Revista Peruana de Computación y Sistemas 2024 6(1):23-37
https://doi.org/10.15381/rpcs.v6i1.28531

ISSN Online: 2617-2003
Facultad de Ingeniería de Sistemas e Informática
Universidad Nacional Mayor de San Marcos

Artículo de Contribución

Factores que inciden en la Seguridad de la Información en las Organizaciones

Factors that affect Information Security in Organizations

Samir B. Rodriguez-Barrantes[1,a]

[1] Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática. Lima, Perú

[a] E-mail: samir.srb@gmail.com, ORCID: https://orcid.org/0000-0003-1199-0284

Resumen

Se revisan los factores de seguridad de la información, debido a que en los últimos años (2021, 2022 y 2023), los delitos informáticos van en aumento, pasando de 415 millones a 463 millones de personas, que alguna vez han experimentado un delito cibernético, a pesar de haber diversos estudios, recomendaciones, reglamentos, marcos de trabajo, entre otros. Por ello es importante identificar los factores que inciden en la seguridad de la información; el presente es una investigación básica, puesto que acrecentara los conocimientos teóricos referentes a la seguridad de la información, y tiene un enfoque cualitativo, empleando entrevistas; al término del mismo se identificaron factores tecnológicos, humanos, normativos y de comunicación, estos resultado son en base a la realidad peruana, las cuales se centrara en las perspectivas que poseen los directores de tecnología de información y Oficiales de seguridad.

Palabras clave: Seguridad de la información, directores de tecnología de información, oficiales de seguridad, ISO/IEC 27001, COBIT, PMBOK, ISACA.

Abstract

It is validated in this research paper that cybercrime has increased from 415 to 463 million people victim of this type of delinquency despite diverse studies, regulations and recommendations, frameworks, among others. Therefore, it is important to identify the factors that affect information security. The current paper is a basic research, since it will increase theoretical knowledge regarding data safety, and it also has a qualitative approach using interviews based on local Peruvian reality focused on the perspectives held by the Chief Information Officer and Chief Security Officer. At the end of it, the factors identified that affect information security: technological, human, regulatory and communication related.

Keywords: Information security, Chief information officer, Chief Security Officer, ISO/IEC 27001, COBIT, PMBOK, ISACA.

Recibido: 09/11/2023 - Aceptado: 07/06/2024 - Publicado: 30/06/2024

Citar como:
Rodriguez-Barrantes, S. (2024). Factores que inciden en la Seguridad de la Información en las Organizaciones. Revista Peruana de Computación y Sistemas, 6(1):23-37. https://doi.org/10.15381/rpcs.v6i1.28531

1. Introducción

En la actualidad, con la irrupción de las nuevas tecnologías y/o tecnologías emergentes, los riesgos ante nuevas amenazas se han incrementado para las diversas empresas en el Perú, tal como lo evidencia la tesis: "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001"[1] en donde se indica, "la información de las empresas, tienen más riesgos con el paso del tiempo, esto debido a muchas fuentes, por ejemplo fraudes, vandalismos, catástrofes naturales entre otras, adicionalmente indica que los ataques de hackers y virus cada vez son más comunes".

El presente trabajo de investigación ha tomado como documento de consulta a la Norma Técnica Peruana de Seguridad de la Información NTP-ISO/IEC 27001:2014, la cual proporciona los requisitos necesarios para establecer, implementar mantener y mejorar continuamente un sistema de gestión de seguridad de la información, encargado de preservar la confidencialidad, integridad y disponibilidad de la información, aplicando un proceso de gestión de riesgos.

El objetivo de la presente investigación es identificar y analizar los factores que afectan la seguridad de la información en las organizaciones y qué relación tienen estos, analizándolos mediante una estrategia metodológica cualitativa, teniendo en cuenta los factores externos e internos a la organización.

Según se desprende, los delitos informáticos se incrementaron en los últimos años, tal y como lo demuestra la empresa Norton en sus reportes: "2021 Norton Cyber Safety Insights Report Global Results" [2], "2022 Cyber Safety Insights Report" [3] y "2023 Norton Cyber Safety Insights Report"[4], en todas estas se evidencia que las personas afectadas por cibercrímenes fueron incrementándose, de 415 millones en el 2021 a 463 millones en el 2022. En la Encuesta Global de Seguridad de la Información (EGSI) -comparativo México- [5], se indica que el 56 por ciento de empresas siguen aumentando sus niveles de riesgo. Todo ello, a pesar de haber diversos estudios, recomendaciones y reglamentos para la seguridad de la información, como son: La Norma Técnica Peruana NTP-ISO/IEC 27001:2014, La Ley de delitos informáticos (Ley N° 30096) [6], La Ley de protección de datos personales (Ley N° 29733) [7], COBIT, PMBOK, Ernst & Young, entre otros.

En el presente trabajo, se puede indicar que "El objetivo de la seguridad es que la información sea integra, siempre esté disponible, sea visible solo para las personas necesarias, poseyendo un debido control de acceso" [8]. Lo cual, en el ámbito de gobierno de tecnologías de información, la seguridad de la información también viene siendo tratada, específicamente en COBIT 5.0 para la seguridad de la información, en los procesos: APO13 Gestionar la seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar los servicios de seguridad [9], los cuales nos dan un lineamiento inicial sobre un sistema de gestión de seguridad donde se describe la seguridad en un contexto empresarial.

Adicionalmente hay estudios realizados por empresas consultoras, en el cual dan recomendaciones para aliviar los riesgos en la seguridad de la información, desde el lado netamente informático, por ejemplo la empresa consultora Ernst & Young, ha desarrollado una estrategia transformacional de seguridad de la información, en el cual detalla 5 aspectos que se debe considerar, para tener una óptima gestión en la seguridad de las organizaciones, indicando en base a su experiencia, cuales son las amenazas más relevantes que enfrenta las organizaciones [5].

En el ámbito de la seguridad de la información en Perú, ésta se ve respaldada por la Ley que se promulgó en el año 2013 sobre delitos informáticos (Ley N° 30096) así como la Ley de protección de datos personales (Ley N° 29733). En ese sentido, se deben tener en cuenta las recomendaciones brindadas por Sebastián Bortnik - CISM, Gerente de Educación y Servicios en ESET Latinoamérica, "La ley de delitos informáticos es el principio de una situación que se va a tener que enfrentar los próximos años, y es que se necesita que por un lado los abogados se especialicen en situaciones técnicas y por otro lado también los técnicos se deberían especializar en cuestiones legales" [10].

Debido a que se está evaluando, los factores que afectan la seguridad de la información en las organizaciones y se ha definido que un factor interno es el personal, según lo citado en la tesis de Borghello, "Seguridad Informática sus Implicancias e Implementación Universidad Tecnológica Nacional, se empleara la documentación relacionada a la cultura organizacional y comportamiento organizacional" [11], "El comportamiento organizacional es un campo de estudio que investiga el impacto que los individuos, los grupos y las estructuras tienen sobre el comportamiento dentro de las organizaciones, con el propósito de aplicar tal conocimiento al mejoramiento de la eficacia de la organización" [12], también hace mención sobre la cultura organización, la cual es definida como "un estado de coherencia entre la persona y los objetivos y el sistema de valores de la empresa y tiene consecuencias que se expresan en términos de cantidad o calidad del trabajo y la posibilidad o no de movilidad".

2. Revisión de la literatura

2.1 Evolución Histórica del término Seguridad:

Se puede definir el termino seguridad de una manera objetiva como, "la ausencia de amenazas materiales concretas" [13].

Basándose en estudios realizados en Colombia, se puede indicar que la sociedad tiene como unidad fundamental a la familia, "esta fue la razón por la cual huir ya no era una opción, y es así como se crearon estrategias, en donde el atacante tuviera más perdidas que ganancias para así evitar la confrontación", ejemplo

colocar trampas en el ingreso para que el atacante corra el riesgo de quedar atrapado, al momento de ingresar o salir. Al especializarse la seguridad, nacen dos tipos, seguridad externa e interna, de las que se distinguen dos subtipos de seguridad, privada y pública, esta última nace con el gobierno y las fuerzas armadas. En este punto es importante parafrasear la tesis presentada por Diana Hernandez, en la cual hace referencia a la definición del objetivo de la Seguridad, en el cual Fayol menciona: "resguardar personas y/o cosas contra desastres naturales o atentados sociales, que atenten contra los mismos, es decir todo lo que se pueda hacer para dar paz y tranquilidad (Peace of Mind) a la persona" [14].

2.2 Definición de Seguridad:

El concepto de Seguridad tiene distintos significados para cada persona y/o compañía, esta es la razón por la cual, en muchos casos, es etiquetada de forma errónea, lo cual hace complicado poder justificar herramientas y decisiones en base a la ambigüedad que presentan desde el concepto.

"En la actualidad las Seguridad es compleja y requiere de mucha especialización para que pueda ser cumplida". Para poder esquematizar la seguridad se puede dividir en 3 actores, el poseedor del valor: Cuidante o poseedor; Un elemento a proteger: Valor; un aspirante a poseedor: Competidor–Agresor. Otra definición de seguridad es "constante competencia entre el aspirante a poseedor y el poseedor para tener el valor".

Se debe considerar que los aspirantes pueden ser interno: los cuales son los mismos colaboradores, que sienten que su interés debe estar por encima de los intereses de la compañía. aspirante externo: son los clientes que buscan poseer en valor de la empresa.

"La seguridad en un problema de antagonismo y competencia. Si no existe un competidor–amenaza el problema no es de seguridad" [15].

2.3 Análisis de Seguridad Informática:

Con el fin de realizar un debido análisis para la seguridad de la información, se debe partir por entender cuáles son las características principales de la información, para realizar esto se parte definiendo "Dato" sirve para deducir las consecuencias derivadas de un hecho.

La información es la adquisición de conocimientos, que permiten ampliar o precisar lo que se posee sobre una materia determinada [16].

Se debe tener en cuenta que la información siempre tiene un valor determinado, el cual es subjetivo a la persona que lo posea.

Se considera que hay información pública y privada, esto se divide en razón a quienes pueden analizar y revisarla, se debe considerar que el énfasis en la seguridad de la información debe de recaer en la privada, ya que se tratan de información sensible y delicada.

Se puede decir que cualquier cosa o persona que comprometa un sistema, se puede definir como Amenaza, esta se puede analizar antes que suceda, en el mismo momento que ocurre y después de sucedido, estas formas de análisis forman parte de las políticas de la empresa.

Según el PMBOK [17], el cual indica que la gestión de los riesgos del proyecto este estrechamente vinculada, con temas como la planificación de la gestión, el análisis, la planificación de respuesta a los riesgos, el monitoreo y control. La principal finalidad de la gestión de riesgos es que haya más probabilidad de eventos positivos, y se reduzcan los eventos negativos (probabilidad).

Entre los puntos más resaltantes de PMBOK, se pueden destacar los siguientes: planificar la gestión de riesgos, es como realizar las actividades de gestión; identificar los riesgos, se determinar cuáles son los riesgos; realizar el análisis cualitativo de riesgos, se prioriza los riesgos a fin de tomar acción; realizar el análisis cuantitativo de riesgos, se analiza numéricamente cada riesgo; planificar la respuesta a los riesgos, se realiza y pone sobre la mesa opciones y acciones para disminuir los riesgos; monitorear y controlar los riesgos, se crea planes de acción ante cada eventualidad.

Cada acción realizada trae consigo el esfuerzo de uno o varios colaboradores, dependiendo de cada plan implementado, se debe de tener claro que la seguridad de la información no es únicamente de una área o áreas dentro de la compañía, sino que es de toda la empresa.

Se debe entender que los riesgos no se ven en pasado o presente, estos siempre son visualizados en futuro, el cual tiene efecto en algún objetivo de la empresa. Los motivos pueden ser varios, por ejemplo, una restricción o una condición, la cual tiene una posibilidad de volverse en un objetivo fallido.

La Seguridad se puede medir por qué tan libre de peligro se encuentra la información, se debe estar conscientes que esto último es difícil de conseguir en su totalidad, por lo que solo se habla de fiabilidad y esta última se define como la probabilidad que todo salga como se espera.

Con la finalidad que un sistema y/o información sea fiable, se debe tener en cuenta y garantizar puntos como que la información sea integra, privada y se tenga un control de acceso.

En enero del 2001 en instalaciones de Cybsec S.A., Julio C. Ardita director de Cybsec S.A. Security System y ex–Hacker, indica que a los intrusos se les puede agrupar en base a su conocimiento; Clase A: el 80% personas que bajan programas de internet y prueban; Clase B: es el 12% más peligroso, compilan programas, pero no saben programar, prueban y detectan las vulnerabilidades de las victimas; Clase C: es el 5%. personas que ya tienen definido que atacar y por qué; Clase D: el 3% ingresan y únicamente buscan la información que requieren.

Para ir subiendo todos los niveles por lo general toman entre 4 a 6 años, lo cual requiere mucho trabajo y dedicación [18].

Se tiene diversos tipos de ataques, los cuales pueden ser ataques pasivos: en este no se modifica la comunicación, solo se monitorea y roba información; ataques activos: en estos si se modifican la comunicación, es realizado por personas con un alto conocimiento (hacker), estos ataques se dividen en 5 tipos: interrupción: hace que el sistema quede fuera de servicio; Intercepción: acceder a un sistema no autorizado; Modificación: modificación de los datos y por consiguiente la información; Fabricación: duplicidad del objeto atacado a fin que sea complicado distinguirlos; Destrucción: destruir la misma.

Para implementar un adecuado control y seguridad, se debe tener en cuenta que debe haber un equilibrio entre la seguridad y la usabilidad, un ejemplo que se podría dar es una casa que tiene 5 puertas con 3 chapas cada una, lo cual hace que sea segura y difícil que ingresen a robar, pero se debe pensar que tan fácil seria para el usuarios salir cuando tenga que ir a comprar, es por este motivo que se debe tener un especial cuidado en encontrar un especial equilibrio entre usabilidad y seguridad.

Existen 3 grandes grupos de personas consideradas amenazas contra la seguridad de la información de una compañía o institución, el primer grupo son considerados los activistas o terroristas cibernéticos, aquellos que atacan a entidades, en favor a algún movimiento por ejemplo Anonymous, el segundo grupo es el crimen organizado, grupo de hackers que tienen como objetivo robar dinero. Por último, el tercer grupo son las mismas empresas, aquellas que utilizan la información para la competencia de sus marcas, dañar reputación etc. [19].

2.4 Estándares de Regulaciones de Seguridad de la Información:

Existen varios estándares de seguridad, pero el más usado y completo desde la perspectiva de varios autores es la familia ISO 27000, el cual posee entre sus principales puntos la gestión de activos, la seguridad asociada al recurso humano, la gestión de comunicaciones y operaciones, el control de acceso y la gestión de la continuidad del negocio, el cual se encuentra en "planear hacer verificar actuar" PHVA; sus siglas en ingles son PDCA, plan do check act, este estándar está enfocado en la mejora continua, el mismo que forma parte de la teoría Total Quality Management (TQM), el cual fue considerado por Walter A. Shewhart y desarrollado por Edwards Deming, también se puede considerar estándares tales como Magerit, Marion, Mehari y Octave son más específicos, estos son para una región y un tipo de empresa, no son tan robustos como los primeros [20].

Surgen otras opciones, que apoyan a optimizar la gestión del área de TI. Una de las más conocidas es Cobit, este es un marco de referencia de gobierno de TI, el cual busca la unión de TI y el negocio [9]. Otra opción es ITIL, en este marco se reúnen las mejores prácticas de servicio de TI [21]. Ambos son frameworks los cuales ayudan en la gestión con TI, los mismo que deben de interpretase y adaptarse a nuestra realidad y no aplicarse al pie de la letra. Además, se integran perfectamente con ISO 27000, la cual esta concebidos sobre el ciclo PHVA, las cuales se pueden apoyar la una con las otras. Un modelo adicional es COSO, el cual surge para dar respuesta a los riesgos de fraude, blanqueo o robo que aparecen en la banca, por las malas intenciones de algunas organizaciones, que utilizan en su beneficio los procedimientos del propio banco. El marco COSO en riesgos sirve como un modelo de control interno de gran utilidad [22].

La familia de normas de SGSI (ISO2700), apoya a las empresas de todo tipo y tamaño a implementar y operar un SGSI, la seguridad de la información queda definida por tres atributos: a) Confidencialidad; b) Integridad; c) Disponibilidad; se puede definir a la seguridad de la información, como la protección de la misma frente a las amenazas.

En lo que respecta a las ISO 27000 se puede encontrar las siguientes [1].

ISO/IEC 27000: Sistema de gestión de seguridad de la información (SGSI), Visión de conjunto y vocabulario.

ISO/IEC 27001: nació el 15OCT2005, posee los requisitos SGSI (Sistema de gestión de seguridad de la información), se originó en la BS 7799-2:2002 en la misma se certifican las empresas por auditores externos.

ISO 27002: nació el 01JUL2007, es para los controles de seguridad de la información, es el nuevo nombre de ISO 17799:2005, cabe indicar que mantiene el 2005 como año de edición. La misma es una relación de buenas prácticas la cual relata objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

ISO/IEC 27003: La presente es un guía de buenas prácticas para la implementación de los sistemas de gestión de seguridad de la información (SGSI).

ISO/IEC 27004: Nos ayuda en la gestión de seguridad de la información, métricas.

ISO/IEC 27005: Es la gestión de riesgos de seguridad de la información.

ISO/IEC 27006: Requisitos para entidades que auditan y certifican sistemas de gestión de seguridad de la información (SGSI).

ISO/IEC 27007: Guía para la auditoria de los sistemas de gestión de seguridad de la información (SGSI).

ISO/IEC 27008: Guía para los auditores de controles de seguridad de la información.

ISO/IEC 27010: Gestión de seguridad de la información en comunicaciones intersectoriales e interorganizacionales.

ISO/IEC 27011: Guía para la gestión de seguridad de la información para las organizaciones de telecomunicaciones basada en la norma ISO/IEC 27002.

ISO/IEC 27013: Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.

ISO/IEC 27014: Gobernanza de la seguridad de la información.

ISO/IEC TR 27015: Guía para la gestión de seguridad de la información para servicios financieros.

ISO/IEC TR 27016: Gestión de seguridad de la información. Economía organizacional.

2.5 Legislación Peruana de Delitos Informáticos

En septiembre del 2013 se promulgo la ley de delitos informáticos (Nro. 30096) [6] y actualizado para corregir ciertas generalidades en marzo del 2014, esta ley inicia la regularización a nivel nacional de sanciones, para las conductas ilícitas que afectan sistemas y datos informáticos mediante el uso de tecnologías de la información o de la comunicación.

Todo lo mencionado en el párrafo precedente, pone especial énfasis en acceso ilícito a la información, lo cual va en contra de la integridad de la protección a niños, niñas y adolescentes, contra proposiciones con fines sexuales mediante TI. y la Interceptación información, Fraude entre otros.

Mediante DECRETO SUPREMO Nro. 003-2013-JUS, publicado 22 de marzo de 2013, se aprobó el reglamento de la Ley Nro. 29733, ley de protección de datos personales, el reglamento es de aplicación al tratamiento de los datos personales contenidos en un banco de datos. En tal sentido, se debe aplicar a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren.

Para un mejor contexto, se procederá a visualizar los datos obtenidos en la encuesta denominada “Seguridad de la información en un mundo sin fronteras” [5]. y los datos obtenidos en 2012, en la encuesta denominada, “Salir de la niebla para entrar en la nube”, las cuales fueron realizadas por la Consultora Ernst & Young sobre 273 empresas de distintos sectores de actividad y países.

La presente encuesta resalta los siguientes resultados, “El 40% de las empresas estudiadas consideran como un problema grave la seguridad informática; la inversión en seguridad informática se encuentra entre el 4% - 10% del gasto total del área de TI; el 83% de las compañías indica que no tomo acción legal después de un ataque cibernético; El 72% no reconoce que fueron víctimas de un ataque; El 79% indica que los ataques solo vienen del exterior; El 66% indica que el crecimiento del e-comerce se limita por la seguridad de la información; El 80% sufrió un ataque el último año; pero sólo el 33% tiene mapeado como detectar los ataques; Sólo el 39% usa software de seguridad y el 20% lo usa de forma avanzada.

Según Ernst & Young en su artículo Seguridad de la información en un mundo sin fronteras, propone una estrategia de transformacional de seguridad la cual es la siguiente:

Tener identificados los riesgos reales, definirlos y ver como cuadra con el riesgo de TI; definir cuales con las aplicaciones core de la empresa y quienes son los responsables de estas; ver cuáles son las amenazas de estas y crear estrategias para evitarlas.

Es muy frecuente que las personas de seguridad indiquen que están saturados con asuntos críticos que requieren atención inmediata y no pueden ser proactivos. Esto es una oportunidad de mejora, ya que para liberar tiempo y recursos, se debe de atacar la root cause, y así eliminar trabajo de bomberos en la empresa.

Tener identificados las aplicaciones core e información sensible de la compañía es el punto clave y punto de partida para que el negocio sepa dónde poner la mayor cantidad de esfuerzo.

Entre las amenazas más constantes, según la Consultora Ernst & Young; se puede señalar las siguiente:

Las amenazas internas, la reciente publicación de WikiLeaks de los cables diplomáticos clasificados del departamento de estado de Estados Unidos es un excelente ejemplo de los ataques maliciosos internos.

Computación en nube, debido a la coyuntura la mayoría de las empresas están utilizando este medio por costos y flexibilidad, pero se debe notar que estos aumentan la posibilidad de ser atacados, por lo cual se debe tener un mayor cuidado en estas herramientas, esto al inicio es poco alentador, pero los beneficios a futuro son mayores.

Dispositivos móviles, en estos días la mayoría de las personas tiene 2 o más dispositivos móviles (Celulares, Tablet, PC entre otros), esto ocasiona que el ingreso de la información de la empresa se realice con equipos ajenos a esta y también puede darse el caso que el ingreso de información, sea remoto, ósea fuera de las instalaciones de la empresa. Está claro que esto aumenta productividad de la empresa, pero también abre una puerta que puede ser difícil de controlar, por lo cual es de suma importancia definir pro y contras en este tema y tomar medidas para reducir los riesgos.

Redes sociales, las mismas son una realidad y van en aumento, por lo cual es importante que los colaboradores tengan bien claro, como utilizar estas pueden ayudar o poner en riesgo a la empresa, en muchas oportunidades revelar información confidencial, o extravió de la misma es consecuencia del mismo colaborador, por lo cual es muy importante concientizar al mismo, sobre los beneficio y riesgos que se tienen en las redes sociales, tanto para el como para la empresa.

Se debe tener en cuenta, que la seguridad de la información es una tarea de todos los colaboradores de la empresa y esto debe ser informado en todo momento por la alta dirección, con la finalidad que todos tengan esto claro.

En la actualidad, adelantarse a las amenazas no es suficiente para tener un sistema de gestión de seguridad, lo más importante es identificar la información sensible de la empresa, para así empezar a desarrollar planes y estrategias para asegurar la misma.

Una vez que se tenga identificada la información core de la empresa, se debe entender, ¿quién la usa?, ¿para qué es importante?, ¿Qué pasaría si se pierde dicha información?, para que en base a esto se pueda definir las herramientas necesarias.

Un punto importante luego de haber definido la información sensible para la compañía, se debe cuantificar los riesgos encontrados, para de esta manera medir el riesgo, en este análisis se define la probabilidad que esto suceda y el daño que ocasionara.

Como resultado de todo lo realizado, se obtendrá un plan para proteger la información, se debe de tener claro que siempre habrá violaciones y ataques, por ende, se deberá de retroalimentar el plan constantemente.

2.6 COBIT 5.0

CobIT 5 [23], ve a la empresa como un TODO, que en ocasiones revisa aspectos que no son visibles por la organización, esto ayuda a validar aspectos nuevos y sugerir cuando es necesario un nuevo proceso, norma u otra opción, esto es lo más resaltante de este marco de trabajo, desde el punto de vista de seguridad todo esto debe de ser considerado en la empresa, ya que es necesario adoptar el enfoque de verlo como un TODO a la empresa [9].

COBIT 5 es la siguiente generación de guía de ISACA, sobre el gobierno de TI en empresas, Proporciona un marco de gestión integral de TI, para apoyar a las organizaciones en su labor de alcanzar objetivos estratégicos de gobierno.

Tener un especial cuidado con la información y más aun con los datos personales, es sumamente crítico en estos momentos para todas las empresas y más aun con la reglamentación de la protección de datos (RGPD), para los dueños de las empresas la seguridad de la información como para todos es de suma importancia.

Para poder tener una debida ciberseguridad en la empresa, se requiere tener medidas adecuadas que brinden seguridad frente a amenazas externas e internas, no se puede estar seguros al 100%, pero si se debe tener un punto de equilibrio entre usabilidad y seguridad.

2.7 Gestión de Riesgos

Se puede definir como un desarrollo de reconocimiento, análisis, evaluación y categorización de riesgos, para posteriormente implementar mecanismos que puedan controlarlos [24], esto ayuda a tener estructurado los riesgos que posee la empresa, se puede definir gestión de riesgos, como mecanismos por el cual se identifica, controla y reduce el riesgo a un costo aceptable, para lograr todo esto primero se debe tener la probabilidad de que suceda y cuando se de, que valor tendría, como siguiente definición se puede indicar, la forma de analizar, valorar y calificar el riesgo, para en base a esto poder implementar planes de acción.

3. Propuesta

De acuerdo con el análisis realizado en la formulación del problema, la seguridad de la información es un tema que debe ser tratado con mucho cuidado en las organizaciones. En base a las entrevistas realizadas a especialistas, se han identificado 4 factores que son factor personal, factor tecnológico, factor normativo y factor de comunicación, según las entrevistas se debe priorizar lo referente al personal, que fue definido como el más importante por los entrevistados, esto es debido a que todos los demás factores previamente identificados, recaen directamente en el factor humano. Por tal motivo se debe tener especial cuidado en puntos clave como lo son, la ética del personal, el clima laboral, capacitaciones, remuneraciones e identificar como motivar al trabajador para que este, sienta que es retribuido correctamente por su labor diaria, por todo lo anteriormente mencionado se debe tener mucho cuidado y dar la debida importancia a la cultura organizacional la cual es definida como, "conocimiento compartido de los empleados de una organización: cómo se hacen las cosas aquí. Estas creencias, valores, normas y filosofías determinan cómo funcionan las cosas. Definen el estándar esperado de comportamiento, habla, presentación de sí mismo y deberes." [25], al enfocarnos y poseer un estado coherente entre el personal, los valores éticos y los objetivos de la empresa, se puede estar dando un paso importante hacia la seguridad de la información y a que todos estén dirigiéndose en un mismo camino. Como segundo paso se debe de atacar el factor normativo, tanto externo como interno. En el caso de las normas externas se debe considerar la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, La Ley de Delitos Informáticos (ley Nro. 30096) [6], La Ley de Protección de Datos Personales (Ley 29733) [7], las cuales deben de ser tomadas como punto de partida para generar las normas internas de la empresa, de tal forma que estas se vean complementadas y respaldadas entre sí, y de esta manera evitar que las normas internas vayan en contra de las normativas externas, esto debido a que podría causar confusión entre los empleados de la empresa e incluso ir en contra de los valores éticos de los colaboradores de la institución.

Luego de tener estos dos factores bien identificados, se puede proceder a cubrir el factor de la comunicación que es detallada por COBIT, en el proceso EDM03: asegurar que la tolerancia al riesgo de la empresa sean entendidos articulado y comunicado; y que el riesgo para el valor de la empresa es identificado y gestionado [9], la cual según los entrevistados, indican que esta es importante debido a que la seguridad de la información recae en toda la organización y no solamente en una área determinada, es por esta razón que todas las áreas deberían de tener bien identificada el plan estratégico de la empresa, como el reglamento de la misma, para apoyar de forma efectiva a la seguridad de la información.

Finalmente en lo referente al factor tecnológico, se debe ser cauteloso y probar debidamente todos los pros y los contras de la tecnología deseada, a fin de evaluar el momento adecuado para adquirirla, teniendo en cuenta la diferencia entre las nuevas tecnologías y tecnologías emergentes (nuevas tecnologías son las que recién están siendo creadas, pero tecnologías emergentes son aquellas

que están siendo utilizadas y han alcanzado un grado de madures), por lo tanto se debe de evaluar las tecnologías emergentes y ver si el personal, está apto para usar estas tecnología e invertir constantemente en capacitar al personal para el uso adecuado de las mismas.

De acuerdo a todo lo antes mencionado se puede llegar a la conclusión, que el factor humano con suficiente capacitación técnica y valores éticos, podría ser un mejor mecanismo de defensa, de ello se desprende, después de realizar un breve análisis sobre todas las entrevistas realizadas los CSO y/o CIO, los cuales coinciden en estos 4 factores y en el cual, el factor humano es la base sobre el que se soportan el factor normativo y el factor tecnológico y de la interacción de los 3 factores (humano, normativo y tecnológico), dan origen al factor de comunicación, como se muestra en la figura 1.

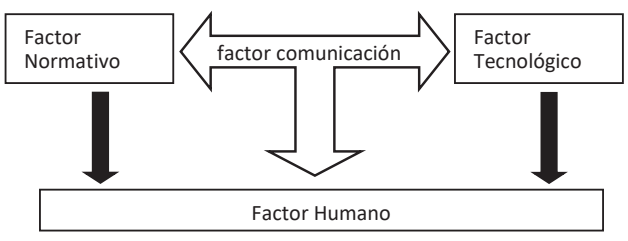
El procedimiento de recolección de datos empleados, se realiza mediante entrevistas, que es una técnica en la que el entrevistador, solicita información de una persona o de un grupo, en este caso el tipo de entrevista empleada es una entrevista de profundidad, en la cual se estableció inicialmente una lista de temas, relacionados con las preguntas de investigación y lo recogido en la revisión de la literatura, las entrevistas se desarrollaron en la empresa del entrevistado, para lo cual se realizó coordinaciones previas a fin de poder realizar las entrevistas, con la menor interrupción posible, adicionalmente a esto, cabe resaltar que al finalizar la entrevista se solicitó, la recomendación de la siguiente persona a entrevistar, lo cual facilito las coordinaciones para la siguiente entrevista.

Debido a que se trata de una investigación cualitativa, esta no posee criterios de cientificidad como la investigación cuantitativa (validez, confiablidad, etc.), respecto de que los criterios de rigor científico deberán referirse tanto al diseño de la investigación y recolección de datos, como al análisis de datos a la elaboración y presentación de los resultados. Adicionalmente no es posible aplicar los criterios de rigor de la investigación cuantitativa sin modificarlos, por tal razón se debe validar en los siguientes aspectos:

Densidad, solicitando información detallada en las entrevistas; profundidad, referido a la triangulación realizada, en donde varias entrevistas con similares preguntas dan similares resultados; Transparencia, se mostrará las entrevistas realizadas y el método empleado para la obtención de los resultados mostrados, debido a que uno de los principios que guía el muestreo es la saturación de datos, esto es, hasta el punto en que ya no se obtiene nueva información y ésta comienza a ser redundante la recolección de datos finaliza en cuanto ya no se encontrará nuevos factores que afecten la seguridad de la información.

Figura 1

Interacción de los factores de seguridad
Fuente. Fuerte propia



El análisis de la información se realizó mediante el software Atlas.TI, en el cual se colocó las entrevistas trascritas y se logró codificar las citas más importantes, las cuales se muestran en el punto de validación.

4. Validación

Luego de haber realizado las entrevistas, centradas en la opinión que tenían los entrevistados, respecto a la seguridad de la información, los factores que están relacionados a la seguridad de la información, cómo estos factores están relacionados entre sí y cuales son realmente los factores más importantes, desde su punto de vista, se identificaron siete familias de conceptos o códigos durante el desarrollo del respectivo análisis. Se procederá a detallar las familias encontradas durante el análisis de datos.

- En la familia "factor comunicación", agrupa los comentarios relacionados con los factores de comunicación y su importancia dentro de la organización.
- En la familia "factores Humanos", se especifican las expresiones del entrevistado sobre el personal y temas relacionados, como la cultura organizacional, capacitaciones brindadas, y remuneración.
- En la familia "factores normativos", se agrupan las opiniones del entrevistado con respecto de los factores de carácter normativo y el papel que juegan las normas y aspectos legales en la seguridad de la información.
- En la familia "factores tecnológicos", se consolidan las percepciones del entrevistado sobre los avances tecnológicos, el uso de estos en la seguridad de la información y como afectan directamente en la organización.
- En la familia "factor importante", se indica cual es el factor más importante que debe ser observado por la organización.
- En la familia "conceptos", el entrevistado mencionó como define el termino seguridad de la información y que tan importante es para la organización.
- En la familia "Expectativas", se indican las expectativas que se posee en cuanto a las nuevas tecnologías y como afectaran estas a la seguridad la información.

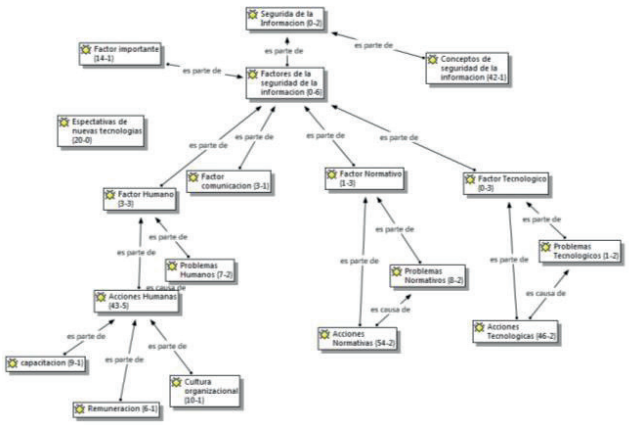
Toda esta información y las cantidades respectivas se puede visualizar en el apéndice 1: Familias de código.

Antes de pasar a las preguntas de investigación, se presenta la red obtenida con el software Atlas.ti, en la

cual se muestra toda la codificación realizada, así como las relaciones que se posee, como se puede observar en la figura 2: Red de codificación y relaciones en seguridad de la información, está conformada por 3 grandes temas, los conceptos de seguridad de la información, la cual fue indicada por los mismos entrevistados, los factores que afectan la seguridad de la información y en base a la experiencia de los entrevistados cual delos factores es al que se debe de poner mayor importancia, además los factores están subdivididos en acciones y problemas, los que se han presentado a lo largo de su experiencia, debido a que los entrevistados han indicado que el factor más importante a tener en cuenta es el factor humano, se ha encontrado factores a mayor detalle en lo referente a cultura organizacional, capacitaciones y remuneraciones.

Figura 2

Red de codificación y relaciones en seguridad de la información
Fuente: Fuerte propia



5. Metodología

5.1 Tipo y diseño de investigación

La presente es una investigación básica puesto que acrecentara los conocimientos teóricos referentes a la seguridad de la información, partiendo de teorías propuestas en diversas investigaciones como lo referente a riesgos, comportamiento organizacional, metodologías propuestas entre otros a fin de lograr una relación entre todas estas a fin de lograr una nueva teoría que las relacione.

La presente investigación tiene un enfoque cualitativo, debido a que se emplearan entrevistas a fin de verificar cuales son las relaciones de diversos factores que afectan la seguridad de la información en las empresas, así como cuáles son los factores que afectan en mayor magnitud la seguridad de la información.

Por alcance es un tipo de investigación descriptiva, ya que se realizará una descripción de todos los factores que afectan la seguridad de la información.

Se empleará datos primarios, los cuales serán tomados en base a cuestionarios y entrevistas realizados a los Chief Security Officer (CSO) y Chief Information Officer-CIO, obteniendo sus percepciones y experiencias en temas de seguridad de la información.

La presente investigación tiene un diseño no experimental ya que no se controlarán las variables que afectan la investigación.

Por la secuencia temporal, será una investigación trasversal, debido a que se implementara una relación de factores que inciden en la seguridad de la información, mas no se realizara una comparación al tener en cuenta los factores y al no tenerlos.

5.2 Unidad de análisis

La unidad de estudio serán los oficiales de seguridad en las organizaciones, en caso de que la organización no cuente con el oficial de seguridad, se procederá a entrevistar a los CIO, ejecutivo encargado del area de informática de las organizaciones (para el presente trabajo se considerara a las medianas y grandes empresas, así como los organismos autónomos del Perú).

5.3 Población de estudio

Todos los CSO's de las medianas y grandes empresas, así como los organismos autónomos, el universo de estas empresas y organismos deben de contar como mínimo con 100 trabajadores y en el caso que la empresa no cuente con el oficial de seguridad – CSO se entrevistara al CIO Ejecutivo encargado del área informática. A diciembre 2023 se cuenta con 3'308,780 empresas según Instituto Nacional de Estadística e Informática - Directorio Central de Empresas y Establecimientos, [26]. y los organismos autónomos son 14 según el portal del estado peruano, para mayor referencia se puede ver el apéndice 2: Organismos autónomos.

5.4 Tamaño de muestra

En el presente trabajo de investigación, la muestra para la metodología a emplear evolucionara con el avance de la investigación, debido a que la decisión sobre el mejor modo de obtener los datos y de quién o quiénes obtenerlos son decisiones que se toman en el campo, pues se desea reflejar la realidad y los diversos puntos de vista de los participantes, por lo que en el tamaño de la muestra cualitativa no hay criterios ni reglas firmemente establecidas, determinándose en base a las necesidades de información, por ello, uno de los principios que guía el muestreo es la saturación de datos, esto es, hasta el punto en que ya no se obtiene nueva información y ésta comienza a ser redundante.

5.5 Selección de muestra

Los entrevistados son oficiales de seguridad CSO, o en el caso que la empresa no posea un oficial de seguridad el entrevistado será el CIO, cabe resaltar que al finalizar la entrevista se solicitó, la recomendación de la siguiente persona a entrevistar, lo cual facilito las coordinaciones para la siguiente entrevista.

5.6 Técnica de recolección de datos

El procedimiento de recolección de datos empleados, se realizaron mediante las entrevistas, que es una técnica en la que una persona (entrevistador), solicita información de otra o de un grupo, en este caso en tipo de entrevista empleada es una entrevista

de profundidad, en la cual se estableció primeramente una lista de temas, en relación con las preguntas de investigación y lo recogido en la revisión de la literatura, las entrevistas se desarrollaron en la empresa del entrevistado, para lo cual se realizaron coordinaciones previas a fin de poder realizar las entrevistas, con la menor interrupción posible.

Los datos serán recopilados mediante entrevistas (Obtener información); la cuáles serán grabadas mediante una grabadora de voz, los mismos que serán trascritos (Capturar, transcribir y ordenar la información); Estos pasos son el resumen de los primeros pasos o fases del análisis de datos cualitativos.

Las respuestas se obtendrán de la entrevista permanecerán de forma anónima y no serán vinculadas a ningún individuo en particular.

5.7 Análisis e interpretación de la información

A fin de analizar las información previamente recopilada, se procederá a agrupar las ideas en conceptos o ideas similares (codificación de la información); luego se relacionan lo encontrado en el punto anterior(Integrar la información), Estos pasos son el resumen de los últimos pasos o fases del análisis de datos cualitativos, para realizar el análisis e interpretación de las información recopilada se empleara la herramienta ATLAS.TI, la cual es empleada para trabajar con datos cualitativos, además se procederá a analizar la información mediante una estrategia metodológica cualitativa, denominada teoría fundamentada (en esta se encarga de descubrir teorías, conceptos, hipótesis y proposiciones partiendo directamente de los datos).

6. Análisis y principales hallazgos

A continuación, se procederá a analizar las preguntas de investigación en base a las citas obtenidas de las entrevistas realizadas, como ya se mencionó anteriormente las entrevistas fueron trabajadas mediante el software Atlas.ti:

6.1 ¿Cuáles son los factores que inciden en la seguridad de la información en las organizaciones?

Los entrevistados indicaron que había diversos factores que afectaban la seguridad de la información, tales como factores humanos (personal, remuneraciones, cultura organizacional, clima laboral, ética, confianza, capacitaciones), factores tecnológicos (nuevas tecnologías, posibilidad que el trabajador lleve su artefactos informáticos al centro laboral), factores normativos (tanto de carácter interno a la institución como: normas y procedimientos, así como externos: legislación), y sobre estos tres antes mencionado nace el factores de comunicación (comunicación entre todos las áreas de la empresa).

Factores humano: De las entrevistas se puede desprender, que para los entrevistados es muy importante que no se rote el personal, otro aspecto importante es la confianza que se debe de tener con el trabajador, debido a que no todo puede estar controlado tecnológicamente, es por eso que se debe tener especial cuidado en la confianza y ética del trabajador, capacitarlo constantemente en lo referente a sus funciones, y en el caso de nuevos trabajadores, preocuparse por la inducción al trabajador, además todo el personal de la institución debe de tener en cuenta que la seguridad de la información no es solo del área de informática, sino de toda la empresa.

Citas referentes al factor Humano.

"la parte de personal en sí, en la parte que es la parte de personal, se tiene que evitar la rotación, la rotación de funciones, por ejemplo, si tú te habrás dado cuenta aquí, no se rota demasiado las funciones de las personas, ya que necesito tener focalizado justamente las acciones de cada persona".

"evitar rotación del personal en varias de sus funciones por qué?, porque si una persona sabe más, de toda la ruta de la información va a poder tener más fuentes o más puertas de donde, poder vulnerar a la base de datos".

"como Recursos Humanos también debes de tener la seguridad de tu información como, por ejemplo, allí también entra un tema de confianza, a que personas tú le vas a designar la función para que tenga el acceso".

"para la institución, la información que maneja es básica es importante, por eso que también acá, como te mencionaba entra un tema de confianza".

"involucrarse con el personal para ver de qué manera también puede actuar, porque también se ve parte de ética, porque, por ejemplo, parte de ética, porque te lo digo, porque si yo considero que la institución me está remunerando mal, lógicamente yo tengo mis necesidades y tengo que ver como obtengo dinero, en este caso específico el xxx como obtiene dinero, a través de xxx su la información, por decirte no? A los xxx, ¿no? Entonces por decirte específicamente si una persona de base de datos, que considera que se le está remunerando mal, que es lo más fácil de hacer para un DBA extraer la información y venderla a un xxx por ejemplo".

"factores humanos, es importante saber cómo está la persona, el personal en relación con la empresa, las motivaciones que pueden tener y conocer la motivación que tiene una persona que está de alguna manera manejando una información confidencial critica de la institución".

"algo que se puede mejorar, pero no manejar, el talento la gente".

"se sabe que las herramientas y todo eso al final el que lo va a usar o emplear de una buena o mala manera seria la persona".

"un factor educativo también, en el sentido que las empresas, deberían de preocuparse, en proporcionar facilidades a sus empleados para que sigan capacitándose, para que sigan estudios, de acuerdo con el giro de la empresa y de acuerdo con la profesión del empleado".

"una empresa contrata un personal, lo primero se debería de hacer es una inducción, entonces en esa inducción de qué manera va a servir, va a servir, para guiar al empleador y decirle mira, nosotros como empresa, se tiene esta misión esta visión estos objetivos".

"porque no se culminó en diciembre, justamente como te decía, porque la mayoría de personal de una empresa cree que solamente lo que respecta a la seguridad de la información, va al área de sistemas y no es así, las personas creen que solamente debería haber normativas o seguridad de la información a todo lo que está guardado, dentro de una computadora, todo lo que este guardado dentro de la base de datos, pero no es así".

"son consiente, porque saben que la mayoría de las empresas no tiene un plan de seguridad de la información integral, esa es la palabra integral, lo tiene para determinadas áreas, pero no para todos".

"el avance tecnológico, el cambio tecnológico es constante, entonces, así como adquieres nuevos productos, estos productos también tiene sus vulnerabilidades y si tu no estas correctamente capacitado, educado en la utilización de esos productos, expones, por allí tiene su punto débil, que a través. Ese puede ser una puerta, para que cualquier ente externo o interno, pero de otra área de la empresa, este por allí hurgando en tu actividad".

"desgraciadamente todo no lo vas a poder controlar mediante el uso de tecnología, hay también un factor humano y en ese factor humano, entra la ética la moral y la confianza".

"siempre va a haber un personal humano del cual tú vas a tener que depender. Depender no, de confiar".

"no me parece mal adquirir experiencias afuera, pero si me parece mucho mejor que esta persona regrese con estos conocimientos para poder plasmarlo en su país".

Como una subcategoría dentro de factores Humanos, los entrevistados indicaron que un punto clave son las capacitaciones, y el clima laboral.

Citas referentes a las capacitaciones.

"las capacitaciones y el clima laboral, que debe de ir de la mano".

"no tan especializado como tú dices, pero todo depende de la capacitación del personal".

"cuando un empleado entra a trabajar a la compañía se le hace una inducción".

"las capacitaciones de las personas muchas veces las personas no cometen errores".

"entrenamiento de información de comunicar de como son los estándares y procedimientos, las personas tendrán un nivel de entendimiento que permitirá evaluar autónomamente si hacen o no lo correcto".

Ante la pregunta de en qué aspecto se debería de tener más cuidado, respondieron que se debe de poner mucha atención a la cultura organizacional y a la resistencia al cambio por parte de los trabajadores.

Citas referentes a los aspectos a tener cuidado en el factor personal.

"que la mayoría de las empresas se habla de una cultura organizacional, y como se llama, a veces la resistencia al cambio por parte del trabajador".

"Se debe tomar en cuenta es decir si tu no generas un clima laboral amigable dentro de tu compañía cualquier persona que tenga acceso a información muy muy privilegiada puede hacer cualquier tipo de daño".

"las capacitaciones clima laboral la confianza que se le tenga al individuo es muy importante para lo que es seguridad de información".

De la misma forma opinaron sobre problemas que tenían de carácter humano, en el que destaca para un entrevistado, que tener personal calificado es un peligro, debido a que tiene todas las habilidades para vulnerar la seguridad de la información y por consiguiente aquí entra un tema de confianza, ética y moral, adicionalmente el personal no debería de traer sus artefactos tales como laptop, Tablet entre otros al centro de labores, debido a que esto se prestaría a malas interpretaciones sobre el uso que le da a la información.

Citas referentes problemas de carácter humano.

"los más crítico es el personal más que todo porque es personal calificado, no es personal operativo básico, que puede ser personal que no son Ing. de informática, que no tenga el conocimiento de cómo acceder a una base de datos o como romper entiendes una base de datos, es el mayor franco donde se tiene que poner y hacer más trabajo".

"yo pienso que es una desventaja en la seguridad de la información, porque en si la empresa te debe de proporcionar todo tu equipo necesario, con el cual tu pueda trabajar, no veo la necesidad que una, se esté exponiendo, trayendo sus aparatos tecnológicos, porque eso mismo se puede prestar a muchas cosas, por ejemplo, se piense que este viene se jala la información, sabe dios qué puede hacer con la mismas, etc. Etc. si la empresa te da tu equipamiento mínimo necesario, para que trabajes no es necesario que el empleador traiga su equipo tecnológico adicional".

"la misma naturaleza humana es impredecible, se vuelve al mismo tema, al mismo factor, ósea es un círculo".

Un factor del que se comentó constantemente es la remuneración del empleado, en el cual los entrevistados indicaban que el sueldo del trabajador, debe de estar siempre de acuerdo con el sueldo del mercado laboral.

Citas referentes a la remuneración.

"La mala remuneración, ósea el factor económico".

"Luego que realmente el aporte económico, porque hay que ser sinceros uno trabajo porque necesita

dinero, entonces que efectivamente su personal este bien remunerado, de acuerdo con el mercado laboral".

"los sueldos están equilibrándose".

"sería importante invertir un poco más para que la gente".

Factores de comunicación: Otro factor importante que se dio a conocer en las entrevistas y no en la revisión de la literatura es el factor de comunicación ente las diversas áreas de la empresa, ya que se debe de tomar a la seguridad de la información como un todo, la seguridad de la información no es competencia únicamente del área de informática.

Citas referentes al factor de comunicación.

"si se quiere un plan integral de la seguridad de la información, yo creo que es básico la comunicación entre todas las áreas que constituye la empresa".

"si bien es cierto hay un equipo que lidera este tipo de iniciativas, el equipo como tal debe estar compuesto por diferentes áreas".

"compuesto por las diferentes áreas dentro de la compañía y en base a las experiencias de todos estos líderes consolidar un único reglamento un único control que te permita velar la seguridad que se está buscando".

Factores Normativos: Adicionalmente indicaron que un factor a tener en cuenta era el de carácter normativo, indicaron que este factor es importante, debido a que varios de los documentos con que cuentan las instituciones protegen a la información, dándonos pautas de hasta donde se puede brindar la información y quienes son los autorizados a tenerla, limitando el trasporte de la misma, también se planteó la idea que la seguridad de la información debería de estar constantemente auditada, de igual forma indicaron que debería de haber una convivencia entre el área legal y el área de informática a fin de poder legislar mejor los problemas informáticos, y por parte de informática tener una mayor comprensión de las normas y leyes.

Citas referentes al factor Normativo.

"se tiene documentos normativos, documentos normativos que protegen justamente a la base de datos".

"un acceso a la base de datos de producción, tipo update, no se le puede dar al usuario y como se ampara, protege la empresa, justamente con un documento normativo, ese documento normativo nos apoya para evitar, justamente que otros usuarios internos, nos puedan hacer presión para darle sus privilegios".

"entonces se tiene normativas que también tiene la subgerencia de soporte técnico operativo, que también sea, se basan justamente en esa seguridad, de acceso a los servidores".

"el personal sabe que, dentro de sus contratos, ¿cuál va a ser trato de infidencia de datos no? Cualquier cosa de infidencia dentro del sistema es penalizada tanto administrativamente como penalmente".

"el organismo que está encargado de ver todo eso, debería de hacer unas auditorías a las entidades que consideren principales, que manejo información que es prioritaria, como el caso de esta institución, en el sentido que se preocupen por que realmente el trabajador de la empresa tenga conocimiento, de cómo se debe de manejar la información y hasta qué grado es sensible y esta se puede divulgar, esto como se logra, como tú lo decías, con documento normativos".

"tendría que ver lo que es gobierno electrónico, en caso de nuestra institución".

"Para que la empresa tenga una cultura organizacional necesita documentación, no es cierto, normas, por lo general estas normas tiene base legal, por ende, yo creo que en este caso cada empresa debe de tener una".

"convivencia por así decirlo entre el área legal y área informático para que se complementen para juntos así vean una mejor solución".

"tu como nuevo personal, tienes que acatar, todo lo que se dispone, para esto se tiene estos documentos normativos".

"porque no se culminó en diciembre, justamente como te decía, porque la mayoría de personal de una empresa cree que solamente lo que respecta a la seguridad de la información, va al área de sistemas y no es así, las personas creen que solamente debería haber normativas o seguridad de la información a todo lo que está guardado, dentro de una computadora, todo lo que este guardado dentro de la base de datos, pero no es así".

"son consiente, porque saben que la mayoría de las empresas no tiene un plan de seguridad de la información integral, esa es la palabra integral, lo tiene para determinadas áreas, pero no para todos".

"puede haber una ley que regule la seguridad de información, pero lo importante de la ley es que este reglamentada que quiere decir la ley, la ley puede ser muy ambigua".

"no se tiene una reglamentación clara, para que las unidades de delito informático de los estados de cada gobierno puedan procesar a las personas por este tipo de delitos".

"al leer el artículo de 2 o 3 líneas, por cada línea se le puede dar interpretaciones diferentes, y pues dependerá del nivel de entendimiento que tenga el abogado".

Factor Tecnológico: Inicialmente las empresas colocan cámaras de seguridad, micrófonos entre otros para tener vigilancia continua sobre su información, pero esto es de manera física, adicionalmente a esto cada área de acuerdo a su competencia coloca mecanismos de seguridad, adicionalmente indicaron que el dinero es una limitante para adquirir software o medios que apoyen a la seguridad de la información, es por tal motivo que se opta por productos hechos en casa, un punto clave en la seguridad de la información es registrar toda actividad,

evaluarla y en base a eso realizar cuestionamientos, adicionalmente indicaron que, para que una empresa adopte nuevas tecnología es sumamente importante realizar análisis de factibilidad y ver si dichos productos cumplen con todos los requerimientos mínimos de la institución.

Citas referentes al factor Tecnológico.

"colocando lo controles de acceso, cámaras a nivel seguridad en todos los pisos, todas las sedes, entonces también hay que micrófonos, y grabación para ver, cualquier tipo de problema que haya dentro de la institución".

"cuando se avanza a nivel tecnológico, a nivel de la subgerencia de gestión de base de datos, tiene como función salvaguardar lo que es la información generada en el registro único, se tiene que ver, tener en cuenta lo principal, cualquier cambio que pueda hacerse a la base de datos, es lo primero que tiene que tenerse, para eso se tiene que guardar, tablas históricas que nos puedan ayudar a generar, lo que es la trazabilidad de cualquier cambio efectuado".

"el servidor no está tampoco solo, no está asilado en una isla, para que nadie ingrese, si no que se tiene el entorno de lo que son telecomunicaciones y telecomunicaciones también tiene controles de acceso de intrusos hacia el servidor, o hacia lo equipos internos o hacia la red interna, allí es donde se pone la mayor fuerza de acceso contra intrusos".

"telecomunicaciones tiene, programas que monitorean justamente el acceso, y lo tiene XXX entonces en la parte de telecomunicaciones, tiene software especializado justamente para eso".

"se está planteando hacer programas que comiencen a almacenar información acerca de la cantidad de accesos del personal, pero en la parte de registrar, va a tener que llegar una fase en la cual, ya se pueda analizar, justamente estos registros, por ejemplo esos registros, yo sé que XXX, entra a las 10 de la noche a la base de datos buscar una forma de sacar reportes, de que cosa hace a esa hora, analizar y de acuerdo a eso cuestionar, a las personas únicamente, o si no registrarlo como algo histórico, entiendes?? Pero derivado a un control de trabajo, por ejemplo, si yo te digo en la noche tiene que cerrar el archivo nacional para lo que son el padrón electoral, entonces tu agarras y dices muy bien entras al as 12 de la noche, comienzas a genera el padrón electoral, pero en tus logs se ve que estas utilizando el sistema de tramite documentario o el de personal, allí viene el cuestionamiento, porque accediste a tal tabla".

"en el mercado hay N productos, pero lamentablemente como se tiene una base de datos bastante cara esos productos son recontra caros por ejemplo se tiene en Oracle el data base vault y el audit vault y todo eso se licencia por procesador entonces se está hablando de 64 procesadores, ósea licencias por 64 procesadores y valen casi igual que una base de datos, es algo millonario que la entidad, no puede sustentar porque tiene que pagar 12 millones para comprar data base vault para la gran base de datos que se tiene".

"controles que se pueda armar en casa "in house", se va a tener que hacer que se logren justamente con lo que te digo, primero registrar, generar el registro y después del registro generar justamente los cuestionamiento y después de ese cuestionamiento, se va a ver quiénes sestan ingresando o no por ejemplo lo que se realizó, en lo referente a los ingreso en otras pc 's eso ha traído resultado, porque tu veías que ingresaban desde otras Pc 's con sus usuarios inmediatamente saltaba el proceso y ya venía el cuestionamiento, porque ingresaste y el usuario indicaba porque ingreso, daba un a escusa pero ya se tenía registrado, que se había registrado la incidencia justamente la generación de esos registros que nos van a ayudar a tener un mejora continua, en el nivel de seguridad nos va a ayudar poco a poco a salvaguardar, el gran problema como te digo en la base de datos es el personal".

"puede sustentar porque tiene que pagar 12 millones para comprar data base vault para la gran base de datos que se tiene, pero tampoco con esas escusas, se puede dejar de lado la parte de seguridad, entonces esos controles que se pueda armar en casa "in house", se va a tener que hacer que se logren".

"en realidad antes de que una empresa adopte una nueva tecnología, tiene que hacer todo un estudio, tiene que hacer un estudio de, primero la factibilidad económica, la factibilidad operativa, en si antes de decir, yo empresa voy a trabajar con esta tecnología, que ventajas que desventajas voy a tener".

"la empresa, este tome una tecnología porque está de moda, sino porque realmente aplica a su giro de negocio y cumple con las condiciones mínimas necesarias".

"convivencia por así decirlo entre el área legal y área informático para que se complementen para juntos así vean una mejor solución".

"son consiente, porque saben que la mayoría de las empresas no tiene un plan de seguridad de la información integral, esa es la palabra integral, lo tiene para determinadas áreas, pero no para todos".

"en el aspecto tecnológico, todo lo que es informática, se está muy bien, para comenzar creo que se está en un buen porcentaje de avance, porque se tiene áreas especializadas".

"el avance tecnológico, el cambio tecnológico es constante, entonces, así como adquieres nuevos productos, estos productos también tiene sus vulnerabilidades y si tu no estas correctamente capacitado, educado en la utilización de esos productos, expones, por allí tiene su punto débil, que a través. Ese puede ser una puerta, para que cualquier ente externo o interno, pero de otra área de la empresa, este por allí hurgando en tu actividad".

6.2 ¿Cuáles son los factores de seguridad de información implementados con mayor frecuencia en nuestro medio, según las perspectivas de los oficiales de seguridad y/o CIO?

En las entrevistas realizadas, los especialistas coincidiendo, en su mayoría, que los factores más importantes y el que se debe de tener mayor cuidado es en el factor Humano, estos indicaron que al final, todo recae en las personas, y es aquí en donde se debería tener un especial cuidado, teniendo en cuenta temas tales como; remuneración, clima laboral, cultura organizacional.

"actualmente se tiene, demasiadas aberturas hacia la base de datos, entonces eso se tiene que cerrar si tú me preguntas, cuál de los tres puntos se tendría que poner más énfasis, es en la parte del personal, porque la parte de personal puede generar riesgos externos como riegos internos, porque el mismo personal podría generar las puertas de enlace hacia afuera, o de lo contrario jalar información y llevarse información interna".

"que la mayoría de las empresas se habla de una cultura organizacional, y como se llama, a veces la resistencia al cambio por parte del trabajador".

"el factor humano, que para mí es el más importante porque, toda política, toda herramienta, todo software, todo hardware finalmente descansa sobre la confianza que tú, le tengas a una persona".

"se debe trabajar en ambos, pues no vale la pena invertir en las últimas tecnologías, agentes de seguridad, si dentro con los empleados son muy prestos que la información salga de ellos".

"soy partidario de este tema de entrenamientos".

"se invierte mucho en medios masivos informando y entrenando a sus usuarios".

6.3 ¿Cuáles son las expectativas de los CSO, CIO respecto a las nuevas tecnologías y/o tecnologías emergentes?

Los entrevistados indicaron que las tecnologías vienen avanzando a pasos agigantados y es demasiado importante la capacitación del personal, a fin de evitar que con el avance de esta, la seguridad de la información se vea afectada, no obstante un entrevistado indico que es un tanto conservador a adaptar tecnologías emergentes, el resto de entrevistados indico, que existe un riesgo en adaptar las tecnologías emergentes, pero el riesgo es mayor al no adoptarlas y siempre procurar que estas sean probadas previamente, es decir tener referencias del uso de estas (casos de éxito).

"todo depende de la capacitación del personal, tú sabes que el avance tecnológico, el cambio tecnológico es constante, entonces, así como adquieres nuevos productos, estos productos también tiene sus vulnerabilidades y si tu no estas correctamente capacitado, educado en la utilización de esos productos, expones, por allí tiene su punto débil, que a través. Ese puede ser una puerta, para que cualquier ente externo o interno, pero de otra área de la empresa, este por allí hurgando en tu actividad".

"siempre hay un riesgo con las nuevas tecnologías".

"para conectarnos a los sistemas o la base de datos o alguna información que había en la compañía eran pc 's, laptops y no más; hoy en día se tiene los teléfonos celulares, las tablets, inclusive los dispositivos como los biométricos que permiten el acceso a diferentes habitaciones dentro de la compañía y definitivamente son tecnologías que van saliendo y como conformemente también van saliendo, van surgiendo también los nuevos controles de acceso que se puedan tener".

"con la seguridad de información este yo prefiero utilizar o que se utilice donde esté en la institución donde yo elaboro que se utilice estas herramientas que ya estén que sean de probada".

"en la seguridad de información yo soy yo te podría decir que yo en ese aspecto soy muy conservadora yo prefiero utilizar algo bueno conocido".

"se tiene tecnología para todo, y tienen su pro y contra".

"realmente la seguridad de la información al 100% es un ideal, es muy difícil conseguir, y más con los avances tecnológicos tan acelerados".

"como empresa se debe asegurar que se esté en línea y a la par con lo que el mercado ofrece y con el desarrollo de la tecnología".

7. Conclusiones

Se identificaron y analizaron los factores en base a los entrevistados, los cuales indicaron que había diversos factores que afectaban la seguridad de la información, tales como factores humanos (personal, remuneraciones, cultura organizacional, clima laboral, ética, confianza, capacitaciones), factores tecnológicos (nuevas tecnologías, posibilidad que el trabajador lleve su artefactos informáticos al centro laboral), factores de comunicación (comunicación entre todos las áreas de la empresa), factores normativos(tanto de carácter interno a la institución-Normas, procedimientos, como externos, legislación).

Se identificó el factor que el CSO, da mayor prioridad y/o importancia el cual es el factor humano, debido a que recomiendan tener el personal realmente calificado, preparado tanto en conocimiento como en valores, cabe recalcar que en base a las opiniones realizadas por los expertos, el factor más importante en la seguridad de la información es el personal, debido a que al final de todos los controles, normas, e ideas, siempre recaen en el personal, ya que es él, quien controla la tecnología, realiza las normas y reglamentos, por lo tanto dentro del factor humano es trascendental la confianza que se tenga con los trabajadores.

Se identificó que las expectativas frente a las nuevas tecnologías y/o tecnologías emergentes, es que si estas

avanzan a pasos agigantados es demasiado importante la capacitación del personal, a fin de evitar que, con el avance de esta, la seguridad de la información se vea afectada.

Se identificó que existe un riesgo en adaptar las tecnologías emergentes, pero existe un riesgo mayor en no adoptarlas y siempre se debe procurar que estas sean probadas previamente, es decir tener referencias del uso de estas (casos de existo).

Se identificó que la seguridad de la información es una tarea que compete a toda la empresa y no únicamente al área de informática o al área legal de manera aislada, sino que toda la empresa debe de tener conciencia de lo que es seguridad de la información.

La presente investigación tienes un carácter social, ya que servirá de inicio a futuras investigaciones, debido a que plantea 4 factores globales, los cuales deben de tenerse en cuenta para optimizar la seguridad de la información en el Perú, tomando como base a las entrevistas realizadas a expertos de las principales empresas del medio

Referencias

[1] Seclen J.: 'Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001'. Tesis de maestría, Universidad Nacional Mayor de San Marcos, 2016

[2] Norton., '2021 Norton Cyber Safety Insights Report Global Results'

[3] Norton., '2022 Cyber Safety Insights Report'

[4] Norton., '2023 Norton Cyber Safety Insights Report'

[5] Mancera, S.C., 'Perspectiva sobre los riesgos de TI, Seguridad de la información en un mundo sin fronteras' (Ernst & Young, 2011)

[6] El Peruano., 'Ley N 30096, Ley de delitos informáticos', 22 de octubre de 2013

[7] [El Peruano., 'Ley N 29733, Ley de protección de datos personales', 3 de julio de 2011

[8] Aldegani, G.M., 'Seguridad Informática. MP Ediciones. Argentina' 1997, pp 22-24

[9] ISACA.: COBIT 2019 Framework: Governance and Management Objectives', 2021

[10] Bortnik, S. [cxocommunity], '¿Qué tienen en común un abogado y un especialista en seguridad? ESET #cxoderecho 2012', [Archivo de video], https://www.youtube.com/watch?v=1m-5LC0L7x8, accesado 16 enero de 2013

[11] Borghello, C. F.: 'Seguridad Informática sus implicancias e implementación'. Tesis Pregrado, Universidad Tecnológica Nacional, 2002

[12] Robbins S.: 'Comportamiento Organizacional' (Editorial Prentice hall hispanoamericana – México, 2009, 13ra ed.)

[13] Sforza, A., 'La evolución del concepto de seguridad desde una perspectiva internacional', 2023

[14] Hernandez D.: 'Diseño del sistema de gestión de seguridad de la información en Angelcom S.A.'. Tesis Pregrado, Universidad Libre Colombia, 2011

[15] Manunta, G., 'Seguridad: una introducción. Seguridad Corporativa. España', 1995

[16] RAE., 'Diccionario online', https://dle.rae.es/dato, accesado 20 diciembre de 2023

[17] PMI - Project Management Institute., 'A Guide to the Project Management Body of Knowledge (PMBOK® Guide)' (Project Management Institute Inc., 2021, 7ma ed.)

[18] Ardita, J. C., 'Tendencias en seguridad de la información', 12 diciembre de 2012

[19] Bhimani, A. [TEDx Talks], 'Information security: Anish Bhimani at TEDxUConn 2013' [Archivo de video], https://www.youtube.com/watch?v=UPmVTPyE5DM, accesado 20 de octubre 2013

[20] Alarcon F & Orjeda J., 'La gestión de conductas y comportamientos en los usuarios De ti y la concientización en la seguridad de la información en La universidad nacional pedro Ruiz Gallo Chiclayo – Lambayeque'. Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo, 2018

[21] AXELOS., 'ITIL Foundation' (The Stationery Office, 2019, 4ta ed.)

[22] Riveros, A., 'Qué es el marco COSO de Gestión de Riesgos y cómo surge', https://www.ealde.es/marco-coso-riesgos/#:~:text=El%20marco%20integrado%20de%20control,los%20procedimientos%20del%20propio%20banco, accesado 12 enero 2024

[23] ESGinnova., '¿Cómo se relaciona COBIT 5 y la seguridad de la información?', https://www.pmg-ssi.com/2018/12/como-se-relaciona-cobit-5-y-la-seguridad-de-la-informacion/, accesado 12 enero 2024

[24] Valverde, D., 'Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria – 2021'. Tesis de pregrado, Universidad Tecnológica del Perú, 2022

[25] Jauregui, K., 'Cultura organizacional: Razones por las que es importante cultivarla', https://www.esan.edu.pe/conexion-esan/cultura-organizacional-razones-por-las-que-es-importante-cultivarla#:~:text=Las%20empresas%20con%20una%20cultura,a%20hacer%20mejor%20su%20trabajo, accesado 10 febrero 2024

[26] NEI., 'Demografía empresarial en el Perú' (INEI, 2024), pp 2-3

Apéndice

Apéndice 1: Familia de códigos

Análisis	Familia	Código		Citas
General (*)	factor comunicación	Factor comunicación	3	3
	factores Humanos	Acciones Humanas	43	78
		Capacitación	9	
		Cultura organizacional	10	
		Factor Humano	3	
		Problemas Humanos	7	
		Remuneración	6	
	factores normativos	Acciones Normativas	54	63
		factor normativo	1	
		Problemas Normativos	8	
	factores tecnológicos	Acciones Tecnológicas	46	47
		Factores Tecnológicos	0	47
		Problemas Tecnológicos	1	
Especi 01 (**)	factor importante	factor importante	14	14
Especi 02 (***)	Conceptos	conceptos de seguridad de la información	42	42
	Expectativas	expectativas de nuevas tecnologías	20	20

Fuente. Fuerte propia

(*) Análisis General ¿Cuáles son los factores que inciden en la seguridad de la información en las organizaciones?

(**) Análisis especifico N° 01 ¿Cuáles son los factores de seguridad de información implementados con mayor frecuencia en nuestro medio según las perspectivas de los oficiales de seguridad y/o CIO?

(***) Análisis especifico N°02¿Cuáles son las expectativas de los CSO, CIO respecto a las nuevas tecnologías y/o tecnologías emergentes?

Apéndice 2: Organismos autónomos

Ítem	Organismos autónomos
1	Oficina Nacional de Procesos Electorales – ONPE
2	Contraloría General de la República
3	Ministerio Público Fiscalía de la Nación
4	Fuero Militar Policial
5	Defensoría del Pueblo
6	Jurado Nacional de Elecciones – JNE
7	Registro Nacional de Identificación y Estado Civil
8	Universidad Nacional de Cajamarca
9	Tribunal Constitucional
10	Universidad Nacional Intercultural de la Amazonía
11	Universidad Nacional de Ucayali
12	Junta Nacional de Justicia
13	Banco Central de Reserva del Perú
14	Federación Peruana de Cajas Municipales de Ahorro y Crédito