procedimiento para atender denuncias sobre datos personales.**

  Tiene como objetivo garantizar que las denuncias relacionadas con datos personales, la empresa las aborde de manera oportuna y transparente, y sean tratadas de manera confidencial, con integridad y brindando confianza a las partes involucradas.

- **Procedimiento de respuesta y recuperación.**

  Tiene como objetivo ofrecer una respuesta ante eventos perturbadores, está orientado a contribuir con la continuidad de operaciones y seguridad de la información y datos de la empresa.

- **Procedimiento de autenticación de la identidad antes de conceder acceso.**

  Tiene como objetivo contribuir con la integridad y confidencialidad de los datos personales y confidenciales de la empresa, al conceder acceso únicamente a personas autenticadas y autorizadas.

- **Procedimiento para cifrar datos personales y confidenciales en reposo.**

  Tiene como objetivo proporcionar una estructura coherente para cifrar y proteger los datos personales y confidenciales en reposo, se busca

minimizar los riesgos asociados con el acceso no autorizado o la exposición accidental de los datos personales y confidenciales.

3.2. Aspectos técnicos de ciberseguridad implementados.

Los siguientes son los aspectos técnicos de ciberseguridad implementados en la empresa durante el año 2023 como consecuencia de la consultoría realizada.

Gestión de incidentes y cambios.

- **Gestión de incidentes de seguridad y datos en ITSM.**

  Implica establecer buenas prácticas en un Sistema ITSM que permita manejar de manera eficiente cualquier amenaza a la seguridad de los datos e información, con el objetivo de minimizar el impacto y restaurar la normalidad de los sistemas informáticos e infraestructura de tecnologías de la información lo más rápido posible.

- **Gestión de cambios en ITSM.**

  Es un proceso que se encarga de planificar, aprobar, implementar y evaluar cambios en la infraestructura de tecnologías de la información. Su objetivo principal es gestionar de manera controlada y eficiente cualquier modificación en sistemas, aplicaciones o hardware.

- **Gestión de activos y herramientas.**

  Se refiere a gestionar los activos de las tecnologías de la información, como hardware, software y otros recursos, a lo largo de su ciclo de vida, incluye la adquisición, seguimiento, mantenimiento y eliminación de activos.

Sistema de inventario de activos.

- **Herramienta de gestión de parches.**

  Es un software diseñado para planificar, implementar y supervisar actualizaciones de seguridad y correcciones (parches) en sistemas informáticos, las cuales ayudan a automatizar el proceso de aplicar y mantener al día las actualizaciones de software en sistemas operativos, aplicaciones y otros componentes de tecnologías de la información.

- **Implementación de sistema de ciberseguridad.**

  Implica la adopción de medidas para proteger los sistemas informáticos e infraestructura de tecnologías de la información contra amenazas. Esto incluye la instalación y configuración de herramientas de seguridad, como firewalls y antivirus, la aplicación de políticas de acceso seguro, el monitoreo constante de actividades sospechosas y la capacitación del personal en prácticas seguras.

- **Implementación de sistema de ciberseguridad (incluye DLP).**

  La implementación de un sistema de ciberseguridad, que incorpora medidas de Prevención de Pérdida de Datos (DLP), implica detectar, monitorear y prevenir la fuga no autorizada de datos sensibles. Este proceso implica la adopción de tecnologías como firewalls y sistemas de detección de intrusiones.

- **Implementación de herramienta de backups.**

  Implementación de una solución de respaldo y recuperación de datos, que permite la creación de copias de seguridad automatizadas de datos, con funciones de restauración de datos.

Medidas específicas de seguridad técnica.

- **Implementación de contraseñas seguras.**

  Implica la creación y mantenimiento de contraseñas robustas, que combinan letras, números y caracteres especiales, evitando patrones predecibles o información personal fácilmente accesible. Además, se promueve la periodicidad en la actualización de contraseñas y se fomenta el uso de autenticación de dos factores para una capa adicional de seguridad.

- **Implementación de encriptación en las laptops de la empresa.**

  Este proceso utiliza algoritmos de cifrado para convertir los datos en un formato ilegible, para que solo aquellos con la clave de desencriptación adecuada puedan acceder a la información. La encriptación en las laptops ayuda a mitigar los riesgos asociados con la pérdida o el robo de dispositivos, garantizando que los datos sensibles permanezcan inaccesibles para personas no autorizadas.

3.3. Capacitación y sensibilización en temas de seguridad de la información y ciberseguridad.

Estuvo orientada a concientizar a los colaboradores de la empresa sobre las mejores prácticas y medidas de seguridad para proteger los datos e información frente a amenazas internas y externas. Tuvo el objetivo de fortalecer la postura de seguridad de la organización al crear una cultura de responsabilidad respecto a la protección de la información sensible y la mitigación de riesgos relacionados con la ciberseguridad.

Como resultado de lo expuesto anteriormente, en el año 2023, la empresa demostró su compromiso con la seguridad de la información, la protección de datos personales y la ciberseguridad al implementar los cincuenta y dos (52) "Requisitos de Protección de Datos para proveedores de Microsoft". Como parte de esta

consultoría, participé en la implementación de documentos, aspectos técnicos de ciberseguridad y capacitaciones. Se establecieron y aprobaron políticas, como la de seguridad de la información y ciberseguridad, adicionalmente a planes y programas, como el plan de respuesta a incidentes y el programa de prevención de pérdida de datos. Además, se implementaron medidas técnicas, incluida la gestión de incidentes, sistemas de inventario y herramientas de gestión de parches. También se desplegaron sistemas de ciberseguridad, incluyendo tecnologías de prevención de pérdida de datos y herramientas de respaldo. Se llevaron a cabo capacitaciones para concientizar a los colaboradores sobre seguridad de la información y ciberseguridad, fortaleciendo la cultura de responsabilidad en la protección de datos sensibles de la empresa.

La implementación de los controles de seguridad de la información y ciberseguridad en la citada empresa, los cuales permitieron cumplir con los cincuenta y dos (52) "Requisitos de Protección de Datos para proveedores de Microsoft"; se alinean con las teorías de los diversos autores señalados en el capítulo anterior, tal como se detalla a continuación:

De acuerdo con Rodríguez, Fernández y Fernández (2023), la importancia de implementar controles de seguridad de la información y ciberseguridad es vital y requiere una inversión considerable para resguardar los datos de los riesgos comunes a los que suelen estar expuestos. Esto coincide con la propuesta de Rodríguez Baca y sus colegas (2020), quienes destacan que la implementación de un SGSI influye en atributos clave como la confidencialidad, integridad y disponibilidad de la información, aspectos cruciales para el éxito organizacional. Además, Cano (2011) enfatiza la importancia de considerar las acciones básicas en ciberseguridad para proteger los activos de información crítica de una organización.

Así mismo, las directrices establecidas por la Organización Internacional de Normalización (2017, 2022) respaldan la necesidad de implementar medidas integrales de seguridad y ciberseguridad, basadas en la evaluación continua de riesgos y la eficacia de los controles implementados. A estas consideraciones se suma la Norma Técnica Peruana NTP-ISO/IEC 27001:2022, la Norma Técnica Peruana NTP-ISO/IEC 27002:2022, y las demás normas técnicas complementarias,

que proporcionan una estructura y guía específica para la implementación de sistemas de gestión de seguridad de la información, controles de seguridad de la información y de ciberseguridad, conforme a los estándares internacionales más reconocidos en la materia. Estas normas son fundamentales para garantizar el cumplimiento de requisitos obligatorios y buenas prácticas en materia de seguridad de la información y ciberseguridad, fortaleciendo así la postura de seguridad de la organización.

Este esfuerzo de LHH DBM Perú no solo responde a las demandas del mercado y los estándares internacionales, sino que también se alinea con las iniciativas gubernamentales promovidas por el Estado peruano para impulsar la transformación digital y garantizar la seguridad de la información a nivel nacional. A través de leyes, reglamentos y decretos, el gobierno peruano ha establecido un marco normativo integral que aborda aspectos clave como el gobierno digital, la protección de datos y la ciberseguridad. La Ley de Gobierno Digital, promulgada en 2018, establece el marco general para la gestión de la identidad digital, servicios digitales y seguridad digital, entre otros aspectos relevantes.

Además, el Reglamento de la Ley de Gobierno Digital detalla aspectos específicos como el Modelo de Identidad Digital del Estado y el Marco de Seguridad Digital, que son fundamentales para garantizar la confianza en el entorno digital. El Estado peruano también ha creado el Sistema Nacional de Transformación Digital para promover el uso de tecnologías digitales y fortalecer la seguridad en línea. Normativas más recientes, como el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, establecen directrices claras para la implementación de sistemas de gestión de seguridad de la información y medidas de ciberseguridad en las organizaciones públicas y privadas.

Estas iniciativas gubernamentales, junto con el compromiso proactivo de empresas como la señalada anteriormente, son pasos cruciales hacia un ecosistema digital más seguro y confiable en el Perú. La colaboración entre el sector público y privado es esencial para enfrentar los desafíos en materia de ciberseguridad y protección de datos, y garantizar la integridad y confianza en el entorno digital del país.

3.4. Beneficios obtenidos.

Durante el año 2023, la empresa ha experimentado una transformación significativa en su enfoque hacia la seguridad de la información y la ciberseguridad, como resultado de su compromiso con los "Requisitos de Protección de Datos para proveedores de Microsoft". La implementación de políticas, programas y procedimientos ha generado una serie de beneficios clave para la empresa, que van desde la protección efectiva de datos sensibles hasta el fortalecimiento de la cultura de seguridad en toda la organización. Este enfoque integral ha permitido mejorar su resiliencia ante incidentes, gestionar de manera eficaz los derechos de acceso y construir una sólida base de confianza con clientes y socios comerciales, lo que a su vez proporciona una ventaja competitiva distintiva en el mercado. La implementación de medidas y controles de ciberseguridad detalladas anteriormente conlleva diversos beneficios que impactan positivamente en la seguridad de la información, la ciberseguridad, la protección de datos, la reputación y la imagen de la organización. A continuación, se describen algunos de estos beneficios importantes:

Cumplimiento de lo señalado en el documento "Requisitos de Protección de Datos para proveedores de Microsoft":

Obtener el cumplimiento de estos requisitos permite a la empresa ser un proveedor de confianza para Microsoft, estableciendo un estándar elevado en la protección de datos, seguridad de la información y ciberseguridad. Al alcanzar este estatus, la empresa obtiene una serie de beneficios significativos, como el fortalecimiento de su reputación como socio confiable y comprometido con la protección de datos. Además, la empresa demuestra su capacidad para proteger los datos sensibles y salvaguardar la integridad de los datos e información, lo que puede generar una mayor satisfacción del cliente y mejorar sus relaciones comerciales en general.

Protección de datos sensibles:

Con la implementación y aprobación de políticas y procedimientos seguridad de la información y ciberseguridad, se protege la confidencialidad, integridad y disponibilidad de los datos sensibles de la empresa, mitigando o reduciendo el riesgo de acceso no permitido.

Cumplimiento normativo:

La implementación de políticas y procedimientos alineados con regulaciones y leyes de privacidad y protección de datos garantiza que la empresa cumpla con los requisitos legales y normativos, evitando posibles sanciones y multas.

Resiliencia ante incidentes:

El establecimiento de planes de respuesta a incidentes y de recuperación de desastres fortalece la capacidad de la empresa para gestionar situaciones de emergencia, minimizando el impacto de posibles eventos adversos.

Gestión efectiva de derechos de acceso:

El plan de gestión de derechos de acceso asegura que los usuarios tengan acceso únicamente a la información necesaria para llevar a cabo sus funciones, reduciendo el riesgo del uso indebido de datos.

Mejora de la conciencia y cultura de seguridad de la información y ciberseguridad.

La implementación de programas de capacitación en seguridad de la información y ciberseguridad contribuye a una mayor conciencia entre los empleados, promoviendo una cultura de seguridad en toda la organización.

Disminución de riesgos de pérdida de datos:

El programa de prevención de pérdida de datos y las políticas de protección de datos reducen la probabilidad de pérdida de información sensible, salvaguardando la reputación de la empresa.

Eficiencia operativa:

La implementación de procedimientos y herramientas técnicas, como la gestión de inventario de activos y la herramienta de gestión de parches, contribuye a la eficiencia operativa y la continuidad del negocio.

Seguridad de dispositivos móviles:

Al contar con políticas específicas para dispositivos móviles, la empresa asegura que la información corporativa en estos dispositivos esté protegida, mitigando riesgos asociados con el uso de dispositivos fuera de las instalaciones.

Mejora en la respuesta a incidentes de seguridad de la información:

La existencia de un plan estructurado para responder proactivamente a incidentes de seguridad de la información permite a la empresa reaccionar rápidamente frente a amenazas, minimizando el tiempo de inactividad y reduciendo los impactos adversos.

Confianza del cliente y socios comerciales:

Cumplir con estándares de ciberseguridad y protección de datos genera confianza entre clientes y socios comerciales, fortaleciendo las relaciones comerciales y proporcionando un diferenciador competitivo.

Esta lista de beneficios obtenidos, son el resultado de implementar controles seguridad de la información y ciberseguridad basados en estándares

internacionales, que permitieron cumplir con los "Requisitos de Protección de Datos para proveedores de Microsoft", los cuales proporcionan una visión integral de los esfuerzos en seguridad de la información y ciberseguridad de la empresa. En conjunto, estos documentos no solo fortalecen la postura de seguridad de la información en la organización, sino que también promueven una cultura de conciencia y responsabilidad en todo el personal, contribuyendo así a la protección efectiva de la información y la prevención de posibles riesgos.

CONCLUSIONES

Considerando lo anteriormente desarrollado, se formulan las siguientes conclusiones:

1. La primera conclusión se orienta a la relevancia de los estándares de seguridad de la información y ciberseguridad en las instituciones y organizaciones. La implementación de un SGSI, respaldado por la Norma Técnica Peruana NTP-ISO/IEC 27001-2022 y su equivalente internacional la ISO/IEC 27001:2022, se presenta como un marco estructurado que permite a las organizaciones gestionar y proteger sus datos e información de manera efectiva. Este estándar, junto con otros como la NTP-ISO/IEC 27002-2022 y su equivalente internacional la ISO/IEC 27002:2022, proporcionan los requisitos y las buenas prácticas internacionales en ciberseguridad, abordando aspectos clave como el conocimiento de la organización, liderazgo, gestión de riesgos y revisiones del desempeño del SGSI. La adopción de estos estándares no solo contribuye significativamente con la confidencialidad, integridad y disponibilidad de los datos e información de las organizaciones, sino que también ayuda a mitigar riesgos y amenazas, promoviendo prácticas consistentes de ciberseguridad. En un entorno global donde la información es un activo crítico, la implementación de un SGSI se vuelve esencial para contribuir con la continuidad de las operaciones y preservar la reputación de las organizaciones en un entorno digital dinámico. Además, la Norma Técnica Peruana específica, como la NTP-ISO/IEC 27036-1-2022 o su equivalente internacional ISO/IEC 27036-1-2021, sobre relaciones con proveedores, destaca la importancia de extender la seguridad de la información y la ciberseguridad a lo largo de la cadena de suministro, fortaleciendo así la confianza de los clientes y mejorando la eficiencia operativa. La ciberseguridad se robustece como un mecanismo clave para el éxito y la sostenibilidad de las organizaciones en el mundo digital actual.

2. Una segunda conclusión surge del análisis de algunas normas peruanas sobre ciberseguridad, donde se destaca la importancia crítica de la ciberseguridad para las organizaciones en el escenario de la transformación digital impulsada por el Estado peruano. Dichas normas, como la Ley de Gobierno Digital, el

Reglamento de la Ley de Gobierno Digital, el Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, entre otras, reconocen ciberseguridad como un pilar fundamental para preservar la confidencialidad, integridad y disponibilidad de los datos e información en entornos digitales. Así mismo, se establece la obligación de implementar y mantener un SGSI, resaltando la necesidad de gestionar los riesgos e incidentes de seguridad de la información y de ciberseguridad de manera proactiva. Además, se subraya la conexión directa entre la ciberseguridad y la confianza digital, reconociendo la importancia de fortalecer la credibilidad de los ciudadanos al interactuar con los servicios digitales. En conjunto, estas normativas forman un marco integral que aborda tanto aspectos técnicos de ciberseguridad, como cuestiones éticas, legales y de gobernanza digital en el ámbito peruano. En este contexto, la implementación efectiva de controles y estratégias de seguridad de la información y ciberseguridad se muestra como una prioridad para las organizaciones, contribuyendo no solo a su seguridad digital sino también al bienestar económico y social del país en la era digital.

3. La tercera conclusión, está referida a que el desarrollo de competencias en seguridad de la información y ciberseguridad es esencial para los futuros profesionales de Ciencias de la Información. Esto no solo les permite adaptarse a los cambios tecnológicos, sino también proteger datos y sistemas informáticos en entornos digitales en constante evolución. La estrecha relación entre estas disciplinas surge de la creciente dependencia de la tecnología digital en la sociedad, lo que incrementa la vulnerabilidad a diversas amenazas. Por ende, la colaboración entre Ciencias de la Información y ciberseguridad se torna fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información en el mundo digital.

4. Una cuarta conclusión, se enmarca en mi experiencia profesional como profesional de las Ciencias de la Información desarrollada en la mencionada organización en el año 2023, respecto a la implementación de estándares de ciberseguridad. Esta se enfocó particularmente en implementar controles de seguridad de la información y ciberseguridad para cumplir con los "Requisitos de Protección de Datos para proveedores de Microsoft", lo cual se realizó a

través de una consultoría integral, donde se abordaron diversas actividades, desde el desarrollo e implementación de documentos de ciberseguridad hasta la implementación de aspectos técnicos de seguridad informática y la capacitación de los trabajadores en cuestiones de seguridad de la información y ciberseguridad. Las acciones emprendidas no solo lograron satisfacer los cincuenta y dos (52) requisitos del documento de Microsoft, sino que también fortalecieron significativamente la postura de seguridad de la información y ciberseguridad de la organización, cabe resaltar la importancia de la adaptabilidad y la respuesta proactiva de las organizaciones ante los desafíos en evolución en el ámbito de la ciberseguridad.

5. Una última conclusión, se refiere a los beneficios alcanzados por la empresa posteriormente a la implementación de controles de seguridad de la información y ciberseguridad en respuesta a los cincuenta y dos (52) "Requisitos de Protección de Datos para proveedores de Microsoft". Estos abarcan desde el cumplimiento de estándares y la protección de datos sensibles hasta la sensibilización y concientización en temas de seguridad de la información. Cabe precisar, que la implementación de políticas, programas y procedimientos de seguridad de la información y ciberseguridad ha propiciado mejoras en la respuesta ante posibles incidentes y eventos de seguridad de la información, ante la gestión de derechos de acceso de los usuarios, en la eficiencia operativa y la confianza del cliente. Estos logros no solo fortalecen la posición de la empresa en términos de ciberseguridad, sino que también la sitúan como un referente confiable y comprometido con la protección de datos personales en un entorno empresarial en constante cambio. Los esfuerzos realizados han generado beneficios integrales que contribuyen con la seguridad de la información, ciberseguridad, en la reputación de la organización y en la mejora de su eficiencia operativa.

RECOMENDACIONES

En función a lo concluido, se formulan las siguientes recomendaciones:

1. Se debiera, considerar para próximas investigaciones ampliar el análisis a otros estándares internacionales de ciberseguridad como, por ejemplo: la ISO/IEC 27017 - Código de Prácticas para Controles de Seguridad de la Información en Servicios de la Nube, ISO/IEC 27035-1 y ISO/IEC 27035-2 - Gestión de Incidentes de Seguridad de la Información, ISO/IEC 27103 – Aspectos de Ciberseguridad, ISO/IEC 27701 - Extensión de la ISO/IEC 27001 para la privacidad de la información, ISO/IEC 21827 - Marco de Evaluación de la Seguridad de la Información, ISO/IEC 38500 - Gobierno Corporativo de las Tecnologías de la Información, ISO/IEC 29100 - Tecnologías de la Información - Marco de Privacidad para la Información Personal, y estándares adicionales de ciberseguridad del National Institute of Standards and Technology, entre otros. Ello, con el fin de ampliar el alcance y profundizar en la relevancia de la ciberseguridad en las empresas, se propone extender el análisis de las normativas legales vigentes, inicialmente en otros países sobre esta temática. Además, se sugiere realizar una comparativa y análisis de los futuros resultados en relación con los presentados en el estudio actual. Esto permitirá ofrecer una perspectiva más completa y detallada sobre la importancia de proteger la información en el entorno digital.

2. Implementar talleres, seminarios, conferencias y cursos sobre seguridad de la información y ciberseguridad como parte del plan de estudios de la especialidad de Ciencias de la Información en la PUCP proporcionaría a los estudiantes una comprensión de los conceptos y prácticas en seguridad de la información y ciberseguridad. Además, les brindaría la oportunidad de interactuar con expertos de la industria. Estas actividades ayudarían a desarrollar competencias técnicas y estratégicas en la protección de datos, información y sistemas informáticos en un entorno digital en constante evolución.

3. Se recomienda a las organizaciones fortalecer la postura de la seguridad de la información y ciberseguridad, considerando lo siguiente:

3.1. Implementación y certificación en normativas internacionales: La implementación y certificación en normativas internacionales de seguridad de la información y ciberseguridad, como la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022. Estos estándares proporcionan un marco estructurado para gestionar y proteger la información de manera positiva, beneficiando a la confidencialidad, integridad y disponibilidad de los datos e información. Además, la certificación brinda reconocimiento internacional y fortalece la confianza de clientes y socios comerciales.

3.2. Integración de la ciberseguridad en la transformación digital: Dada la jerarquía crítica de la ciberseguridad en el trasfondo de la transformación digital, se recomienda integren la ciberseguridad desde las etapas iniciales de sus proyectos digitales. Esto implica considerar la seguridad de la información y la ciberseguridad como un componente fundamental en el diseño e implementación de sistemas digitales, asegurando así la protección integral de los datos e información.

3.3. Capacitación continua del personal: La capacitación continua del personal de las empresas en materias de seguridad de la información y ciberseguridad es esencial. Las organizaciones deben desarrollar programas de formación para sensibilizar a los empleados sobre las amenazas digitales, promover buenas prácticas de seguridad y fortalecer la cultura de ciberseguridad dentro de la empresa. Esto contribuirá a reducir riesgos asociados a errores humanos y mejorar la postura general de seguridad de la información y ciberseguridad.

3.4. Monitoreo y evaluación constante: Establecer procesos de monitoreo y evaluación constante de la eficacia de los controles de seguridad de la información y ciberseguridad implementados. Esto implica la revisión periódica de los riesgos, la concreción de auditorías internas y externas,

y la actualización de las medidas de seguridad según las amenazas emergentes. La ciberseguridad es un campo dinámico, y la adaptabilidad continua es esencial para enfrentar los desafíos cambiantes del mundo actual.

3.5. **Colaboración y compartir buenas prácticas:** Fomentar la colaboración entre organizaciones y compartir buenas prácticas en ciberseguridad es clave. La participación en comunidades, foros y grupos de intercambio de información sobre amenazas permite a las organizaciones aprender de las experiencias de otros, fortaleciendo así sus estrategias de ciberseguridad. La ciberseguridad es un esfuerzo colectivo y la colaboración puede mejorar la resiliencia frente a amenazas digitales.

3.6. **Evaluación periódica de la postura de ciberseguridad:** Efectuar evaluaciones y valoraciones habituales de la postura de ciberseguridad de la organización. Estas evaluaciones pueden incluir pruebas de penetración, simulacros de incidentes y revisiones de la infraestructura de seguridad. Identificar y corregir posibles vulnerabilidades de manera proactiva garantiza una defensa sólida contra amenazas digitales.

3.7. **Compromiso de la alta dirección:** Que la alta dirección de las organizaciones asuma y demuestren un compromiso claro con la seguridad de la información y ciberseguridad. Este compromiso se refleja en la asignación de recursos adecuados, la definición de políticas claras, y el respaldo a las iniciativas de seguridad de la información. La cultura organizacional debe promover la importancia de la ciberseguridad en todos los niveles de la empresa de manera constante.

Implementar estas recomendaciones contribuirá significativamente a fortalecer la postura de seguridad de la información y ciberseguridad de las organizaciones, asegurando la protección integral de los activos digitales y la preservación de la confianza en un entorno empresarial cada vez más digitalizado. Además, permitirá a los futuros profesionales de Ciencias de la Información adquirir las competencias necesarias para enfrentar los desafíos emergentes en las disciplinas y áreas de

estudio de seguridad de la información y ciberseguridad, preparándolos para liderar iniciativas que promuevan la integridad, confidencialidad y disponibilidad de la información en el mundo digital actual.

REFERENCIAS

Bermúdez Torres, M. A. (2022). *Importancia de desarrollar las competencias digitales de seguridad del DigComp 2.2, desde el sétimo ciclo de la EBR en el Perú.* Pontificia Universidad Católica del Perú, Facultad de Educación, Lima. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/23667/Berm%c3%badez_Torres_Importancia_desarrollar_competencias1.pdf?sequence=1&isAllowed=y

Cano, J. J. (2020). Retos de seguridad/ciberseguridad en el 2030. *Revista Sistemas*, (154), 68-79. ttps://sistemas.acis.org.co/index.php/sistemas/article/view/94/78

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas (asociación colombiana de ingenieros de sistemas)*, *119*(4.7). https://acis.org.co/archivos/Revista/119/Editorial.pdf

Carrillo, M. R. (2015). El ciberespacio y la ciberseguridad: Consideraciones sobre la necesidad de un modelo jurídico. *Pre-bie3, (6), 25.* https://dialnet.unirioja.es/servlet/articulo?codigo=7688324

Desarrollo Personal y Gestión de Talento - LHH DBM Perú. (2023, May 29). LHH DBM. https://lhh.pe/

European Comission. (2007). *Competencias clave para un aprendizaje a lo largo de la vida un marco de referencia europeo. Bélgica: Comunidades Europeas.* https://www.educacionyfp.gob.es/dctm/ministerio/educacion/mecu/movilidad-europa/competenciasclave.pdf?documentId=0901e72b80685fb1

García Forero, L. F. G. (2020). Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2c%20el%20personal.pdf?sequence=1&isAllowed=y

Instituto Nacional de Calidad. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos, 3° Edición* (NTP 27001). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información, 2° Edición* (NTP 27002). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2019). *Tecnología de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información. Orientación, 2° Edición* (NTP 27003). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2018). *Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación, 2° Edición* (NTP 27004). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información, 3° Edición* (NTP 27005). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2020). *Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información, 3° Edición* (NTP 27007). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2022). Ciberseguridad. Relaciones con Proveedores. Parte 1: Visión general y conceptos, *1° Edición* (NTP 27036-1). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Instituto Nacional de Calidad. (2018). *Gestión del Riesgo. Directrices, 2° Edición* (NTP 31000). https://www.inacal.gob.pe/cid/categoria/normas-tecnicas-peruanas

Mario, J. y Correa, A. (2018). *Adaptación del modelo de madurez en ciberseguridad basado en C2M2, para la industria manufacturera del sector textil que utiliza sistemas SCADA.* Instituto Tecnológico Metropolitano. https://repositorio.itm.edu.co/handle/20.500.12622/4681

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel-Bit: Revista de Medios y Educación, 63, 197-225.* https://idus.us.es/bitstream/handle/11441/145488/Formaci%c3%b3n%20y%20concienciaci%c3%b3n%20en%20ciberseguridad%20basada%20en%20competencias.pdf?sequence=1&isAllowed=y

National Institute of Standards and Technology. (2015). *NIST Special Publication 800-16.* Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-16/800- 16.pdf

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

OECD (2018). The future of education and skills. Education 2030: the future we want (position paper). OECD Publishing. https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos* (ISO 27001). https://www.iso.org/store.html

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información* (ISO 27002). https://www.iso.org/store.html

Organización Internacional de Normalización. (2017). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Orientación* (ISO 27003). https://www.iso.org/store.html

Organización Internacional de Normalización. (2016). *Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación* (ISO 27004). https://www.iso.org/store.html

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información* (ISO 27005). https://www.iso.org/store.html

Organización Internacional de Normalización. (2020). *Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información* (ISO 27007). https://www.iso.org/store.html

Organización Internacional de Normalización. (2021). Ciberseguridad. Relaciones con Proveedores. Parte 1: Visión general y conceptos (ISO 27036-1). https://www.iso.org/store.html

Organización Internacional de Normalización. (2018). *Gestión del Riesgo. Directrices* (ISO 31000). https://www.iso.org/store.html

Pacheco A, E. J. (2020). *Oportunidades de Ciberdiplomacia para la Política Exterior del Perú*. http://repositorio.adp.edu.pe/handle/ADP/143

Presidencia del Consejo de Ministros. (2018). *Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital*. https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf?v=1566312763

Presidencia del Consejo de Ministros. (2018). *Decreto Supremo N° 050-2018-PCM que aprueba la definición de Seguridad Digital en el ámbito nacional.* https://busquedas.elperuano.pe/normaslegales/aprueban-la-definicion-de-seguridad-digital-en-el-ambito-nac-decreto-supremo-n-050-2018-pcm-1647865-1/

Presidencia del Consejo de Ministros. (2019*). Ley N° 3099 Ley de Ciberdefensa.* https://cdn.www.gob.pe/uploads/document/file/1671813/Ley%20N%C2%B030999%2C%20Ley%20de%20Ciberdefensa.pdf

Presidencia del Consejo de Ministros. (2020*). Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.* https://cdn.www.gob.pe/uploads/document/file/2790485/Decreto%20de%20Urgencia%20N%C2%BA%20007-2020.pdf?v=1643322610

Presidencia del Consejo de Ministros. (2020). *Decreto de Urgencia N° 0006-2020 que crea el Sistema Nacional de Transformación Digital.* https://cdn.www.gob.pe/uploads/document/file/1671822/Decreto%20Urgencia%20N%C2%B0006-2020.pdf.pdf?v=1613166781

Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento de la Ley de Gobierno Digital.* https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-del-decreto-legisl-decreto-supremo-n-029-2021-pcm-1929103-3/

Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N° 157-2021-PCM que aprueba el Reglamento del Sistema Nacional de Transformación Digital.* https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-del-decreto-de-urg-decreto-supremo-n-157-2021-pcm-1995486-1/

Presidencia del Consejo de Ministros. (2023). *Directiva Nº 001-2023-PCM/SGTD que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital para las entidades públicas.* https://busquedas.elperuano.pe/dispositivo/NL/2212867-1

Presidencia del Consejo de Ministros. (2023). *Resolución N° 003-2023-PCM/SGTD que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.* https://busquedas.elperuano.pe/dispositivo/NL/2212869-1

Presidencia del Consejo de Ministros. (2024). *Decreto Supremo N° 017-2024-PCM que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa.* https://cdn.www.gob.pe/uploads/document/file/5858763/5192944-decreto-supremo-n-017-2024-pcm.pdf?v=1707918727

Reyes, M. y Gálvez Pacheco, R. (2020). *La recepción e incorporación del principio de cooperación internacional en materia de ciberseguridad en el derecho chileno.* Universidad de Chile. http://repositorio.uchile.cl/handle/2250/176706

Revilla F., D. y Sime P, L. (Eds.) (2021). *Perspectivas y reflexiones sobre el Proyecto Educativo Nacional al 2036.* Pontificia Universidad Católica del Perú, Facultad de Educación, Departamento Académico de Educación y Centro de Investigaciones y Servicios Educativos (CISE). p.87-95. https://repositorio.pucp.edu.pe/index/handle/123456789/180968

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Diaz, M. A. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la

información de una empresa privada peruana. *Propósitos y Representaciones, 8(3), 9.* http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Rodríguez, G. D. L. C., Fernández, R. A. M., & Fernández, A. C. M. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Innovación y Software*, *4*(1), 219-236. https://www.redalyc.org/journal/6738/673874721015/673874721015.pdf

Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. (2009). *Circular N° G-140-2009 que establece disposiciones referidas a la Gestión de la seguridad de la información.* https://www.sbs.gob.pe/Portals/0/jer/Auto_Nuevas_Empresas/Normas_Comunes/9.%20Gesti%C3%B3n%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n_Circ.%20SBS%20G-140-2009.pdf

Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. (2012). *Circular N° G-167-2012 que modifica el literal d) del artículo 2º de la Circular N° G-140-2009.* https://intranet2.sbs.gob.pe/dv_int_cn/161/v1.0/Adjuntos/g-167-2012.c.pdf

Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. (2021). *Resolución S.B.S. Nº 504-2021 que aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.* https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf

Supplier Security & Privacy Assurance. (s. f.). *Microsoft.com*. Recuperado 18 de enero de 2024, de https://www.microsoft.com/en-us/procurement/sspa?activetab=pivot1:primaryr6

Vuorikari, R., K, S. y Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes.* Oficina de Publicaciones de la Unión Europea. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415

Anexo A: Curriculum Vitae resumido

Marco Antonio Bermúdez Torres cuenta con una amplia experiencia como consultor, auditor y docente universitario en áreas clave como Transformación Digital, Gobierno Digital, Control Interno, Gestión de Seguridad de la Información y Ciberseguridad. Obtuvo su Bachillerato en Humanidades con mención en Ciencias de la Información y la Licenciatura en Educación con especialidad en Educación para el Desarrollo, ambas en la Pontificia Universidad Católica del Perú (PUCP), así como el título de Ingeniero de Sistemas en la Universidad Inca Garcilaso de la Vega (UIGV). Además, posee un Máster en Seguridad de la Información y Continuidad del Negocio (Ciberseguridad) de la Universidad Rey Juan Carlos de España, y un Máster en Ciencias de la Gestión y Management de la Universidad Bordeaux IV en Francia, con énfasis en Investigación en Gestión de Organizaciones, grados registrados en la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU). Es miembro activo del Comité Técnico de Normalización N° 21 (CTN 21) "Codificación e Intercambio Electrónico de Datos" del Instituto Nacional de Calidad (INACAL), entidad nacional de normalización de Perú. Desde 2012, ha participado en el análisis, adecuación y aprobación de todas las Normas Técnicas Peruanas relacionadas con la Seguridad de la Información, Ciberseguridad y Gestión de Riesgos de Seguridad de la Información, basadas en estándares internacionales de la Organización Internacional de Normalización (ISO).

Anexo B: Requisitos de Protección de Datos para proveedores de Microsoft

Requisitos de Protección de Datos para proveedores de Microsoft

Aplicabilidad

Los Requisitos de Protección de Datos ("**DPR**", por sus siglas en inglés) para proveedores de Microsoft se aplican a cada proveedor de Microsoft que trata Datos Personales o Confidenciales de Microsoft en relación con las actividades realizadas por dicho proveedor (por ejemplo, prestación de servicios, licencias de software o servicios en la nube) según sus condiciones contractuales con Microsoft (por ejemplo, términos de Órdenes de Compra y contrato marco) ("**Actividad**", "**Actividades**" o "**Realización de Actividades**").

- En caso de conflicto entre los DPR y los requisitos que se especifican en los acuerdos contractuales celebrados entre el proveedor y Microsoft, prevalecerán los DPR, a menos que el proveedor identifique en el contrato la disposición correcta que sustituya el requisito de protección de datos aplicable (en cuyo caso, prevalecerán los términos del contrato).
- Si hubiera algún conflicto entre los requisitos que se incluyen en el presente y cualquier requisito legal o reglamentario, prevalecerán estos últimos.
- En caso de que el proveedor de Microsoft actúe como Responsable del Tratamiento, el proveedor puede tener requisitos reducidos en los DPR.
- En caso de que el proveedor de Microsoft no trate Datos Personales de Microsoft, sino únicamente Datos Confidenciales de Microsoft, con respecto a estos DPR, se podrían reducir sus requisitos.

Transferencia internacional de datos

Sin limitar el resto de sus obligaciones, el proveedor no realizará ninguna transferencia internacional de Datos Personales de Microsoft a menos que Microsoft lo haya autorizado previamente por escrito y, en todo caso, el proveedor deberá cumplir con los Requisitos de Protección de Datos, incluidas las Cláusulas Contractuales Tipo o, a discreción de Microsoft, otros mecanismos adecuados de transferencia transfronteriza aprobados por una autoridad de protección de datos competente o por la Comisión Europea,
según corresponda, y adoptados o acordados por Microsoft. Las Cláusulas Contractuales Estándar sucesoras adoptadas por (i) la Comisión Europea o adoptadas por el Supervisor Europeo de Protección de Datos y aprobadas por la Comisión Europea; (ii) el Reino Unido en virtud de la Ley Federal General de Protección de Datos del Reino Unido; (iii) Suiza en virtud de la Ley Federal de Protección de Datos de Suiza; o (iv) las cláusulas que rigen la transferencia internacional de datos personales, adoptadas oficialmente por un gobierno en una jurisdicción distinta de Suiza, el Reino Unido y las jurisdicciones que comprenden la Unión Europea/Espacio Económico Europeo, se incorporarán y serán vinculantes para el proveedor a partir del día de su adopción. Asimismo, el proveedor se asegurará de que todos y cada uno de los Subencargados del Tratamiento (tal y como se definen en las Cláusulas Contractuales Estándar) también las cumplan.

Definiciones clave

Los siguientes términos utilizados en estos DPR tienen el significado que se indica a continuación. Se interpreta que las listas de ejemplos que siguen a los términos "incluido/a(s)", "como", "por ejemplo" o similares utilizados a lo largo de estos DPR incluyen "de manera enunciativa mas no limitativa" o "entre otros", a menos que se califiquen con palabras como "solamente" o "únicamente". Para más definiciones, consulte el Glosario que se encuentra al final del presente documento.

"**Responsable del Tratamiento**" se refiere a la entidad que determina los fines y los medios del Tratamiento de los Datos Personales. "Responsable del Tratamiento" se refiere a una Empresa, al Responsable del Tratamiento (tal y como se define este término en el RGPD) y a términos equivalentes que se encuentran en las Leyes de Protección de Datos, según lo requiera el contexto.

Las "**Cookies**" son pequeños archivos de texto que los sitios web y/o las aplicaciones almacenan en los dispositivos y que contienen información utilizada para reconocer a una Persona Interesada o a un dispositivo.

"**Incidente de Datos**" se refiere a (1) una violación de la seguridad que provoque, de manera accidental o ilegal, la destrucción, la pérdida, la alteración,
la divulgación no autorizada o el acceso a los Datos Personales de Microsoft o a los Datos Confidenciales de Microsoft transmitidos, almacenados o

Tratados de alguna otra manera por el proveedor o sus Subcontratistas, o (2) una vulnerabilidad de seguridad relacionada con el manejo de los
Datos Personales de Microsoft o los Datos Confidenciales de Microsoft o incidente de confidencialidad según se define en el Proyecto de ley 64 (2021, capítulo 25).

"**Persona Interesada**" es una persona física identificable que se puede identificar, ya sea directa o indirectamente, en particular, haciendo referencia a un elemento de identificación, como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más aspectos específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física.

"**Derecho de la Persona Interesada**" significa el derecho de la Persona Interesada a acceder, eliminar, editar, exportar, restringir u oponerse al Tratamiento de los
Datos Personales de Microsoft de dicha Persona Interesada, si así lo exigiera la Legislación.

"**Legislación**" significa todas las leyes, normas, estatutos, decretos, decisiones, órdenes, reglamentos, sentencias, códigos, promulgaciones, resoluciones y requisitos aplicables de cualquier autoridad de gobierno (ya sea federal, estatal, local o internacional) que tenga jurisdicción. "**Ilegal**" se refiere a cualquier violación de la Legislación.

"**Datos Confidenciales de Microsoft**" se refiere a toda información que, de ponerse en riesgo su confidencialidad o integridad de la manera que fuere, puede suponer una pérdida considerable para Microsoft en términos financieros o de reputación. Esto incluye productos de hardware y software de Microsoft, aplicaciones internas de línea de negocio, materiales de comercialización previos al lanzamiento, claves de licencia de productos y documentación técnica relacionada con los productos y servicios de Microsoft.

"**Datos Personales de Microsoft**" significa cualquier Dato personal Tratado por Microsoft o en su nombre.

"**Datos Personales**" se refiere a toda información relativa a una Persona Interesada y cualquier otra información que constituya "datos personales" o "información personal" de conformidad con la Legislación.

"**Tratamiento**" significa cualquier operación o conjunto de operaciones que se realicen sobre Datos Personales o Datos Confidenciales de Microsoft, ya sea de manera automatizada o de cualquier otro modo, como la recopilación, el registro, la grabación, la organización, la estructuración, el almacenamiento, la adaptación o alteración, la recuperación, la consulta, el uso, la divulgación por transmisión, la difusión o puesta a disposición de cualquier otro modo, la alineación o combinación, la restricción, la eliminación o la destrucción. Los términos "Tratamiento", "Tratar" y "Tratado" tendrán los significados correspondientes.

"**Encargado del Tratamiento**" se refiere a la entidad que Trata Datos Personales en nombre de otra entidad e incluye al Proveedor de Servicios, al Encargado del Tratamiento (tal como se define ese término en el RGPD) y a términos equivalentes que se encuentran en las Leyes de Protección de Datos, según lo requiera el contexto.

"**Información Médica Protegida**" (o "**PHI**", por sus siglas en inglés) se refiere a los Datos Personales de Microsoft protegidos por la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA, por sus siglas en inglés).

"**Subcontratista**" significa un tercero al cual el proveedor delega sus obligaciones en relación con el contrato que ampara su Actividad, incluida cualquier filial del proveedor que no haya celebrado un contrato directamente con Microsoft.

"**Subencargado del Tratamiento**" se refiere a un tercero que Microsoft contrata para la realización de la Actividad en los casos en los que la Actividad incluye el Tratamiento de los
Datos Personales de Microsoft para los cuales Microsoft es el Encargado del Tratamiento.

Respuesta del proveedor

Los proveedores confirman anualmente el cumplimiento de estos requisitos mediante un servicio en línea administrado

por Microsoft. Consulte la Guía del programa de la SSPA para entender cómo se administra el cumplimiento.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección A: Administración	
1	Cada contrato aplicable entre Microsoft y el proveedor (por ejemplo, contrato marco, declaración de trabajo, órdenes de compra y otros pedidos) contiene lenguaje de protección de datos de privacidad y seguridad con respecto a los Datos Confidenciales y Personales de Microsoft, según corresponda, incluidas las prohibiciones sobre la venta de Datos Personales de Microsoft y el Tratamiento de Datos Personales de Microsoft fuera de la relación comercial directa entre Microsoft y el proveedor. En el caso de las empresas que operan como Encargados o Subencargados del Tratamiento, con respecto a los Datos Personales de Microsoft, el contrato debe incluir el objeto, la duración, la naturaleza y la finalidad del Tratamiento, el tipo de Datos Personales de Microsoft y las categorías de Personas Interesadas, así como las obligaciones y los derechos de Microsoft.	El proveedor debe presentar el contrato aplicable entre Microsoft y el proveedor. En el caso de los Encargados y Subencargados del Tratamiento, las descripciones del Tratamiento se incluyen en el contrato aplicable (*por ejemplo*, declaración de trabajo, órdenes de compra). Nota: Las empresas que tengan órdenes de compra en proceso pueden solicitar que la descripción necesaria de las actividades de Tratamiento se agregue más tarde en el proceso de compra.
2	Cuando Microsoft confirme que sus compromisos cumplen una función de Subencargado del Tratamiento, el Proveedor debe contar con contratos de protección de datos aplicables celebrados con Microsoft. Si Microsoft confirma que sus compromisos implican el tratamiento de PHI, el proveedor debe tener un Contrato de Socio Comercial y/u otro contrato vigente con Microsoft. Nota: Microsoft publicará esta designación en su perfil cuando corresponda.	Cláusulas Contractuales Tipo, Adenda de Datos de Clientes en Línea, Adenda de Tratamiento de Datos de Servicios Profesionales del Proveedor o Socio y/o Contrato de Socio Comercial.
3	Asignar la responsabilidad y la obligación de rendir cuentas sobre el cumplimiento de los DPR a una persona o grupo designado dentro de la empresa.	Indicar la función de la persona o el grupo encargado de garantizar el cumplimiento de los DPR para proveedores de Microsoft. Un documento que describa la autoridad y la obligación de rendir cuentas de esta persona o grupo que demuestre una función de privacidad y/o seguridad.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección A: Administración (continuación)	
4	Establecer, mantener y llevar a cabo una capacitación anual sobre privacidad y seguridad para los empleados que tendrán acceso a los Datos Personales Tratados por el proveedor en relación con la Realización de la Actividad o los Datos Confidenciales de Microsoft. Si su empresa no tiene contenido preparado, puede utilizar este esquema y adaptarlo a su empresa. Nota: Es posible que el personal de los proveedores deba realizar cursos adicionales de capacitación impartidos por las divisiones de Microsoft.	Los registros anuales de asistencia están disponibles y pueden proporcionarse a Microsoft si lo solicita. El contenido de la capacitación incluye principios de privacidad y seguridad. Si los datos personales de Microsoft tratados por el proveedor incluyen PHI, el contenido de la capacitación debe incluir formación sobre la HIPAA, incluidos los usos y divulgaciones permitidos por el proveedor según lo previsto en el Contrato de Socio Comercial. La documentación del cumplimiento de los requisitos de capacitación incluirá pruebas de la capacitación relacionada con los requisitos reglamentarios de privacidad, las obligaciones de seguridad y el cumplimiento de los requisitos y las obligaciones contractuales aplicables.
5	Aplicar sanciones adecuadas a los empleados que incumplan las políticas de privacidad y seguridad del proveedor.	Documentación de las políticas de privacidad y seguridad que describan las sanciones por incumplimiento (por ejemplo, hasta el despido).
6	Tratar los Datos Personales de Microsoft únicamente de acuerdo con las instrucciones documentadas por Microsoft, incluyendo los escenarios con respecto a las transferencias de Datos Personales de Microsoft a un tercer país o a una organización internacional, a menos que lo exija la Legislación; en tal caso, el Encargado del Tratamiento o el Subencargado del Tratamiento (proveedor) informará al responsable del tratamiento (Microsoft) dicho requisito legal antes del Tratamiento, a menos que dicha Legislación prohíba dicha información por motivos importantes de interés público.	El proveedor recopila y mantiene todas las instrucciones documentadas por Microsoft (por ejemplo, el acuerdo, la declaración de trabajo o la documentación del pedido) de forma electrónica, en un lugar fácilmente accesible para los empleados y contratistas del proveedor que participan en la Realización de la Actividad.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección B: Aviso	
7	El proveedor debe utilizar la Declaración de Privacidad de Microsoft cuando recopile Datos Personales en nombre de Microsoft. El aviso de privacidad debe ser obvio y estar disponible para las Personas Interesadas para ayudarlas a decidir si entregan sus Datos Personales al proveedor. Nota: Si su empresa es el Responsable del Tratamiento, usted deberá publicar su propio aviso de privacidad.	El proveedor utiliza un fwdlink para la Declaración de Privacidad de Microsoft publicada actualmente. La Declaración de Privacidad se publica en cualquier contexto en el que se recopilen los Datos Personales de un usuario. Si corresponde, existe una versión sin conexión que se facilita antes de la recopilación de datos. Toda Declaración de Privacidad sin conexión utilizada será la versión publicada más reciente y estará debidamente fechada. Para los servicios de los empleados de Microsoft, se utiliza el Aviso de Privacidad de Datos de Microsoft.
8	Cuando se recopilen Datos Personales de Microsoft a través de una llamada de voz en directo o grabada, los proveedores deben estar preparados para debatir las prácticas de recopilación, tratamiento, uso y conservación de datos aplicables con las Personas Interesadas.	El guion para las grabaciones de voz debe informar cómo se Tratan los Datos Personales de Microsoft e incluir: ▪ recopilación, ▪ uso y ▪ conservación.
	Sección C: Elección y consentimiento	
9	Cuando corresponda, el proveedor debe obtener y registrar el consentimiento de la Persona Interesada para todas sus actividades de Tratamiento (incluida cualquier actividad de Tratamiento nueva y actualizada) antes de recopilar los Datos Personales de dicha Persona Interesada. El proveedor monitorea la eficacia de la gestión de las preferencias para garantizar que el plazo para cumplir con algún cambio de preferencia sea el más restrictivo de los requisitos legales locales que se aplican.	El proveedor debe poder demostrar cómo una Persona Interesada da su consentimiento para una actividad de Tratamiento y que el alcance del consentimiento ampara todas las actividades de Tratamiento del proveedor con respecto a los Datos Personales de dicha Persona Interesada. El proveedor debe poder demostrar cómo una Persona Interesada retira su consentimiento para una actividad de Tratamiento. El proveedor debe poder demostrar cómo se comprueban las preferencias antes de iniciar una nueva actividad de Tratamiento. Nota: Las pruebas pueden ser capturas de pantalla de la interacción con el usuario, la experiencia con el servicio o la oportunidad de ver la documentación técnica.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección C: Elección y consentimiento (continuación)	
10	Los proveedores que crean y gestionan sitios web y/o aplicaciones de Microsoft o sitios que llevan la marca de Microsoft deben proporcionar a las Personas Interesadas un aviso transparente y la posibilidad de elegir sobre el uso de las cookies de acuerdo con los compromisos de la Declaración de Privacidad de Microsoft y los requisitos legales locales. A menos que la unidad de negocio contratante lo solicite específicamente, los proveedores deben utilizar el Banner estándar elaborado por 1ES para gestionar los controles de elección. Este requisito se aplica cuando los sitios se dirigen a usuarios dentro de la Unión Europea o el Espacio Económico Europeo y otras regiones con leyes de privacidad aplicables y siempre que se utilice la Declaración de Privacidad de Microsoft. Nota: Los patrocinadores comerciales de Microsoft deben registrar los sitios web de Microsoft en el portal interno de Cumplimiento web (http://aka.ms/wcp) para tener el inventario de cookies catalogado y administrado.	El propósito de cada cookie debe estar documentado y debe informar el tipo de cookie implementado. ▪ Las cookies persistentes no deben utilizarse cuando las cookies de sesión sean suficientes. ▪ Cuando se utilizan cookies persistentes, estas no deben tener una fecha de caducidad superior a 13 meses después de que el usuario haya visitado el sitio. Validar el cumplimiento de las leyes de la UE según corresponda, como: ▪ uso de la convención de etiquetado, "Privacidad y Cookies" ▪ para la declaración de privacidad, ▪ obtener el consentimiento afirmativo del usuario antes de utilizar cookies "no esenciales" para fines como la publicidad, y ▪ el consentimiento debe caducar o volver a obtenerse a más tardar cada 6 meses.
	Sección D: Recopilación	
11	El proveedor deberá supervisar la recopilación de Datos Personales y/o Confidenciales de Microsoft para garantizar que los únicos datos recopilados sean los necesarios para la Realización de la Actividad.	El proveedor puede proporcionar documentación que demuestre que los Datos Personales y/o Confidenciales de Microsoft recopilados son necesarios para la Realización de la Actividad. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
12	Antes de recopilar datos de niños (según la definición de la jurisdicción aplicable), el proveedor debe obtener el consentimiento según las leyes locales de privacidad.	El proveedor puede aportar documentación que demuestre el consentimiento de los padres o tutores. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

13	Cuando el proveedor reciba un conjunto de datos de Microsoft con identificabilidad reducida, incluido un seudónimo, persona no identificable (NPI, por sus siglas en inglés), seudónimo no vinculado, agregado, anónimo o cualquier término que se relacione con una de esas clasificaciones (como no identificado), el proveedor mantendrá los datos en el estado en que se recibieron.	El proveedor no aumentará la identificabilidad de los conjuntos de datos (es decir, no reidentificará a las personas que forman parte de un conjunto de datos mediante la unión a otros conjuntos de datos, etc.). El proveedor dispone de una política/proceso de eliminación de identificación/anonimización de datos.
#	**Requisitos de Protección de Datos para proveedores de Microsoft**	**Pruebas del cumplimiento**
	Sección E: Conservación	
14	Garantizar que los Datos Personales y Confidenciales de Microsoft no se conserven durante más tiempo del necesario para la Realización de la Actividad, a menos que la ley exija la conservación continuada de los Datos Personales y/o Confidenciales de Microsoft.	El proveedor cumple con las políticas de conservación documentadas o los requisitos de conservación especificados por Microsoft en el contrato (por ejemplo, declaración de trabajo, orden de compra). El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
15	Garantizar que, a discreción de Microsoft, los Datos Personales y Confidenciales de Microsoft que estén en posesión del proveedor o bajo su control se devuelvan a Microsoft o se destruyan al finalizar la Realización de la Actividad o a petición de Microsoft. Dentro de las aplicaciones, deben existir procesos que garanticen que, cuando los datos sean eliminados de la aplicación, ya sea explícitamente por los usuarios o en función de otros factores desencadenantes, como la antigüedad de los datos, se eliminen de forma segura. Cuando sea necesaria la destrucción de Datos Personales o Confidenciales de Microsoft, el proveedor deberá quemar, pulverizar o triturar los activos físicos que contengan Datos Personales y/o Confidenciales de Microsoft de forma que la información no pueda ser leída o reconstruida.	Mantener un registro de la disposición de los Datos Personales y Confidenciales de Microsoft (esto puede incluir la devolución a Microsoft para su destrucción). Si Microsoft exige o solicita la destrucción, proporcionar un certificado de destrucción firmado por un funcionario del proveedor.
	Sección F: Personas Interesadas	
	Las Personas Interesadas tienen ciertos derechos conforme a la ley, incluido el derecho a acceder, eliminar, editar, exportar, restringir y oponerse al tratamiento de sus Datos Personales ("Derechos de las Personas Interesadas"). Cuando una Persona Interesada busca ejercer sus derechos en virtud de la Legislación con respecto a sus Datos Personales de Microsoft, el proveedor debe permitir a Microsoft hacer lo siguiente o realizar estas acciones en nombre	

	de Microsoft:	
16	Ayudar a Microsoft, a través de medidas técnicas y organizativas apropiadas, cuando sea posible, a cumplir con sus obligaciones de responder a las solicitudes de las Personas Interesadas que buscan ejercer sus Derechos de las Personas Interesadas sin demoras indebidas. A menos que Microsoft indique lo contrario, el proveedor remitirá a todas las Personas Interesadas que se pongan en contacto con el proveedor directamente a Microsoft para que ejerzan los Derechos de las Personas Interesadas.	El proveedor mantendrá pruebas de los procesos y procedimientos documentados para respaldar la ejecución de los Derechos de las Personas Interesadas. El proveedor mantendrá evidencia documental de las pruebas. La evidencia estará disponible a petición de Microsoft.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección F: Personas Interesadas (continuación)	
17	Cuando se responde directamente a la Persona Interesada o cuando el proveedor proporciona un mecanismo de autoservicio en línea, el proveedor cuenta con procesos y procedimientos para identificar a la Persona Interesada que realiza la solicitud.	El proveedor ha documentado el método utilizado para identificar a las Personas Interesadas de Microsoft. El proveedor proporcionará evidencia documental a Microsoft cuando se le solicite.

18	Si Microsoft le pide que localice Datos Personales de Microsoft sobre una Persona Interesada que no están disponibles a través de un mecanismo de autoservicio en línea, el proveedor hará un esfuerzo razonable para localizar los datos solicitados y mantendrá registros suficientes para demostrar que se hizo una búsqueda razonable.	El proveedor mantendrá evidencia documental de los procedimientos implementados para determinar si se conservan los Datos Personales de Microsoft y proporcionará la documentación a Microsoft si esta lo solicita. El proveedor mantiene un registro que demuestra las medidas adoptadas para satisfacer las solicitudes de Derechos de las Personas Interesadas. La documentación incluye: ▪ fecha y hora de la solicitud, ▪ las medidas adoptadas para responder a la solicitud y el registro de cuándo se le informó a Microsoft. El proveedor proporcionará a Microsoft pruebas de la conservación de los registros cuando se le solicite.
19	El proveedor comunicará a las Personas Interesadas los pasos que deben seguir para acceder a sus Datos Personales de Microsoft o para ejercer sus derechos con respecto a sus datos.	El proveedor mantendrá evidencia documental de las comunicaciones y procedimientos de acceso a los Datos Personales de Microsoft. El proveedor mantendrá evidencia documental y proporcionará dicha evidencia a Microsoft cuando se le solicite.
20	Registrar la fecha y la hora de las solicitudes de Derechos de las Personas Interesadas y las medidas adoptadas por el proveedor en respuesta a dichas solicitudes. Si su solicitud es denegada, a instancias de Microsoft, proporcionar a la Persona Interesada una explicación por escrito. Proporcionar los registros de las solicitudes de las Personas Interesadas a Microsoft cuando lo solicite.	El proveedor mantiene registros de las solicitudes de acceso/borrado y documenta los cambios realizados en los Datos Personales de Microsoft. Documentar los casos en los que se deniegan las solicitudes y conservar las pruebas de la revisión y aprobación de Microsoft. El proveedor proporcionará pruebas de la conservación de registros de solicitudes y denegaciones de acceso a los Datos Personales de Microsoft.
21	El proveedor debe brindar acceso a Microsoft u obtener una copia de los Datos Personales de Microsoft solicitados para la Persona Interesada autentificada en un formato apropiado impreso, electrónico o verbal.	El proveedor suministra los Datos Personales de Microsoft a la Persona Interesada en un formato comprensible y en una forma conveniente para la Persona Interesada y el proveedor.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección F: Personas Interesadas (continuación)	

22	El proveedor debe tomar precauciones razonables para garantizar que los Datos Personales de Microsoft entregados a Microsoft o a una Persona Interesada autentificada no puedan ser utilizados para identificar a otra persona.	El proveedor mantendrá evidencia documental de los procedimientos relacionados con las precauciones para evitar la identificación de la Persona Interesada en contra de los términos del Contrato. El proveedor proporcionará las pruebas a Microsoft cuando se le solicite.
23	Si una Persona Interesada cree que sus Datos Personales de Microsoft no están completos y no son precisos, el proveedor debe elevar el problema a Microsoft y cooperar con Microsoft según sea necesario para resolver el problema.	El proveedor documenta los casos de desacuerdo y eleva la cuestión a Microsoft. El proveedor proporcionará a Microsoft las pruebas documentales cuando se le solicite.
	Sección G: Subcontratistas	
	Si el proveedor pretende utilizar a un Subcontratista para el Tratamiento de los Datos Personales o Confidenciales de Microsoft, deberá:	
24	Notificar a Microsoft antes de subcontratar servicios o realizar cualquier cambio relativo a la adición o sustitución de subcontratistas. Nota: Indique su aceptación de esta obligación, incluso si no contrata actualmente a subcontratistas pero puede hacerlo en el futuro.	Validar que los Datos Personales de Microsoft sean Tratados únicamente por empresas conocidas por Microsoft, tal y como se requiere en el contrato aplicable (por ejemplo, declaración de trabajo, adenda, orden de compra) o capturados en la base de datos de la SSPA. El proveedor puede publicar su lista de subcontratistas en línea e incluir un enlace a la página en la base de datos de la SSPA.
25	Documentar la naturaleza y el alcance de los Datos Personales y Confidenciales de Microsoft procesados por los Subcontratistas, para garantizar que la información recopilada sea necesaria para la Realización de la Actividad.	El proveedor mantiene la documentación relativa a los Datos Personales y Confidenciales de Microsoft divulgados o transferidos a los subcontratistas. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
26	Cuando Microsoft sea el Responsable del Tratamiento de los Datos Personales de Microsoft, garantizar que el subcontratista utilice los Datos Personales de Microsoft de acuerdo con las preferencias de contacto indicadas de la Persona Interesada.	Demostrar cómo los subcontratistas utilizan la preferencia de la Persona Interesada de Microsoft. Proporcionar documentación de apoyo (por ejemplo, captura de pantalla, SLA, SOW, etc.) que incluya el plazo para que un subcontratista cumpla con un cambio de preferencia.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección G: Subcontratistas (continuación)	
27	Limitar el Tratamiento de los Datos Personales o Confidenciales de Microsoft por parte del subcontratista para los fines necesarios para cumplir el contrato del proveedor con Microsoft. Si los Datos Personales de Microsoft son PHI, celebre también un Contrato de Socio Comercial con el Subcontratista que limite el Tratamiento de los Datos Personales de Microsoft por parte del Subcontratista y proteja la confidencialidad y seguridad de los Datos Personales de Microsoft del mismo modo que el Contrato de Socio Comercial entre Microsoft y el proveedor.	El proveedor puede proporcionar documentación que demuestre que los Datos Personales de Microsoft proporcionados a un Subcontratista son necesarios para la Realización de la Actividad. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite, incluido el Contrato de Socio Comercial, si corresponde.
28	Revisar las quejas en busca de indicios de cualquier Tratamiento no autorizado o ilegal de los Datos Personales de Microsoft.	El proveedor puede demostrar que dispone de sistemas y procesos para atender las quejas relativas al uso o divulgación no autorizados de los Datos Personales de Microsoft por parte de un subcontratista. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
29	Notificar a Microsoft de inmediato al enterarse de que un subcontratista ha Tratado Datos Personales o Confidenciales de Microsoft para cualquier propósito que no esté relacionado con la Realización de la Actividad.	El proveedor ha proporcionado las instrucciones y los medios para que un subcontratista informe el uso indebido de los datos de Microsoft. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
30	Si el proveedor recopila Datos Personales de terceros en nombre de Microsoft, deberá validar que las políticas y prácticas de protección de datos de terceros son coherentes con el contrato del proveedor con Microsoft y los DPR.	El proveedor puede proporcionar la documentación de la diligencia debida realizada en relación con las políticas y prácticas de protección de datos del tercero. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
31	Adoptar de inmediato medidas para mitigar cualquier daño real o potencial causado por el Tratamiento no autorizado o ilegal de los Datos Personales y Confidenciales de Microsoft por parte de un subcontratista.	El proveedor debe mantener pruebas documentales del plan y del procedimiento, y proporcionar pruebas de la documentación a Microsoft cuando se le solicite.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección H: Calidad	
32	El proveedor debe mantener la integridad de todos los Datos Personales de Microsoft, garantizando que sigan siendo precisos, completos y pertinentes para los fines declarados para los que fueron Tratados.	El proveedor puede demostrar que existen procedimientos para validar los Datos Personales de Microsoft cuando se recopilan, crean y actualizan. El proveedor puede demostrar que existen procedimientos de monitoreo, revisión de la actividad del sistema de información y muestreo para verificar la precisión de forma continua y corregirla, si es necesario. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
	Sección I: Monitoreo y aplicación de la ley	
33	El proveedor tiene un plan de respuesta a incidentes que requiere que el proveedor notifique a Microsoft según los requisitos contractuales o sin demora indebida, lo que ocurra antes, al tomar conocimiento de un Incidente de Datos. El proveedor debe, a petición o según la indicación de Microsoft, cooperar con Microsoft en cualquier investigación, mitigación o reparación del incidente, incluida la facilitación a Microsoft de datos, información, acceso al personal del proveedor o al hardware necesario para llevar a cabo una revisión forense. Nota: Consulte la Guía del programa SSPA para saber cómo notificar un incidente a Microsoft.	El proveedor tiene un plan de respuesta a incidentes que incluye un paso para notificar a los clientes (Microsoft) como se describe en esta sección. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
34	Aplicar un plan de corrección y supervisar la resolución de cada Incidente de Datos para garantizar que se tomen las medidas correctivas adecuadas en el momento oportuno.	El proveedor ha documentado los procedimientos que adoptará para responder a un Incidente de Datos hasta su cierre. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.
35	Cuando Microsoft sea el Responsable del Tratamiento de los Datos Personales de Microsoft, establecerá un proceso de queja formal para responder a todas las quejas de protección de datos que impliquen Datos Personales de Microsoft.	El proveedor dispone de medios para recibir quejas relacionadas con los Datos Personales de Microsoft y cuenta con un procedimiento de quejas documentado para atender las reclamaciones. El proveedor proporcionará pruebas documentales a Microsoft cuando se le solicite.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad	
	El proveedor debe establecer, implementar y mantener un programa de seguridad de la información que incluya políticas y procedimientos, para proteger y mantener seguros los Datos Personales y Confidenciales de Microsoft de acuerdo con las buenas prácticas de la industria y como lo exige la Legislación. El programa de seguridad del proveedor debe cumplir con las normas que se indican a continuación, requisitos 36-52. Si los Datos Personales de Microsoft son PHI, el proveedor también deberá realizar una evaluación periódica técnica y no técnica en respuesta a los cambios ambientales y operativos que afecten a la seguridad de la PHI que establezca hasta qué punto las políticas y procedimientos del proveedor cumplen los requisitos de la Norma de Seguridad de la HIPAA.	Una certificación ISO 27001 válida es un sustituto aceptable de la Sección J. Póngase en contacto con la SSPA para aplicar esta sustitución. Nota: Deberá proporcionar la certificación.
36	Realizar evaluaciones anuales de la seguridad de la red que incluyan lo siguiente: ▪ la evaluación de los riesgos y vulnerabilidades potenciales para la confidencialidad, integridad y disponibilidad de los Datos Personales de Microsoft y la aplicación de medidas para reducir los riesgos, ▪ revisión de cambios importantes en el entorno, como un nuevo componente del sistema, la topología de la red o las reglas del cortafuegos, y ▪ el mantenimiento de los registros de cambios.	El proveedor ha documentado las evaluaciones de la red, los registros de cambios y los resultados de los escaneos. Mediante los registros de cambios requeridos se debe hacer un seguimiento de los cambios, proporcionar información sobre el motivo del cambio e incluir el nombre y el cargo del aprobador designado.
37	El proveedor debe definir, comunicar y aplicar una política de dispositivos móviles que proteja y limite el uso de los Datos Personales o Confidenciales de Microsoft a los que se accede o que se utilizan en un dispositivo móvil.	El proveedor demuestra el uso de una política de dispositivos móviles conforme cuando el Tratamiento de Datos Personales o Confidenciales de Microsoft requiere el uso de un dispositivo móvil.
38	Se debe rendir cuentas de todos los activos utilizados para apoyar la Realización de la Actividad, los cuales deben tener un propietario identificado. El proveedor es responsable de mantener un inventario de estos activos de información, establecer el uso aceptable y autorizado de los activos, y proporcionar el nivel apropiado de protección para los activos a lo largo de su ciclo de vida.	Inventario de los activos de los dispositivos utilizados para apoyar la Realización de la Actividad, la seguridad y las operaciones. El inventario de estos activos debe incluir lo siguiente: ▪ ubicación del dispositivo, ▪ clasificación de los datos del activo, ▪ registro de la recuperación de activos tras la finalización del contrato de trabajo o del contrato comercial, y ▪ registro de la eliminación de los soportes de almacenamiento de datos cuando ya no son necesarios.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
39	Establecer y mantener procedimientos de gestión de derechos de acceso para evitar el acceso no autorizado a cualquier Dato Personal o Confidencial de Microsoft que esté bajo el control del proveedor.	El proveedor demuestra que ha implementado un plan de gestión de derechos de acceso que incluye lo siguiente: ▪ procedimientos de control de acceso, ▪ procedimientos de identificación, ▪ procedimientos de bloqueo después de intentos fallidos, ▪ cierre automático de sesión tras inactividad, ▪ parámetros robustos para seleccionar las credenciales de autenticación, y ▪ desactivación de las cuentas de los usuarios (incluidas las cuentas utilizadas por empleados o subcontratistas) en caso de cese de la relación laboral en un plazo de 48 horas, ▪ controles sólidos de las contraseñas en cuanto a su longitud y complejidad que eviten su reutilización. El proveedor demuestra que cuenta con un proceso establecido para revisar el acceso de los usuarios a los Datos Personales y Confidenciales de Microsoft, y que aplica el principio de mínimo privilegio. El proceso incluye lo siguiente: ▪ funciones de los usuarios claramente definidas, ▪ procedimientos para revisar y justificar la aprobación del acceso a las funciones, y ▪ comprobación de que los usuarios de las funciones con acceso a los datos de Microsoft tienen una justificación documentada para estar en el grupo/función.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
40	Definir e implementar procedimientos de gestión de parches que den prioridad a los parches de seguridad para los sistemas utilizados para tratar Datos Personales o Confidenciales de Microsoft. Estos procedimientos incluyen lo siguiente: ▪ realizar escaneos de vulnerabilidad todos los meses con un informe de cumplimiento de alto nivel que muestre los escaneos mensuales de los 12 meses anteriores, ▪ enfoque de riesgo definido para priorizar los parches de seguridad, ▪ capacidad para manejar e implementar parches de emergencia, ▪ aplicabilidad al sistema operativo y al software del servidor, como el servidor de aplicaciones y el software de base de datos, ▪ documentar el riesgo que el parche mitiga y hacer un seguimiento de las excepciones, y ▪ requisitos para la retirada del software que ya no cuente con el soporte de la empresa creadora.	El proveedor puede demostrar que ha implementado un procedimiento de gestión de parches que cumple con este requisito y que cubre, como mínimo, lo siguiente: ▪ Asignación de la gravedad para informar sobre la priorización (las definiciones de gravedad están documentadas). ▪ Procedimiento documentado para implementar parches de emergencia. ▪ Validar que no se utilicen sistemas operativos que ya no sean compatibles con la empresa creadora. ▪ Registros de gestión de parches que hagan un seguimiento de las aprobaciones y excepciones.
41	Instalar software antivirus y antimalware en los equipos conectados a la red utilizados para el Tratamiento de los Datos Personales y Confidenciales de Microsoft, incluidos los servidores y las computadoras de producción y de capacitación, a fin de protegerlos contra los virus potencialmente dañinos y las aplicaciones de software malintencionado. El software antivirus y antimalware debe parchearse y actualizarse con frecuencia. Actualizar diariamente las definiciones del antimalware o según las indicaciones del proveedor de antivirus/antimalware. Nota: Esto se aplica a todos los sistemas operativos, incluido Linux.	Existen registros que demuestran que el uso de software antivirus y antimalware está activo. Nota: Este requisito se aplica a todos los sistemas operativos.
42	Los proveedores que desarrollan software para Microsoft deben incorporar los principios de seguridad por diseño en el proceso de construcción.	Los documentos de especificaciones técnicas de los proveedores incluyen puntos de control para la validación de la seguridad en sus ciclos de desarrollo.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
43	Se debe emplear un programa de Prevención de Pérdida de Datos ("DLP", por sus siglas en inglés) para evitar intrusiones, pérdidas y otras actividades no autorizadas a nivel de aplicación, sistema e infraestructura. Los datos deben estar debidamente clasificados, etiquetados y protegidos, y el proveedor debe monitorear los sistemas de información en uso en los que se Traten Datos Personales o Confidenciales de Microsoft para evitar intrusiones, pérdidas y otras actividades no autorizadas. El programa DLP, como mínimo: ▪ exige el uso de Sistemas de Detección de Intrusiones ("IDS", por sus siglas en inglés) estándar basados en el host, la red y la nube si se conservan los Datos Personales o Confidenciales de Microsoft, ▪ requiere la implementación de Sistemas de Protección contra Intrusiones ("IPS", por sus siglas en inglés) avanzados configurados para monitorear y detener activamente la pérdida de datos, ▪ requiere un análisis del sistema (en caso de que sea vulnerado) para garantizar que también se resuelva cualquier vulnerabilidad residual, ▪ describe los procedimientos necesarios para monitorear las herramientas de detección de riesgos del sistema, ▪ establece un proceso de respuesta y gestión de incidentes que debe llevarse a cabo cuando se detecta un Incidente de Datos, y ▪ requiere comunicaciones (con todos los empleados del proveedor y los subcontratistas que se encuentren fuera de la Actividad del proveedor) en relación con la descarga y el uso no autorizados de Datos Personales o Confidenciales de Microsoft.	Programa DLP documentado e implementado con procedimientos para prevenir intrusiones, pérdidas y otras actividades no autorizadas (y como mínimo, todos los elementos especificados en esta sección).

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
44	Comunicar de inmediato los resultados de la investigación de la respuesta a incidentes a la alta dirección y a Microsoft.	Deben existir sistemas y procesos para comunicar a Microsoft los resultados de la investigación de la respuesta a incidentes.
45	Los administradores de sistemas, el personal de operaciones, la gestión de terceros y cualquier persona que acceda a Datos Personales o Confidenciales de Microsoft deben recibir una capacitación anual en materia de seguridad.	Se debe establecer un programa de capacitación anual en materia de seguridad que incluya lo siguiente: ▪ Capacitación sobre respuesta a incidentes, y simulaciones de incidentes y mecanismos automatizados para facilitar una respuesta eficaz ante las situaciones de crisis. ▪ Creación de conciencia sobre la prevención de incidentes, incluida la protección de contraseñas, la supervisión de inicios de sesión, los riesgos relacionados con la descarga de software malintencionado y otros recordatorios de seguridad pertinentes. ▪ Si los datos personales de Microsoft son PHI, el programa de concienciación y capacitación debe incluir recordatorios de seguridad y abordar la supervisión del inicio de sesión y la protección de las contraseñas. ▪ Contenido actualizado periódicamente.
46	El proveedor debe garantizar que los procesos de planificación de copias de seguridad protegen los Datos Personales y Confidenciales de Microsoft del uso, acceso, divulgación, alteración y destrucción no autorizados.	El proveedor puede demostrar procedimientos documentados de respuesta y recuperación que detallen cómo la organización gestionará un evento perturbador y mantendrá su seguridad de la información a un nivel predeterminado basado en los objetivos de continuidad de la seguridad de la información aprobados por la dirección. El proveedor puede demostrar que ha definido e implementado procedimientos para realizar periódicamente copias de seguridad, almacenar de forma segura y recuperar eficazmente los datos críticos.

#	Requisitos de Protección de Datos para proveedores de Microsoft	Pruebas del cumplimiento
	Sección J: Seguridad (continuación)	
47	Establecer y probar los planes de continuidad del negocio y de recuperación de desastres.	Un plan de recuperación de desastres debe incluir lo siguiente: ▪ Criterios definidos para determinar si un sistema es crítico para el funcionamiento de la empresa del proveedor. ▪ Enumerar los sistemas críticos en función de los criterios definidos que deben ser objeto de recuperación en caso de un desastre. ▪ Procedimiento de recuperación de desastres definido para cada sistema crítico que garantice que un ingeniero que no conozca el sistema pueda recuperar la aplicación en menos de 72 horas. ▪ Pruebas y revisiones anuales (o más frecuentes) de los planes de recuperación de desastres para garantizar que los objetivos de recuperación se puedan cumplir.
48	Autenticar la identidad de una persona antes de concederle acceso a los Datos Personales o Confidenciales de Microsoft y garantizar que el acceso se limite al ámbito de actividad de la persona en particular que tiene permiso para apoyar la Realización de la Actividad.	Asegurarse de que todos los identificadores de usuario sean únicos y que cada uno tenga un método de autenticación estándar de la industria, como Azure Active Directory. El acceso elevado (privilegios administrativos o de otro tipo) debe requerir el uso de un segundo factor, como una tarjeta inteligente o un autenticador basado en el teléfono. Programa documentado de seguridad de la información que cubra el proceso para garantizar que el acceso de todos los empleados y subcontratistas del proveedor a los Datos Personales o Confidenciales de Microsoft no sea mayor o de mayor duración de lo necesario para apoyar la Realización de la Actividad.
49	El proveedor debe proteger todos los datos Tratados en relación con la Realización de la Actividad en tránsito a través de las redes con un cifrado que utilice Transport Layer Security ("TLS") o Internet Protocol Security ("IPsec"). Estos métodos se describen en los documentos NIST 800-52 y NIST 800-57; también puede utilizarse una norma industrial equivalente. El proveedor debe rechazar la entrega de cualquier Dato Personal o Confidencial de Microsoft transmitido por medios no cifrados.	El proceso de creación, implementación y sustitución de certificados TLS o de otro tipo debe definirse y aplicarse.
50	Todos los dispositivos de los proveedores (computadoras portátiles, estaciones de trabajo, etc.) que accedan o manejen Datos Personales o Confidenciales de Microsoft deben emplear un cifrado basado en disco.	Cifrar todos los dispositivos para cumplir con BitLocker u otra solución de cifrado de disco equivalente en el sector para todos los dispositivos cliente utilizados para manejar Datos Personales o Confidenciales de Microsoft.

51	Deben existir sistemas y procedimientos (que utilicen los estándares actuales del sector, como los descritos en la norma NIST 800-111) deben estar implementados para cifrar en reposo (cuando se almacenan) todos y cada uno de los Datos Personales o Confidenciales de Microsoft. Los ejemplos incluyen, entre otros: ▪ datos de credenciales (por ejemplo, nombre de usuario o contraseñas), ▪ datos de los instrumentos de pago (por ejemplo, números de tarjetas de crédito y cuentas bancarias), ▪ datos personales relacionados con la inmigración, ▪ datos de perfiles médicos (por ejemplo, números de historiales médicos o marcadores o identificadores biométricos, como el ADN, las huellas dactilares, las retinas y los iris, los patrones de voz, los patrones faciales y las medidas de las manos, utilizados con fines de autenticación), ▪ datos de identificación emitidos por el Gobierno (por ejemplo, números del seguro social o de la licencia de conducir), ▪ datos pertenecientes a clientes de Microsoft (por ejemplo, SharePoint, documentos de O365, clientes de OneDrive), ▪ material relacionado con productos de Microsoft no anunciados, ▪ fecha de nacimiento, ▪ información sobre el perfil de los niños, ▪ datos geográficos en tiempo real, ▪ dirección personal física (no comercial), ▪ números de teléfono personales (no comerciales), ▪ religión, ▪ opciones políticas, ▪ orientación o preferencia sexual, ▪ respuestas a la pregunta de seguridad (por ejemplo, autenticación de 2 factores, restablecimiento de la contraseña), ▪ nombre de soltera de la madre.	Comprobar que los Datos Personales y Confidenciales de Microsoft estén cifrados en reposo.

Sección J: Seguridad (continuación)		
52	Anonimizar todos los Datos Personales de Microsoft utilizados en un entorno de desarrollo o prueba.	Los Datos Personales de Microsoft no deben utilizarse en entornos de desarrollo o de prueba; cuando no haya otra alternativa, deben anonimizarse para evitar la identificación de las Personas Interesadas o el uso indebido de los Datos Personales. Nota: Los datos anonimizados son distintos de los datos seudonimizados. Los datos anonimizados son aquellos que no se refieren a una persona física identificada o identificable en los que la Persona Interesada no es identificable o deja de serlo. Si los datos personales de Microsoft son PHI, la anonimización debe cumplir la norma de eliminación de identificación de la HIPAA.

Glosario

"**Representante Autorizado**" es una persona que tiene el nivel adecuado de autoridad para firmar en nombre de la empresa. Esta persona deberá tener los conocimientos necesarios sobre privacidad y seguridad, o haber consultado a un experto en la materia antes de presentar su respuesta a una acción del programa SSPA. Asimismo, el hecho de agregar su nombre al formulario de SSPA implica certificar que han leído y entendido los DPR.

"**RDPUE**": Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo del 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º
1247/2002/CE.

"**Trabajador Autónomo**" es la persona que realiza tareas o servicios a solicitud, que se contratan a través de plataformas digitales u otros medios.

"**RGPD**" se refiere al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

"**Requisitos de Protección de Datos de Privacidad**" significa el RGPD, el EUDPR, las Leyes Locales de Protección de Datos de la UE/EEE, la Ley de Privacidad del Consumidor de California, el Código Civil de California, sección 1798.100 y siguientes (*"CCPA"*), la Ley de Protección de Datos del Reino Unido de 2018 y cualquier ley, reglamento y otros requisitos legales relacionados o subsiguientes aplicables en el Reino Unido, y cualquier ley, reglamento y otros requisitos legales aplicables relacionados con (a) la privacidad y la seguridad de los datos; o (b) el uso, la recopilación, la conservación, el almacenamiento, la seguridad, la divulgación, la transferencia, la eliminación y otro tratamiento de cualquier Dato Personal.

Las **"Cláusulas Tipo de la UE" y "Cláusulas Contractuales Tipo"** son (i) las cláusulas tipo de protección de datos para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen un nivel adecuado de protección de datos, descritas en el artículo 46 del RGPD y aprobadas por la Decisión de la Comisión Europea (UE) 2021/914 del 4 de junio de
2021; (ii) cualquier cláusula contractual tipo adoptada en el futuro por (a) la Comisión Europea, (b) el Supervisor Europeo de Protección de Datos y aprobada por la Comisión Europea, (c) el Reino Unido en virtud de la Ley Federal General de Protección de Datos del Reino Unido, (d) Suiza en virtud de la Ley Federal de Protección de Datos de Suiza, o (e) por un Gobierno en una jurisdicción distinta de Suiza, el Reino Unido y las jurisdicciones que comprenden la Unión Europea o el Espacio Económico Europeo, donde las cláusulas rigen la transferencia internacional de datos personales, que se incorporarán y serán vinculantes para el proveedor a partir del día de su adopción.

"Alojamiento de Sitios Web" se refiere a un servicio de alojamiento de sitios web es un servicio en línea que crea o mantiene sitios web en nombre de Microsoft bajo el dominio de Microsoft; es decir, el proveedor proporciona todos los materiales y servicios necesarios para crear y mantener un sitio y lo hace accesible en Internet. El "proveedor de servicios de alojamiento web" o "web host" es el proveedor que proporciona las herramientas y los servicios necesarios para que el sitio o la página web se vean en Internet, como, por ejemplo, las cookies o las balizas web (web beacons) para la publicidad.