UNIVERSIDAD PERUANA LOS ANDES

Facultad de Ingeniería

Escuela Profesional de Ingeniería de Sistemas y Computación

TESIS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE RIESGOS EN ACTIVOS DE INFORMACIÓN

Autor:
Bach. Miguel Angel Porras Ruiz

Línea de Investigación Institucional:
Ciencias Empresariales y Gestión de los Recursos

Para optar el Título Profesional de:
Ingeniero de Sistemas y Computación

Huancayo - Perú
2019

ASESORES

DR. BALDEON TOVAR MAGNO TEOFILO

ASESOR METODOLOGICO

MG. QUISPE REYES CARLOS FELIX

ASESOR TEMÁTICO

DEDICATORIA

A mis padres por su absoluto apoyo, amor, seguimiento y por ser la fuente de motivación en mi formación profesional.

El Autor

AGRADECIMIENTO

A la entidad Privada DIGITEX PERU SAC, por facilitar los recursos necesarios para el desarrollo de la presente investigación.

A mis Asesores los Ingenieros David Fermín Cerrón León y Carlos F. Quispe Reyes, por su guía en el desarrollo y sus orientaciones en la realización de la presente investigación.

A todos Gracias.

Bach. Miguel Angel Porras Ruiz

HOJA DE CONFORMIDAD DE LOS JURADOS

DR. TORRES LÓPEZ CASIO AURELIO

PRESIDENTE

DR. BUSTINZA ZUASNABAR EDWARD EDDIE

JURADO 01

MG. PACHAS HUAYTAN JORGE VLADIMIR

JURADO 02

ING. GORDILLO FLORES RAFAEL EDWIN

JURADO 03

MG. CARLOS CANALES MIGUEL ANGEL

SECRETARIO DOCENTE

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El problema general de la investigación fue ¿Cuáles son los resultados de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la gestión de riegos en activos de información?, como objetivo general se tuvo que determinar los resultados de la implementación del SGSI en la gestión de riegos en activos de información. La investigación acerca del SGSI de la ISO/IEC 27001:2013 nos permitió distinguir con claridad las ventajas que se obtienen al haberla implementado y la eficacia al alinearse con los procesos de negocio. En la hipótesis general se definió que la implementación del SGSI genera resultados en la gestión de riegos de activos de información. La metodología de la investigación fue Científica del tipo Aplicada, de nivel Explicativo, con diseño de investigación Pre experimental con Pre test y Post test. Se consideró como población a los 114 controles del ANEXO A de la ISO 27001 y como muestra a 70 controles aplicables para el alcance definido, el resultado fue que la implementación del SGSI basado en los controles de seguridad mejoró la madurez de la gestión de riesgos en activos de información y el valor promedio subió de 3,65 a 5,22, se concluye que la implementación del SGSI genera resultados favorables en la gestión de Riesgos de Activos de Información.

Palabras claves: Sistema de Gestión de Seguridad de la Información, SGSI, ISO/IEC 27001:2013, Gestión de Riesgo, Activos de información.

ABSTRACT

The general problem of the investigation was: What are the results of the implementation of the Information Security Management System (ISMS) in the management of risks in information assets? of the ISMS in the management of risks in information assets. The investigation about the ISMS of ISO / IEC 27001: 2013 allowed us to clearly distinguish the advantages obtained by having implemented it and the efficiency of aligning with the business processes. In the general hypothesis, it was defined that the implementation of the ISMS generates results in the management of information asset risks. The methodology of the research was Scientific of the Applied type, of Explanatory level, with Pre experimental research design with Pre test and Post test. The 114 controls of ANNEX A of ISO 27001 were considered as a population and as a sample of 70 applicable controls for the defined scope, the result was that the implementation of the ISMS based on security controls improved the maturity of risk management in information assets and the average value rose from 3.65 to 5.22, it is concluded that the implementation of the ISMS generates favorable results in the management of Information Asset Risks

Keywords: Information Security Management System, ISMS, ISO/IEC 27001:2013, Risk Management, Information Assets.

INTRODUCCIÓN

La Seguridad de la Información es uno de los eslabones más débiles que tienen todas las organizaciones en la actualidad, así mismo las legislaciones a nivel global demandan seguir los estándares de seguridad para garantizar un adecuado tratamiento de la información, esto nos llevó a tener como problema general el siguiente ¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima?, desde ese punto de partida el objetivo de la investigación fue el de determinar los resultados del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima; para lograr el propósito definido se utilizó como metodología al estándar ISO:IEC 27001:2013 específicamente a los controles del Anexo A y se estructuró el desarrollo en base al Ciclo PDCA al tratarse de un Sistemas de Gestión, así mismo se utilizó los niveles de madurez CMMI como métrica.

El desarrollo de la tesis se enmarca en seis capítulos, los cuales se detalla a continuación.

En el primer capítulo se trata el problema de investigación, en el cual se describe el planteamiento del problema y el marco que engloba la problemática que da lugar a la investigación, también se define la justificación, la delimitación y objetivos de la investigación.

En el segundo capítulo marco teórico, se realiza la presentación de los antecedentes nacionales e internacionales que aportan a la presente investigación, así mismo se hace referencia a las diferentes teorías que respaldan el desarrollo; se definieron las hipótesis y las variables de investigación que se utilizaron en el desarrollo de la investigación,

En el tercer capítulo se presenta la metodología de la investigación, se remarcan la población y muestra, se define el instrumento de recolección de datos, así mismo las técnicas de análisis de datos y se mencionan los aspectos éticos de la investigación.

En el cuarto capítulo se describen los resultados de la investigación, así como la contratación con las hipótesis correspondientes.

En el quinto capítulo se presenta la discusión de resultados, en el que se describe el impacto generado al haber culminado la investigación.

Y finalmente se presenta las conclusiones, recomendaciones, referencias bibliográficas y anexos generados a partir de la presente investigación.

CAPÍTULO I

1. EL PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

El crecimiento exponencial de grandes volúmenes de información en el mundo ha desbordado la capacidad de gestión de las organizaciones. Las expectativas de los clientes, de socios, proveedores y partes interesadas se han incrementado cada vez más y exigen servicios rápidos, eficientes y sobre todo seguros con resultados efectivos. Los directivos no disponen de la información adecuada para tomar decisiones y establecer las estrategias más adecuadas de negocio; los procesos en los que intervienen activos de información no se controlan, retienen y preservan. La organización que no sea capaz de enfrentarse al reto de gestionar toda esta información de manera segura en el futuro perderá productividad y no logrará ser competitiva en un mercado global. “17% de las organizaciones afirmaron que su mayor miedo es perder la información de sus clientes” (ERNST & YOUNG, 2019)

“El Perú es segundo, en ser víctimas de ciberataques a nivel Latinoamérica. Esto demuestra que preparados no estamos. ¿Qué hace falta?” (GIL MENA, 2018). Nuestro país no está exento del crecimiento de los procesos que involucran a los activos de información, por lo tanto, los riesgos que involucran a los activos de información se incrementan día a día y al no ser Gestionados de manera oportuna y adecuada se obtiene un resultado negativo de pérdida de información.

El sector privado de nuestro país es uno de los más afectados por los riesgos en los activos de información, el principal motivo es que no existen los procesos de seguridad de información implementados o si existen estos no cumplen con un estándar que garantice una gestión de riesgos eficiente.

“Más que perder dinero con un ciberataque, lo que pierden las empresas es la reputación. El 70% del valor de la empresa se puede ver afecto por un ciberataque.” (GIL MENA, 2018).

En la Empresa de BPO Contac Center Digitex Perú SAC en el Distrito de Surquillo, de la Región Lima - Perú, en el año 2019, se ha identificado ausencia de los procesos y procedimientos de seguridad de la información, es decir hay una clara inexistencia de controles de seguridad de la información en la organización, al realizar el diagnóstico basado en el ANEXO A de la ISO 27001:2013 se evidenció que el nivel de madurez de los 114 controles de seguridad recomendados se encuentran en un estado 45% Inexistente, 1% Inicial, 15% Limitado, 1% Definido y 38% son controles No Aplicables para el alcance de la investigación. Los datos son mostrados a continuación para un mejor entendimiento.

Estado de Madurez	Proporción de Controles de Seguridad de la Información
? Desconocido	0%
Inexistente	45%
Inicial	1%
Limitado	15%
Definido	1%
Administrado	0%
Optimizado	0%
No aplicable	38%

Tabla 1 - Estado de Madurez de los Controles de Seguridad.

Fuente: Elaboración propia de acuerdo a los resultados del diagnóstico basado en los controles del Anexo A de la ISO 27001:2013.

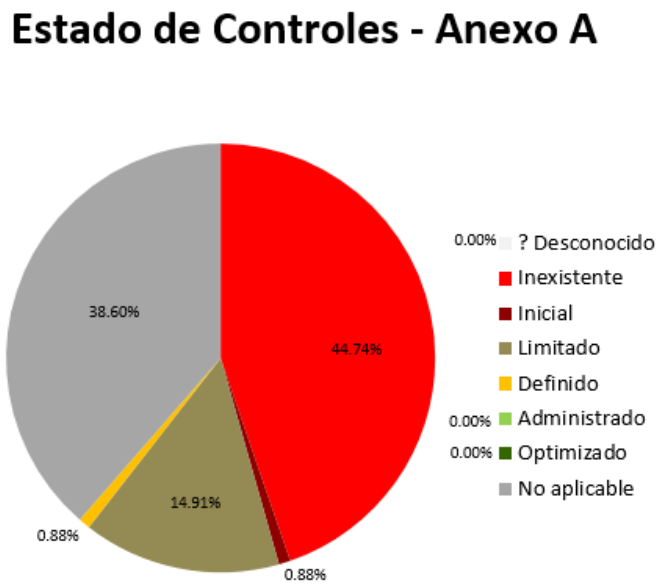


Figura 1 - Gráfica de porcentajes de Nivel de Madurez

Fuente: Elaboración propia se tomó los datos de la Tabla 1.

Continuando con las evidencias obtenidas en el diagnóstico de los 114 Controles del SGSI 41 Controles son No Aplicables y 70 Controles son Aplicables de los cuales 19 están Implementados y 51 NO están Implementados. Se espera que al finalizar la investigación se logre la implementación de la totalidad de controles aplicables.

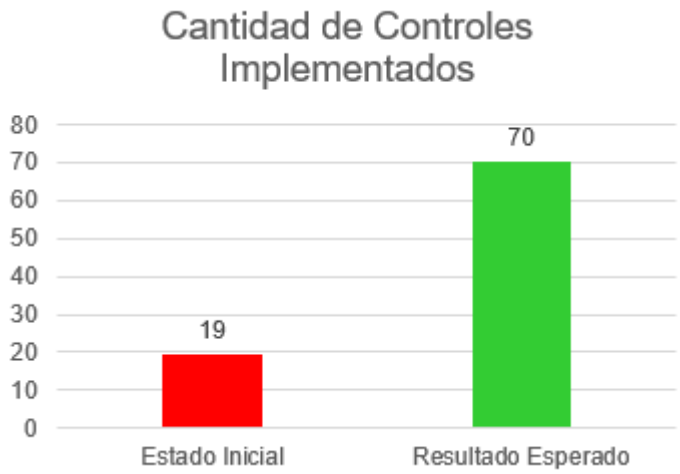


Figura 2 - Gráfica comparativa de controles Estado Actual vs el Resultado Esperado.

Fuente: Elaboración propia.

1.2. Formulación y sistematización del problema

1.2.1. Problema General

¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima?

1.2.2. Problemas Específicos

¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima?

¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima?

¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima?

1.3. Justificación

1.3.1. Social

El diseñar un SGSI para su aplicación generará un ambiente de trabajo más seguro a nivel corporativo, ello sumará valor a la reputación de la empresa Digitex Perú y a la percepción que se tiene de la organización tanto interna como externamente. Internamente los trabajadores afianzarán su confianza con la organización y esto impacta directamente en el clima laboral; de forma externa será percibida como una entidad con la solidez de una organización que cumple con los estándares internacionales para la Seguridad de la Información y será más atractiva para los potenciales clientes.

1.3.2. Teórica

Un eficiente Sistema de Gestión de Seguridad de la Información comienza con estrategias y fundamentos que devienen del

desarrollo de estudios e investigaciones basados en teorías y temas académicos. Un aspecto que se debería destacar es la concientización a los niveles ejecutivos de las organizaciones, de forma tal se consiga lograr un entendimiento adecuado de los riesgos. Por tanto, teóricamente, el presente estudio plantea alinear al SGSI con el proceso general de toma de decisiones en la organización. Este alineamiento resultará clave para que la inversión en seguridad de la información sea adecuadamente percibida por el negocio. Es por ello que se pretende la implementación de los controles necesarios que nos permitirá salvaguardar los activos (información) de la empresa.

1.3.3. Metodológica

La presente investigación busca diseñar una solución a partir la ISO/IEC 27001:2013 orientado a la gestión de riesgo en activos de información para lo cual el pilar angular es el cálculo de los riesgos asociados a los activos de la información en tal sentido es interés aportar el conocimiento de una metodología de acuerdo a los alineamientos de dicha norma para minimizar los riesgos de los activos de información a un nivel aceptable pero con más énfasis sería cumplir con la el modelo de SGSI garantizando un nivel de madurez eficiente y que pueda ser utilizado como referencia para futuras investigaciones.

1.4. Delimitaciones

1.4.1. Espacial

La investigación se centrará en la empresa de BPO Contac Center DIGITEX PERU, ubicada en el departamento de Lima, Provincia de Lima, Distrito de Surquillo.

1.4.2. Temporal

El trabajo de investigación se realiza desde el mes de julio del 2019, ya que los indicadores se obtienen de acuerdo la realidad actual de la empresa.

1.4.3. Económica

El proyecto de tesis se realizó con los recursos propios del investigador y de la Empresa Digitex Perú.

1.5. Limitaciones

Escasa información de antecedentes internacionales y nacionales con respecto a ISO 27001 dentro de los trabajos de investigación.

1.6. Objetivos

1.6.1. Objetivo General

Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima.

1.6.2. Objetivo(s) Específico(s)

Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.

Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.

Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.

CAPÍTULO II

2. MARCO TEÓRICO:

2.1. Antecedentes (nacionales e internacionales)

Nacionales

"En el presente informe de investigación, se pretende verificar la existencia de riesgos en la seguridad de la información que corresponde al Departamento de Admisión y Registro Académico (DARA) de la Universidad Privada Antonio Guillermo Urrelo. Específicamente se trata de la preocupación por los riesgos que puedan encontrar. Esto impulsa a proponer una alternativa para proteger los activos de la información con base en la preservación de los tres principios básicos: la integridad, la confidencialidad y la disponibilidad de la información. Para ello se propone un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como metodología lo señalado en la norma internacional ISO/IEC 27000, que nos provee las estrategias a seguir, teniendo en cuenta la aplicación de los instrumentos de investigación, estas estrategias son: a)definir los procesos core del DARA, b)definir los activos de información que son utilizados en los procesos hallados, los cuales fueron clasificados en tres grupos fundamentales que son la misma información, los equipos e infraestructura que la soportan y las personas que la utilizan; c)identificación de los riesgos que pueden afectar a los activos, d)valoración de los elementos antes mencionados. Concluido el trabajo se concluyó en que los activos del DARA tienen riesgos que podrían afectar la continuidad de los procesos; por ello es necesario definir la propuesta. Se sugiere, además, la implementación inmediata del SGSI, así como la utilización de un software especializado que soporte al SGSI y e te adecuado a la norma para un efectivo control." (ATALAYA VÁSQUEZ, 2016). *"Propuesta de un sistema de seguridad de la información para la oficina de admisión y registro académico de la Universidad Privada Antonio Guillermo Urrelo, 2016."*

*"*En la presente investigación se analizaron y se evaluaron los niveles del riesgo que cuentan seis sedes de una entidad bancaria del Perú en el periodo de investigación de setiembre del 2016 a setiembre del 2017, así como la propuesta realizada sobre la implementación del sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2005 y las etapas del modelo Deming (Plan-Do-Check-Act) y que pueda ser aplicado, mantenido y auditado por la misma entidad, el cual garantiza que se logren los objetivos de la herramienta de seguridad y beneficiar a la empresa en la protección de sus activos, el cual permitirá el cumplimiento de las normas de manera eficiente para la protección de los activos de información.

Para lo cual, la metodología de investigación utilizada fue la de un diseño descriptivo puesto que nos enfocamos en el uso de cuadros y gráficos estadísticos por toda la información recopilada en los usuarios del banco intervinientes en los procesos seleccionados de la investigación.

Investigación que cuenta con resultados favorables para el diseño puesto que con la propuesta de la herramienta de seguridad se encontraron niveles de riesgos medios y altos (72% de riesgos en las áreas de estudio) que son los ideales para realizar la implementación de un sistema de gestión de seguridad de la información en las áreas de Seguridad, Usuarios de banca, TI, Sistemas, Helpdesk, observando en algunos casos que no cuentan con capacitaciones en seguridad de información, con los hallazgos obtenidos se demostró a la Alta Gerencia que el análisis y la evaluación de los riesgos deben ser mitigados o transferidos a un tercero de ser el caso estableciendo políticas de seguridad. En la fase de ejecución del sistema de gestión de seguridad de la información la alta gerencia debe poner mucho énfasis para que la herramienta de seguridad pueda mantenerse y ser monitoreada por especialistas en seguridad con el fin de preservar la confidencialidad, disponibilidad e integridad de los activos.

Estos activos se encuentran dentro de la propuesta, pues su fin es mejorar la seguridad en los procesos seleccionados de la entidad bancaria ya que se consideró que son los procesos más importantes en

la entidad bancaria, del cual se realizó la propuesta en 6 de sus sedes principales y se demostró que es factible la propuesta para tomar acciones sobre la implementación en los procesos y que la entidad bancaria esté al nivel que las demás organizaciones se encuentran con esta herramienta ya implementada." (SALINAS Y VALENCIA, 2017). *"Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú."*

"La seguridad de la información tiene un papel importante en las organizaciones, por ello en el presente informe tesis titulado Sistema de gestión de seguridad de información basado en la norma de ISO 27001 para el Hospital nivel 2 La Caleta, tuvo como propósito mostrar como el análisis de los riesgos y vulnerabilidades a los que está expuesto una organización en la actualidad pueden ser gestionados a través de políticas, procedimientos y mecanismos necesarios para para salvaguardar la información. Para lograr el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI) se hizo la norma ISO 27001:2013 donde proporciono las recomendaciones de las mejores prácticas sobre la gestión de la seguridad de la información las cuales ayudan a todos los interesados y responsables en iniciar, implantar o mantener un sistema de gestión de la seguridad de la información. Con la implementación del SGSI ayudara a gestionar la información esté segura haciendo uso de controles y procedimientos formales que eviten pérdidas de información, las cuales puedan ocurrir por los riesgos y vulnerabilidades a las que está expuesta el Hospital nivel 2 La Caleta. El SGSI ayudara a minimizar las incidencias de alteración o perdida de información que se presenten en los procesos críticos del negocio ocurran con menos frecuencia ayudando establecer una cultura organizacional sobre seguridad de la información y de apoyo a la continuidad del negocio." (CARRANZA Y GÓMEZ, 2018). *"Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001 para el Hospital Nivel 2 - La Caleta"*

“El presente trabajo aborda temas de seguridad e inseguridad en los sistemas informáticos, debido a la incertidumbre sobre la percepción de seguridad existente. Se espera cumplir con la con la confidencialidad, integridad y disponibilidad de la información según ISO 27001, esto se aplica en diversos escenarios de desarrollo de software en forma empírica, estos requerimientos toman mayor valor en la administración de datos de entidades públicas y privadas, debido a que la ausencia de la seguridad en los sistemas desestabiliza el orden social global. El presente trabajo se asocia a un grupo de Mypes muestreadas, en el cual se evidencia la inseguridad, debido al modo de desarrollo de sus procesos para el aseguramiento de la información. En cuanto al método se evaluaron cuatro tratamientos tecnológicos en dos factores fijos midiendo así el grado se seguridad e inseguridad en las Mypes a través del Diseño Factorial Completamente al Azar. Los cuatro tratamientos han sido aplicados al grupo muestral, buscando así identificar diferencias entre los tratamientos. En cuanto a los resultados y según el planteamiento de la hipótesis general, la prueba de Análisis Factorial Univariante resultó no significativo P-valor > nivel se significancia, lo que conlleva a indicar como conclusiones que no es suficiente suministrar tratamientos tecnológicos físicos y lógicos a las Mypes muestreadas, esto si el personal que los dirige no tiene solvencia académica requerida para el desarrollo adecuado de los protocolos de seguridad, planes de gestión tecnológica y sistemas de gestión de seguridad de la información, las cuales contribuyen en el aseguramiento de la información.” (HUANCA SUAQUITA, 2018). *“La falsa percepción en la seguridad de los sistemas informáticos”*

“Existe una necesidad creada por obtener herramientas de verificación del cumplimiento de la aplicación de la “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición” que es de uso obligatorio para las empresas públicas integrantes del Sistema Nacional de Informática y que la Oficina Nacional de Gobierno

Electrónico e Informática ONGEI exige para su aplicación. Las Instituciones que prestan servicios de Salud cuentan con su principal activo de información la Historia Clínica que al ser un documento médico-legal y que tiene que ver con los procesos de atención de los pacientes y el Seguro Social de Salud – EsSalud cuenta con una norma a nivel nacional para cumplimiento en todos sus centros asistencial sobre Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD del año 2014. La hipótesis planteada para esta investigación es que la dimensión Administrativa de la Gestión de la Historia Clínica es la más relevante en la Seguridad de la Información, es por eso que el objetivo busca aplicar una evaluación normativa a la Gestión de las Historias Clínicas y la evaluación de las cláusulas y controles necesarios para la Seguridad de la Información para analizar las características de estos dos aspectos. De los resultados encontrados se observa que en el Hospital II Cajamarca – EsSalud existen un cumplimiento del 60% de las buenas prácticas y recomendaciones sobre la Norma de Gestión de las Historias Clínicas de los pacientes del Centro Asistencial, repercutiendo significativamente en los principios de la Seguridad de la Información como son la confidencialidad, disponibilidad e integridad. Se realiza unas recomendaciones para establecer los mecanismos necesarios para fortalecer la seguridad de la información y proteger los activos relacionados al proceso de la Gestión de las Historias Clínicas, que son el pilar de futuras investigaciones que complementen la Seguridad de la Información y que son el Análisis de Riesgos y la Continuidad del Negocio." (CUEVA Y RÍOS, 2018). *"Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014"*

Internacionales

“El presente Trabajo Final de Especialización se enfoca en detallar las bases principales del Marco de Referencia Unificado en Seguridad de la Información (en adelante, MRU). El cual tiene como objetivo brindar un marco de referencia holístico y práctico para todos aquellos que deseen alcanzar un nivel óptimo en materia de Seguridad de la Información, a medida de su propia organización. El Marco de Referencia se encuentra dirigido a compañías públicas y privadas, instituciones y entes públicos, asociaciones sin fines de lucro y cualquier otro tipo de organización que desee alcanzar la mejora continua en Seguridad de la Información. El MRU facilitará significativamente a las organizaciones el cumplimiento de sus objetivos estratégicos y su misión, a través de la disminución al máximo posible los riesgos de seguridad asociados al activo más preciado que poseen: su información. A su vez, el MRU combinará los requerimientos de toda la documentación fuente mencionada anteriormente con la metodología de gestión de procesos. Esto último permitirá optimizar la eficiencia y la eficacia de todos los procesos relativos a la seguridad de la información de la organización. Por último, el objetivo final del presente trabajo consiste en establecer las bases de un Sistema de Mejora Continua en Seguridad de la Información basado en un marco de referencia holístico que a largo plazo, podría de tomarse como puntapié inicial para la creación de un nuevo estándar dentro del mundo de la Seguridad de la Información.” (FALIVENE, 2018). *“Marco de Referencia Unificado en Seguridad de la Información”*

“La presente tesis detalla la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño utilizando herramientas open source y modelos de desarrollo de mejora continua para dar cumplimiento a un subconjunto de 44 objetivos de control del anexo normativo de la norma ISO27001:2013. La presente tesis no cubre la implementación de los 114 objetivos de control de la norma ISO27001, pero cierra las principales

brechas de seguridad de la información existentes en la organización al cubrir en forma completa el primer ciclo PDCA del SGSI, escogiendo un subconjunto de 44 objetivos de control priorizados por una análisis de brechas, incorporando las recomendaciones de DIPRES y cuya selección se realizó por un comité de seguridad de la Información constituido en el presente trabajo Las políticas y procedimientos son mantenidos en régimen mediante los seis sistemas que forman el SGSI y cuyo objetivo es administrar, monitorear, documentar y mejorar en forma continua la seguridad de la información La metodología que se utiliza esta tesis, se centra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información. Esta tesis propone que la metodología de implementación de SGSI se apoye en la gestión de riesgos, utilizando las guías y buenas prácticas de la norma ISO31000. Con ello los procesos estratégicos de la subsecretaría son clasificados por prioridad según su exposición a los riesgos y su impacto. De este modo se optimiza la asignación de recursos a los proyectos de seguridad de la información, se favorece el aprendizaje y la creación de equipos de trabajo orientados a los objetivos prioritarios, sin que ellos perdieran la visión de conjunto y objetivo final. Como evaluación de la implementación del SGSI y de las políticas y procedimientos de seguridad de la información se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorias fueron totalmente independientes al equipo que diseñó e implementó tanto el SGSI como las políticas y procedimientos de seguridad de la información. Ambas auditorias llegaron a la conclusión que el estado actual de seguridad de la información está en un nivel medio. Esto es un avance sustancial pues al inicio de la presente tesis no había un SGSI ni políticas y procedimientos efectivos para proteger la seguridad de la información. La principal recomendación entregada por las auditorías fue profundizar la difusión de las políticas y procedimientos de seguridad de la información, continuar con la implementación de los restantes 70 objetivos de control

de la norma ISO27001:2013 y realizar una nueva evaluación durante el 2017 del funcionamiento del SGSI, es decir se han implementado los restantes objetivos de control y evaluar el grado de institucionalización de las políticas y procedimientos de seguridad de la información." (YAÑEZ CACERES, 2017). "*Sistema de Gestión de Seguridad de la Información para La Subsecretaria De Economía y Empresas de Menor Tamaño"*

"La Empresa de Consultoría para la Industria Petrolera maneja dentro de su área de Sistemas y Comunicaciones varios procesos relacionados con la Seguridad de la Información, de los cuales se categorizó los más críticos y evaluó la oportunidad de optimizar la gestión de seguridad de la información para el proceso de "Alta y Baja de Usuarios" mediante la aplicación de 114 objetivos de control y controles que dicta la norma ISO 27001:2013, con el objetivo de reducir el porcentaje de reprocesos que se presentaban en este proceso. Para ello se efectuó: Diagnóstico de la situación actual del proceso de "Alta y Baja de Usuarios", desarrollo e implementación de los 114 requisitos aplicables de la norma ISO 27001:2013 al proceso y evaluación de la optimización de desempeño del proceso en base al control de reprocesos efectuados luego de la implementación y la medición de tiempo de cada sub proceso. El resultado fue la implementación de los objetivos de control de la norma ISO 27001:2013 para el proceso de "Alta y Baja de Usuarios", reducir el número de re procesos en un 76,84% y reducir los tiempos de ejecución de ciclo de los subprocesos de "Alta de Usuarios" en un 71% y de "Baja de Usuarios" en un 31%." (CHANGOLUISA, 2017). "*Optimización del Proceso de Alta y Baja De Usuarios a Través De La Implementación De Gestión De Seguridad De La Información, Basado En La Norma ISO 27001:2013 En Una Empresa De Consultoría Para La Industria Petrolera"*

"La gran mayoría de las empresas que conforman el motor laboral de Latinoamérica son de carácter PyMe; es decir, pequeñas y medianas empresas mercantiles, industriales o de otro tipo, que tienen un número

reducido de trabajadores y registran ingresos moderados, pero que en conjunto constituyen un eje fundamental que sustenta la generación de riqueza y desarrollo para nuestros países. Es menester entonces que este nicho empresarial tan importante y a la vez tan vulnerable por sus propias particularidades, proteja mínimamente sus sistemas informáticos, a las personas que los gestionan y a la información que generan, con un impacto manejable para la disponibilidad limitada de recursos que las caracteriza. A partir del análisis de modelos y metodologías existentes, el presente trabajo final de especialización desarrolla un modelo de política de seguridad de la información (PSI) que incluye un sistema de controles de seguridad aplicable a una PyME. Este modelo procura brindar un marco lo suficientemente amplio y flexible como para facilitar la protección de la información de las organizaciones de este tipo, consumiendo una cantidad acotada de recursos." (ÁLVAREZ, 2016). *"Propuesta para La Gestión De La Seguridad de la Información en una Pequeña o Mediana Empresa"*

"Todas las empresas tienen problemas con sus tecnologías de la información esto repercute en afectaciones en su operación cotidiana en servidores, sistemas, redes, servicios y aplicaciones. Existen varias alternativas para solucionar lo anterior, sin embargo, sugerimos por la experiencia adquirida en servicio social la implementación de un Sistemas de Gestión de Seguridad de la Información "SGSI" por ser un sistema más integral además de dar una solución más completa a la seguridad de la empresa y por ende seguir asegurando la continuidad y su correcta operación cotidiana. Y es en este trabajo de investigación a lo largo de sus capítulos se podrá adentrar y apreciar el cómo se gestiona la seguridad de la información, que estándares la rigen, que indicadores y controles de aplican y que metodología se sigue y en una manera general como es que en si es la estructura del Sistema de Gestión de la Seguridad de la Información (SGSI)." (NICASIO, 2015). *"Diseño e Implementación de un Sistemas de Gestión de Calidad en Seguridad de la Información (*SGSI*)"*

2.2. Marco conceptual

2.2.1. Sistema de Gestión de Seguridad de Información (SGSI)

¿Qué es un SGSI?

Un SGSI consiste en las políticas, procedimientos, directrices y recursos y actividades asociados, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar y mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y en los niveles de aceptación de riesgos de la organización diseñados para tratar y administrar los riesgos de manera efectiva. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles apropiados para garantizar la protección de estos activos de información, según sea necesario, contribuyen a la implementación exitosa de un SGSI. (ISO/IEC 27001:2013).

Los siguientes principios fundamentales también contribuyen a la implementación exitosa de un SGSI:

- Conciencia de la necesidad de seguridad de la información.
- Asignación de responsabilidad por la seguridad de la información.
- Incorporar el compromiso de gestión y los intereses de las partes interesadas.
- Mejorar los valores sociales.
- Evaluaciones de riesgos que determinan controles apropiados para alcanzar niveles aceptables de riesgo.
- La seguridad incorporada como elemento esencial de las redes y sistemas de información.
- Prevención activa y detección de incidentes de seguridad de la información.

- Garantizar un enfoque integral de la gestión de la seguridad de la información.
- Reevaluación continúa de la seguridad de la información y realización de modificaciones según corresponda. (ISO/IEC 27001:2013).

2.2.2. Información

La información es un activo que, al igual que otros activos comerciales importantes, es esencial para el negocio de una organización y, en consecuencia, debe protegerse adecuadamente. La información puede almacenarse en muchas formas, incluyendo: forma digital (por ejemplo, archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo, en papel), así como información no representada en forma de conocimiento de los empleados. La información puede transmitirse por diversos medios, incluidos: mensajería, comunicación electrónica o verbal. Cualquiera sea la forma que tome la información, o el medio por el cual se transmite, siempre necesita la protección adecuada. (ISO/IEC 27001:2013).

En muchas organizaciones, la información depende de la tecnología de la información y las comunicaciones. Esta tecnología es a menudo un elemento esencial en la organización y ayuda a facilitar la creación, el procesamiento, el almacenamiento, la transmisión, la protección y la destrucción de información. (ISO/IEC 27001:2013).

2.2.3. Seguridad de la información

La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información. La seguridad de la información implica la aplicación y gestión de controles apropiados que implica la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito y la continuidad del negocio

sostenido, y minimizar las consecuencias de los incidentes de seguridad de la información. (ISO/IEC 27001:2013).

La seguridad de la información se logra mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos elegido y gestionados mediante un SGSI, que incluye políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados. Estos controles deben especificarse, implementarse, monitorearse, revisarse y mejorarse cuando sea necesario, para garantizar que se cumplan los objetivos comerciales y de seguridad de la información específicos de la organización. Se espera que los controles de seguridad de la información relevantes se integren perfectamente con los procesos comerciales de una organización. (ISO/IEC 27001:2013).

2.2.4. Gestión

La administración involucra actividades para dirigir, controlar y mejorar continuamente la organización dentro de las estructuras apropiadas. Las actividades de gestión incluyen el acto, la manera o la práctica de organizar, manejar, dirigir, supervisar y controlar los recursos. Las estructuras de gestión se extienden de una persona en una organización pequeña a jerarquías de gestión que consisten en muchos individuos en grandes organizaciones. (ISO/IEC 27001:2013).

En términos de un SGSI, la administración implica la supervisión y la toma de decisiones necesarias para lograr los objetivos comerciales a través de la protección de los activos de información de la organización. La gestión de la seguridad de la información se expresa a través de la formulación y el uso de políticas, procedimientos y pautas de seguridad de la información, que luego se aplican en toda la organización por todas las personas asociadas con la organización. (ISO/IEC 27001:2013).

2.2.5. Sistema de gestión

Un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. En términos de seguridad de la información. (ISO/IEC 27001:2013).

Un sistema de gestión permite a una organización:

- Satisfacer los requisitos de seguridad de la información de los clientes y otras partes interesadas.
- Mejorar los planes y actividades de una organización.
- Cumplir con los objetivos de seguridad de la información de la organización.
- Cumplir con los reglamentos, la legislación y los mandatos de la industria. y
- Gestionar los activos de información de manera organizada que facilite la mejora continua y el ajuste a los objetivos organizacionales actuales. (ISO/IEC 27001:2013).

2.2.6. Establecer, monitorear, mantener y mejorar un SGSI

2.2.6.1. Descripción general

Una organización necesita llevar a cabo los siguientes pasos para establecer, monitorear, mantener y mejorar su SGSI:

a) Identificar activos de información y sus requisitos de seguridad de información asociados
b) Evaluar los riesgos de seguridad de la información y tratar los riesgos de seguridad de la información.
c) Seleccionar e implementar controles relevantes para gestionar riesgos inaceptables.

d) Monitorear, mantener y mejorar la efectividad de los controles asociados con los activos de información de la organización.
e) Para garantizar que el SGSI esté protegiendo efectivamente los activos de información de la organización de forma continua, es necesario que los pasos a) ad) se repitan continuamente para identificar cambios en los riesgos o en las estrategias u objetivos comerciales de la organización. (ISO/IEC 27001:2013).

2.2.6.2. Identificación de los requisitos de seguridad de la información

Dentro de la estrategia general y los objetivos comerciales de la organización, su tamaño y distribución geográfica, los requisitos de seguridad de la información pueden identificarse mediante la comprensión de lo siguiente:

a) Activos de información identificados y su valor.
b) Necesidades comerciales de procesamiento de información, almacenamiento y comunicación.
c) Requisitos legales, reglamentarios y contractuales. (ISO/IEC 27001:2013).

2.2.6.3. Evaluación de riesgos de seguridad de la información

La gestión de los riesgos de seguridad de la información requiere una evaluación de riesgos adecuada y un método de tratamiento de riesgos que puede incluir una estimación de los costos y beneficios, los requisitos legales, las preocupaciones de las partes interesadas y otras entradas y variables, según corresponda. (ISO/IEC 27001:2013).

La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos según los criterios de aceptación de riesgos y los objetivos relevantes para la organización. Los resultados deben

guiar y determinar la acción de gestión adecuada y las prioridades para gestionar los riesgos de seguridad de la información y para implementar controles seleccionados para proteger contra estos riesgos. (ISO/IEC 27001:2013).

La evaluación de riesgos debe incluir:

- El enfoque sistemático de estimar la magnitud de los riesgos (análisis de riesgos).
- El proceso de comparar los riesgos estimados con los criterios de riesgo para determinar la importancia de los riesgos (evaluación de riesgos). (ISO/IEC 27001:2013).

La evaluación de riesgos debe realizarse periódicamente para abordar los cambios en los requisitos de seguridad de la información y en la situación de riesgo, por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, la evaluación de riesgos y cuando ocurren cambios significativos. Estas evaluaciones de riesgos deben llevarse a cabo de manera metódica capaz de producir resultados comparables y reproducibles. (ISO/IEC 27001:2013).

La evaluación de riesgos de seguridad de la información debe tener un alcance claramente definido para ser efectiva y debe incluir relaciones con evaluaciones de riesgos en otras áreas, si corresponde. (ISO/IEC 27001:2013).

2.2.6.4. Tratamiento de riesgos de seguridad de la información

Antes de considerar el tratamiento de un riesgo, la organización debe definir criterios para determinar si los riesgos pueden o no ser aceptados. Se pueden aceptar riesgos si, por ejemplo, se evalúa que el riesgo es bajo o que el costo del tratamiento no es rentable para la organización. Dichas decisiones deben registrarse. (ISO/IEC 27001:2013).

Para cada uno de los riesgos identificados después de la evaluación de riesgos, se debe tomar una decisión de

tratamiento de riesgos. Las posibles opciones para el tratamiento del riesgo incluyen las siguientes:

a. Aplicar controles apropiados para reducir los riesgos.
b. Aceptar riesgos a sabiendas y objetivamente, siempre que satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
c. Evitar riesgos al no permitir acciones que puedan causar que ocurran los riesgos.
d. Compartir los riesgos asociados con otras partes, por ejemplo, aseguradoras o proveedores. (ISO/IEC 27001:2013).

Para aquellos riesgos en los que la decisión del tratamiento de riesgos ha sido aplicar los controles apropiados, estos controles deben seleccionarse e implementarse. (ISO/IEC 27001:2013).

2.2.6.5. Seleccionar e implementar controles

Una vez que se han identificado los requisitos de seguridad de la información, se han determinado y evaluado los riesgos de seguridad de la información para los activos de información identificados y se han tomado decisiones para el tratamiento de los riesgos de seguridad de la información, luego se aplica la selección e implementación de controles para la reducción de riesgos. (ISO/IEC 27001:2013).

Los controles deben garantizar que los riesgos se reduzcan a un nivel aceptable teniendo en cuenta lo siguiente:

a. Requisitos y limitaciones de la legislación y las reglamentaciones nacionales e internacionales.
b. Objetivos organizacionales.
c. Requisitos y limitaciones operacionales.

d. Su costo de implementación y operación en relación con los riesgos que se reducen y siguen siendo proporcionales a los requisitos y limitaciones de la organización.
e. Sus objetivos para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad de la información para apoyar los objetivos de la organización. La selección e implementación de controles debe documentarse dentro de una declaración de aplicabilidad para ayudar con los requisitos de cumplimiento.
f. La necesidad de equilibrar la inversión en implementación y operación de controles contra la pérdida que probablemente resulte de incidentes de seguridad de la información. (ISO/IEC 27001:2013).

Los controles especificados en ISO / IEC 27002 se reconocen como las mejores prácticas aplicables a la mayoría de las organizaciones y se adaptan fácilmente para acomodar organizaciones de varios tamaños y complejidades. Otros estándares de la familia de estándares SGSI brindan orientación sobre la selección y aplicación de los controles ISO/IEC 27002 para el SGSI. Los controles de seguridad de la información deben considerarse en la especificación de requisitos de sistemas y proyectos y en la etapa de diseño. De lo contrario, se pueden generar costos adicionales y soluciones menos efectivas y, en el peor de los casos, la incapacidad para lograr la seguridad adecuada. Los controles se pueden seleccionar desde ISO/IEC 27002 o desde otros conjuntos de control. Alternativamente, se pueden diseñar nuevos controles para satisfacer las necesidades específicas de la organización. Es necesario reconocer la posibilidad de que algunos controles no sean aplicables a todos los sistemas o entornos de información, y no sean practicables para todas las organizaciones. (ISO/IEC 27001:2013).

A veces, implementar un conjunto de controles elegido lleva tiempo y, durante ese tiempo, el nivel de riesgo puede ser más alto de lo que se puede tolerar a largo plazo. Los criterios de riesgo deben cubrir la tolerabilidad de los riesgos a corto plazo mientras se implementan los controles. Las partes interesadas deben ser informadas de los niveles de riesgo que se estiman o anticipan en diferentes momentos a medida que se implementan progresivamente los controles. (ISO/IEC 27001:2013).

Debe tenerse en cuenta que ningún conjunto de controles puede lograr la seguridad completa de la información. Se deben implementar acciones de administración adicionales para monitorear, evaluar y mejorar la eficiencia y la efectividad de los controles de seguridad de la información para apoyar los objetivos de la organización. (ISO/IEC 27001:2013).

La selección e implementación de controles debe documentarse dentro de una declaración de aplicabilidad para ayudar con los requisitos de cumplimiento. (ISO/IEC 27001:2013).

2.2.7. La implementación de un SGSI

A la hora de implementar un Sistema de Gestión de Seguridad de la Información basado en el estándar internacional ISO 27001, debemos utilizar el ciclo PDCA (siglas en inglés) o PHVA (siglas en español). (ISOTOOLS EXCELLENCE, 2015).

Dicho ciclo cuenta con los siguientes pasos:

- Planificar: se establece el Sistema de Gestión de Seguridad de la Información.
- Hacer: se implementa el SGSI.

- Verificar: revisión del Sistema de Gestión de Seguridad de la Información.
- Actuar: en este paso del ciclo lo que se hace es mantener y mejorar el SGSI. (ISOTOOLS EXCELLENCE, 2015).

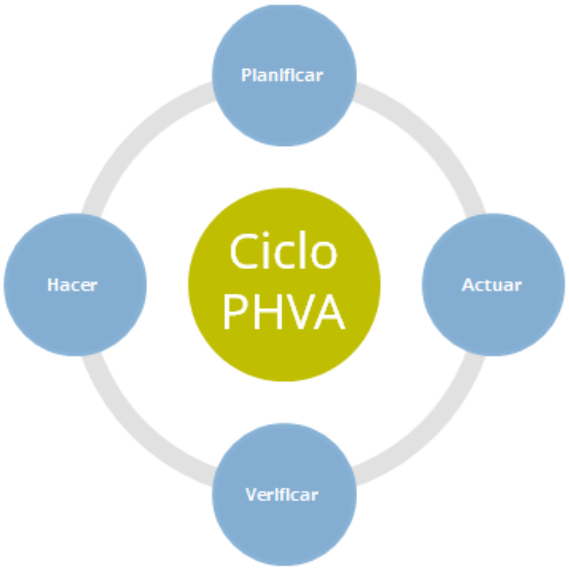


Figura 3 - Gráfica ilustrativa del Ciclo PDCA

Fuente: Blog ISO Tools www.pmg-ssi.com

2.2.7.1. Planificar

Debemos definir el alcance del Sistema de Gestión de Seguridad de la Información según la norma ISO 14001, es decir, definir los términos de negocio, la organización, la localización de esta, los activos y la tecnología con la que cuenta, además de establecer la justificación necesaria de cualquier exclusión. (ISOTOOLS EXCELLENCE, 2015).

Hay que definir perfectamente una política de seguridad en la que se incluyen:

- El marco general y los objetivos de seguridad de la información que persigue la empresa.
- Los requerimientos legales que afectan a la organización en materia de seguridad de la información.

- Debe estar alineada con el contexto estratégico de gestión de riesgos que tenga implantado la organización, gracias al que se establecerá y mantendrá el Sistema de Gestión de Seguridad de la Información basado en la norma ISO27001.
- Deben quedar claros cuáles serán los criterios a seguir a la hora de evaluar los diferentes riesgos.
- Finalmente, debe estar aprobada por la alta dirección de la organización. (ISOTOOLS EXCELLENCE, 2015).

Durante este paso del ciclo también debemos definir la metodología de evaluación del riesgo que sea más apropiada para el Sistema de Gestión de Seguridad de la Información y todos los requerimientos que tenga el negocio, también hay que establecer todos los criterios sobre la aceptación del riesgo y especificar cuáles serán los niveles de riesgo aceptables. Lo principal que debemos tener en cuenta es que los resultados que obtengamos se puedan comparar y se puedan repetir.
Para poder identificar los riesgos debemos:

- Identificar los activos que se encuentran al alcance del Sistema de Gestión de Seguridad de la Información y los responsables directos de estos.
- Conocer las amenazas en relación con los activos.
- Determinar cuáles son las vulnerabilidades que pueden ser aprovechadas por las amenazas.
- Identificar los impactos que se pueden generar en la confidencialidad, la integridad y la disponibilidad de los activos.
- Tenemos que realizar un análisis y una evaluación de riesgos:
- Hay que evaluar el impacto que puede causar en el negocio un fallo en la seguridad que suponga la pérdida de datos confidenciales, la disponibilidad de un activo de información, etc.

- Se debe estimar el nivel de riesgo.
- Conocer si el riesgo es aceptable o no según los criterios de aceptación que hayan sido previamente establecidos.
- Hay que identificar y evaluar todas las opciones de tratamiento de riesgos para poder:
- Aplicar los controles adecuados.
- Aceptar el riesgo, siempre que se cumplan todos los requisitos en las políticas. (ISOTOOLS EXCELLENCE, 2015).

Seleccionamos los objetivos de control y los controles de la norma ISO-27001 para poder tratar el riesgo, y así se cumplan todos los requerimientos identificados durante el proceso de evaluación del riesgo. Se debe aprobar por parte de la alta dirección de la organización los riesgos residuales y la implantación del Sistema de Gestión de Seguridad de la Información.

Definimos una declaración de aplicabilidad que incluya:

- Los diferentes objetivos de control y los controles seleccionados, además de todos los motivos que han declinado elegir esa selección.
- Todos los objetivos de control y los controles que se encuentran actualmente implementados. (ISOTOOLS EXCELLENCE, 2015).

2.2.7.2. Hacer

Hay que definir un plan de tratamiento de riesgos en que se identifique las acciones, recursos, responsabilidades y prioridades durante la gestión de riesgos en el Sistema de Gestión de Seguridad de la Información.

Se debe implementar un plan de tratamiento de riesgos, persiguiendo el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, las responsabilidades y las prioridades.

Se implementan controles que manejen los objetivos de control. Definimos un sistema de métricas que permita conseguir los resultados reproducibles y comparables a la hora de medir la eficacia de los controles. Hay que generar programar de formación y concienciación con relación a la seguridad de la información de todo el personal. Se deben gestionar todas las operaciones referidas al Sistema de Gestión de Seguridad de la Información y gestionar todos los recursos necesarios para que el SGSI se mantenga. (ISOTOOLS EXCELLENCE, 2015).

2.2.7.3. Verificar

La empresa tiene que ejecutar los procedimientos de monitorización y revisión para detectar a tiempo todos los errores generados en los resultados obtenidos en el procesamiento de la información. Debe identificar las fisuras y los incidentes de seguridad y ayudar a la dirección de la organización a determinar si las actividades desarrolladas por las personas y los dispositivos tecnológicos que ayudan a garantizar la seguridad de la información.

Se deben detectar y prevenir, en la medida de lo posible, todos los incidentes de seguridad mediante la utilización de indicadores.

Y hay que determinar si las acciones que se realizaron para resolver las fisuras de seguridad, de las que hablábamos anteriormente, fueron efectivas.

La organización debe revisar regularmente la efectividad del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, que se cumple la política de seguridad y los objetivos del SGSI, además de revisar todos los resultados obtenidos en las auditorías, de los incidentes y las mediciones de eficacia, sugerencias y observaciones realizadas por todas las partes interesadas. (ISOTOOLS EXCELLENCE, 2015).

2.2.7.4. Actuar

La empresa deberá, cada cierto tiempo, implementar en el Sistema de Gestión de Seguridad de la Información todas las mejoras identificadas, realizar las acciones preventivas y correctivas que sean necesarias en relación a lo que disponga la norma ISO27001 y aprender de las experiencias propias que han ido viviendo y de otras organizaciones. Hay que comunicar las acciones de mejora que se han tomado a toda la organización, con el nivel de detalle necesario y además, si es oportuno indicar la forma de proceder. Se deben asegurar de que las mejoras introducidas están a la altura de todos los objetivos previstos por la organización. (ISOTOOLS EXCELLENCE, 2015).

2.2.8. MAGERIT

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan, complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una

aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. (MAGERIT V.3, 2012).

Magerit persigue los siguientes objetivos:

Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. (MAGERIT V.3, 2012).

2.2.8.1. Introducción al análisis y gestión de riesgos

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que compro metan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. (MAGERIT V.3, 2012).

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad:

Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad:

Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad:

La información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autoriza-dos. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la con-fianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. (MAGERIT V.3, 2012).

2.2.8.2. Método de análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza con el objeto de organizar la presentación, se introducen los conceptos de “impacto y riesgo potenciales” entre los pasos 2 y 3. (MAGERIT V.3, 2012).

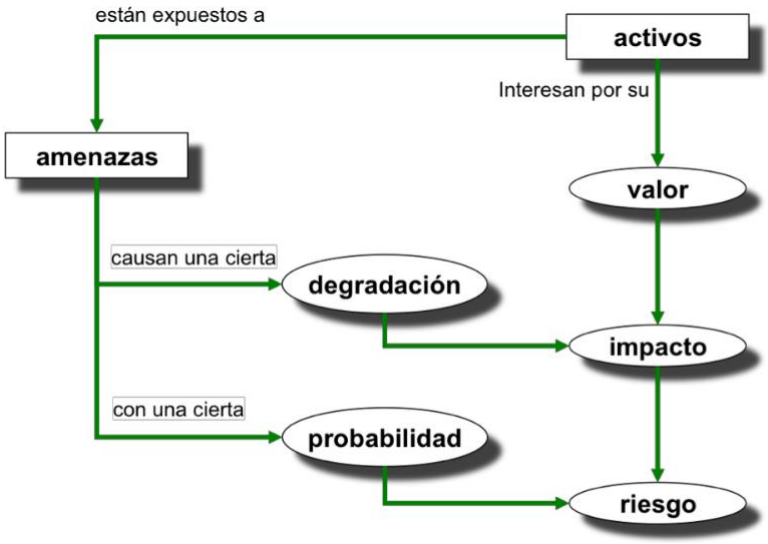


Figura 4 - Elementos del Análisis de riesgos potenciales.

Fuente: MAGERIT V3 - Libro I – Método.

Paso 1: Activos

(MAGERIT V.3, 2012). Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008].

En un sistema de información hay 2 cosas esenciales:

- la información que maneja
- y los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

Valoración

(MAGERIT V.3, 2012). ¿Por qué interesa un activo? Por lo que vale.
No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale, eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite

caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

Dimensiones

(MAGERIT V.3, 2012). De un activo puede interesar calibrar diferentes dimensiones:

Su confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
Su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
Su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

Paso 2: Amenazas

(MAGERIT V.3, 2012). El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño.

Identificación de las amenazas

El capítulo 5 del "Catálogo de Elementos" presenta una relación de amenazas típicas.

De origen natural

Hay accidentes naturales (terremotos, inundaciones, etc.). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, etc.) ante los cuales el sistema de información es víctima pasiva, pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’.

Causadas por las personas de forma accidental

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados. Bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas

(MAGERIT V.3, 2012). Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo.
En dos sentidos:
Degradación: cuán perjudicado resultaría el [valor del] activo
Probabilidad: cuán probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

(MAGERIT V.3, 2012). La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal.

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 2 - Ejemplo de escala nominal de Probabilidad

Fuente: MAGERIT V3 - Libro I – Método.

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos.

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 3 - Probabilidad de ocurrencia.

Fuente: MAGERIT V3 - Libro I – Método.

Determinación del impacto potencial

(MAGERIT V.3, 2012). Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta. Pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

Impacto repercutido
Es el calculado sobre un activo teniendo en cuenta

- su valor propio
- las amenazas a que están expuestos los activos de los que depende.

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las

decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Determinación del riesgo potencial

(MAGERIT V.3, 2012). Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.
El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables pero de muy alto impacto.

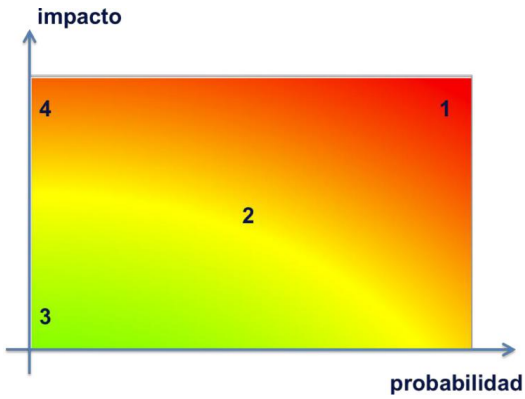


Figura 5 - El riesgo en función del impacto y la probabilidad.

Fuente: MAGERIT V3 - Libro I – Método.

Riesgo repercutido

(MAGERIT V.3, 2012). Es el calculado sobre un activo teniendo en cuenta

- el impacto repercutido sobre un activo debido a una amenaza y
- la probabilidad de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

2.2.8.3. Auditorías

(MAGERIT V.3, 2012). Aunque no sea lo mismo, no están muy lejos de este mundo las auditorías, internas o externas, a las que se someten los sistemas de información.

- Unas veces requeridas por ley para poder operar en un cierto sector (cumplimiento),
- Otras veces requeridas por la propia dirección de la organización,
- Otras veces requeridas por entidades colaboradoras que ven su propio nivel de riesgo liga-do al nuestro.

Una auditoría puede servirse de un análisis de riesgos que le permita 1. Saber qué hay en juego, 2. Saber a qué está expuesto el sistema y 3. Valorar la eficacia y eficiencia de las salvaguardas.

Frecuentemente, los auditores parten de un análisis de riesgos, implícito o explícito, que, o bien realizan ellos mismos, o bien lo auditan. Siempre en la primera fase de la auditoría, pues es difícil opinar de lo que no se conoce. A partir del análisis de riesgos se puede analizar el sistema e informar a la gerencia de si el sistema está bajo control. Es decir, si las medidas de seguridad adoptadas están justificadas, implantadas y monitorizadas, de forma que se puede confiar en el sistema de indicadores de que dispone la gerencia para gestionar la seguridad de los sistemas.

La conclusión de la auditoría es un informe de insuficiencias detectadas, que no son sino incoherencias entre las necesidades identificadas en el análisis de riesgos y la realidad detectada duran-te la inspección del sistema en operación.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Las auditorías deben repetirse regularmente tanto para seguir la evolución del análisis de riesgos (que se debe

actualizar regularmente) como para seguir el desarrollo del plan de seguridad determinado por las actividades de gestión de riesgos.

2.2.9. Ley de Protección de Datos Personales

Como un marco jurídico y de cumplimiento, es importante para la presente investigación comentar sobre la ley de Protección de Datos Personales (LEY Nro. 29733). Esta ley fue aprobada mediante Decreto Supremo N°003-2013-JUS.

"La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen." (LEGISLACIÓN PERUANA, 2013).

"Toda persona tiene derecho a que los servicios informativos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar…" (Constitución Política del Perú, Artículo 2, inciso 6: "Derecho a la Autodeterminación Informativa"). (LEGISLACIÓN PERUANA, 2013).

2.2.9.1. Directiva de Seguridad aplicada a la LDPDP

(APDP, 2013). La presente directiva orienta sobre las condiciones, los requisitos y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley N°29733 en materia de medidas de Seguridad de los bancos de datos personales.

(APDP, 2013). ANEXO C: ORIENTACIÓN PARA BANCOS DE DATOS DE TIPO COMPLEJO O CRÍTICO

- Las personas jurídicas pueden implementar el ISO/IEC 27001 en su edición vigente incorporando, en el alcance del SGSI, a los bancos de datos personales. Con lo cual, el sistema de gestión ayudará al cumplimiento de la mayor parte de los requisitos y medidas señaladas en la directiva de seguridad de la información administrada por los bancos de datos personales, incluso a mayor nivel del definido en la directiva. Siendo necesario identificar cuáles son los aspectos que el SGSI no cubre y que la directiva señala.
- Las instituciones pueden utilizar el ISO 31000 o ISO/IEC 27005 como referencias de gestión del riesgo.
- Las instituciones pueden utilizar un Análisis de Impacto en la Privacidad (PIA por sus siglas en inglés) como insumo u orientación en la fase de planificación y gestión del riesgo.
- Las instituciones pueden utilizar el enfoque de “Privacidad por Diseño” como referencia en la evaluación de sus procesos y herramientas que determinen deban incorporarse o modificarse para el cumplimiento de la Ley Nro. 29733, Ley de Protección de Datos Personales.

2.3. Definición de términos

2.3.1. Sistema de Gestión de la Seguridad de la Información (SGSI)

(ISO/IEC 27000:2018). Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y en los niveles de aceptación de riesgos de la organización diseñados para tratar y administrar los riesgos de manera efectiva. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles apropiados para garantizar la protección de estos activos de información, según sea necesario, contribuyen a la implementación exitosa de un SGSI.

2.3.2. Riesgo

(ISO/IEC 27000:2018). El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

2.3.3. Activos (Activos de Información)

(MAGERIT V.3, 2012). Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

2.3.4. Gestión de riesgos

(ISO/IEC 27000:2018). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

2.3.5. Proceso de gestión de riesgos

(ISO/IEC 27000:2018). Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consultoría, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos.

2.3.6. Evaluación de riesgos

(ISO/IEC 27000:2018). Proceso global de identificación, análisis y estimación de riesgos.

2.3.7. Estimación de riesgos

(ISO/IEC 27000:2018). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

2.3.8. Objetivo de control

(ISO/IEC 27000:2018). Declaración que describe lo que se debe lograr como resultado de la implementación de controles.

2.3.9. Control

(ISO/IEC 27000:2018). Medida que modifica el riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo.

2.3.10. Controles de Seguridad de Gestión

(ACOSTA RODRÍGUEZ, 2018). Son aquellos controles procedimentales, administrativos y/o documentales que establecen las reglas a seguir para la protección del entorno.

2.3.11. Controles de Seguridad Lógicos

(ACOSTA RODRÍGUEZ, 2018). Son aquellos controles basados en una combinación de hardware y software.

2.3.12. Controles de Seguridad Físicos

(ACOSTA RODRÍGUEZ, 2018). Son aquellos tipos de controles tangibles orientados a la protección del entorno y de los recursos físicos de la organización.

2.4. Hipótesis

2.4.1. Hipótesis General

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima.

2.4.2. Hipótesis específica

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.

2.5. Variables

Definiciones y Operacionalización se encuentran en el ANEXO 3.

CAPÍTULO III

3. METODOLOGÍA

3.1. Método de Investigación

Como método general el científico (el método inductivo y el método hipotético - deductivo), porque nos ayudó a observar, hipotetizar, predecir, verificar y explicar la relación entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgo en Activos de Información.

(HERNÁNDEZ CHANTO, 2008). El Círculo de Viena nace a partir de las reuniones sostenidas por un conjunto de científicos y filósofos alrededor de la figura de Ernst Mach -considerado por muchos como el primer filósofo de la ciencia-. Paradójicamente este autor estuvo al frente de la Cátedra de Filosofía de las Ciencias Inductivas, creada en la Universidad de Viena en 1895. Sus miembros más destacados -Schlick, Feigl, Menger y Carnap- tenían un afán por establecer un concepto de la ciencia que se basara en una colección de proposiciones ulteriores -sobre las que debía descansar toda teoría- las cuales pudiesen ser verificables tanto lógica como empíricamente. De igual forma, estaban preocupados por establecer las relaciones básicas entre cualquier ciencia y la física, considerada por éstos como “la ciencia por antonomasia.” Con el afán de conseguir este propósito, los miembros del Círculo de Viena propugnaban que la metodología inductivista, descrita anteriormente, se remplazara por un procedimiento basado en dos principios: el método hipotético deductivo y la verificación.

De acuerdo con el método hipotético - deductivo, la lógica de la investigación científica se basa en la formulación de una ley universal y en el establecimiento de condiciones iniciales relevantes que constituyen la premisa básica para la construcción de teorías. Dicha ley universal se deriva de especulaciones o conjeturas más que de consideraciones

inductivistas. Así las cosas, la ley universal puede corresponder a una proposición como la siguiente: Si “X sucede, Y sucede" o en forma estocástica: “X sucede si Y sucede con probabilidad P."

Una consecuencia que se deriva de esta manera de formular leyes universales es la simetría que existe entre la explicación y la predicción. La única diferencia que subyace entre ellas es que la primera tiene lugar a posteriori mientras que la segunda funciona a priori. Esta acotación es especialmente importante a la hora de analizar el papel de los modelos en economía, ya que, si se considera la explicación como su rol fundamental, la abstracción de los modelos teóricos es válida mientras propicie un mayor entendimiento de los fenómenos económicos estudiados. Por otra parte, si se juzga la predicción como el aporte sustantivo de los modelos, la validez de los supuestos tiene una relevancia particular. Este enfoque se verá más claro cuando se analice el papel de los modelos macro econométricos surgidos en el seno de la Comisión Cowles, a principios de los años cuarenta.

(HERNÁNDEZ CHANTO, 2008). El otro punto trascendental del Círculo de Viena es la introducción del principio de verificación el cual propone que el significado de una proposición es su método de verificación. Es decir, establecen una equivalencia entre el significado de una oración, sus reglas de uso y el método de su verificación. De esta manera, consideran que una teoría científica es un conjunto de proposiciones que pueden ser verificadas lógica y empíricamente, por cuanto el establecimiento del significado y el método de verificación son actos simultáneos. Si bien es cierto que, para estos filósofos de la ciencia, la posibilidad de verificación lógica de una teoría no descansa sobre un hecho experimental sino solamente sobre las propiedades y reglas del lenguaje, dichas reglas están relacionadas ulteriormente con definiciones extensivas y por ende con la experiencia.

3.2. Tipo de Investigación

Es una investigación de tipo aplicada, (SÁNCHEZ & REYES, 2006) la investigación aplicada busca conocer para hacer, para actuar, para construir, para modificar. Le preocupa la aplicación inmediata sobre una realidad circunstancial antes que el desarrollo de un conocimiento de valor universal.

3.3. Nivel de Investigación

El nivel de la investigación fue de nivel explicativo, con este nivel de investigación se busca explicar que ocurre y que resulta entre la implementación del SGSI y la gestión de Riego en Activos de Información en la Empresa Digitex Perú.

(HERNÁNDEZ, FERNÁNDEZ & BAPTISTA, 2014). Los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables.

3.4. Diseño de la Investigación

El diseño que guio el trabajo de investigación fue Diseño Experimental - Pre experimental con un solo grupo. Al respecto (HERNÁNDEZ, FERNÁNDEZ & BAPTISTA, 2014). Sostienen que A un grupo se le aplica una prueba previa al estímulo o tratamiento experimental, después se le administra el tratamiento y finalmente se le aplica una prueba posterior al estímulo.

Esquema:

G O1 X O2

Donde:

G: Grupo de sujetos o casos.

O1: Medición del Pre test.

O2: Medición del Post test.

X: Tratamiento, estímulo o condición experimental (presencia de algún nivel o modalidad de la variable independiente).

3.5. Población y muestra

(ARIAS, 1999). Señala que la población es el conjunto de elementos con características comunes que son objetos de análisis y para los cuales serán válidas las conclusiones de la investigación.

Mientras que (MEJÍA, 2005). Manifiesta que: Una población es la totalidad de sujetos o elementos que tienen características comunes. En otras palabras, una población es la totalidad de los miembros de la unidad de análisis. El concepto de población equivale al concepto de conjunto y éste es delimitado por el investigador según los criterios que considere pertinentes.

Según (VARA HORNA, 2008). Si la población es pequeña y se puede acceder a ella sin restricciones, entonces es mejor trabajar con toda la población. En este caso, ya no necesitas muestreo. Pero si la población es muy grande o es demasiado costoso trabajar con toda, entonces conviene seleccionar una muestra.

Según Arias (1999). La muestra es un subconjunto representativo y finito que se extrae de la población accesible. Para la investigación se consideró como población a los 114 controles del ANEXO A de la ISO 27001 y como muestra a 70 controles Aplicables, se realizó un muestreo intencional u opinático basado en cumplir el criterio de: El Control debe ser Aplicable de acuerdo a la Declaración de Aplicabilidad (SOA).

3.6.Técnicas e Instrumentos de recolección de datos

- ✓ Auditoria basada en Controles Anexo A de la ISO 27001

3.7.Procesamiento de la información

- ✓ Análisis GAP de Nivel de Madurez.
- ✓ Tabulación de datos.

3.8.Técnicas y análisis de datos

- ✓ Análisis Estadístico de Datos.

CAPÍTULO IV

4. RESULTADOS

En este capítulo se presentan los resultados obtenidos en el desarrollo de la investigación, para ello se tuvo como principal fuente los datos obtenidos que fueron brindados por los responsables de la Dirección de Tecnología, quienes aportaron la información necesaria en las auditorías realizadas haciendo uso del instrumentos de recolección de datos de la investigación.

4.1. Descripción de resultados

4.1.1. Desarrollo de la Metodología de Implementación del SGSI.

Se realizó el desarrollo de la metodología utilizando las bases teóricas del Capítulo 2, el mismo se encuentra descrito al detalle en el Anexo 1 de la investigación.

4.1.2. Datos obtenidos

A continuación, muestro los datos obtenidos en la investigación, la interpretación se hizo según las dimensiones de la variable.

Variable: Gestión de Riesgos en Activos de Información.

Dimensión 1: Controles de Seguridad de Gestión.
Dimensión 2: Controles de Seguridad Lógicos.
Dimensión 3: Controles de Seguridad Físicos.

Valor	Estado
0	? Desconocido
1	Inexistente
2	Inicial
3	Limitado
4	Definido
5	Administrado
6	Optimizado
7	No aplicable

Tabla 4 - Métricas utilizadas.

Fuente: Elaboración propia en basado en el Anexo 4.

Tabla 5 - Consolidado de resultados obtenidos con el instrumento de investigación.

Fuente: Elaboración propia en base los datos del Anexo 1: Desarrollo de la metodología del SGSI.

	Dominios		Objetivos de Control		Sección	Controles de Seguridad de la Información	INICIAL		FINAL	
							Estado	Valor	Estado	Valor
A5	Políticas de seguridad de la información	A5.1	Directrices de gestión de la seguridad de la información	**1**	A5.1.1	Políticas para la seguridad de la información	Limitado	3	Administrado	5
				2	A5.1.2	Revisión de las políticas para la seguridad de la información	Limitado	3	Administrado	5
A6	Organización de la seguridad de la información	A6.1	Organización interna	**3**	A6.1.1	Roles y responsabilidades en seguridad de la información	Limitado	3	Administrado	5
				4	A6.1.2	Segregación de tareas	Limitado	3	Administrado	5
				5	A6.1.3	Contacto con las autoridades	Limitado	3	Limitado	3
				6	A6.1.4	Contacto con grupos de interés especial	Inexistente	1	Limitado	3
				7	A6.1.5	Seguridad de la información en la gestión de proyectos	No aplicable	7	No aplicable	7
		A6.2	Los dispositivos móviles y el teletrabajo	**8**	A6.2.1	Política de dispositivos móviles	Inexistente	1	Administrado	5
				9	A6.2.2	Teletrabajo	No aplicable	7	No aplicable	7

A7	Seguridad relativa a los recursos humanos	A7.1	Antes del empleo	**10**	A7.1.1	Investigación de antecedentes	No aplicable	7	No aplicable	7
				11	A7.1.2	Términos y condiciones del empleo	No aplicable	7	No aplicable	7
		A7.2	Durante el empleo	**12**	A7.2.1	Responsabilidades de gestión	Inexistente	1	Limitado	3
				13	A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inexistente	1	Limitado	3
				14	A7.2.3	Proceso disciplinario	Inexistente	1	Limitado	3
		A7.3	Finalización del empleo o cambio en el puesto de trabajo	**15**	A7.3.1	Responsabilidades ante la finalización o cambio	Inexistente	1	Definido	4
A8	Gestión de activos	A8.1	Responsabilidad sobre los activos	**16**	A8.1.1	Inventario de activos	Inexistente	1	Definido	4
				17	A8.1.2	Propiedad de los activos	Inexistente	1	Definido	4
				18	A8.1.3	Uso aceptable de los activos	Limitado	3	Definido	4
				19	A8.1.4	Devolución de activos	Definido	4	Definido	4
		A8.2	Clasificación de la información	**20**	A8.2.1	Clasificación de la información	Inexistente	1	Definido	4
				21	A8.2.2	Etiquetado de la información	Inexistente	1	Definido	4

				22	A8.2.3	Manipulado de la información	Inexistente	1	Definido	4
		A8.3	Manipulación de los soportes	**23**	A8.3.1	Gestión de soportes extraíbles	No aplicable	7	No aplicable	7
				24	A8.3.2	Eliminación de soportes	No aplicable	7	No aplicable	7
				25	A8.3.3	Soportes físicos en tránsito	No aplicable	7	No aplicable	7
A9	Control de acceso	A9.1	Requisitos de negocio para el control de acceso	**26**	A9.1.1	Política de control de acceso	Inexistente	1	Administrado	5
				27	A9.1.2	Acceso a las redes y a los servicios de red	Inicial	2	Definido	4
		A9.2	Gestión de acceso de usuario	**28**	A9.2.1	Registro y baja de usuario	Inexistente	1	Administrado	5
				29	A9.2.2	Provisión de acceso de usuario	Inexistente	1	Definido	4
				30	A9.2.3	Gestión de privilegios de acceso	Inexistente	1	Administrado	5
				31	A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inexistente	1	Administrado	5
				32	A9.2.5	Revisión de los derechos de acceso de usuario	Inexistente	1	Administrado	5
				33	A9.2.6	Retirada o reasignación de los derechos de acceso	Inexistente	1	Administrado	5

		A9.3	Responsabilidades del usuario	**34**	A9.3.1	Uso de la información secreta de autenticación	Inexistente	1	Definido	4
		A9.4	Control de acceso a sistemas y aplicaciones	**35**	A9.4.1	Restricción del acceso a la información	Inexistente	1	Definido	4
				36	A9.4.2	Procedimientos seguros de inicio de sesión	Inexistente	1	Definido	4
				37	A9.4.3	Sistema de gestión de contraseñas	Inexistente	1	Definido	4
				38	A9.4.4	Uso de utilidades con privilegios del sistema	Inexistente	1	Definido	4
				39	A9.4.5	Control de acceso al código fuente de los programas	Inexistente	1	Definido	4
A10	Criptografía	A10.1	Controles criptográficos	**40**	A10.1.1	Política de uso de los controles criptográficos	Inexistente	1	Administrado	5
				41	A10.1.2	Gestión de claves	Inexistente	1	Limitado	3
A11	Seguridad física y del entorno	A11.1	Areas seguras	**42**	A11.1.1	Perímetro de seguridad física	No aplicable	7	No aplicable	7
				43	A11.1.2	Controles físicos de entrada	No aplicable	7	No aplicable	7
				44	A11.1.3	Seguridad de oficinas, despachos y recursos	Inexistente	1	Limitado	3
				45	A11.1.4	Protección contra las amenazas externas y ambientales	Inexistente	1	Limitado	3

				22	A8.2.3	Manipulado de la información	Inexistente	1	Definido	4
		A8.3	Manipulación de los soportes	**23**	A8.3.1	Gestión de soportes extraíbles	No aplicable	7	No aplicable	7
				24	A8.3.2	Eliminación de soportes	No aplicable	7	No aplicable	7
				25	A8.3.3	Soportes físicos en tránsito	No aplicable	7	No aplicable	7
A9	Control de acceso	A9.1	Requisitos de negocio para el control de acceso	**26**	A9.1.1	Política de control de acceso	Inexistente	1	Administrado	5
				27	A9.1.2	Acceso a las redes y a los servicios de red	Inicial	2	Definido	4
		A9.2	Gestión de acceso de usuario	**28**	A9.2.1	Registro y baja de usuario	Inexistente	1	Administrado	5
				29	A9.2.2	Provisión de acceso de usuario	Inexistente	1	Definido	4
				30	A9.2.3	Gestión de privilegios de acceso	Inexistente	1	Administrado	5
				31	A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inexistente	1	Administrado	5
				32	A9.2.5	Revisión de los derechos de acceso de usuario	Inexistente	1	Administrado	5
				33	A9.2.6	Retirada o reasignación de los derechos de acceso	Inexistente	1	Administrado	5

				46	A11.1.5	El trabajo en áreas seguras	Limitado	3	Definido	4
				47	A11.1.6	Areas de carga y descarga	No aplicable	7	No aplicable	7
		A11.2	Seguridad de los equipos	**48**	A11.2.1	Emplazamiento y protección de equipos	Limitado	3	Definido	4
				49	A11.2.2	Instalaciones de suministro	Inexistente	1	Definido	4
				50	A11.2.3	Seguridad del cableado	Inexistente	1	Limitado	3
				51	A11.2.4	Mantenimiento de los equipos	Inexistente	1	Limitado	3
				52	A11.2.5	Retirada de materiales propiedad de la empresa	No aplicable	7	No aplicable	7
				53	A11.2.6	Seguridad de los equipos fuera de las instalaciones	No aplicable	7	No aplicable	7
				54	A11.2.7	Reutilización o eliminación segura de equipos	Limitado	3	Administrado	5
				55	A11.2.8	Equipo de usuario desatendido	Limitado	3	Administrado	5
				56	A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Limitado	3	Administrado	5
A12	Seguridad de las operaciones	A12.1		**57**	A12.1.1	Documentación de procedimientos operacionales	Limitado	3	Definido	4

			Procedimientos y responsabilidades operacionales	**58**	A12.1.2	Gestión de cambios	No aplicable	7	No aplicable	7
				59	A12.1.3	Gestión de capacidades	Inexistente	1	Definido	4
				60	A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable	7	No aplicable	7
		A12.2	Protección contra el software malicioso (malware)	**61**	A12.2.1	Controles contra el código malicioso	Limitado	3	Administrado	5
		A12.3	Copias de seguridad	**62**	A12.3.1	Copias de seguridad de la información	Limitado	3	Administrado	5
		A12.4	Registros y supervisión	**63**	A12.4.1	Registro de eventos	Inexistente	1	Definido	4
				64	A12.4.2	Protección de la información del registro	Inexistente	1	Definido	4
				65	A12.4.3	Registros de administración y operación	Inexistente	1	Definido	4
				66	A12.4.4	Sincronización del reloj	Inexistente	1	Definido	4
		A12.5	Control del software en producción	**67**	A12.5.1	Instalación del software en producción	Inexistente	1	Administrado	5
		A12.6	Gestión de la vulnerabilidad técnica	**68**	A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente	1	Limitado	3
				69	A12.6.2	Restricción en la instalación de software	Inexistente	1	Definido	4

		A12.7	Consideraciones sobre la auditoria de sistemas de información	**70**	A12.7.1	Controles de auditoría de sistemas de información	Inexistente	1	Limitado	3
A13	Seguridad de las comunicaciones	A13.1	Gestión de la seguridad de las redes	**71**	A13.1.1	Controles de red	Limitado	3	Definido	4
				72	A13.1.2	Seguridad de los servicios de red	No aplicable	7	No aplicable	7
				73	A13.1.3	Segregación en redes	No aplicable	7	No aplicable	7
		A13.2	Intercambio de información	**74**	A13.2.1	Políticas y procedimientos de intercambio de información	Limitado	3	Administrado	5
				75	A13.2.2	Acuerdos de intercambio de información	No aplicable	7	No aplicable	7
				76	A13.2.3	Mensajería electrónica	Inexistente	1	Definido	4
				77	A13.2.4	Acuerdos de confidencialidad o no revelación	Inexistente	1	Limitado	3
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	A14.1	Requisitos de seguridad en los sistemas de información	**78**	A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No aplicable	7	No aplicable	7
				79	A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No aplicable	7	No aplicable	7
				80	A14.1.3	Protección de las transacciones de servicios de aplicaciones	No aplicable	7	No aplicable	7
		A14.2	Seguridad en el desarrollo y en los	**81**	A14.2.1	Política de desarrollo seguro	No aplicable	7	No aplicable	7

			procesos de soporte	**82**	A14.2.2	Procedimiento de control de cambios en sistemas	No aplicable	7	No aplicable	7
				83	A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No aplicable	7	No aplicable	7
				84	A14.2.4	Restricciones a los cambios en los paquetes de software	No aplicable	7	No aplicable	7
				85	A14.2.5	Principios de ingeniería de sistemas seguros	No aplicable	7	No aplicable	7
				86	A14.2.6	Entorno de desarrollo seguro	No aplicable	7	No aplicable	7
				87	A14.2.7	Externalización del desarrollo de software	No aplicable	7	No aplicable	7
				88	A14.2.8	Pruebas funcionales de seguridad de sistemas	No aplicable	7	No aplicable	7
				89	A14.2.9	Pruebas de aceptación de sistemas	No aplicable	7	No aplicable	7
		A14.3	Datos de prueba	**90**	A14.3.1	Protección de los datos de prueba	No aplicable	7	No aplicable	7
A15	Relación con proveedores	A15.1	Seguridad en las relaciones con proveedores	**91**	A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No aplicable	7	No aplicable	7
				92	A15.1.2	Requisitos de seguridad en contratos con terceros	No aplicable	7	No aplicable	7
				93	A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No aplicable	7	No aplicable	7

		A15.2	Gestión de la provisión de servicios del proveedor	**94**	A15.2.1	Control y revisión de la provisión de servicios del proveedor	No aplicable	7	No aplicable	7
				95	A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No aplicable	7	No aplicable	7
A16	Gestión de incidentes de seguridad de la información	A16.1	Gestión de incidentes de seguridad de la información y mejoras	**96**	A16.1.1	Responsabilidades y procedimientos	Limitado	3	Administrado	5
				97	A16.1.2	Notificación de los eventos de seguridad de la información	Inexistente	1	Administrado	5
				98	A16.1.3	Notificación de puntos débiles de la seguridad	Inexistente	1	Limitado	3
				99	A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	No aplicable	7	No aplicable	7
				100	A16.1.5	Respuesta a incidentes de seguridad de la información	Inexistente	1	Definido	4
				101	A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente	1	Definido	4
				102	A16.1.7	Recopilación de evidencias	Inexistente	1	No aplicable	7
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	A17.1	Continuidad de la seguridad de la información	**103**	A17.1.1	Planificación de la continuidad de la seguridad de la información	No aplicable	7	No aplicable	7
				104	A17.1.2	Implementar la continuidad de la seguridad de la información	No aplicable	7	No aplicable	7
				105	A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No aplicable	7	No aplicable	7

4.1.3. Interpretación

4.1.3.1. De los controles de Seguridad de Gestión

Se identificaron 43 controles Aplicables, al ser auditados se les colocó un estado de acuerdo a la tabla de métricas para luego determinar el nivel de madurez total en base al porcentaje de controles que encajen en cada estado. La siguiente tabla se contrastan los datos del antes y después, seguido de las ilustraciones que demuestran que el estado de madurez pasó de ser Inexistente a ser Administrado/Definido.

Estado	Inicial	Final
Inexistente	70%	0%
Inicial	2%	0%
Limitado	26%	28%
Definido	2%	32%
Administrado	0%	40%
Optimizado	0%	0%

Tabla 6 - Resumen del antes y después del nivel de madurez de los Controles de Gestión.

Fuente: Elaboración propia en base a los datos obtenidos en el Anexo 1.

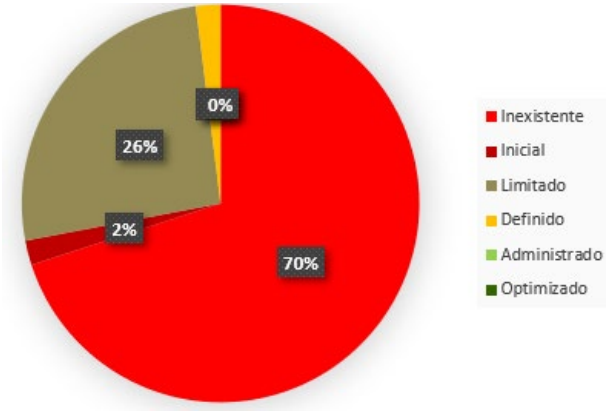


Figura 6 - Gráfica del estado Inicial. Basado en la Tabla 6.

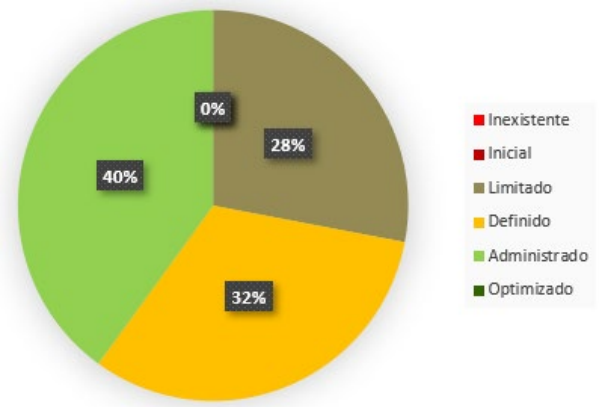


Figura 7 - Gráfica del estado Final. Basado en la Tabla 6.

4.1.3.2. De los controles de Seguridad Lógicos

Se identificaron 20 controles Aplicables, al ser auditados se les colocó un estado de acuerdo a la tabla de métricas para luego determinar el nivel de madurez total en base al porcentaje de controles que encajen en cada estado. La siguiente tabla se contrastan los datos del antes y después, seguido de las ilustraciones que demuestran que el estado de madurez pasó de ser Inexistente a ser Definido.

Estado	Inicial	Final
Inexistente	80%	0%
Inicial	0%	0%
Limitado	20%	10%
Definido	0%	70%
Administrado	0%	20%
Optimizado	0%	0%

Tabla 7 - Resumen del antes y después del nivel de madurez de los Controles Lógicos.

Fuente: Elaboración propia en base a los datos obtenidos en el Anexo 1.

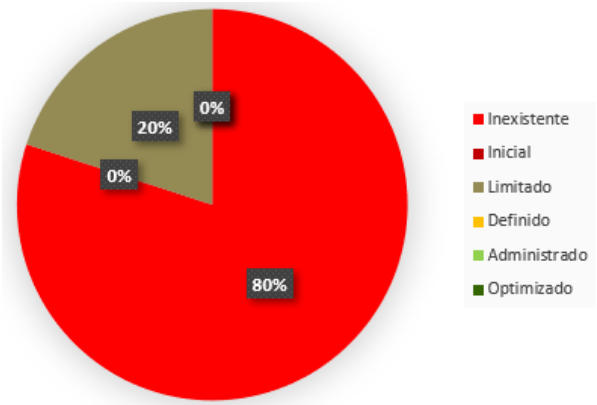


Figura 8 - Gráfica del estado Inicial. Basado en la Tabla 7.

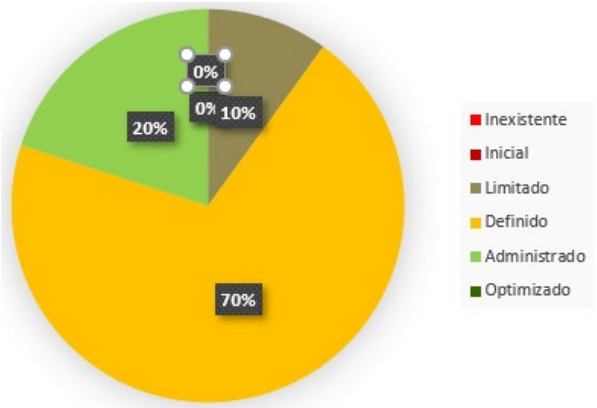


Figura 9 - Gráfica del estado Final. Basado en la Tabla 7.

4.1.3.3. De los controles de Seguridad Físicos

Se identificaron 7 controles Aplicables, al ser auditados se les colocó un estado de acuerdo a la tabla de métricas para luego determinar el nivel de madurez total en base al porcentaje de controles que encajen en cada estado. La siguiente tabla se contrastan los datos del antes y después, seguido de las ilustraciones que demuestran que el estado de madurez pasó de ser Inexistente a ser Definido.

Estado	Inicial	Final
Inexistente	70%	0%
Inicial	0%	0%
Limitado	30%	43%
Definido	0%	57%
Administrado	0%	0%
Optimizado	0%	0%

Tabla 8 - Resumen del antes y después del nivel de madurez de los Controles Físicos.

Fuente: Elaboración propia en base a los datos obtenidos en el Anexo 1: Desarrollo.

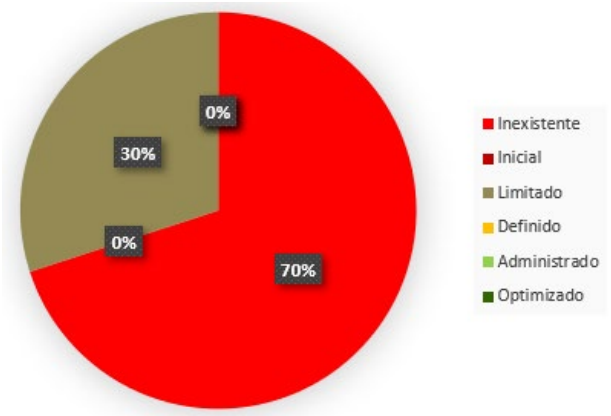


Figura 10 - Gráfica del estado Inicial. Basado en la Tabla 8.

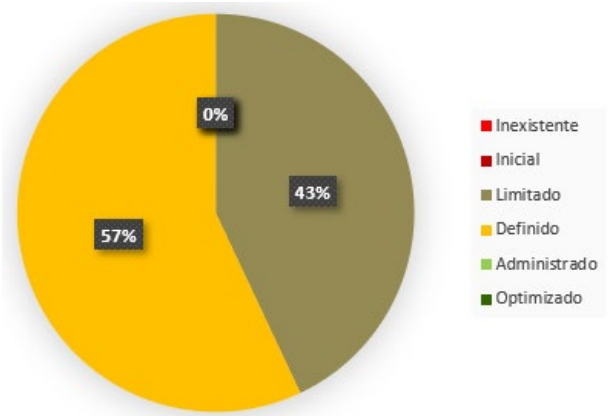


Figura 11 - Gráfica del estado Inicial. Basado en la Tabla 8.

4.2. Contrastación de Hipótesis

4.2.1. Validez del instrumento

El instrumento fue validado en por expertos en el tema, la evidencia de la validación se encuentra en el Anexo 6 de la presente investigación.

4.2.2. Hipótesis General

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima.

1. Redactar las Hipótesis H_0 y H_1

Donde H_0 es la Hipótesis Nula y **H_1** es la Hipótesis Alterna.

H_0 = La implementación del Sistema de Gestión de Seguridad de la Información NO influye significativamente en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima.

H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima.

2. Definir Alfa α

Alfa = 0.05 = 5%

3. Calcular el P-Valor

NORMALIDAD

- Kolmogorov-Smirnov muestras grandes (>30 individuos)
- Shápiro Wilk muestras pequeñas (<30 individuos).

Criterio para determinar Normalidad:

P-valor => α,

Aceptar Ho = Los datos provienen de una distribución normal.

P-valor < α,

Aceptar H1 = Los datos NO provienen de una distribución normal.

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Inicial	,279	114	,000	,714	114	,000
Final	,269	114	,000	,809	114	,000
a. Corrección de significación de Lilliefors						

Tabla 9 - Pruebas de normalidad para la Hipótesis General.

NORMALIDAD		
P-Valor (inicial) = 0,000	<	α = 0.05
P-Valor (final) = 0,000	<	α = 0.05
Interpretación: **Los datos del pre test (inicial) y post test (final) NO provienen de una distribución** normal		

Tabla 10 - Interpretación de la normalidad para la Hipótesis General.

4. Elección de la Prueba

Tal como se muestra en el siguiente cuadro:

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
VARIABLE ALEATORIA VARIABLE FIJA		NOMINAL DICOTOMICA	NOMINAL POLITÓMICA	ORDINAL	NUMÉRICA
Estudio Transversal Muestras Independientes	Un grupo	X^2 Bondad de Ajuste Binomial	X^2 Bondad de Ajuste	X^2 Bondad de Ajuste	T de Student para una muestra
	Dos grupos	X^2 de Homogeneidad Corrección de Yates. Test exacto de Fisher	X^2 de Homogeneidad	U Mann-Withney	T de Student para muestras independientes
	Más de dos grupos	X^2 de Homogeneidad	Análisis de correspondencias	H Kruskal-Wallis	ANOVA con un factor INTERsujetos
Estudio Longitudinal Muestras Relacionadas	Dos medidas	McNemar	McNemar-Bowker	Wilcoxon	T de Student para muestras relacionadas
	Mas de dos medidas	Q de Cochran	Q de Cochran	Friedman	ANOVA para medidas repetidas

Tabla 1 - Cuadro de ayuda para elección de la Prueba para la Hipótesis General.

- Estudio Longitudinal (Muestras Relacionadas)
- Variable Aleatoria (Dos medidas)
- Pruebas No Paramétricas (Ordinal)
- Prueba Wilcoxon

5. Calcular Prueba Wilcoxon

Decisión Estadística

Descriptivos				
			Estadístico	Desv. Error
Inicial	Media		3,65	,259
	95% de intervalo de confianza para la media	Límite inferior	3,14	
		Límite superior	4,16	
	Media recortada al 5%		3,61	
	Mediana		3,00	
	Varianza		7,628	
	Desv. Desviación		2,762	
	Mínimo		1	
	Máximo		7	
	Rango		6	
	Rango intercuartil		6	
	Asimetría		,299	,226
	Curtosis		-1,787	,449
Final	Media		5,22	,146
	95% de intervalo de confianza para la media	Límite inferior	4,93	
		Límite superior	5,51	
	Media recortada al 5%		5,24	
	Mediana		5,00	
	Varianza		2,421	
	Desv. Desviación		1,556	
	Mínimo		3	
	Máximo		7	
	Rango		4	
	Rango intercuartil		3	
	Asimetría		,028	,226
	Curtosis		-1,595	,449

Tabla 12 - Cálculo de la Prueba Wilcoxon para la Hipótesis General.

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre Inicial y Final es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Tabla 2 - Resumen de la Prueba Wilcoxon para la Hipótesis General.

P-Valor = 0,000 **<** **α = 0.05**

Interpretación**:**

Hay una diferencia significativa en las medidas de la gestión de riegos en activos de información del inicio (antes) y final (después) de la implementación del sistema de Gestión de Seguridad de la Información.

Por lo cual se concluye que la implementación del SGSI SI INFLUYE SIGNIFICATIVAMENTE **en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima.**

De hecho, La implementación del Sistema de Gestión de Seguridad de la Información en promedio de su media, subieron la gestión de riegos en activos de información de 3,65 a 5,22

EL CRITERIO PARA DECIDIR ES:

Si la probabilidad obtenida:

P-valor <= α, rechace H0, (Se acepta H1)

Si la probabilidad obtenida:

P-valor > α, no rechace H0, (Se acepta H0).

ENTONCES SE ACEPTA H_1:

H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima.

4.2.3. Hipótesis Especifica 01

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.

1. **Redactar las Hipótesis H_0 y H_1**

   Donde H_0 es la Hipótesis Nula y **H_1** es la Hipótesis Alterna.

   H_0 = La implementación del Sistema de Gestión de Seguridad de la Información NO influye significativamente en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.

   H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.

2. **Definir Alfa α**

   Alfa = 0.05 = 5%

3. **Calcular el P-Valor**

   NORMALIDAD

   - Kolmogorov-Smirnov muestras grandes (>30 individuos)
   - Shápiro Wilk muestras pequeñas (<30 individuos).

   Criterio para determinar Normalidad:

   P-valor => α,

   Aceptar H_0 = Los datos provienen de una distribución normal.

   P-valor < α,

Aceptar H_1 = Los datos NO provienen de una distribución normal.

Pruebas de normalidad							
		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Dimensiones	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Inicial	Controles de Seguridad de Gestión	,316	81	,000	,716	81	,000
Final	Controles de Seguridad de Gestión	,312	81	,000	,787	81	,000
a. Corrección de significación de Lilliefors							

Tabla 14 - Pruebas de normalidad para la Hipótesis Específica 01.

NORMALIDAD		
P-Valor (inicial) = 0,000	<	α = 0.05
P-Valor (final) = 0,000	<	α = 0.05
Interpretación: **Los datos del pre test (inicial) y post test (final) NO provienen de una distribución** normal		

Tabla 15 - Interpretación de la normalidad para la Hipótesis Específica 01.

4. Elección de la Prueba

Tal como se muestra en el siguiente cuadro:

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
VARIABLE ALEATORIA / VARIABLE FIJA		NOMINAL DICOTOMICA	NOMINAL POLITÓMICA	ORDINAL	NUMÉRICA
Estudio Transversal Muestras Independientes	Un grupo	X^2 Bondad de Ajuste Binomial	X^2 Bondad de Ajuste	X^2 Bondad de Ajuste	T de Student para una muestra
	Dos grupos	X^2 de Homogeneidad Corrección de Yates. Test exacto de Fisher	X^2 de Homogeneidad	U Mann-Withney	T de Student para muestras independientes
	Más de dos grupos	X^2 de Homogeneidad	Análisis de correspondencias	H Kruskal-Wallis	ANOVA con un factor INTERsujetos
Estudio Longitudinal Muestras Relacionadas	Dos medidas	McNemar	McNemar-Bowker	Wilcoxon	T de Student para muestras relacionadas
	Mas de dos medidas	Q de Cochran	Q de Cochran	Friedman	ANOVA para medidas repetidas

Tabla 3 - Cuadro de ayuda para elección de la prueba para la Hipótesis Específica 01.

- Estudio Longitudinal (Muestras Relacionadas)
- Variable Aleatoria (Dos medidas)
- Pruebas No Paramétricas (Ordinal)
- Prueba Wilcoxon

5. Calcular Prueba Wilcoxon

Decisión Estadística

Descriptivos					
	Dimensiones			Estadístico	Desv. Error
Inicial	Controles de Seguridad de Gestión	Media		4,14	,311
		95% de intervalo de confianza para la media	Límite inferior	3,52	
			Límite superior	4,75	
		Media recortada al 5%		4,15	
		Mediana		3,00	
		Varianza		7,819	
		Desv. Desviación		2,796	
		Mínimo		1	
		Máximo		7	
		Rango		6	
		Rango intercuartil		6	
		Asimetría		-,034	,267
		Curtosis		-1,904	,529
Final	Controles de Seguridad de Gestión	Media		5,52	,172
		95% de intervalo de confianza para la media	Límite inferior	5,18	
			Límite superior	5,86	
		Media recortada al 5%		5,58	
		Mediana		5,00	
		Varianza		2,403	
		Desv. Desviación		1,550	
		Mínimo		3	
		Máximo		7	
		Rango		4	
		Rango intercuartil		3	
		Asimetría		-,345	,267
		Curtosis		-1,468	,529

Tabla 17 - Cálculo de la Prueba Wilcoxon para la Hipótesis Específica 01.

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre Controles de Seguridad de Gestión y Controles de Seguridad de Gestión es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Tabla 4 - Resumen de la Prueba Wilcoxon para la Hipótesis General.

P-Valor = 0,000 **<** **α = 0.05**

Interpretación**:**

Hay una diferencia significativa en las medidas de los Controles de Seguridad Gestión del inicio (antes) y final (después) de la implementación del sistema de Gestión de Seguridad de la Información.

Por lo cual se concluye que la implementación del SGSI SI INFLUYE SIGNIFICATIVAMENTE **los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.**

De hecho, La implementación del Sistema de Gestión de Seguridad de la Información en promedio de su media, subieron los Controles de Seguridad de Gestión de 4,14 a 5,52

EL CRITERIO PARA DECIDIR ES:

Si la probabilidad obtenida:

P-valor <= α, rechace H0, (Se acepta H1)

Si la probabilidad obtenida:

P-valor > α, no rechace H0, (Se acepta H0).

ENTONCES SE ACEPTA H1:

H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.

4.2.4. Hipótesis Especifica 02

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.

1. **Redactar las Hipótesis H_0 y H_1**

   Donde H_0 es la Hipótesis Nula y **H_1** es la Hipótesis Alterna.

   H_0 = La implementación del Sistema de Gestión de Seguridad de la Información NO influye significativamente en los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.

   H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.

2. **Definir Alfa α**

   Alfa = 0.05 = 5%

3. **Calcular el P-Valor**

   NORMALIDAD

   - Kolmogorov-Smirnov muestras grandes (>30 individuos)
   - Shápiro Wilk muestras pequeñas (<30 individuos).

   Criterio para determinar Normalidad:

   P-valor => α,

   Aceptar H_0 = Los datos provienen de una distribución normal.

   P-valor < α,

Aceptar H_1 = Los datos NO provienen de una distribución normal.

Pruebas de normalidad							
		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Dimensiones	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Inicial	Controles de Seguridad Lógicos	,438	21	,000	,521	21	,000
Final	Controles de Seguridad Lógicos	,375	21	,000	,715	21	,000
a. Corrección de significación de Lilliefors							

Tabla 19 - Pruebas de normalidad para la Hipótesis Específica 02.

NORMALIDAD		
P-Valor (inicial) = 0,000	<	α = 0.05
P-Valor (final) = 0,000	<	α = 0.05
Interpretación: **Los datos del pre test (inicial) y post test (final) NO provienen de una distribución** normal		

Tabla 20 - Interpretación de la normalidad para la Hipótesis Específica 02.

4. Elección de la Prueba

Tal como se muestra en el siguiente cuadro:

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
VARIABLE ALEATORIA / VARIABLE FIJA		NOMINAL DICOTOMICA	NOMINAL POLITÓMICA	ORDINAL	NUMÉRICA
Estudio Transversal Muestras Independientes	Un grupo	X^2 Bondad de Ajuste Binomial	X^2 Bondad de Ajuste	X^2 Bondad de Ajuste	T de Student para una muestra
	Dos grupos	X^2 de Homogeneidad Corrección de Yates. Test exacto de Fisher	X^2 de Homogeneidad	U Mann-Withney	T de Student para muestras independientes
	Más de dos grupos	X^2 de Homogeneidad	Análisis de correspondencias	H Kruskal-Wallis	ANOVA con un factor INTERsujetos
Estudio Longitudinal Muestras Relacionadas	Dos medidas	McNemar	McNemar-Bowker	Wilcoxon	T de Student para muestras relacionadas
	Mas de dos medidas	Q de Cochran	Q de Cochran	Friedman	ANOVA para medidas repetidas

Tabla 5- Cuadro de ayuda para la elección de la prueba para la Hipótesis Específica 02.

- Estudio Longitudinal (Muestras Relacionadas)
- Variable Aleatoria (Dos medidas)
- Pruebas No Paramétricas (Ordinal)
- Prueba Wilcoxon

5. Calcular Prueba Wilcoxon

Decisión Estadística

Descriptivos					
	Dimensiones			Estadístico	Desv. Error
Inicial	Controles de Seguridad Lógicos	Media		1,67	,319
		95% de intervalo de confianza para la media	Límite inferior	1,00	
			Límite superior	2,33	
		Media recortada al 5%		1,42	
		Mediana		1,00	
		Varianza		2,133	
		Desv. Desviación		1,461	
		Mínimo		1	
		Máximo		7	
		Rango		6	
		Rango intercuartil		1	
		Asimetría		2,775	,501
		Curtosis		8,734	,972
Final	Controles de Seguridad Lógicos	Media		4,24	,181
		95% de intervalo de confianza para la media	Límite inferior	3,86	
			Límite superior	4,62	
		Media recortada al 5%		4,16	
		Mediana		4,00	
		Varianza		,690	
		Desv. Desviación		,831	
		Mínimo		3	
		Máximo		7	
		Rango		4	
		Rango intercuartil		1	
		Asimetría		1,816	,501
		Curtosis		5,598	,972

Tabla 22 - Cálculo de la Prueba Wilcoxon para la Hipótesis Específica 02.

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre Controles de Seguridad Lógicos y Controles de Seguridad Lógicos es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Tabla 6 - Resumen de la Prueba Wilcoxon para la Hipótesis Específica 02.

P-Valor = 0,000 < α = 0.05

Interpretación**:**

Hay una diferencia significativa en las medidas de los Controles de Seguridad Lógicos del inicio (antes) y final (después) de la implementación del Sistema de Gestión de Seguridad de la Información.

Por lo cual se concluye que la implementación del SGSI SI INFLUYE SIGNIFICATIVAMENTE **a los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.**

De hecho, La implementación del Sistema de Gestión de Seguridad de la Información en promedio de su media, subieron los Controles de Seguridad Lógicos de 1,67 a 4,24

EL CRITERIO PARA DECIDIR ES:

Si la probabilidad obtenida:

P-valor <= α, rechace H0, (Se acepta H1)

Si la probabilidad obtenida:

P-valor > α, no rechace H0, (Se acepta H0).

ENTONCES SE ACEPTA H1:

H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.

4.2.5. Hipótesis Especifica 03

La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.

1. **Redactar las Hipótesis H_0 y H_1**

   Donde H_0 es la Hipótesis Nula y **H_1** es la Hipótesis Alterna.

   H_0 = La implementación del Sistema de Gestión de Seguridad de la Información NO influye significativamente en los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.

   H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.

2. **Definir Alfa α**

   Alfa = 0.05 = 5%

3. **Calcular el P-Valor**

   NORMALIDAD

   - Kolmogorov-Smirnov muestras grandes (>30 individuos)
   - Shápiro Wilk muestras pequeñas (<30 individuos).

   Criterio para determinar Normalidad:

   P-valor => α,

   Aceptar Ho = Los datos provienen de una distribución normal.

   P-valor < α,

Aceptar H1 = Los datos NO provienen de una distribución normal.

Pruebas de normalidad							
		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Dimensiones	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Inicial	Controles de Seguridad Físicos	,280	12	,010	,733	12	,002
Final	Controles de Seguridad Físicos	,283	12	,009	,741	12	,002
a. Corrección de significación de Lilliefors							

Tabla 24 - Pruebas de normalidad para la Hipótesis Específica 03.

NORMALIDAD		
P-Valor (inicial) = 0,000	<	α = 0.05
P-Valor (final) = 0,000	<	α = 0.05
Interpretación: **Los datos del pre test (inicial) y post test (final) NO provienen de una distribución** normal		

Tabla 25 - Interpretación de la normalidad para la Hipótesis Específica 03.

4. Elección de la Prueba

Tal como se muestra en el siguiente cuadro:

		PRUEBAS NO PARAMETRICAS			PRUEBAS PARAMETRICAS
VARIABLE ALEATORIA / VARIABLE FIJA		NOMINAL DICOTOMICA	NOMINAL POLITÓMICA	ORDINAL	NUMÉRICA
Estudio Transversal Muestras Independientes	Un grupo	X^2 Bondad de Ajuste Binomial	X^2 Bondad de Ajuste	X^2 Bondad de Ajuste	T de Student para una muestra
	Dos grupos	X^2 de Homogeneidad Corrección de Yates. Test exacto de Fisher	X^2 de Homogeneidad	U Mann-Withney	T de Student para muestras independientes
	Más de dos grupos	X^2 de Homogeneidad	Análisis de correspondencias	H Kruskal-Wallis	ANOVA con un factor INTERsujetos
Estudio Longitudinal Muestras Relacionadas	Dos medidas	McNemar	McNemar-Bowker	Wilcoxon	T de Student para muestras relacionadas
	Mas de dos medidas	Q de Cochran	Q de Cochran	Friedman	ANOVA para medidas repetidas

Tabla 7 - Cuadro de ayuda para la elección de la prueba para la Hipótesis Específica 03.

- Estudio Longitudinal (Muestras Relacionadas)
- Variable Aleatoria (Dos medidas)
- Pruebas No Paramétricas (Ordinal)
- Prueba Wilcoxon

5. Calcular Prueba Wilcoxon

Decisión Estadística

Descriptivos					
	Dimensiones			Estadístico	Desv. Error
Inicial	Controles de Seguridad Físicos	Media		3,83	,833
		95% de intervalo de confianza para la media	Límite inferior	2,00	
			Límite superior	5,67	
		Media recortada al 5%		3,81	
		Mediana		3,00	
		Varianza		8,333	
		Desv. Desviación		2,887	
		Mínimo		1	
		Máximo		7	
		Rango		6	
		Rango intercuartil		6	
		Asimetría		,199	,637
		Curtosis		-2,159	1,232
Final	Controles de Seguridad Físicos	Media		4,92	,543
		95% de intervalo de confianza para la media	Límite inferior	3,72	
			Límite superior	6,11	
		Media recortada al 5%		4,91	
		Mediana		4,00	
		Varianza		3,538	
		Desv. Desviación		1,881	
		Mínimo		3	
		Máximo		7	
		Rango		4	
		Rango intercuartil		4	
		Asimetría		,242	,637
		Curtosis		-2,141	1,232

Tabla 27 - Cálculo de la Prueba Wilcoxon para la Hipótesis Específica 03.

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre Controles de Seguridad Físicos y Controles de Seguridad Físicos es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,016	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Tabla 8 - Resumen de la Prueba Wilcoxon para la Hipótesis Específica 03.

P-Valor = 0,000 < α = 0.05

Interpretación**:**

Hay una diferencia significativa en las medidas de los Controles de Seguridad Físicos del inicio (antes) y final (después) de la implementación del Sistema de Gestión de Seguridad de la Información.

Por lo cual se concluye que la implementación del SGSI SI INFLUYE SIGNIFICATIVAMENTE **a los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.**

De hecho, La implementación del Sistema de Gestión de Seguridad de la Información en promedio de su media, subieron los Controles Físicos de 3,83 a 4,92

EL CRITERIO PARA DECIDIR ES:

Si la probabilidad obtenida:

P-valor <= α, rechace H0, (Se acepta H1)

Si la probabilidad obtenida:

P-valor > α, no rechace H0, (Se acepta H0).

ENTONCES SE ACEPTA H1:

H_1 = La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.

CAPÍTULO V

5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Con los resultados obtenidos se logró determinar el rechazo de las Hipótesis nulas y se evidencia el impacto que produjo el trabajo de investigación al haber determinado los resultados favorables de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, considerando que el valor en promedio de la Gestión de riesgos subió de 3,65 a 5,22, en otros términos el nivel de Madurez respecto a la seguridad de la información mejoró considerablemente.

Al determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en los Controles de Seguridad de Gestión, se evidenció una mejora del valor promedio de 4,14 a 5,52, esto quiere decir que la documentación, procesos y procedimientos se gestionan de manera más eficiente, dejando un presente de la importancia inherente que tienen estos controles para la gestión de los riesgos.

Al haber mejorado el valor promedio de los Controles Lógicos de 1,67 a 4,24 se determinó en qué medida favorece la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Lógicos y como parte fundamental de la gestión de riesgos estos controles son de gran importancia para la mejora del estado de madurez de la gestión de riegos en activos de información.

Se determinó en qué grado favorece la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Físicos con una mejora del valor promedio de 3,83 a 4,92, siguiendo el esquema de niveles de madurez se demuestra la imperante necesidad de implementar controles físicos para una eficiente gestión de riesgos en activos de información, en otras palabras se subió un escalón en la escala de madurez del SGSI.

Un SGSI consiste en las políticas, procedimientos, directrices y recursos y actividades asociados, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información. (ISO/IEC 27001:2013). Como podemos ver la teoría aplicada va de la mano con los resultados obtenidos demostrando que el SGSI siendo un conjunto de diversos controles al ser implementado logra salvaguardar los activos de información de manera óptima es decir la gestión de riesgos se realiza y se mantiene de manera eficiente, con estos resultados considero que el presente trabajo de investigación puede ser referente para futuras investigaciones siendo un hito que pueda servir de partida para la innovación de proyectos.

CONCLUSIONES

1. Se cumplieron los objetivos definidos para la investigación al determinar que existe una influencia evidente de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima.
2. Al resolver un claro incremento en los valores obtenidos del pre test y post test se ultima que la hipótesis “La implementación del Sistema de Gestión de Seguridad de la Información genera resultados en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima, es aceptada, a su vez se rechaza la hipótesis nula.
3. De cara a futuros estudios sería conveniente ampliar la muestra de la población para analizar y contrastar los nuevos resultados con los obtenidos en la investigación asimismo se puede combinar metodologías para analizar si los resultados tienen alguna variación.
4. Se concluye que el trabajo de investigación demuestra con resultados positivos que la metodología y pautas de las bases teóricas son confiables y que pueden ser aplicados para futuras investigaciones.
5. Por último, podemos concluir que con los resultados obtenidos se logró determinar el incremento del valor promedio de la Gestión de Riesgos en activos de información de un 3,65 a un 5,22, en otras palabras su nivel madurez mejoró llegando a un estado Definido/Administrado existiendo una relación clara entre el SGSI y la gestión de riegos en activos de información.

RECOMENDACIONES

1. Se recomienda que los resultados obtenidos sean publicados para que puedan servir de referencia para futuras investigaciones.
2. Se recomienda que la información de gestión, procedimientos y documentación sean utilizadas para la capacitación de usuarios y concientización de estos con respecto a la Seguridad de la Información.
3. Se recomienda replicar la metodología para los demás procesos de la organización o para toda la organización.
4. Es recomendable tener cuidado con la aplicación incorrecta de los resultados especialmente si se busca una certificación con la ISO 27001.

REFERENCIAS BIBLIOGRAFICAS

1. ERNST & YOUNG. 21: 21a Encuesta Global de Seguridad de la Información (GISS) [online]. Encuesta. 2019. [Accessed 17 January 2020]. Available from: https://americas.ey-vx.com/916/14087/landing-pages/ey-ec-giss-2019-26mar19-secured.pdf
2. GIL MENA, Fiorella. Redacción. Ciberseguridad: El 70% del valor de una empresa puede ser afectado tras un ataque informático. Gestión [online]. 27 September 2018. [Accessed 22 November 2019]. Available from: https://gestion.pe/tecnologia/ciberseguridad-70-empresa-afectado-ataque-informatico-245430-noticia/Pese a esto, aún son muy pocas empresas las que están preparadas para un ciberataque. El 80% de ataques provienen de adentro de la compañía.
3. ATALAYA VÁSQUEZ, Oscar. Propuesta de un sistema de seguridad de la información para la oficina de admisión y registro académico de la Universidad Privada Antonio Guillermo Urrelo, 2016 [online]. 2016. [Accessed 22 November 2019]. Available from: http://repositorio.upagu.edu.pe/handle/UPAGU/96
4. SALINAS RODRÍGUEZ, Michael Steve y VALENCIA MONCADA, Julio Andrés. Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú. [online]. 2017. [Accessed 22 November 2019]. Available from: http://repositorio.upn.edu.pe/handle/11537/11865
5. CARRANZA LUJÁN, Jorge y GÓMEZ HURTADO, Heber. Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001 para el Hospital Nivel 2 - La Caleta [online]. 2017. [Accessed 22 November 2019]. Available from: http://repositorio.usanpedro.edu.pe//handle/USANPEDRO/2473
6. HUANCA SUAQUITA, Jhon Richard. La falsa percepción en la seguridad de los sistemas informáticos [online]. 2018. [Accessed 22 November 2019]. Available from: http://repositorio.unap.edu.pe/handle/UNAP/8235

7. CUEVA ARAUJO, Paul Omar y RÍOS MERCADO, Juan Antonio. Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014 [online]. 2018. [Accessed 22 November 2019]. Available from: http://repositorio.upn.edu.pe/handle/11537/13676
8. FALIVENE, Lucas. Marco de referencia unificado en seguridad de la información [online]. Buenos Aires, Argentina, 2018. Available from: http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-1062_FaliveneL
9. YÁÑEZ CÁCERES, Nelson Alejandro. Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño [online]. Santiago de Chile, Chile, 2017. [Accessed 22 November 2019]. Available from: http://repositorio.uchile.cl/handle/2250/147976
10. CHANGOLUISA CRIOLLO, Wilson Fernando. Optimización del proceso de alta y baja de usuarios a través de la implementación de gestión de seguridad de la información, basado en la norma ISO 27001:2013 en una empresa de consultoría para la industria petrolera [online]. Quito, Ecuador, 2017. [Accessed 22 November 2019]. Available from: http://repositorio.puce.edu.ec:80/xmlui/handle/22000/13999
11. ÁLVAREZ ESPINOZA, Miguel Eduardo. Propuesta para La Gestión De La Seguridad de la Información en una Pequeña o Mediana Empresa [online]. Buenos Aires, Argentina, 2016. Available from: http://bibliotecadigital.econ.uba.ar/econ/collection/todo/document/1502-1059_AlvarezEspinosaME?p.s=TextQuery
12. NICASIO CHAVEZ, Omar. Diseño e Implementación de un Sistemas de Gestión de Calidad en Seguridad de la Información (SGSI) [online]. DF, México, 2015. Available from: http://132.248.9.195/ptd2015/mayo/0730130/0730130.pdf
13. ISO. ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements [online]. Geneva, Switzerland, 2013. [Accessed 22 November 2019]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

14. ISOTOOLS EXCELLENCE. ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información. [online]. 28 January 2015. [Accessed 30 November 2019]. Available from: https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/A la hora de implementar un Sistema de Gestión de Seguridad de la Información basado en el estándar internacional ISO 27001, debemos utilizar el ciclo PDCA (siglas en inglés) o PHVA (siglas en español).
15. MAGERIT V.3. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método [online]. Madrid, España, 2012. Available from: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
16. LEGISLACIÓN PERUANA. LEY 29733 - Ley de Protección de Datos Personales [online]. 2013. [Accessed 17 January 2020]. Available from: https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf
17. APDP, AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES. Directiva-de-Seguridad [online]. 2013. [Accessed 17 January 2020]. Available from: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf
18. ISO. ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary [online]. Geneva, Switzerland, 2018. [Accessed 17 January 2020]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
19. ACOSTA RODRÍGUEZ, David E. Despliegue de Medidas – Revista SIC. 2018 [online]. 2018. Vol. 130. [Accessed 27 November 2019]. Available from: https://www.deacosta.com/wp-content/uploads/2018/06/SIC130_122-124.pdfhttps://www.deacosta.com/wp-content/uploads/2018/06/SIC130_122-124.pdfCategorización funcional de los diferentes tipos de controles de seguridad y su aplicabilidad en la estrategia de protección corporativa

20. HERNÁNDEZ CHANTO, Allan. El método hipotético-deductivo como legado del positivismo lógico y el racionalismo crítico: Su influencia en la economía. Ciencias Económicas. 2008. No. 2, p. 13.
21. SÁNCHEZ, H. y REYES, C. Metodología y Diseños en la Investigación Científica. Lima: Visión Universitaria, 2006.
22. HERNÁNDEZ SAMPIERI, Roberto, FERNÁNDEZ COLLADO, Carlos y BAPTISTA LUCIO, Pilar. Metodología de la investigación. México: McGraw Hill Interamericana, 2014. ISBN 978-1-4562-2396-0.
23. ARIAS, F. El Proyecto de Investigación. Caracas, Venezuela: EPISTEME, C.A., 1999.
24. MEJÍA MEJÍA, Elías. Metodología de La Investigación. Primera. Lima, Perú, 2005.
25. VARA HORNA, Arístides Alfredo. ¿Cómo hacer una tesis en ciencias empresariales? Manual breve para los tesistas de Administración, Negocios Internacionales, Recursos Humanos y Marketing. Facultad de Ciencias Administrativas y Recursos Humanos de la Universidad de San Martín de Porres. Primera edición (versión extendida). Lima, Perú, 2008.
26. ÑAUPAS PAITÁN, Humberto, MEJÍA MEJÍA, Elías, NOVOA RAMÍREZ, Eliana y VILLAGÓMEZ PAUCAR, Alberto. Metodología de la investigación: cuantitativa-cualitativa y redacción de la tesis. 2014. ISBN 978-958-762-188-4.

ANEXOS

ANEXO 1: DESARROLLO DE LA METODOLOGÍA DEL SGSI.

El trabajo de investigación está basado en la implantación de un SGSI específicamente en la aplicación de los Objetivos de Control de Seguridad de la Información recomendados y especificados en la norma internacional ISO 27001:2013 aplicados a la Gestión de Riesgos de Activos de información en empresa Digitex Perú SAC, el desarrollo del trabajo al tratarse de un Sistema de Gestión se estructuró tomando como base el Ciclo de Deming (Ciclo PDCA).

6. PLANIFICACIÓN (PLAN)

En la primera etapa de acuerdo al Ciclo PDCA, se conoció a la organización para establecer el Alcance, se definieron los contenidos que tendrá la Política de Seguridad de la Información, se propuso los miembros del comité del SGSI, se realizó al análisis de riesgo de los activos de información para definir la aplicabilidad de los controles y se realizó el análisis de brechas para conocer el estado de controles del SGSI para determinar el estado actual.

6.1. Alcance

6.1.1. La Organización

Existe información importante y crítica ya sea de los clientes, otros comercios, infraestructura interna como hardware y software, documentación de gestión y jurídica, datos personales, etc. que se son activos de información fundamentales en los procesos la organización, es por ello la necesidad imperante de una adecuada gestión de riesgos de los activos de información, este proceso actualmente no se encuentra revisado ni auditado a pesar de contar con documentación inicial y una política de seguridad de la información definida. Con la propuesta de mejora e implementación de los Controles de Seguridad del SGSI se quiere reducir

significativamente las brechas encontradas en la Gestión de Riesgos y hacer cumplir con la Política de Seguridad de la Información haciendo participes activos a todos los involucrados dentro del proceso definido en el alcance.

6.1.2. Alcance

En coordinación con la Dirección, se consideró para la investigación el proceso “PSSGG_01 Gestión de Recursos Asignados al Personal” que engloba dos procedimientos importantes de la organización e involucra a tres de las principales áreas de esta (RRHH, IT, SSGG). De este modo precisamos el alcance del SGSI, en el Documento “1_Alcance_SGSI” que será detallado en la segunda etapa del Ciclo PDCA.

Nombre: Sistema de Gestión de Seguridad de la información

Alcance: Proceso
PSSGG_01 Gestión de Recursos Asignados al Personal

Descripción
Incluye para los siguientes procedimientos:

Procedimiento de registro de recursos para nuevas incorporaciones.
Procedimiento de baja de recursos de personal cesado.
Adicionalmente, incluye los servicios internos de IT que soportan estos procedimientos.

Proceso: PSSGG_01 Gestión de Recursos Asignados al Personal

Procedimiento de Registro de recursos para nuevas incorporaciones

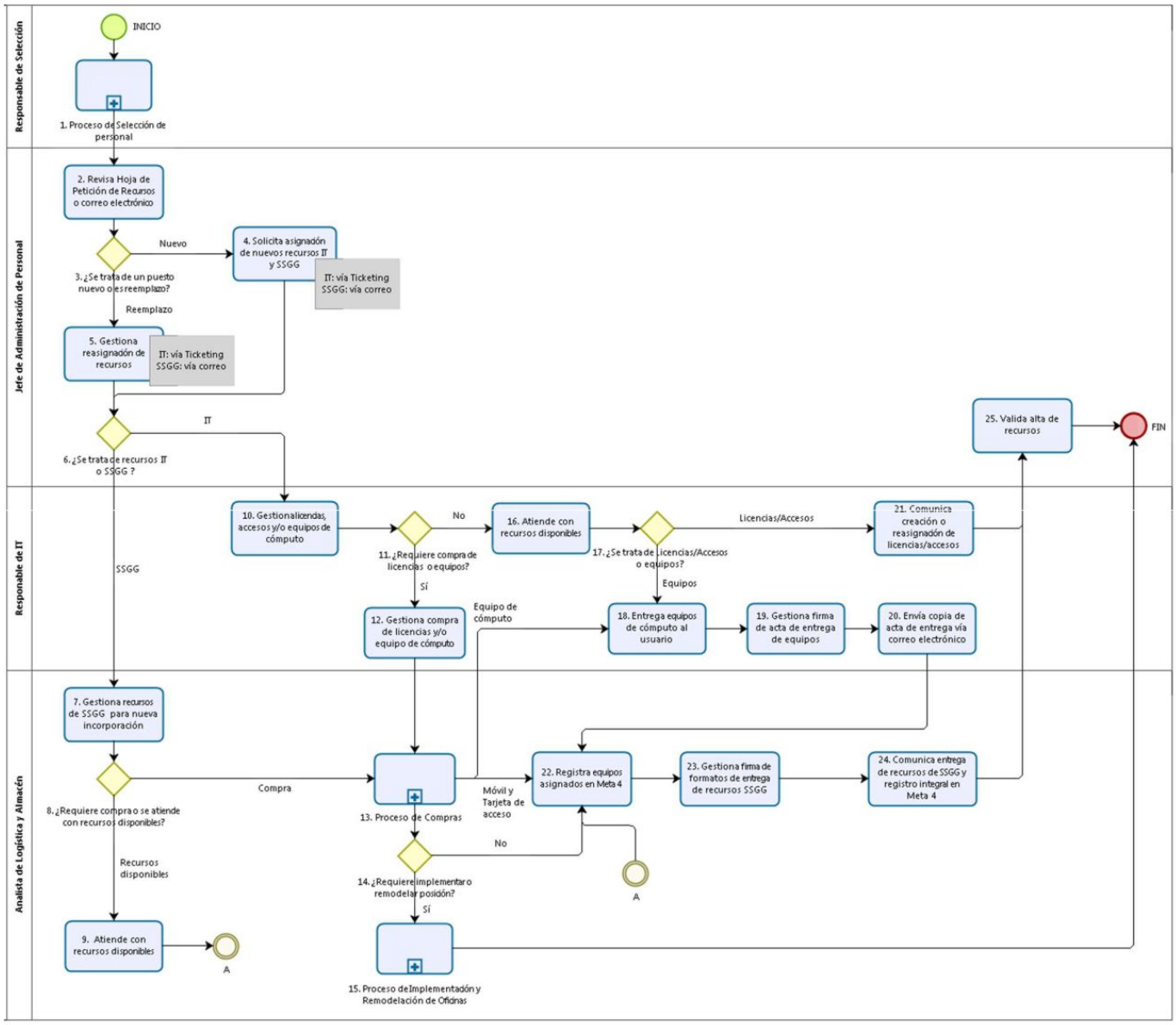


Figura 12 - Flujograma del procedimiento de registro de recursos para nuevas incorporaciones.

Fuente: Proceso PSSGG_01 - Digitex Perú SAC.

Procedimiento de Baja de recursos de personal cesado.

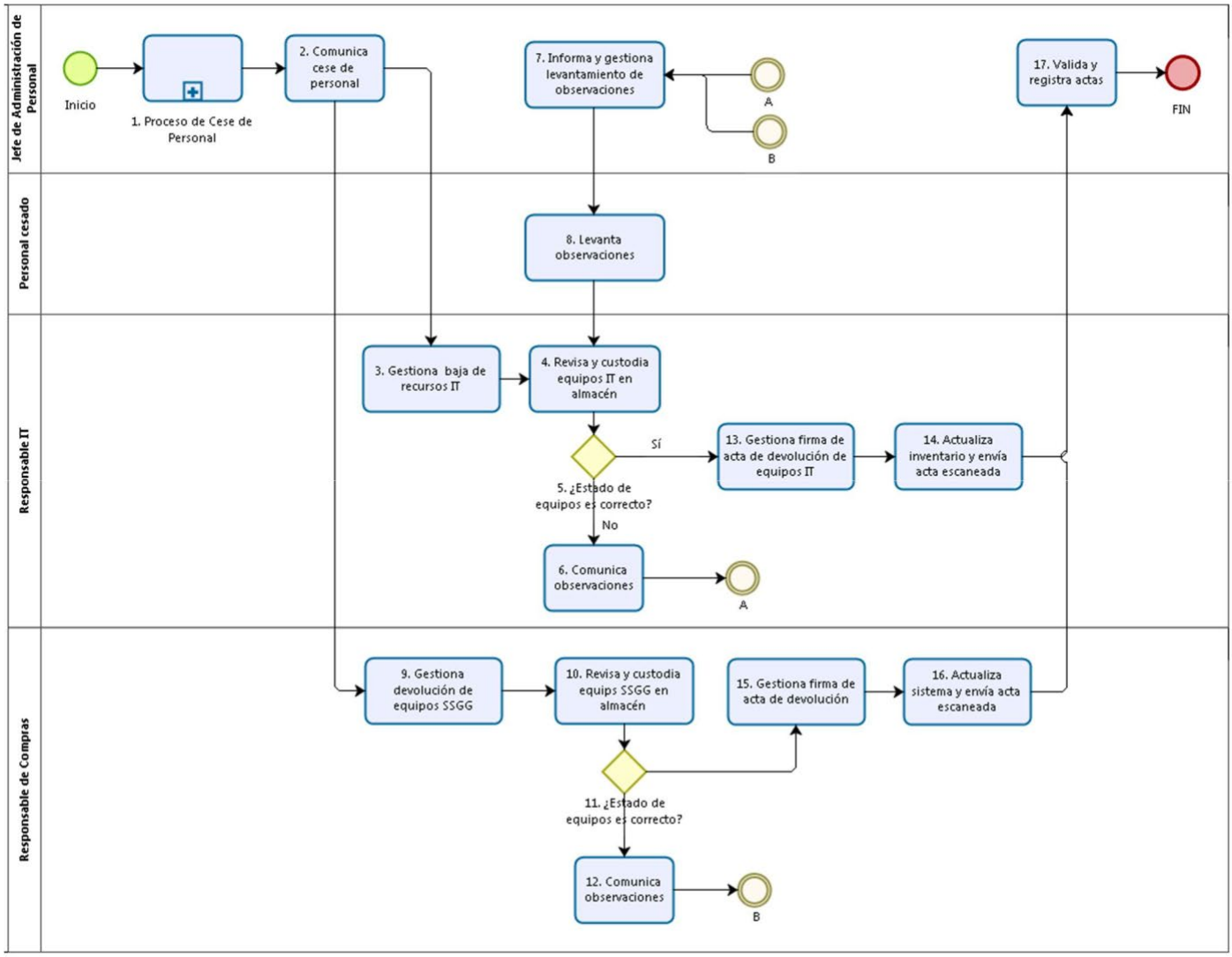


Figura 13 - Flujograma del procedimiento de Baja de recursos de personal cesado.

Fuente: Proceso PSSGG_01 - Digitex Perú SAC.

6.2. Política de seguridad de la Información.

6.2.1. Marco Legal

Es indiscutible que la Ley de Datos Personales N°29733 da un aval importante en el presente trabajo de investigación, teniendo en cuenta lo indicado en el Anexo “C” de la Directiva sobre la aplicabilidad de la norma ISO/IEC 27001:2013 para la gestión de bancos de datos personales.

6.2.2. Definición de la Política

En la presente investigación se dio a conocer la documentación propuesta que define las políticas de seguridad de la información luego de la aplicación de la metodología de análisis de riesgos en los activos de información y con la revisión de la Dirección de IT se seleccionaron las políticas que son parte de los controles del SGSI y están en base a los procesos definidos en el alcance, los puntos considerados son los siguientes y serán detallados en la Segunda Fase del Ciclo PDCA (DO o *Hacer*).

- Control de acceso
- Gestión de activos
- Uso de dispositivos móviles
- Responsabilidad por los activos
- Áreas seguras
- Seguridad en las operaciones
- Política de copias de respaldo de la información
- Seguridad en las comunicaciones
- Uso de correo electrónico
- Uso adecuado de internet
- Gestión de incidentes de seguridad
- Tratamiento y gestión del riesgo en seguridad de la información.

6.3. Metodología de Análisis de riesgos

Siguiendo con la fase de Planificación elegimos y definimos como metodología a “MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, así mismo nos apoyaremos en los Catálogos de la metodología para poder hacer una identificación de activos con la mayor exactitud dentro del proceso definido en el alcance.

6.3.1. Paso 1: Activos

La identificación de activos de información se realizó tomando como base la documentación de los flujos (procedimientos) incluidos en el proceso definido dentro del alcance de la presente investigación, de acuerdo a la MAGERIT se entiende como Activo a un “Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización”, dentro del proceso se identificaron los siguientes activos:

- Correo Electrónico
- Sistema CIA
- Formato de Petición de Recursos
- Formato de Recursos de SSGG
- Contratos del Personal
- Sistema Ticketing
- Equipos de Cómputo
- Internet
- Impresora
- Teléfono IP
- Directorio Activo
- Sistema Oracle
- Sistemas META4

- Sistema SIM
- Software Ofimática
- Fotocheck
- Smartphone
- Sistema de SSGG
- Sistema de Inventario TI
- Formato de Entrega de Recursos
- Servidor de Archivos
- Red Interna
- Responsable de RRHH
- Responsable de SSGG
- Responsable de TI
- Personal de mando medio
- Personal operativo

Siguiendo los criterios de la MAGERIT para poder clasificar los activos identificados utilizaremos los siguientes tipos:

TIPOS DE ACTIVOS DE INFORMACIÖN	
[D]	Datos / Información
[K]	Claves criptográficas
[S]	Servicios
[SW]	Aplicaciones (software)
[HW]	Equipamiento informático (hardware)
[COM]	Redes de comunicaciones
[Media]	Soportes de información
[AUX]	Equipamiento auxiliar
[L]	Instalaciones
[P]	Personal

Tabla 29 - Tipos de Activos de Información.

Fuente: Elaboración propia basado en el Catálogo de MAGERIT V3.

Clasificación de activos de la información en base a los Tipos definidos.

Inventario de Activos de Información		Tipos de Activos de Información									
Nro.	Nombre	[D]	[K]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]
1	Correo Electrónico			X							
2	Sistema CIA				X						
3	Formato de Petición de Recursos	X						X			
4	Formato de Recursos de SSGG	X						X			
5	Contratos del Personal	X						X			
6	Sistema Ticketing				X						
7	Equipos de Cómputo					X				X	
8	Internet			X							
9	Impresora					X				X	
10	Teléfono IP					X					
11	Directorio Activo	X		X		X				X	
12	Sistema Oracle				X						
13	Sistemas META4				X						
14	Sistema SIM				X						
15	Software Ofimática				X						
16	Fotocheck	X						X			
17	Smartphone					X					
18	Sistema de SSGG				X						
19	Sistema de Inventario TI				X						
20	Formato de Entrega de Recursos	X						X			
21	Servidor de Archivos	X		X		X				X	
22	Red Interna					X	X				
23	Responsable de RRHH										X
24	Responsable de SSGG										X
25	Responsable de TI										X
26	Personal de mando medio										X
27	Personal operativo										X

Tabla 30 - Clasificación de los Activos de la Información.

Fuente: Elaboración propia en base al Inventario de Activos vs Tabla 29.

Para la valoración de los activos de información utilizamos:

Dimensiones de valoración	
[C]	Confidencialidad
[I]	Integridad
[D]	Disponibilidad

Tabla 31 - Dimensiones de Valoración de Activos de Información.

Fuente: Elaboración propia en base a la MAGERIT V.3.

Criterios de valoración según las Dimensiones de MAGERIT V.3

CRITERIOS		DIMENSIONES DE VALORACIÓN		
CUALITATIVA	VALOR	CONFIDENCIALIDAD [C]	INTEGRIDAD [I]	DISPONIBILIDAD [D]
MUY BAJO	1	El acceso no autorizado a la información que gestiona el activo o el propio activo de la información no tiene Ningún impacto en el Proceso u Organización.	La falta de completitud o exactitud de la información que gestiona el activo o el propio activo de la información no tiene Ningún impacto en el Proceso u Organización.	La indisponibilidad parcial o total de la información que gestiona el activo o el propio activo de la información no tiene Ningún impacto en el Proceso u Organización.
BAJO	2	El acceso no autorizado a la información que gestiona el activo o el propio activo de la información tiene un impacto Bajo en el Proceso u Organización.	La falta de completitud o exactitud de la información que gestiona el activo o el propio activo de la información tiene un impacto Bajo en el Proceso u Organización.	La indisponibilidad parcial o total de la información que gestiona el activo o el propio activo de la información tiene un impacto Bajo en el Proceso u Organización.
MEDIO	3	El acceso no autorizado a la información que gestiona el activo o el propio activo de la información tiene un impacto Moderado en el Proceso u Organización.	La falta de completitud o exactitud de la información que gestiona el activo o el propio activo de la información tiene un impacto Moderado en el Proceso u Organización.	La indisponibilidad parcial o total de la información que gestiona el activo o el propio activo de la información tiene un impacto Moderado en el Proceso u Organización.
ALTO	4	El acceso no autorizado a la información que gestiona el activo o el propio activo de la información tiene un impacto Alto en el Proceso u Organización.	La falta de completitud o exactitud de la información que gestiona el activo o el propio activo de la información tiene un impacto Alto en el Proceso u Organización.	La indisponibilidad parcial o total de la información que gestiona el activo o el propio activo de la información tiene un impacto Alto en el Proceso u Organización.
MUY ALTO	5	El acceso no autorizado a la información que gestiona el activo o el propio activo de la información tiene un impacto Muy Alto (Crítico) en el Proceso u Organización.	La falta de completitud o exactitud de la información que gestiona el activo o el propio activo de la información tiene un impacto Muy Alto (Crítico) en el Proceso u Organización.	La indisponibilidad parcial o total de la información que gestiona el activo o el propio activo de la información tiene un impacto Muy Alto (Crítico) en el Proceso u Organización.

Tabla 32 - Criterios de valoración de acuerdo a las Dimensiones.

Fuente: Elaboración propia en base a la MAGERIT V.3.

En base a los criterios se diseñó un formulario en línea para que los responsables de cada área involucrada en la organización les otorguen la valoración correspondiente a los activos de la información del inventario.

Link del Formulario

https://docs.google.com/forms/d/e/1FAIpQLSfRS8n7tbgHmm_tmGX4dTlXymbzXFkkAKHwJDOIXzIozJ1qvQ/viewform

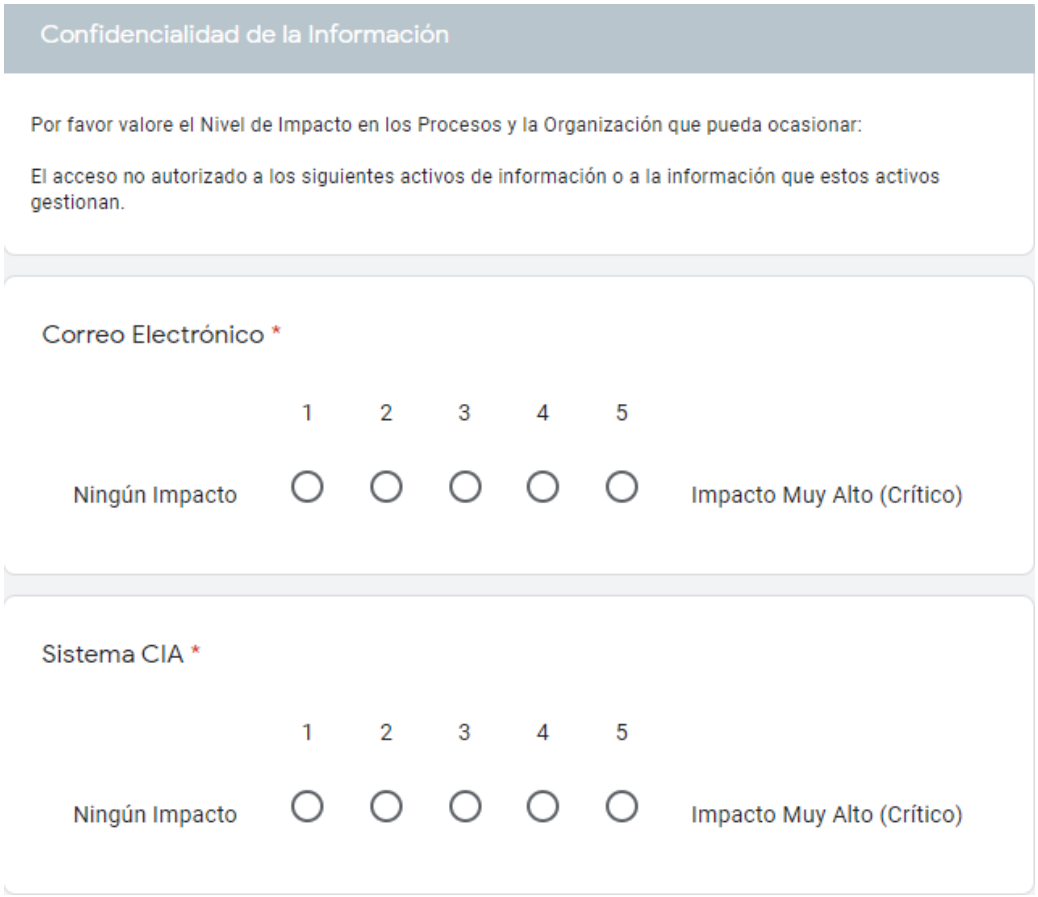


Figura 14 - Evidencia del Formulario para Valoración de Activos de Información.

Fuente: Elaboración propia basado en el inventario de activos y los criterios de valoración.

Una vez recopilados los datos de valoración de cada activo se consolidaron para hacer los cálculos correspondientes y obtener el promedio de valoración de cada activo, de esta misma manera se hizo la valoración cualitativa en base a los criterios de la Tabla 32.

Nro.	NOMBRE	CRITERIOS DE VALORACION									TOTAL	
		RRHH			SSGG			TI			CUANTITATIVA	CUALITATIVA
		[C]	[I]	[D]	[C]	[I]	[D]	[C]	[I]	[D]		
1	Correo Electrónico	4	4	5	5	4	4	5	5	5	5	MUY ALTO
2	Sistema CIA	5	5	5	3	3	2	3	2	2	4	ALTO
3	Formato de Petición de Recursos TI	3	3	2	3	3	3	4	4	4	4	ALTO
4	Formato de Recursos de SSGG	3	3	2	5	5	5	1	1	1	3	MEDIO
5	Contratos del Personal	5	5	5	3	2	2	1	2	1	3	MEDIO
6	Sistema Ticketing Service Desk	3	3	2	3	2	2	4	4	4	3	MEDIO
7	Equipos de Cómputo	5	3	4	5	4	4	4	4	4	5	MUY ALTO
8	Internet	4	4	4	4	4	4	4	4	4	4	ALTO
9	Impresora	5	5	2	3	3	3	2	2	2	3	MEDIO
10	Teléfono IP	2	2	2	3	2	2	1	2	2	2	BAJO
11	Directorio Activo	3	3	3	3	4	3	5	5	5	4	ALTO
12	Sistema Oracle	5	5	5	5	5	5	3	4	3	5	MUY ALTO
13	Sistema META4	5	5	5	3	2	2	3	3	3	4	ALTO
14	Sistema SIM	5	5	5	3	2	2	3	2	1	4	ALTO
15	Software Ofimática	2	3	3	4	4	3	2	2	3	3	MEDIO
16	Fotochek	5	3	4	5	3	4	5	5	5	5	MUY ALTO
17	Smartphone	3	3	3	3	4	3	3	3	3	4	ALTO
18	Sistema de SSGG	3	3	2	5	5	5	1	1	1	3	MEDIO
19	Sistema de Inventario TI	3	3	2	4	2	2	4	4	4	4	ALTO
20	Formato de Entrega de Recursos	2	3	2	2	5	4	3	3	3	3	MEDIO
21	Servidor de Archivos	5	5	5	5	5	4	5	5	5	5	MUY ALTO
22	Red Interna	4	4	5	4	4	4	4	4	4	5	MUY ALTO
23	Responsable de RRHH	5	5	5	4	3	2	2	2	2	4	ALTO
24	Responsable de SSGG	4	4	3	5	5	5	2	2	2	4	ALTO
25	Responsable de TI	4	5	3	4	4	3	5	5	5	5	MUY ALTO
26	Personal de mando medio	4	4	4	4	4	4	4	4	4	4	ALTO
27	Personal operativo	3	3	3	3	3	3	3	3	3	3	MEDIO

Tabla 33 - Consolidado de datos de valoración y valoración final de cada activo de información.

Fuente: Elaboración propia en base a los datos obtenidos con el Formulario de Valoración.

6.3.2. Paso 2: Amenazas

Para identificar las amenazas se utilizó el catálogo de la MAGERIT V.3 y la clasificación de activos de la Tabla 30.

Amenazas identificadas:

- Acceso no autorizado
- Errores de mantenimiento
- Difusión de software dañino
- Fugas de información
- Modificación deliberada de la información
- Abuso de privilegios de acceso
- Incendio
- Daños por agua
- Desastres naturales
- Falla Eléctrica
- Avería de HW
- Error de Configuración
- Destrucción de información
- Manipulación de los equipos
- Manipulación de programas
- Robo
- Manipulación de los registros de actividad
- Alteración accidental de la información
- Perdida de medios de comunicación
- Error de Usuario
- Avería de HW
- Falla Eléctrica
- Pérdida de equipos
- Ingeniería social

Valoración de Amenazas.

Siguiendo la metodología se debe valorar las amenazas identificadas en función a la Degradación que provocaría en el activo de información (Impacto) y a la Probabilidad que se materialice la amenaza.

Para fines de la investigación el valor del Impacto será el obtenido del promedio de la valoración de cada activo de información en base a sus dimensiones de acuerdo a la Tabla 33.

Para determinar el valor de la Probabilidad de ocurrencia de la amenaza se diseñó un formulario en línea para que los responsables de cada área involucrada determinen en base a su criterio y experiencia el valor adecuado para la ocurrencia de cada amenaza de acuerdo al cuadro de Probabilidades elaborado en base a la MAGERIT.

VALORES DE PROBABILIDAD		
CUANTITATIVO	**CUALITATIVO**	**DESCRIPCIÓN**
5	MA	Probabilidad Muy Alta
4	A	Probabilidad Alta
3	M	Probabilidad Media
2	B	Probabilidad Baja
1	MB	Probabilidad Muy Baja

Tabla 34 - Escala de probabilidad de ocurrencia de Amenazas.

Fuente: Elaboración propia en base a la MAGERIT V.3.

Link:
https://docs.google.com/forms/d/e/1FAIpQLSfQfe7L7VFiqr973IVJuIH5QKBgQyWWUAUAWgkXf2cdYBFUKg/viewform

Formulario de Probabilidad de Ocurrencia:

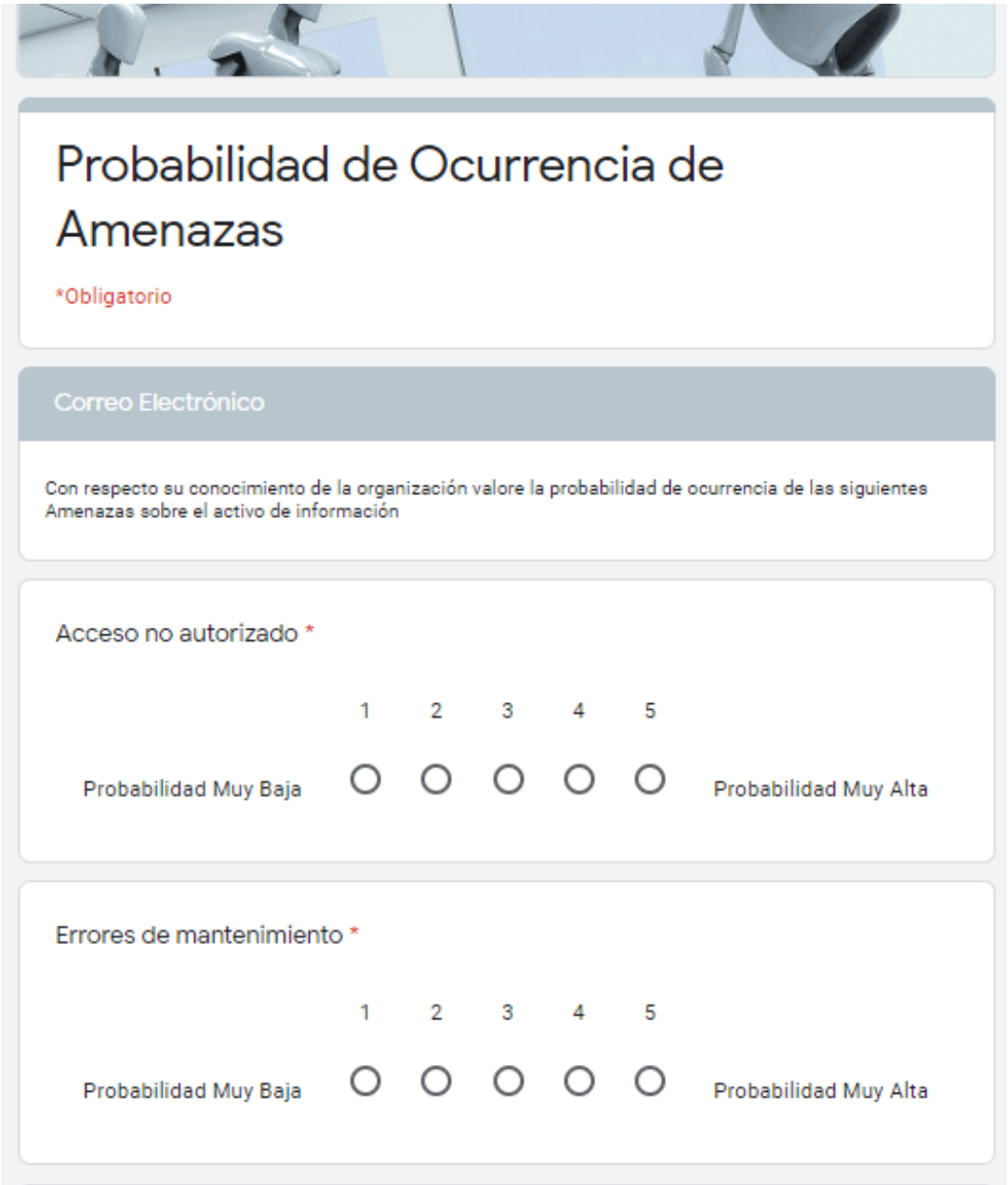


Figura 15 - Evidencia del Formulario para determinar la probabilidad de ocurrencia de las Amenazas en los Activos de Información.

Fuente: Elaboración propia.

Se procesaron los datos obtenidos de los responsables de cada área con respecto a la ocurrencia de cada amenaza en el respectivo activo de información que le corresponde de acuerdo a su clasificación, se promediaron los valores obtenidos para poder utilizarlos posteriormente para el cálculo del riesgo de las amenazas sobre los activos de información.

Tabla 35 - Consolidado de datos de Probabilidad de Ocurrencia de Amenazas.

Fuente: Elaboración propia.

ACTIVO	AMENAZA	PROBABILIDAD			
		RRHH	SSGG	TI	PROMEDIO
Correo Electrónico	Acceso no autorizado	1	2	5	3
	Errores de mantenimiento	1	2	2	2
	Difusión de software dañino	1	5	5	4
	Fugas de información	1	5	5	4
Servidor de Archivos	Modificación deliberada de la información	2	5	2	3
	Acceso no autorizado	1	5	5	4
	Abuso de privilegios de acceso	2	4	5	4
	Errores de mantenimiento	1	4	2	3
	Incendio	1	2	3	2
	Daños por agua	1	2	3	2
	Desastres naturales	1	1	1	1
	Falla Eléctrica	1	2	3	2
	Avería de HW	1	1	4	2
	Error de Configuración	1	1	3	2
	Destrucción de información	1	2	4	3
Equipos de Cómputo	Abuso de privilegios de acceso	2	4	4	4
	Acceso no autorizado	1	3	3	3
	Avería de HW	1	3	2	2
	Daños por agua	1	3	2	2
	Desastres naturales	1	2	1	2
	Difusión de software dañino	1	4	2	3
	Errores de mantenimiento	1	3	2	2
	Falla Eléctrica	1	2	2	2
	Incendio	1	2	2	2
	Manipulación de los equipos	1	3	3	3
	Manipulación de programas	1	2	5	3
	Robo	1	1	3	2
Internet	Abuso de privilegios de acceso	2	4	5	4
	Errores de mantenimiento	1	4	2	3

Directorio Activo	Abuso de privilegios de acceso	2	2	5	3
	Avería de HW	1	1	2	2
	Errores de mantenimiento	1	1	2	2
	Error de Configuración Perfiles	1	3	5	3
	Manipulación de los registros de actividad	1	2	4	3
Sistema Oracle	Abuso de privilegios de acceso	2	2	5	3
	Alteración accidental de la información	1	2	4	3
	Destrucción de información	1	1	3	2
	Errores de mantenimiento	1	1	2	2
Fotochek	Abuso de privilegios de acceso	2	1	5	3
	Robo	1	1	2	2
Red Interna	Acceso no autorizado	1	2	5	3
	Avería de HW	1	2	2	2
	Daños por agua	1	1	1	1
	Desastres naturales	1	1	1	1
	Errores de mantenimiento	1	1	2	2
	Falla Eléctrica	1	1	2	2
	Incendio	1	1	1	1
	Manipulación de los equipos	1	2	2	2
	Perdida de medios de comunicación	1	2	3	2
Sistema CIA	Abuso de privilegios de acceso	1	2	3	2
	Alteración accidental de la información	1	2	2	2
	Destrucción de información	1	1	2	2
	Errores de mantenimiento	1	1	2	2
	Manipulación de los registros de actividad	1	1	3	2
Formato de Petición de Recursos TI	Alteración accidental de la información	1	2	3	2
	Daños por agua	1	1	1	1
	Desastres naturales	1	1	1	1
	Destrucción de información	1	1	1	1
	Error de Usuario	2	1	1	2
	Incendio	1	1	1	1
Formato de Recursos de SSGG	Alteración accidental de la información	1	1	1	1
	Daños por agua	1	1	1	1
	Desastres naturales	1	1	1	1
	Destrucción de información	1	1	1	1
	Error de Usuario	2	1	1	2
	Incendio	1	1	1	1
Contratos del Personal	Acceso no autorizado	1	3	3	3
	Alteración accidental de la información	1	2	3	2
	Daños por agua	1	1	1	1
	Desastres naturales	1	1	1	1
	Destrucción de información	1	1	1	1
	Error de Usuario	2	1	1	2

	Fugas de información	1	1	1	1
	Incendio	1	2	1	2
Sistema Ticketing Service Desk	Abuso de privilegios de acceso	1	2	5	3
	Alteración accidental de la información	1	1	2	2
	Avería de HW	1	2	2	2
	Destrucción de información	1	1	1	1
	Error de Usuario	1	2	2	2
	Errores de mantenimiento	1	2	2	2
	Manipulación de los registros de actividad	1	1	2	2
Impresora	Avería de HW	1	2	1	2
	Daños por agua	1	1	1	1
	Desastres naturales	1	2	1	2
	Falla Eléctrica	1	3	1	2
	Incendio	1	1	1	1
	Manipulación de los equipos	1	3	1	2
	Fugas de información	1	4	1	2
	Robo	1	3	1	2
Sistema META4	Abuso de privilegios de acceso	1	4	4	3
	Alteración accidental de la información	1	2	4	3
	Destrucción de información	1	2	1	2
	Errores de mantenimiento	1	1	1	1
	Manipulación de los registros de actividad	1	1	1	1
Sistema SIM	Abuso de privilegios de acceso	1	2	1	2
	Alteración accidental de la información	1	1	1	1
	Destrucción de información	1	1	1	1
	Errores de mantenimiento	1	1	1	1
	Manipulación de los registros de actividad	1	1	1	1
Software Ofimática	Abuso de privilegios de acceso	1	2	1	2
	Manipulación de programas	1	2	1	2
Smartphone	Difusión de software dañino	1	4	5	4
	Avería de HW	1	4	1	2
	Pérdida de equipos	1	3	1	2
	Robo	1	3	1	2
Sistema de SSGG	Abuso de privilegios de acceso	1	2	1	2
	Alteración accidental de la información	1	1	1	1
	Destrucción de información	1	2	1	2
	Errores de mantenimiento	1	1	1	1
	Fugas de información	1	2	1	2
	Manipulación de los registros de actividad	1	1	1	1
Sistema de Inventario TI	Abuso de privilegios de acceso	1	2	5	3
	Alteración accidental de la información	1	2	4	3
	Destrucción de información	1	2	1	2

	Errores de mantenimiento	1	3	1	2
	Fugas de información	1	3	1	2
	Manipulación de los registros de actividad	1	3	1	2
Formato de Entrega de Recursos	Alteración accidental de la información	1	4	4	3
	Daños por agua	1	4	1	2
	Desastres naturales	1	4	1	2
	Destrucción de información	1	4	1	2
	Error de Usuario	1	5	1	3
	Incendio	1	2	1	2
Responsable de TI	Fugas de información	1	4	5	4
	Ingeniería social	1	4	5	4
Responsable de SSGG	Fugas de información	1	4	3	3
	Ingeniería social	1	4	3	3
Responsable de RRHH	Fugas de información	1	4	5	4
	Ingeniería social	1	4	5	4
Personal de mando medio	Fugas de información	1	4	5	4
	Ingeniería social	1	4	5	4
Personal operativo	Fugas de información	1	4	1	2
	Ingeniería social	1	4	1	2

Determinación del Riesgo.

Con los datos obtenidos de Impacto y Probabilidad hacemos el cálculo para obtener una estimación del riesgo para cada amenaza como se muestra en la siguiente Tabla.´

Tabla 36 - Determinación del Riesgo de cada Amenaza.

Fuente: Elaboración propia.

ACTIVO	AMENAZA	IMPACTO	PROBABILIDAD	RIESGO
Correo Electrónico	Acceso no autorizado	5	3	15
	Errores de mantenimiento	5	2	10
	Difusión de software dañino	5	4	20
	Fugas de información	5	4	20
Servidor de Archivos	Modificación deliberada de la información	5	3	15
	Acceso no autorizado	5	4	20
	Abuso de privilegios de acceso	5	4	20
	Errores de mantenimiento	5	3	15
	Incendio	5	2	10
	Daños por agua	5	2	10
	Desastres naturales	5	1	5
	Falla Eléctrica	5	2	10
	Avería de HW	5	2	10
	Error de Configuración	5	2	10
	Destrucción de información	5	3	15
Equipos de Cómputo	Abuso de privilegios de acceso	5	4	20
	Acceso no autorizado	5	3	15
	Avería de HW	5	2	10
	Daños por agua	5	2	10
	Desastres naturales	5	2	10
	Difusión de software dañino	5	3	15
	Errores de mantenimiento	5	2	10
	Falla Eléctrica	5	2	10
	Incendio	5	2	10
	Manipulación de los equipos	5	3	15
	Manipulación de programas	5	3	15
	Robo	5	2	10
Internet	Abuso de privilegios de acceso	4	4	16
	Errores de mantenimiento	4	3	12
Directorio Activo	Abuso de privilegios de acceso	4	3	12
	Avería de HW	4	2	8

	Errores de mantenimiento	4	2	8
	Error de Configuración Perfiles	4	3	12
	Manipulación de los registros de actividad	4	3	12
Sistema Oracle	Abuso de privilegios de acceso	5	3	15
	Alteración accidental de la información	5	3	15
	Destrucción de información	5	2	10
	Errores de mantenimiento	5	2	10
Fotochek	Abuso de privilegios de acceso	5	3	15
	Robo	5	2	10
Red Interna	Acceso no autorizado	5	3	15
	Avería de HW	5	2	10
	Daños por agua	5	1	5
	Desastres naturales	5	1	5
	Errores de mantenimiento	5	2	10
	Falla Eléctrica	5	2	10
	Incendio	5	1	5
	Manipulación de los equipos	5	2	10
	Perdida de medios de comunicación	5	2	10
Sistema CIA	Abuso de privilegios de acceso	4	2	8
	Alteración accidental de la información	4	2	8
	Destrucción de información	4	2	8
	Errores de mantenimiento	4	2	8
	Manipulación de los registros de actividad	4	2	8
Formato de Petición de Recursos TI	Alteración accidental de la información	4	2	8
	Daños por agua	4	1	4
	Desastres naturales	4	1	4
	Destrucción de información	4	1	4
	Error de Usuario	4	2	8
	Incendio	4	1	4
Formato de Recursos de SSGG	Alteración accidental de la información	4	1	4
	Daños por agua	4	1	4
	Desastres naturales	4	1	4
	Destrucción de información	4	1	4
	Error de Usuario	4	2	8
	Incendio	4	1	4
Contratos del Personal	Acceso no autorizado	3	3	9
	Alteración accidental de la información	3	2	6
	Daños por agua	3	1	3
	Desastres naturales	3	1	3
	Destrucción de información	3	1	3
	Error de Usuario	3	2	6
	Fugas de información	3	1	3
	Incendio	3	2	6

Sistema Ticketing Service Desk	Abuso de privilegios de acceso	3	3	9
	Alteración accidental de la información	3	2	6
	Avería de HW	3	2	6
	Destrucción de información	3	1	3
	Error de Usuario	3	2	6
	Errores de mantenimiento	3	2	6
	Manipulación de los registros de actividad	3	2	6
Impresora	Avería de HW	3	2	6
	Daños por agua	3	1	3
	Desastres naturales	3	2	6
	Falla Eléctrica	3	2	6
	Incendio	3	1	3
	Manipulación de los equipos	3	2	6
	Fugas de información	3	2	6
	Robo	3	2	6
Sistema META4	Abuso de privilegios de acceso	4	3	12
	Alteración accidental de la información	4	3	12
	Destrucción de información	4	2	8
	Errores de mantenimiento	4	1	4
	Manipulación de los registros de actividad	4	1	4
Sistema SIM	Abuso de privilegios de acceso	4	2	8
	Alteración accidental de la información	4	1	4
	Destrucción de información	4	1	4
	Errores de mantenimiento	4	1	4
	Manipulación de los registros de actividad	4	1	4
Software Ofimática	Abuso de privilegios de acceso	3	2	6
	Manipulación de programas	3	2	6
Smartphone	Difusión de software dañino	4	4	16
	Avería de HW	4	2	8
	Pérdida de equipos	4	2	8
	Robo	4	2	8
Sistema de SSGG	Abuso de privilegios de acceso	3	2	6
	Alteración accidental de la información	3	1	3
	Destrucción de información	3	2	6
	Errores de mantenimiento	3	1	3
	Fugas de información	3	2	6
	Manipulación de los registros de actividad	3	1	3
Sistema de Inventario TI	Abuso de privilegios de acceso	4	3	12
	Alteración accidental de la información	4	3	12
	Destrucción de información	4	2	8
	Errores de mantenimiento	4	2	8
	Fugas de información	4	2	8

	Manipulación de los registros de actividad	4	2	8
Formato de Entrega de Recursos	Alteración accidental de la información	3	3	9
	Daños por agua	3	2	6
	Desastres naturales	3	2	6
	Destrucción de información	3	2	6
	Error de Usuario	3	3	9
	Incendio	3	2	6
Responsable de TI	Fugas de información	5	4	20
	Ingeniería social	5	4	20
Responsable de SSGG	Fugas de información	4	3	12
	Ingeniería social	4	3	12
Responsable de RRHH	Fugas de información	4	4	16
	Ingeniería social	4	4	16
Personal de mando medio	Fugas de información	4	4	16
	Ingeniería social	4	4	16
Personal operativo	Fugas de información	3	2	6
	Ingeniería social	3	2	6

Aceptación del Riesgo.

Continuando con la metodología vamos a valorar el riesgo en base a los indicadores de la Tabla 37 para luego determinar la aceptación y el plan tratamiento de los riesgos en base a los criterios de la tabla 38.

VALORACIÓN DEL RIESGO							
RIESGO			PROBABILIDAD				
			MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
			1	2	3	4	5
IMPACTO	MUY BAJO	1	1	2	3	4	5
	BAJO	2	2	4	6	8	10
	MEDIO	3	3	6	9	12	15
	ALTO	4	4	8	12	16	20
	MUY ALTO	5	5	10	15	20	25

Tabla 37 - Cuadro de valoración del Riesgo

Fuente: Elaboración propia basado en la MAGERIT V.3.

VALORES DE RIESGO			
ESCALA		NIVEL DE ACEPTACIÓN DEL RIESGO	
MUY BAJO	1 - 2	ACEPTABLE	RIESGO ACEPTABLE PARA LA ORGANIZACIÓN NO REQUIERE TRATAMIENTO.
BAJO	3 - 4	ACEPTABLE	RIESGO ACEPTABLE PARA LA ORGANIZACIÓN NO REQUIERE TRATAMIENTO.
MEDIO	5 - 9	INACEPTABLE	RIESGO INACEPTABLE PARA LA ORGANIZACIÓN REQUIERE TRATAMIENTO.
ALTO	10 - 19	INACEPTABLE	RIESGO INACEPTABLE PARA LA ORGANIZACIÓN REQUIERE TRATAMIENTO.
MUY ALTO	20 - 25	CRÍTICO	RIESGO CRÍTICO PARA LA ORGANIZACIÓN REQUIERE TRATAMIENTO PRIORITARO.

Tabla 38 - Escala de Aceptación de Riesgos.

Fuente: Elaboración propia basado en la MAGERIT V.3.

Valoración y aceptación de riesgos.

Tabla 39 - Valoración cualitativa de los Riesgos y Aceptación de Riesgos.

Fuente: Elaboración propia en base a los criterios de las Tablas 37 y 38.

ACTIVO	AMENAZA	RIESGO		ACEPTACION DE RIESGOS
		CUANTITATIVO	CUALITATIVO	
Correo Electrónico	Acceso no autorizado	15	ALTO	INACEPTABLE
	Errores de mantenimiento	10	ALTO	INACEPTABLE
	Difusión de software dañino	20	MUY ALTO	CRITICO
	Fugas de información	20	MUY ALTO	CRITICO
Servidor de Archivos	Modificación deliberada de la información	15	ALTO	INACEPTABLE
	Acceso no autorizado	20	MUY ALTO	CRITICO
	Abuso de privilegios de acceso	20	MUY ALTO	CRITICO
	Errores de mantenimiento	15	ALTO	INACEPTABLE
	Incendio	10	ALTO	INACEPTABLE
	Daños por agua	10	ALTO	INACEPTABLE
	Desastres naturales	5	MEDIO	INACEPTABLE
	Falla Eléctrica	10	ALTO	INACEPTABLE
	Avería de HW	10	ALTO	INACEPTABLE
	Error de Configuración	10	ALTO	INACEPTABLE
	Destrucción de información	15	ALTO	INACEPTABLE
Equipos de Cómputo	Abuso de privilegios de acceso	20	MUY ALTO	CRITICO
	Acceso no autorizado	15	ALTO	INACEPTABLE

	Avería de HW	10	ALTO	INACEPTABLE
	Daños por agua	10	ALTO	INACEPTABLE
	Desastres naturales	10	ALTO	INACEPTABLE
	Difusión de software dañino	15	ALTO	INACEPTABLE
	Errores de mantenimiento	10	ALTO	INACEPTABLE
	Falla Eléctrica	10	ALTO	INACEPTABLE
	Incendio	10	ALTO	INACEPTABLE
	Manipulación de los equipos	15	ALTO	INACEPTABLE
	Manipulación de programas	15	ALTO	INACEPTABLE
	Robo	10	ALTO	INACEPTABLE
Internet	Abuso de privilegios de acceso	16	ALTO	INACEPTABLE
	Errores de mantenimiento	12	ALTO	INACEPTABLE
Directorio Activo	Abuso de privilegios de acceso	12	ALTO	INACEPTABLE
	Avería de HW	8	MEDIO	INACEPTABLE
	Errores de mantenimiento	8	MEDIO	INACEPTABLE
	Error de Configuración Perfiles	12	ALTO	INACEPTABLE
	Manipulación de los registros de actividad	12	ALTO	INACEPTABLE
Sistema Oracle	Abuso de privilegios de acceso	15	ALTO	INACEPTABLE
	Alteración accidental de la información	15	ALTO	INACEPTABLE
	Destrucción de información	10	ALTO	INACEPTABLE
	Errores de mantenimiento	10	ALTO	INACEPTABLE
Fotochek	Abuso de privilegios de acceso	15	ALTO	INACEPTABLE
	Robo	10	ALTO	INACEPTABLE
Red Interna	Acceso no autorizado	15	ALTO	INACEPTABLE
	Avería de HW	10	ALTO	INACEPTABLE
	Daños por agua	5	MEDIO	INACEPTABLE
	Desastres naturales	5	MEDIO	INACEPTABLE

	Errores de mantenimiento	10	ALTO	INACEPTABLE
	Falla Eléctrica	10	ALTO	INACEPTABLE
	Incendio	5	MEDIO	INACEPTABLE
	Manipulación de los equipos	10	ALTO	INACEPTABLE
	Perdida de medios de comunicación	10	ALTO	INACEPTABLE
Sistema CIA	Abuso de privilegios de acceso	8	MEDIO	INACEPTABLE
	Alteración accidental de la información	8	MEDIO	INACEPTABLE
	Destrucción de información	8	MEDIO	INACEPTABLE
	Errores de mantenimiento	8	MEDIO	INACEPTABLE
	Manipulación de los registros de actividad	8	MEDIO	INACEPTABLE
Formato de Petición de Recursos TI	Alteración accidental de la información	8	MEDIO	INACEPTABLE
	Daños por agua	4	MEDIO	INACEPTABLE
	Desastres naturales	4	MEDIO	INACEPTABLE
	Destrucción de información	4	MEDIO	INACEPTABLE
	Error de Usuario	8	MEDIO	INACEPTABLE
	Incendio	4	BAJO	ACEPTABLE
Formato de Recursos de SSGG	Alteración accidental de la información	4	BAJO	ACEPTABLE
	Daños por agua	4	BAJO	ACEPTABLE
	Desastres naturales	4	BAJO	ACEPTABLE
	Destrucción de información	4	BAJO	ACEPTABLE
	Error de Usuario	8	MEDIO	INACEPTABLE
	Incendio	4	BAJO	ACEPTABLE
Contratos del Personal	Acceso no autorizado	9	MEDIO	INACEPTABLE
	Alteración accidental de la información	6	MEDIO	INACEPTABLE
	Daños por agua	3	BAJO	ACEPTABLE
	Desastres naturales	3	BAJO	ACEPTABLE
	Destrucción de información	3	BAJO	ACEPTABLE

	Error de Usuario	6	MEDIO	INACEPTABLE
	Fugas de información	3	BAJO	ACEPTABLE
	Incendio	6	MEDIO	INACEPTABLE
Sistema Ticketing Service Desk	Abuso de privilegios de acceso	9	MEDIO	INACEPTABLE
	Alteración accidental de la información	6	MEDIO	INACEPTABLE
	Avería de HW	6	MEDIO	INACEPTABLE
	Destrucción de información	3	BAJO	ACEPTABLE
	Error de Usuario	6	MEDIO	INACEPTABLE
	Errores de mantenimiento	6	MEDIO	INACEPTABLE
	Manipulación de los registros de actividad	6	MEDIO	INACEPTABLE
Impresora	Avería de HW	6	MEDIO	INACEPTABLE
	Daños por agua	3	BAJO	ACEPTABLE
	Desastres naturales	6	MEDIO	INACEPTABLE
	Falla Eléctrica	6	MEDIO	INACEPTABLE
	Incendio	3	BAJO	ACEPTABLE
	Manipulación de los equipos	6	MEDIO	INACEPTABLE
	Fugas de información	6	MEDIO	INACEPTABLE
	Robo	6	MEDIO	INACEPTABLE
Sistema META4	Abuso de privilegios de acceso	12	ALTO	CRITICO
	Alteración accidental de la información	12	ALTO	CRITICO
	Destrucción de información	8	MEDIO	INACEPTABLE
	Errores de mantenimiento	4	BAJO	ACEPTABLE
	Manipulación de los registros de actividad	4	BAJO	ACEPTABLE
Sistema SIM	Abuso de privilegios de acceso	8	MEDIO	INACEPTABLE
	Alteración accidental de la información	4	BAJO	ACEPTABLE
	Destrucción de información	4	BAJO	ACEPTABLE
	Errores de mantenimiento	4	BAJO	ACEPTABLE

	Manipulación de los registros de actividad	4	BAJO	ACEPTABLE
Software Ofimática	Abuso de privilegios de acceso	6	MEDIO	INACEPTABLE
	Manipulación de programas	6	MEDIO	INACEPTABLE
Smartphone	Difusión de software dañino	16	ALTO	INACEPTABLE
	Avería de HW	8	MEDIO	INACEPTABLE
	Pérdida de equipos	8	MEDIO	INACEPTABLE
	Robo	8	MEDIO	INACEPTABLE
Sistema de SSGG	Abuso de privilegios de acceso	6	MEDIO	INACEPTABLE
	Alteración accidental de la información	3	BAJO	ACEPTABLE
	Destrucción de información	6	MEDIO	INACEPTABLE
	Errores de mantenimiento	3	BAJO	ACEPTABLE
	Fugas de información	6	MEDIO	INACEPTABLE
	Manipulación de los registros de actividad	3	BAJO	ACEPTABLE
Sistema de Inventario TI	Abuso de privilegios de acceso	12	ALTO	INACEPTABLE
	Alteración accidental de la información	12	ALTO	INACEPTABLE
	Destrucción de información	8	MEDIO	INACEPTABLE
	Errores de mantenimiento	8	MEDIO	INACEPTABLE
	Fugas de información	8	MEDIO	INACEPTABLE
	Manipulación de los registros de actividad	8	MEDIO	INACEPTABLE
Formato de Entrega de Recursos	Alteración accidental de la información	9	MEDIO	INACEPTABLE
	Daños por agua	6	MEDIO	INACEPTABLE
	Desastres naturales	6	MEDIO	INACEPTABLE
	Destrucción de información	6	MEDIO	INACEPTABLE
	Error de Usuario	9	MEDIO	INACEPTABLE
	Incendio	6	MEDIO	INACEPTABLE
Responsable de TI	Fugas de información	20	MUY ALTO	CRITICO

	Ingeniería social	20	MUY ALTO	CRITICO
Responsable de SSGG	Fugas de información	12	ALTO	INACEPTABLE
	Ingeniería social	12	ALTO	INACEPTABLE
Responsable de RRHH	Fugas de información	16	ALTO	INACEPTABLE
	Ingeniería social	16	ALTO	INACEPTABLE
Personal de mando medio	Fugas de información	16	ALTO	INACEPTABLE
	Ingeniería social	16	ALTO	INACEPTABLE
Personal operativo	Fugas de información	6	MEDIO	INACEPTABLE
	Ingeniería social	6	MEDIO	INACEPTABLE

Salvaguardas.

Una vez definida la aceptación del riesgo procederemos con la estrategia para el tratamiento de los riesgos de los riesgos Inaceptables y Críticos identificados, para así poder elegir las salvaguardas adecuadas en base a los controles del Anexo A de la ISO 27001.

Opciones de Tratamiento del Riesgo:

Son las opciones que la organización toma para el tratamiento de los riesgos identificados. Las opciones son: Mitigar, Aceptar, Transferir y Eliminar el riesgo.

Tabla 40 - Elección de estrategia de Tratamiento de los Riesgos.

Fuente: Elaboración propia.

ACTIVO	AMENAZA	RIESGO	ACEPTACION DE RIESGOS	PLAN DE TRATAMIENTO
				ESTRATEGIA
Correo Electrónico	Acceso no autorizado	ALTO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	ALTO	INACEPTABLE	MITIGAR
	Difusión de software dañino	MUY ALTO	CRITICO	MITIGAR
	Fugas de información	MUY ALTO	CRITICO	MITIGAR
Servidor de Archivos	Modificación deliberada de la información	ALTO	INACEPTABLE	MITIGAR
	Acceso no autorizado	MUY ALTO	CRITICO	MITIGAR
	Abuso de privilegios de acceso	MUY ALTO	CRITICO	MITIGAR
	Errores de mantenimiento	ALTO	INACEPTABLE	MITIGAR
	Incendio	ALTO	INACEPTABLE	MITIGAR
	Daños por agua	ALTO	INACEPTABLE	MITIGAR

	Desastres naturales	MEDIO	INACEPTABLE	MITIGAR
	Falla Eléctrica	ALTO	INACEPTABLE	MITIGAR
	Avería de HW	ALTO	INACEPTABLE	MITIGAR
	Error de Configuración	ALTO	INACEPTABLE	MITIGAR
	Destrucción de información	ALTO	INACEPTABLE	MITIGAR
Equipos de Cómputo	Abuso de privilegios de acceso	MUY ALTO	CRITICO	MITIGAR
	Acceso no autorizado	ALTO	INACEPTABLE	MITIGAR
	Avería de HW	ALTO	INACEPTABLE	MITIGAR
	Daños por agua	ALTO	INACEPTABLE	MITIGAR
	Desastres naturales	ALTO	INACEPTABLE	MITIGAR
	Difusión de software dañino	ALTO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	ALTO	INACEPTABLE	MITIGAR
	Falla Eléctrica	ALTO	INACEPTABLE	MITIGAR
	Incendio	ALTO	INACEPTABLE	MITIGAR
	Manipulación de los equipos	ALTO	INACEPTABLE	MITIGAR
	Manipulación de programas	ALTO	INACEPTABLE	MITIGAR
	Robo	ALTO	INACEPTABLE	MITIGAR
Internet	Abuso de privilegios de acceso	ALTO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	ALTO	INACEPTABLE	MITIGAR
Directorio Activo	Abuso de privilegios de acceso	ALTO	INACEPTABLE	MITIGAR
	Avería de HW	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	MEDIO	INACEPTABLE	MITIGAR
	Error de Configuración Perfiles	ALTO	INACEPTABLE	MITIGAR
	Manipulación de los registros de actividad	ALTO	INACEPTABLE	MITIGAR
Sistema Oracle	Abuso de privilegios de acceso	ALTO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	ALTO	INACEPTABLE	MITIGAR
	Destrucción de información	ALTO	INACEPTABLE	MITIGAR

	Errores de mantenimiento	ALTO	INACEPTABLE	MITIGAR
Fotochek	Abuso de privilegios de acceso	ALTO	INACEPTABLE	MITIGAR
	Robo	ALTO	INACEPTABLE	MITIGAR
Red Interna	Acceso no autorizado	ALTO	INACEPTABLE	MITIGAR
	Avería de HW	ALTO	INACEPTABLE	MITIGAR
	Daños por agua	MEDIO	INACEPTABLE	MITIGAR
	Desastres naturales	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	ALTO	INACEPTABLE	MITIGAR
	Falla Eléctrica	ALTO	INACEPTABLE	MITIGAR
	Incendio	MEDIO	INACEPTABLE	MITIGAR
	Manipulación de los equipos	ALTO	INACEPTABLE	MITIGAR
	Perdida de medios de comunicación	ALTO	INACEPTABLE	MITIGAR
Sistema CIA	Abuso de privilegios de acceso	MEDIO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	MEDIO	INACEPTABLE	MITIGAR
	Destrucción de información	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	MEDIO	INACEPTABLE	MITIGAR
	Manipulación de los registros de actividad	MEDIO	INACEPTABLE	MITIGAR
Formato de Petición de Recursos TI	Alteración accidental de la información	MEDIO	INACEPTABLE	MITIGAR
	Daños por agua	MEDIO	INACEPTABLE	MITIGAR
	Desastres naturales	MEDIO	INACEPTABLE	MITIGAR
	Destrucción de información	MEDIO	INACEPTABLE	MITIGAR
	Error de Usuario	MEDIO	INACEPTABLE	MITIGAR
	Incendio	BAJO	ACEPTABLE	ACEPTAR
Formato de Recursos de SSGG	Alteración accidental de la información	BAJO	ACEPTABLE	ACEPTAR
	Daños por agua	BAJO	ACEPTABLE	ACEPTAR
	Desastres naturales	BAJO	ACEPTABLE	ACEPTAR
	Destrucción de información	BAJO	ACEPTABLE	ACEPTAR

	Error de Usuario	MEDIO	INACEPTABLE	MITIGAR
	Incendio	BAJO	ACEPTABLE	ACEPTAR
Contratos del Personal	Acceso no autorizado	MEDIO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	MEDIO	INACEPTABLE	MITIGAR
	Daños por agua	BAJO	ACEPTABLE	ACEPTAR
	Desastres naturales	BAJO	ACEPTABLE	ACEPTAR
	Destrucción de información	BAJO	ACEPTABLE	ACEPTAR
	Error de Usuario	MEDIO	INACEPTABLE	MITIGAR
	Fugas de información	BAJO	ACEPTABLE	ACEPTAR
	Incendio	MEDIO	INACEPTABLE	MITIGAR
Sistema Ticketing Service Desk	Abuso de privilegios de acceso	MEDIO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	MEDIO	INACEPTABLE	MITIGAR
	Avería de HW	MEDIO	INACEPTABLE	MITIGAR
	Destrucción de información	BAJO	ACEPTABLE	ACEPTAR
	Error de Usuario	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	MEDIO	INACEPTABLE	MITIGAR
	Manipulación de los registros de actividad	MEDIO	INACEPTABLE	MITIGAR
Impresora	Avería de HW	MEDIO	INACEPTABLE	MITIGAR
	Daños por agua	BAJO	ACEPTABLE	ACEPTAR
	Desastres naturales	MEDIO	INACEPTABLE	MITIGAR
	Falla Eléctrica	MEDIO	INACEPTABLE	MITIGAR
	Incendio	BAJO	ACEPTABLE	ACEPTAR
	Manipulación de los equipos	MEDIO	INACEPTABLE	MITIGAR
	Fugas de información	MEDIO	INACEPTABLE	MITIGAR
	Robo	MEDIO	INACEPTABLE	MITIGAR
Sistema META4	Abuso de privilegios de acceso	ALTO	CRITICO	MITIGAR
	Alteración accidental de la información	ALTO	CRITICO	MITIGAR

	Destrucción de información	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	BAJO	ACEPTABLE	ACEPTAR
	Manipulación de los registros de actividad	BAJO	ACEPTABLE	ACEPTAR
Sistema SIM	Abuso de privilegios de acceso	MEDIO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	BAJO	ACEPTABLE	ACEPTAR
	Destrucción de información	BAJO	ACEPTABLE	ACEPTAR
	Errores de mantenimiento	BAJO	ACEPTABLE	ACEPTAR
	Manipulación de los registros de actividad	BAJO	ACEPTABLE	ACEPTAR
Software Ofimática	Abuso de privilegios de acceso	MEDIO	INACEPTABLE	MITIGAR
	Manipulación de programas	MEDIO	INACEPTABLE	MITIGAR
Smartphone	Difusión de software dañino	ALTO	INACEPTABLE	MITIGAR
	Avería de HW	MEDIO	INACEPTABLE	MITIGAR
	Pérdida de equipos	MEDIO	INACEPTABLE	MITIGAR
	Robo	MEDIO	INACEPTABLE	MITIGAR
Sistema de SSGG	Abuso de privilegios de acceso	MEDIO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	BAJO	ACEPTABLE	ACEPTAR
	Destrucción de información	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	BAJO	ACEPTABLE	ACEPTAR
	Fugas de información	MEDIO	INACEPTABLE	MITIGAR
	Manipulación de los registros de actividad	BAJO	ACEPTABLE	ACEPTAR
Sistema de Inventario TI	Abuso de privilegios de acceso	ALTO	INACEPTABLE	MITIGAR
	Alteración accidental de la información	ALTO	INACEPTABLE	MITIGAR
	Destrucción de información	MEDIO	INACEPTABLE	MITIGAR
	Errores de mantenimiento	MEDIO	INACEPTABLE	MITIGAR
	Fugas de información	MEDIO	INACEPTABLE	MITIGAR
	Manipulación de los registros de actividad	MEDIO	INACEPTABLE	MITIGAR

Formato de Entrega de Recursos	Alteración accidental de la información	MEDIO	**INACEPTABLE**	MITIGAR
	Daños por agua	MEDIO	**INACEPTABLE**	MITIGAR
	Desastres naturales	MEDIO	**INACEPTABLE**	MITIGAR
	Destrucción de información	MEDIO	**INACEPTABLE**	MITIGAR
	Error de Usuario	MEDIO	**INACEPTABLE**	MITIGAR
	Incendio	MEDIO	**INACEPTABLE**	MITIGAR
Responsable de TI	Fugas de información	**MUY ALTO**	**CRITICO**	MITIGAR
	Ingeniería social	**MUY ALTO**	**CRITICO**	MITIGAR
Responsable de SSGG	Fugas de información	**ALTO**	**INACEPTABLE**	MITIGAR
	Ingeniería social	**ALTO**	**INACEPTABLE**	MITIGAR
Responsable de RRHH	Fugas de información	**ALTO**	**INACEPTABLE**	MITIGAR
	Ingeniería social	**ALTO**	**INACEPTABLE**	MITIGAR
Personal de mando medio	Fugas de información	**ALTO**	**INACEPTABLE**	MITIGAR
	Ingeniería social	**ALTO**	**INACEPTABLE**	MITIGAR
Personal operativo	Fugas de información	MEDIO	**INACEPTABLE**	MITIGAR
	Ingeniería social	MEDIO	**INACEPTABLE**	MITIGAR

Elección de Controles (Declaración de Aplicabilidad)

Continuando con el Plan de tratamiento de Riesgos se eligieron los siguientes controles del Anexo A de la ISO 27001 para el Tratamiento de estos y así cumplir con la Estrategia y Mitigar los riesgos identificados

Tabla 41 - Aplicabilidad de controles de Seguridad de la Información.

Fuente: Instrumento de la investigación basado en la estrategia de tratamiento de Riesgos

Sección	Controles de Seguridad de la Información	Estado
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	APLICABLE
A5.1.2	Revisión de las políticas para la seguridad de la información	APLICABLE
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades en seguridad de la información	APLICABLE
A6.1.2	Segregación de tareas	APLICABLE
A6.1.3	Contacto con las autoridades	APLICABLE
A6.1.4	Contacto con grupos de interés especial	APLICABLE
A6.2	**Los dispositivos móviles y el teletrabajo**	
A6.2.1	Política de dispositivos móviles	APLICABLE
A7	**Seguridad relativa a los recursos humanos**	
A7.2	**Durante el empleo**	
A7.2.1	Responsabilidades de gestión	APLICABLE
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	APLICABLE
A7.2.3	Proceso disciplinario	APLICABLE
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	
A7.3.1	Responsabilidades ante la finalización o cambio	APLICABLE
A8	**Gestión de activos**	
A8.1	**Responsabilidad sobre los activos**	
A8.1.1	Inventario de activos	APLICABLE
A8.1.2	Propiedad de los activos	APLICABLE
A8.1.3	Uso aceptable de los activos	APLICABLE
A8.1.4	Devolución de activos	APLICABLE
A8.2	**Clasificación de la información**	
A8.2.1	Clasificación de la información	APLICABLE
A8.2.2	Etiquetado de la información	APLICABLE

A8.2.3	Manipulado de la información	APLICABLE
A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	
A9.1.1	Política de control de acceso	APLICABLE
A9.1.2	Acceso a las redes y a los servicios de red	APLICABLE
A9.2	**Gestión de acceso de usuario**	
A9.2.1	Registro y baja de usuario	APLICABLE
A9.2.2	Provisión de acceso de usuario	APLICABLE
A9.2.3	Gestión de privilegios de acceso	APLICABLE
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	APLICABLE
A9.2.5	Revisión de los derechos de acceso de usuario	APLICABLE
A9.2.6	Retirada o reasignación de los derechos de acceso	APLICABLE
A9.3	**Responsabilidades del usuario**	
A9.3.1	Uso de la información secreta de autenticación	APLICABLE
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción del acceso a la información	APLICABLE
A9.4.2	Procedimientos seguros de inicio de sesión	APLICABLE
A9.4.3	Sistema de gestión de contraseñas	APLICABLE
A9.4.4	Uso de utilidades con privilegios del sistema	APLICABLE
A9.4.5	Control de acceso al código fuente de los programas	APLICABLE
A10	**Criptografía**	
A10.1	**Controles criptográficos**	
A10.1.1	Política de uso de los controles criptográficos	APLICABLE
A10.1.2	Gestión de claves	APLICABLE
A11	**Seguridad física y del entorno**	
A11.1	**Áreas seguras**	
A11.1.3	Seguridad de oficinas, despachos y recursos	APLICABLE
A11.1.4	Protección contra las amenazas externas y ambientales	APLICABLE
A11.1.5	El trabajo en áreas seguras	APLICABLE
A11.2	**Seguridad de los equipos**	
A11.2.1	Emplazamiento y protección de equipos	APLICABLE
A11.2.2	Instalaciones de suministro	APLICABLE
A11.2.3	Seguridad del cableado	APLICABLE
A11.2.4	Mantenimiento de los equipos	APLICABLE
A11.2.7	Reutilización o eliminación segura de equipos	APLICABLE
A11.2.8	Equipo de usuario desatendido	APLICABLE
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	APLICABLE
A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	
A12.1.1	Documentación de procedimientos operacionales	APLICABLE
A12.1.3	Gestión de capacidades	APLICABLE

A12.2	**Protección contra el software malicioso (malware)**	
A12.2.1	Controles contra el código malicioso	APLICABLE
A12.3	**Copias de seguridad**	
A12.3.1	Copias de seguridad de la información	APLICABLE
A12.4	**Registros y supervisión**	
A12.4.1	Registro de eventos	APLICABLE
A12.4.2	Protección de la información del registro	APLICABLE
A12.4.3	Registros de administración y operación	APLICABLE
A12.4.4	Sincronización del reloj	APLICABLE
A12.5	**Control del software en explotación**	
A12.5.1	Instalación del software en producción	APLICABLE
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	APLICABLE
A12.6.2	Restricción en la instalación de software	APLICABLE
A12.7	**Consideraciones sobre la auditoria de sistemas de información**	
A12.7.1	Controles de auditoría de sistemas de información	APLICABLE
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	
A13.1.1	Controles de red	APLICABLE
A13.2	**Intercambio de información**	
A13.2.1	Políticas y procedimientos de intercambio de información	APLICABLE
A13.2.3	Mensajería electrónica	APLICABLE
A13.2.4	Acuerdos de confidencialidad o no revelación	APLICABLE
A16	**Gestión de incidentes de seguridad de la información**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A16.1.1	Responsabilidades y procedimientos	APLICABLE
A16.1.2	Notificación de los eventos de seguridad de la información	APLICABLE
A16.1.3	Notificación de puntos débiles de la seguridad	APLICABLE
A16.1.5	Respuesta a incidentes de seguridad de la información	APLICABLE
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	APLICABLE
A16.1.7	Recopilación de evidencias	APLICABLE
A18	**Cumplimiento**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	APLICABLE
A18.2	**Revisiones de la seguridad de la información**	
A18.2.1	Revisión independiente de la seguridad de la información	APLICABLE
A18.2.2	Cumplimiento de las políticas y normas de seguridad	APLICABLE
A18.2.3	Comprobación del cumplimiento técnico	APLICABLE

6.4. Análisis actual de Seguridad de la Información en la Organización (Análisis GAP de controles de seguridad)(Pre test)

En este apartado realizamos el Análisis de Brechas o Análisis Gap para poder tener un punto de partida e identificar la distancia entre la situación actual de Seguridad de la Información y la aplicabilidad recomendada de los controles de la ISO 20001.

Para lograr este objetivo se realizó una auditoria basada en el ANEXO A de la ISO 27001 donde se especifican los controles recomendados por este estándar internacional.

Para las métricas se utilizaron los niveles de madurez diseñados en base a la Herramienta publicada en la web de ISO27001security que están basadas en los niveles de Madurez de CMMI.

VALOR	Estado	Significado
0	? Desconocido	No ha sido verificado
1	Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
2	Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
3	Limitado	La medida de seguridad se aplica de un modo informal (Con propuestas para un procedimiento formal). La responsabilidad es individual. No hay formación.
4	Definido	El control se aplica conforme a un procedimiento formal y verificado.
5	Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
6	Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
7	No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Tabla 42 - Métricas para la Auditoria.

Fuente: Instrumento de Investigación Anexo 5.

Auditoria de Controles de Seguridad

Se realizó la auditoria en base a los Controles de Seguridad del Anexo A de la ISO 27001.

Se muestra la evidencia de los datos obtenidos en la Auditoria.

Tabla 43 - Evidencia de aplicación del Instrumento para la Auditoria en el Pre Test.

Fuente: Instrumento de Investigación Anexo 5.

Sección	Controles de Seguridad de la Información	Estado	Resultado
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A5.1.2	Revisión de las políticas para la seguridad de la información	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde
A6.1.2	Segregación de tareas	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde
A6.1.3	Contacto con las autoridades	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde

A6.1.4	Contacto con grupos de interés especial	Inexistente	No existe documentación u procedimiento.
A6.1.5	Seguridad de la información en la gestión de proyectos	No aplicable	No aplicable para el alcance de la investigación.
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	Inexistente	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A6.2.2	Teletrabajo	No aplicable	No aplicable para el alcance de la investigación.
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	No aplicable	No aplicable para el alcance de la investigación.
A7.1.2	Términos y condiciones del empleo	No aplicable	No aplicable para el alcance de la investigación.
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Inexistente	No existe documentación u procedimiento.
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inexistente	No existe documentación u procedimiento.
A7.2.3	Proceso disciplinario	Inexistente	No existe documentación u procedimiento.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Inexistente	No existe documentación u procedimiento.
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Inexistente	No existe documentación u procedimiento.
A8.1.2	Propiedad de los activos	Inexistente	No existe documentación u procedimiento.

A8.1.3	Uso aceptable de los activos	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A8.1.4	Devolución de activos	Definido	Existe procedimiento documentado, pero no es revisado.
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Inexistente	No existe documentación u procedimiento.
A8.2.2	Etiquetado de la información	Inexistente	No existe documentación u procedimiento.
A8.2.3	Manipulado de la información	Inexistente	No existe documentación u procedimiento.
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	No aplicable	No aplicable para el alcance de la investigación.
A8.3.2	Eliminación de soportes	No aplicable	No aplicable para el alcance de la investigación.
A8.3.3	Soportes físicos en tránsito	No aplicable	No aplicable para el alcance de la investigación.
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Inexistente	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A9.1.2	Acceso a las redes y a los servicios de red	Inicial	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Inexistente	No existe documentación u procedimiento.
A9.2.2	Provisión de acceso de usuario	Inexistente	No existe documentación u procedimiento.

A9.2.3	Gestión de privilegios de acceso	Inexistente	No existe documentación u procedimiento.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inexistente	No existe documentación u procedimiento.
A9.2.5	Revisión de los derechos de acceso de usuario	Inexistente	No existe documentación u procedimiento.
A9.2.6	Retirada o reasignación de los derechos de acceso	Inexistente	No existe documentación u procedimiento.
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Inexistente	No existe documentación u procedimiento.
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Inexistente	No existe documentación u procedimiento.
A9.4.2	Procedimientos seguros de inicio de sesión	Inexistente	No existe documentación u procedimiento.
A9.4.3	Sistema de gestión de contraseñas	Inexistente	No existe documentación u procedimiento.
A9.4.4	Uso de utilidades con privilegios del sistema	Inexistente	No existe documentación u procedimiento.
A9.4.5	Control de acceso al código fuente de los programas	Inexistente	No existe documentación u procedimiento.
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Inexistente	No existe documentación u procedimiento.
A10.1.2	Gestión de claves	Inexistente	No existe documentación u procedimiento.
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	No aplicable	No aplicable para el alcance de la investigación.

A11.1.2	Controles físicos de entrada	No aplicable	No aplicable para el alcance de la investigación.
A11.1.3	Seguridad de oficinas, despachos y recursos	Inexistente	No existe documentación u procedimiento.
A11.1.4	Protección contra las amenazas externas y ambientales	Inexistente	No existe documentación u procedimiento.
A11.1.5	El trabajo en áreas seguras	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A11.1.6	Àreas de carga y descarga	No aplicable	No aplicable para el alcance de la investigación.
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A11.2.2	Instalaciones de suministro	Inexistente	No existe documentación u procedimiento.
A11.2.3	Seguridad del cableado	Inexistente	No existe documentación u procedimiento.
A11.2.4	Mantenimiento de los equipos	Inexistente	No existe documentación u procedimiento.
A11.2.5	Retirada de materiales propiedad de la empresa	No aplicable	No aplicable para el alcance de la investigación.
A11.2.6	Seguridad de los equipos fuera de las instalaciones	No aplicable	No aplicable para el alcance de la investigación.
A11.2.7	Reutilización o eliminación segura de equipos	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A11.2.8	Equipo de usuario desatendido	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.

A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	Limitado	Existen algunos procedimientos documentos pero no se revisa el cumplimiento ni se difunde.
A12.1.2	Gestión de cambios	No aplicable	No aplicable para el alcance de la investigación.
A12.1.3	Gestión de capacidades	Inexistente	No existe documentación u procedimiento.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable	No aplicable para el alcance de la investigación.
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Limitado	No existe documentación u procedimiento.
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Limitado	Existe procedimiento documentado, pero no es revisado.
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	Inexistente	No existe documentación u procedimiento.
A12.4.2	Protección de la información del registro	Inexistente	No existe documentación u procedimiento.
A12.4.3	Registros de administración y operación	Inexistente	No existe documentación u procedimiento.
A12.4.4	Sincronización del reloj	Inexistente	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A12.5	**Control del software en explotación**		

A12.5.1	Instalación del software en producción	Inexistente	No existe documentación u procedimiento.
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente	No existe documentación u procedimiento.
A12.6.2	Restricción en la instalación de software	Inexistente	No existe documentación u procedimiento.
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Inexistente	No existe documentación u procedimiento.
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A13.1.2	Seguridad de los servicios de red	No aplicable	No aplicable para el alcance de la investigación.
A13.1.3	Segregación en redes	No aplicable	No aplicable para el alcance de la investigación.
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A13.2.2	Acuerdos de intercambio de información	No aplicable	No aplicable para el alcance de la investigación.
A13.2.3	Mensajería electrónica	Inexistente	No existe documentación u procedimiento.
A13.2.4	Acuerdos de confidencialidad o no revelación	Inexistente	No existe documentación u procedimiento.
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		

A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No aplicable	No aplicable para el alcance de la investigación.
A14.1.3	Protección de las transacciones de servicios de aplicaciones	No aplicable	No aplicable para el alcance de la investigación.
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	No aplicable	No aplicable para el alcance de la investigación.
A14.2.2	Procedimiento de control de cambios en sistemas	No aplicable	No aplicable para el alcance de la investigación.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No aplicable	No aplicable para el alcance de la investigación.
A14.2.4	Restricciones a los cambios en los paquetes de software	No aplicable	No aplicable para el alcance de la investigación.
A14.2.5	Principios de ingeniería de sistemas seguros	No aplicable	No aplicable para el alcance de la investigación.
A14.2.6	Entorno de desarrollo seguro	No aplicable	No aplicable para el alcance de la investigación.
A14.2.7	Externalización del desarrollo de software	No aplicable	No aplicable para el alcance de la investigación.
A14.2.8	Pruebas funcionales de seguridad de sistemas	No aplicable	No aplicable para el alcance de la investigación.
A14.2.9	Pruebas de aceptación de sistemas	No aplicable	No aplicable para el alcance de la investigación.
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	No aplicable	No aplicable para el alcance de la investigación.
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No aplicable	No aplicable para el alcance de la investigación.

A15.1.2	Requisitos de seguridad en contratos con terceros	No aplicable	No aplicable para el alcance de la investigación.
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No aplicable	No aplicable para el alcance de la investigación.
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	No aplicable	No aplicable para el alcance de la investigación.
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No aplicable	No aplicable para el alcance de la investigación.
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Limitado	Existe documento, pero no se revisa el cumplimiento ni se difunde.
A16.1.2	Notificación de los eventos de seguridad de la información	Inexistente	No existe documentación u procedimiento.
A16.1.3	Notificación de puntos débiles de la seguridad	Inexistente	No aplicable para el alcance de la investigación.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	No aplicable	No aplicable para el alcance de la investigación.
A16.1.5	Respuesta a incidentes de seguridad de la información	Inexistente	No existe documentación u procedimiento.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente	No existe documentación u procedimiento.
A16.1.7	Recopilación de evidencias	Inexistente	No aplicable para el alcance de la investigación.
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.

A17.1.2	Implementar la continuidad de la seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	No aplicable	No aplicable para el alcance de la investigación.
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inexistente	No existe documentación u procedimiento.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	No aplicable	No aplicable para el alcance de la investigación.
A18.1.3	Protección de los registros de la organización	No aplicable	No aplicable para el alcance de la investigación.
A18.1.4	Protección y privacidad de la información de carácter personal	No aplicable	No aplicable para el alcance de la investigación.
A18.1.5	Regulación de los controles criptográficos	No aplicable	No aplicable para el alcance de la investigación.
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Inexistente	No existe documentación u procedimiento.
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inexistente	No existe documentación u procedimiento.
A18.2.3	Comprobación del cumplimiento técnico	Inexistente	No existe documentación u procedimiento.

Estado Actual de Controles

Luego de la revisión de la auditoria del total de 114 controles incluidos en el Anexo A de la ISO 27001, se identificaron:

- 19 controles Implementados
- 51 controles No Implementados (Inexistentes)
- 44 controles No Aplicables de acuerdo al alcance definido.

Basado en los estados de Madures se identificó la siguiente proporción de Controles de Seguridad del total de 114 Controles.

Estado de Madurez	Proporción de Controles de Seguridad de la Información
? Desconocido	0%
Inexistente	45%
Inicial	1%
Limitado	15%
Definido	1%
Administrado	0%
Optimizado	0%
No aplicable	38%

Tabla 44 - Proporción de Controles de Seguridad de acuerdo a su estado.

Fuente: Elaboración propia de los datos obtenidos en la Auditoria.

Podemos evidenciar en que el nivel de Madures del estado de la Implementación de los Controles de seguridad se encuentra en un estado Inexistente y Limitado, en la siguiente ilustración no se considera los controles No Aplicables de acuerdo al alcance de la Investigación.

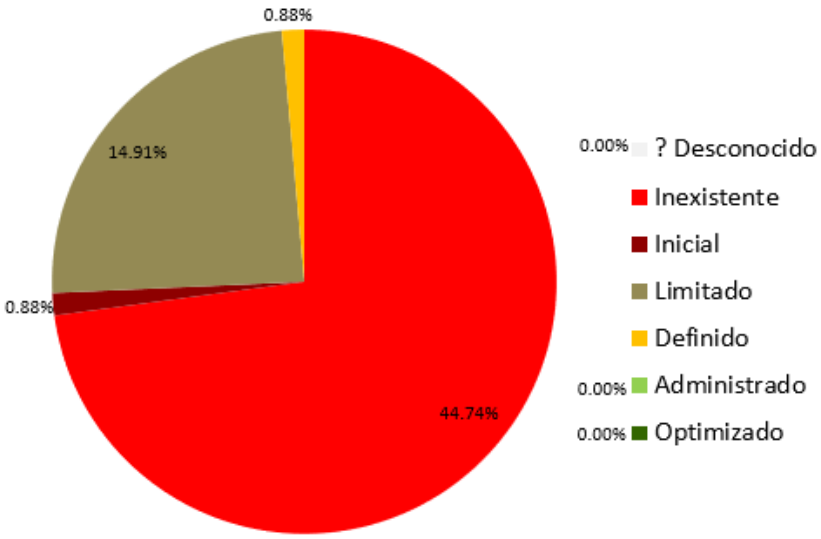


Figura 16 - Grafica ilustrativa de estado actual de los Controles de Seguridad.

Fuente: Elaboración propia en base a la Tabla 44.

7. HACER (DO)

Luego de conocer a la organización, obtener un punto de partida y habiendo aplicado la metodología de análisis de riesgos, en la segunda etapa del Ciclo PDCA (DO) se puso en marcha el plan de tratamiento de riesgos que consiste en la implementación de controles de acuerdo a la declaración de aplicabilidad.

7.1. Plan de Tratamiento de Riesgos

Se implementaron los siguientes controles que para un mejor orden y desarrollo se utilizó la categorizaron de acuerdo a su aplicabilidad.

7.1.1. Controles de Seguridad de Gestión

7.1.1.1. Documento de Alcance SGSI

A continuación se detalla el contenido desarrollado del archivo "*1 Alcance SGSI*".

Nombre	Sistema de Gestión de Seguridad de la información
Alcance	Proceso: PSSGG_01 Gestión de Recursos Asignados al Personal
Descripción	Incluye para los siguientes procedimientos: Procedimiento de registro de recursos para nuevas incorporaciones. Procedimiento de baja de recursos de personal cesado. Adicionalmente, incluye los servicios internos de IT que soportan estos procedimientos.

SG

SG	Fecha Alta SG	Fecha Baja SG
ISO 27001	Agosto 2019	-

Áreas

Servicios/Procesos
Dirección TI
Dirección RRHH
Jefatura de SSGG

MIEMBROS

Comité	Pensando en los distintos procesos administrados dentro de Digitex Perú hemos definido que deben participar dentro del comité de Seguridad los siguientes perfiles: - Director General - Director IT - Director Recursos Humanos - Jefe de compras y SSGG: Pendiente - Director Operaciones

- Responsable de Sistemas de Gestión

- Oficial de Seguridad

- Responsable de Sistemas IT

En el caso de empate en las votaciones, al Director de IT se le otorga el voto de calidad para evitar ese empate.

Dependiendo de los temas a tratar en los comités de seguridad se citara a los responsables de otras áreas en caso de ser necesario.

OBJETIVOS

- Dirigir y coordinar el sistema de gestión de seguridad de la información (SGSI) de DIGITEX, asegurando que el proceso sea llevado a cabo con éxito y cumpliendo todo lo dispuesto en el estándar ISO 27001.

- Será el encargado de tomar las acciones de mejora oportunas.

- Adoptara medidas para mejorar el tratamiento de los temas críticos y permanentes de la seguridad informática corporativa.

FUNCIONES Y ORGANIZACIÓN DEL COMITÉ SEGURIDAD

Funciones

Su labor principal será la de ser responsables de que lo dispuesto por el responsable del SGSI relativo a su departamento será llevado a cabo con éxito.

- Avalar y aprobar la ejecución de proyectos de seguridad de la información.

- Presupuestar los recursos necesarios para la implementación de nuevos controles y para mantener o mejorar los ya existentes.

- Planificar un análisis y evaluación de riesgos de Digitex, mínimo cada año.

- Validar los requerimientos jurídicos de las medidas o controles que se van a implantar.

Organización

Su labor principal será la de ser responsables de que lo dispuesto por el responsable del SGSI relativo a su departamento será llevado a cabo con éxito.

Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de DIGITEX, sean preexistente o

	nuevos. Así mismo deberán revisar la política de seguridad una vez al año. Harán de intermediarios entre el responsable global del SGSI y todas las personas de su departamento involucradas en el alcance. El Comité se reunirá al menos 2 veces al año, lo que implica un promedio de una reunión cada 6 meses. En caso de que el Comité lo considere oportuno y debido a circunstancias que así lo requieran, se podrán convocar reuniones extraordinarias. El Responsable del SGSI, el Oficial de Seguridad o el Auditor Interno realiza una convocatoria previa, enviado por correo electrónico a todos los componentes del Comité, así como a aquellas personas que se consideren oportunas, el orden del día con todos los puntos a tratar en dicha reunión. Se redactará un acta de cada reunión del Comité de Seguridad con las conclusiones acordadas en ella, la cual debe ser guardada como registro del funcionamiento de este comité en Global Suite. Estas actas se archivan por el Responsable de SGSI o por el Oficial de Seguridad o por otra persona en la que se delegue esta tarea.
Departamentos	Operaciones, IT, Compras y SSGG, RRHH, Calidad, Dirección General
Localizaciones Físicas	Lima, Perú
Exclusiones en el Alcance	Según Declaración de Aplicabilidad (SOA), Controles Anexo A

Partes Interesadas

Nombre	Requisitos	Descripción
Departamentos	Desarrollar e implementar los controles y procedimientos del SGSI	La operación del sistema está en manos de los trabajadores que hacen parte de los diferentes departamentos
Clientes potenciales	Exigen implementación de controles del estándar para contratar con nosotros	Algunos de nuestros clientes, conscientes del valor de la información, requieren que la compañía demuestre una adecuada gestión de la seguridad de la información como requisito para contratarnos.

Contexto

Nombre	Interno/Externo	Descripción
Dirección General	Interno	Apoyar el SGSI como parte de la alineación estratégica con el negocio
Dirección Corporativa de Calidad	Interno	Apoyar la implementación, mantenimiento y certificación del SGSI
Dirección Corporativa de IT	Interno	Desarrollar e implementar controles de seguridad informática, el Oficial de Seguridad hace parte de esta Dirección.
Dirección de Operaciones	Interno	Hacer parte de la operación del SGSI en

		cuanto al cumplimiento de controles, análisis de riesgos, registro de incidentes
Clientes potenciales	Externo	Solicitar la implementación del SGSI como requisito para contratar a Digitex
Gerencia de Compras y Servicios Generales	Interno	Apoyar la implementación y operación de controles, en su mayoría de seguridad física
ISO 27001	Externo	Los requisitos propios del estándar
Gobierno Peruano	Externo	Marco Legal

Validez de alcance

Nombre	Fecha Inicio	Duración	Comentarios
Gestión de Riesgo y Controles de SGSI	16/08/2019 00:00:00	Actual alcance	Alcance elaborado por: Miguel A. Porras

7.1.1.2. Documento de Política de Seguridad de la Información.

A continuación, se detalla el contenido desarrollado del archivo "*2_POLITICA DE SEGURIDAD DE LA INFORMACION"*.

DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El presente documento tiene por objeto establecer la política de seguridad de la información para DIGITEX, en sus actividades de Experiencia de cliente, Gestión Inteligente de Procesos y Soluciones y Servicios Tecnológicos, en base a los requisitos dispuestos en el estándar de seguridad de la información ISO 27001, asegurando así la confidencialidad, integridad y disponibilidad de los sistemas de información de DIGITEX PERU y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

Como punto fundamental de la política está la implantación, operación y mantenimiento de un SGSI basado en ISO 27001.

Aspectos básicos de la política de seguridad de DIGITEX PERU:

- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Gestión de la continuidad de la seguridad de la información en situaciones de contingencia.
- Formar y concienciar a todos los empleados en materia de seguridad de la información.
- Gestionar adecuadamente todas las incidencias ocurridas.
- Todos los empleados son informados de sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Hay un responsable de seguridad encargado del sistema de gestión la seguridad de la información (SGSI) de la organización.
- Mejorar de forma continua el SGSI y por ende, la seguridad de la información de la organización.
- Definición de políticas y procedimientos documentados en instrucciones técnicas.
- Cumplimiento de todos los requisitos legales, regulatorios y contractuales aplicables.
- Gestión de riesgos sobre los activos de información, basado en un procedimiento de análisis, evaluación y tratamiento de los mismos.

POLÍTICA DE SEGURIDAD

OBJETIVOS

La política de seguridad de DIGITEX PERU tiene por objetivo marcar las pautas de alto nivel a seguir para que todos los tratamientos de información relativos a los procesos de negocio indicados en el alcance se realicen de forma segura y únicamente por personal autorizado, así como proteger la información de la organización ante posibles pérdidas de confidencialidad, integridad y/o disponibilidad.

Para todo ello, existe un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001 que sigue un ciclo de mejora continua.

ALCANCE

Esta política aplica para todos los trabajadores, aprendices, practicantes, contratistas y/o terceros de la compañía. Cualquiera de ellos que incumpla esta política deberá asumir las responsabilidades de tipo disciplinario definidas en los reglamentos o convenios regulados, así como en los contratos establecidos con las partes externas.

PLANIFICACIÓN

Las actuaciones a llevar a cabo para cumplir con la declaración de la política de seguridad pasan por la implantación, operación y mantenimiento de un SGSI, que en todo momento está alineado con esta política.

En la fase de planificación se incluye como punto fundamental un estudio de la seguridad de la compañía a través de un análisis de riesgos y el establecimiento de su correspondiente plan de tratamiento de riesgos no aceptados por la organización.

IMPLANTACIÓN

La implantación del SGSI es responsabilidad principal del responsable de seguridad (o responsable del SGSI) apoyado en todo momento por personal técnico y con el total apoyo de gerencia.

En base a los resultados obtenidos en la fase de planificación se implantan determinados controles de seguridad, además de operar los procedimientos del SGSI para dar cumplimiento a las exigencias del estándar ISO 27001.

RESPONSABILIDADES ASOCIADAS A LOS ACTIVOS

EQUIPOS INFORMÁTICOS Y DE COMUNICACIONES Y SUS PROGRAMAS DE SOFTWARE

Los usuarios de los sistemas informáticos de DIGITEX PERU deben esforzarse en hacer y promover un uso eficiente de los mismos a fin de evitar tráfico innecesario en la red e interferencias con su trabajo o el de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen.

El uso de los sistemas de DIGITEX PERU quedará reservado para las actividades propias a desempeñar en su puesto de trabajo.

Se promoverá el uso responsable de la red interna de la organización.

Será responsabilidad de los propios usuarios la correcta custodia de los activos que tengan en posesión para el desempeño de sus labores contractuales.

PROTECCIÓN DEL CONOCIMIENTO

No podrán divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con DIGITEX PERU, tanto en soporte material como electrónico. Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral con la organización.

PROPIETARIOS DE LA INFORMACIÓN

El propietario de la información será la Dirección de DIGITEX PERU o un delegado que haya sido nombrado para tal efecto, que definirá las directrices sobre los activos (inventario, uso aceptable, propiedad y devolución de activos), la clasificación de la información (categorización, etiquetado y manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito). Sin embargo, será responsabilidad de los usuarios el correcto tratamiento, almacenamiento y no divulgación de la información a la que tengan acceso como consecuencia del desempeño de sus actividades laborales.

SEGURIDAD DE LA GESTIÓN DE RECURSOS HUMANOS

Se asegurará que todos los empleados, contratistas y los terceros entienden sus responsabilidades y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos puestos a su disposición.

Se asegurará que todos los empleados, contratistas y los terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.

Se asegurará que todos los empleados, contratistas y los terceros abandonan la organización o cambian de puesto de trabajo de forma ordenada y sin comprometer la seguridad de la misma.

SEGURIDAD FÍSICA Y DEL ENTORNO

Se prevendrá todo tipo de acceso físico no autorizado, daños o intromisiones en las instalaciones y en la información de DIGITEX.

Se tomarán las medidas de seguridad necesarias para evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades de DIGITEX PERU.

No se dejarán puestas llaves en puertas, armarios o cajones ni se dejarán puertas o ventanas abiertas cuando no haya nadie en la oficina.

Los portátiles serán llevados en todo momento con la persona asignada al uso del mismo, no dejándolos bajo ningún concepto, sin las medidas de seguridad necesarias, en la oficina cuando dicha persona se ausente de la misma y esta quede vacía.

En caso de trabajar fuera de las instalaciones de la empresa, tanto DIGITEX como el empleado, se asegurarán de disponer de un entorno de trabajo adecuado y proteger los sistemas de los que es responsable. El acceso remoto seguro se hará a través de Global Protect, habilitado de forma permanente para la Dirección y las posiciones establecidas en la Tabla de Asignación de Activos a Empleados, por criterio de disponibilidad/movilidad o por autorización de la Dirección Corporativa RRHH, y de forma temporal, para las excepciones debidamente autorizadas por la Dirección Corporativa o General que corresponda, que se solicitarán según el procedimiento establecido.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Los usuarios de Internet deben esforzarse en hacer y promover un uso eficiente de las redes a fin de evitar tráfico innecesario en la red e interferencias con el trabajo de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen.

El uso del sistema informático de DIGITEX PERU para acceder a redes privadas o públicas, se limitará a los temas directamente

relacionados con la actividad y los cometidos del puesto de trabajo del usuario.

Se hará un uso responsable del correo electrónico, así como de la información transmitida a través de este medio, preservando su confidencialidad e integridad. Todos los mails enviados a más de un destinatario que no sean de la compañía y con los que no exista relación contractual, serán enviados con copia oculta.

Cualquier fichero introducido en la red o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus o cualquier tipo de código malicioso.

Cualquier soporte informático con datos de carácter personal recibido deberá ser registrado, siguiendo el procedimiento establecido. Dicho registro será realizado exclusivamente por el Responsable de Seguridad de la Información o persona en quien delegue. Los soportes que contengan información de carácter personal tendrán una parte cifrada en la que se almacenarán dichos datos.

Está permitido utilizar la información a la que tenga acceso en DIGITEX únicamente en la forma exigida por el desempeño de sus funciones en la organización y no puede disponer de ella de ninguna otra forma o para otra finalidad diferente.

La salida de soportes informáticos y dispositivos móviles fuera de la organización precisa de autorización. Dicha autorización deberá ser obtenida siguiendo el procedimiento establecido mediante petición a través de Ticketing al Responsable de Seguridad, que la autorizará en la misma herramienta.

Se deberán realizar copias de seguridad periódicas de la información contenida en los sistemas de información del Grupo, de forma que se asegure su recuperación en caso de materialización incidente de seguridad de la información.

Cualquier cambio a realizar sobre la infraestructura tecnológica del Grupo deberá ser gestionado de forma adecuada. En concreto, deberá comunicarse por escrito y autorizarse por los responsables que correspondan.

El uso de dispositivos de almacenamiento (memorias USB, tarjetas SD, discos duros, teléfonos en modo almacenamiento, entre otros) está por defecto prohibido debido al riesgo de fuga de información que ello representa. Si existe una justificación de negocio válida, se debe solicitar la excepción al Responsable de Seguridad a través del Ticketing, adjuntando la aprobación del gerente o director del área correspondiente. En la solicitud debe indicarse el periodo de

la excepción, cuál es la información a leer y/o copiar y los destinatarios de la misma, esto último en caso de que aplique.

El uso de dispositivos móviles personales (tablets, Smartphone) con información de la compañía se autorizará únicamente para el acceso al correo vía web, no permitiendo la integración en la red local para el acceso a recursos compartidos (intranet, carpetas en red). La autorización se dará de forma expresa por el Responsable de Seguridad a través de Ticketing. En caso de baja del empleado en la compañía, el Administrador del Sistema, podrá reiniciar el dispositivo de forma remota para la eliminación de información y de las configuraciones. En el caso de los agentes que forman parte de la Operación, no está permitido el uso de dispositivos portátiles o móviles personales en el lugar del trabajo.

Se prohíben expresamente las siguientes actividades:

- No está permitido instalar “motu proprio” ningún producto informático en el sistema de información de DIGITEX. Todas aquellas aplicaciones necesarias para el desempeño de su trabajo serán instaladas únicamente por personal debidamente autorizado de la organización o empresa prestataria de los servicios informáticos.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de DIGITEX o de terceros.
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento de DIGITEX.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de

cualquier elemento destinado a destruir o corromper los datos informáticos.

- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por DIGITEX PERU, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los corporativos.
- Borrar cualquiera de los programas instalados sin autorización de DIGITEX PERU.
- Utilizar los recursos telemáticos de DIGITEX PERU, incluido el acceso a la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Queda prohibido utilizar los recursos del sistema de información a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de las estrictamente laborales.
- Queda terminantemente prohibido facilitar a persona alguna ajena a DIGITEX PERU ningún soporte conteniendo datos, a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.
- Queda terminantemente prohibido utilizar ninguna información que hubiese podido obtener por su condición de empleado de DIGITEX PERU y que no sea necesario para el desempeño de sus funciones.
- No podrán divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con DIGITEX PERU, tanto en soporte material como electrónico. Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral con DIGITEX PERU.
- En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, o titularidad o copia sobre la referida información. Asimismo, el trabajador deberá devolver dichos materiales a DIGITEX PERU inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la

empresa, no supondrá, en ningún caso, una modificación de esta cláusula. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y dará derecho a DIGITEX PERU a exigir al usuario una indemnización económica. Asimismo, se recuerda que el trabajador será responsable frente a la organización y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a DIGITEX las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para las finalidades propias de la empresa, en la red corporativa del mismo.
- Enviar o reenviar mensajes en cadena o de tipo piramidal
- Queda terminantemente prohibido la creación o modificación de Documentación implicada en el alcance o de nuevos ficheros por parte de los usuarios no autorizados.

DIGITEX se reserva el derecho de revisar, con previo aviso, los mensajes de correo electrónico de los usuarios de la red y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la organización como responsable civil subsidiario.

La documentación en soporte papel deberá ser guardada y custodiada en sus archivos correspondientes.

Cuando concluya la jornada laboral, el usuario deberá evitar dejar documentación encima de las mesas o fuera de sus lugares de archivo, que deberán permanecer cerrados con llave.

Respecto a la documentación que se imprima, el usuario será responsable de su recogida, que deberá efectuarse con carácter inmediato, evitando el acceso a la documentación por usuarios no autorizados.

La documentación que no sea de utilidad para el usuario, deberá ser destruida utilizando para ello las destructoras de papel existentes.

CONTROL DE ACCESOS

Se controlará el acceso a los sistemas de información de DIGITEX PERU para que solo sea realizado por personal autorizado y en las condiciones de seguridad que la organización ha decido operar.

Se asegurará el acceso de un usuario autorizado y se prevendrá el acceso de usuarios no autorizados a los sistemas de información de DIGITEX PERU.

Identificación y autentificación de los usuarios

Se prevendrá el acceso no autorizado a los servicios de red para los usuarios que no hayan sido legitimados.

Se usarán métodos seguros de autenticación para conexiones externas por parte de usuario autorizados.

Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en la red.

La información transmitida a través de redes de telecomunicaciones se hará de forma segura.

Con relación a las contraseñas se habrán de observar las siguientes normas:

- La contraseña de acceso al sistema caducará como máximo a los 24 días. El sistema recuerda como mínimo las 24 últimas contraseñas. Todas las contraseñas deben cumplir con la política, a excepción de los usuarios genéricos de configuración de BBDD y Aplicaciones y de SharePoint, que sólo utilizan los Administradores de Seguridad y de Sistemas. Las contraseñas del portal del empleado de Meta4 caducan a los 90 días, debido a que la aplicación no está dentro de directorio activo, al ser externa.
- El usuario será el encargado de modificarla en el momento de realizar el primer acceso al sistema, ya que se le solicitará automáticamente, caso contrario, será el usuario el encargado de realizar dicho cambio.
- La contraseña se considera información secreta, al ser personal e intransferible.
- El usuario se bloqueará a los 5 intentos fallidos de inicio de sesión.
- Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.

- Las contraseñas usadas en cualquier sistema o servicio serán como mínimo de 8 caracteres, alfanuméricas y con letras mayúsculas y minúsculas, no permitiendo ni el nombre ni el apellido del usuario.
- Se usarán reglas nemotécnicas para la generación de contraseñas. Ejemplo: **H**oy **e**s **l**unes, **10 d**e **M**arzo **d**e **2**008. Contraseña: Hel10dMd2.
- No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.
- Se debe bloquear el equipo cuando no vaya a ser usado, o usar mecanismos automáticos, no dejándolo nunca desatendido.
- Se seguirá una política de puesto de trabajo despejado y mesas limpias, no dejando información confidencial o privada a la vista.
- Si se sospecha que la contraseña es conocida por otros usuarios, se procederá a informar al administrador de sistemas para su revocación y sustitución por una nueva.
- Se prohíben expresamente las siguientes actividades:
- Compartir o facilitar el identificador de usuario y la contraseña para acceder a los sistemas de información a otra persona física, incluido el personal de DIGITEX. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física que utilice de forma no autorizada el identificador del usuario.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad.

Acceso a Internet

- El uso del sistema informático de DIGITEX PERU para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de DIGITEX PERU y los cometidos del puesto de trabajo del usuario.
- El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido. En este sentido, se dispone de Hangout como herramienta corporativa de mensajería instantánea, que se deberá utilizar de manera general.
- El acceso a páginas web (WWW) y otras utilidades como FTP, Telnet, etc. se limita a aquéllos que contengan información relacionada con la actividad de DIGITEX o con los cometidos del puesto de trabajo del usuario.
- El acceso a páginas web para escuchar música on-line, consume muchos recursos del caudal de Internet, con lo que su uso queda estrictamente prohibido.
- DIGITEX se reserva el derecho de comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa con el fin de prevenir un uso fraudulento, ilegal, abusivo o no autorizado de Internet. Dicha comprobación incluye la revisión de registros que muestran los ficheros cargados, los que se han accedido, las páginas web visitadas y los usuarios que han ejecutado tales acciones, así como el momento en el que se han producido.
- Cualquier persona que acceda a Internet a través de la red de DIGITEX PERU acepta esta comprobación, así como las normas aquí establecidas, asumiendo la imposición de acciones disciplinarias por incumplimiento de las citadas normas.
- Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- El usuario deberá tener especial precaución con:
- No abrir archivos adjuntos de correos que lleguen a la bandeja de Spam o que vengan de cuentas desconocidas.
- No hacer clic en enlaces de correos que lleguen a la bandeja de Spam o que vengan de cuentas desconocidas.
- No visitar páginas o sitios WEB desconocidas
- Se prohíbe la descarga a través de Internet de software de origen desconocido o de propiedad del usuario en los

sistemas de DIGITEX, salvo que exista una autorización previa.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La política de seguridad relativa a la adquisición, desarrollo y mantenimiento de sistemas consta de las siguientes partes:

- Contemplar requisitos de seguridad en las fases de análisis y diseño de sistemas de información.
- Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas.
- Separar los entornos de prueba y producción.
- Avisar al administrador de sistemas cuando haya cambios importantes en los sistemas para el correcto desempeño de las copias de seguridad.

Protección de los Sistemas Operativos y Otras Utilidades

Se prevendrá el acceso no autorizado a los sistemas operativos, así como su actualización para corregir vulnerabilidades detectadas y se proveerán de las medidas técnicas de seguridad oportunas.

Estará restringido y controlado el uso de aplicaciones no autorizadas que puedan invalidar las medidas de seguridad implantadas.

GESTIÓN DE INCIDENTES

Todo incidente en materia de seguridad deberá comunicarse, siguiendo el procedimiento establecido. Dicha notificación será realizada a través de Ticketing, en el Departamento de Sistemas, categoría Incidente de Seguridad, subcategoría correspondiente. Una vez recibida, el Responsable de Seguridad será el encargado de darle seguimiento, completar las notificaciones establecidas en el procedimiento correspondiente, establecer las acciones para su corrección y comunicar al usuario la resolución o estado de la misma.

SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

Todos los empleados colaborarán en la oportuna reanudación de todos los servicios críticos para DIGITEX en caso de una contingencia grave, manteniendo sus obligaciones y responsabilidades de seguridad de la información tal cual como lo hacen en condiciones normales.

Planificación

Planes de continuidad y contingencia

En Grupo Digitex los planes de contingencia y continuidad del negocio incluirán dentro de sus fases de planificación los requisitos de seguridad que garanticen adecuados niveles de confidencialidad, integridad y disponibilidad de la información. Para tal fin, se han definido las siguientes políticas:

- En Contingencia o Continuidad se debe mantener al menos los mismos controles de seguridad existentes en la operación normal.
- Se deben revisar los compromisos legales o regulatorios de seguridad aplicables cuando se opere en contingencia o continuidad.
- La planificación de pruebas deberá incluir un apartado de pruebas de seguridad.

Para tal fin, se incluirá al Responsable de Seguridad en el proceso de elaboración de los planes desde sus etapas iniciales.

A nivel de personal, el Gerente de Tecnología del país asumirá las responsabilidades del Responsable de Seguridad en su ausencia, garantizando así la continuidad de los procesos. Por tal motivo, el Gerente de Tecnología deberá poder asumir las mismas funciones que el Responsable de Seguridad.

Con respecto a la seguridad informática, en la medida de lo posible y realizando un análisis costo beneficio, se brindará continuidad sobre los controles implementados en la organización, como lo son:

- Firewalls
- Filtrado Web
- Servidores de antivirus
- Directorio activo

Implementación

La implementación de los planes de continuidad y contingencia incluirán la implementación de los controles de seguridad definidos en la planificación. Un plan de continuidad o contingencia no será aceptado si no ha culminado la implementación de los controles.

Verificación, revisión y evaluación

Como parte de las pruebas realizadas a los planes de continuidad y contingencia, el Responsable de Seguridad evaluará la eficacia de los controles de seguridad implementados, identificando oportunidades de mejora a que haya lugar.

El acta de pruebas incluirá un apartado de seguridad donde se incluyan los resultados de las pruebas sobre los controles, así como las acciones correctivas a tomar en caso de que los resultados no sean satisfactorios.

CUMPLIMIENTO LEGAL

Se evitará cualquier tipo de incumplimiento de las leyes u obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad que afecten a los sistemas de información de DIGITEX PERU Se deberá tener muy en cuenta las regulaciones en materia de protección de datos personales y las normativas de privacidad locales en los territorios donde se encuentra el Grupo.

7.1.1.3. Documento de Política de Uso de Dispositivos Móviles.

A continuación, se detalla el contenido desarrollado del archivo "*3_POLITICA_DE_USO_DISPOSITIVOS_MOVILES"*.

DISPOSITIVOS SUMINISTRADOS POR DIGITEX PERU

POLITICAS GENERALES

Los dispositivos móviles utilizados por el personal de DIGITEX PERU, deben ser configurados al menos con los siguientes controles:

- Protección con contraseña, PIN, Patrón o Huella.
- Bloqueo al quinto 5to intento fallido de acceso
- Configurar un PIN de acceso a la SIM Card.
- Habilitación de la funcionalidad de borrado remoto

- No se deben instalar aplicaciones descargadas fuera de la tienda (Google Play, Apple Store, etc.)

USO ACEPTABLE DE DISPOSITIVOS SUMINISTRADOS POR DIGITEX PERU

- Se debe proteger y cuidar los dispositivos para que se conserven durante el tiempo, tal y como lo haría con un dispositivo de su propiedad.
- Se debe proteger la SIM Card y evitar insertarla en otros equipos.
- No se permite instalar aplicaciones no relacionadas con los temas laborales.
- No se permite utilizar el dispositivo para evadir o incumplir otras políticas de seguridad del Grupo DIGITEX PERU.
- Los equipos de DIGITEX PERU podrán ser administrados remotamente por el departamento de Tecnología.

PÉRDIDA O ROBO DEL DISPOSITIVO MÓVIL

Es obligación de los colaboradores notificar la pérdida o robo del dispositivo como incidente de seguridad a través del Ticketing, y de forma urgente a través del teléfono de incidencias 24 horas de Sistemas de cada país. Adicionalmente, se deberá realizar el borrado remoto mediante la funcionalidad propia del equipo (Android, Apple, etc.), por parte del equipo de Sistemas.

ALMACENAMIENTO DE INFORMACIÓN EN DISPOSITIVOS

Archivos que contengan información confidencial (por ejemplo, de clientes, nómina, datos personales, etc.) no deben ser almacenarlos en los dispositivos móviles. Si es estrictamente necesario realizar la descarga de este tipo de archivos, se deberá realizar un borrado de los mismos tan pronto termine el trabajo con ellos, es decir se tratará de un almacenamiento temporal (máximo 24 horas).

AUDITORÍA

La política de seguridad en dispositivos móviles podrá ser auditada por el área de Tecnología y su incumplimiento acarreará las sanciones disciplinarias correspondientes de conformidad con el Reglamento Interno de trabajo o Convenio Colectivo y el contrato laboral.

CONTROL FISICO

DIGITEX PERU tiene la facultad de grabar, monitorear y revisar en cualquier momento los dispositivos proporcionados por DIGITEX PERU y la información contenida en ellos, e incluso el uso o porte de los mismos en las plataformas o espacios de DIGITEX PERU. Este control incluye la facultad de revisar los puestos de trabajo, bolsos, o maletines y demás sitios donde el colaborador podría portar los dispositivos móviles. Esta actividad se realizará en presencia del colaborador y en ningún caso se le vulnerará el derecho a la intimidad.

7.1.1.4. Documento de uso aceptable de activos y equipos de infraestructura.

A continuación, se detalla el contenido desarrollado del archivo "*4_POLITCA DE USO ACEPTABLE DE ACTIVOS Y EQUIPOS DE INFRAESTRUCTURA"*.

USO ACEPTABLE DE ACTIVOS Y EQUIPOS DE INFRAESTRUCTURA

Definiciones

Sistema de infraestructura: incluye todos los aires acondicionados, ascensores, motobombas, ups, moto-generadores, sistema eléctrico, alarmas y detección de incendios, cctv y demás subsistemas y componentes que pertenecen o son utilizados por la organización, o que se encuentran bajo responsabilidad de la organización. El uso de un elemento de infraestructura también incluye el uso de todos los servicios internos o externos, como el acceso a cuartos de cableado, cuartos de moto-generadores, etc.

Uso aceptable

Todo elemento y/o uso de equipamiento que utilice algún colaborador de DIGITEX PERU, necesariamente debe tener como fin alguno de los siguientes propósitos:

- Docencia
- Aprendizaje
- Ejecución de tareas laborales
- Administración
- Prevención y promoción sobre los elementos de trabajo.

Es decir, todo uso de recursos materiales por parte de los trabajadores, debe ser con fines laborales para el desarrollo de las funciones del cargo para el cual fue contratado.

Responsabilidad sobre los activos y equipos de infraestructura

Será responsable de los activos o equipos de infraestructura toda persona vinculada laboralmente con DIGITEX PERU y tendrán las siguientes responsabilidades sobre el uso adecuado de los mismos:

- Utilizar los activos y equipos de infraestructura únicamente para el desarrollo de actividades establecidas por DIGITEX PERU.
- No exponer ni permitir que los activos y equipos de infraestructura sean expuestos a algún tipo de riesgo o peligro que ocasione su daño temporal o permanente.
- Notificar de manera oportuna a la Gerencia de SSGG y Compras o al Responsable de Infraestructura, sobre el uso indebido o daño de activos y equipos de infraestructura, con el fin de gestionar su mantenimiento o garantía.
- Informar inmediatamente sobre la pérdida o hurto de algún activo o equipo de infraestructura, con el fin de iniciar el proceso y trámites correspondientes.
- Los activos y equipos de infraestructura se deben usar dentro de las instalaciones de DIGITEX PERU; en caso que se deba retirar algún portátil u otro equipo, es indispensable informar al vigilante de la sede correspondiente con el fin de que su salida quede registrada en la minuta.
- En caso de que una persona responsable del activo o equipo de infraestructura se traslade a otra sede o se desvincule de la empresa, deberá entregar correctamente los activos o equipos a su cargo por medio de acta de entrega o traspaso.

Actividades prohibidas

Los activos y equipos de infraestructura no deben ser utilizados para actividades que se contrapongan con los Estatutos y Principios que DIGITEX PERU, tales como:

- Violación del Uso Aceptable enunciado con anterioridad.
- Violación de las políticas de seguridad de DIGITEX PERU sobre el Uso de los elementos de infraestructura.
- Violación de las políticas de calidad sobre el Uso de activos fijos.
- Cualquier daño o interferencia en la funcionalidad de los recursos de infraestructura y usuarios, sean estos de DIGITEX PERU u otras entidades. Esto incluye, entre otros, la violación de chapas, daño de lockers y en general cualquier actividad maliciosa o negligente que afecte su normal funcionamiento.

- Intentar acceder sin autorización a los sitios o servicios de alguna sede adscrita a DIGITEX PERU o de otra institución, mediante la utilización de herramientas intrusivas o cualquier otro medio no permitido o legítimo.
- El uso de los recursos para fines personales o particulares, incluyendo cualquier actividad comercial o fin de lucro personal.
- Revelar a terceros las contraseñas de acceso o compartirlas con otros usuarios.
- Violación o intento de violación de los sistemas de seguridad de DIGITEX PERU o de cualquier tercero.
- Manipulación de maquinaria, equipos o recursos sin la debida autorización.
- Llevar a cabo actos que pongan en riesgo el personal y los bienes de la empresa.
- Establecer conexiones o realizar acometidas fraudulentas.

7.1.1.5. Documento de Procedimiento de Borrado Seguro de la Información.

A continuación, se detalla el contenido desarrollado del archivo "*5_BORRADO SEGURO DE LA INFORMACIÓN ESTACIONES DE TRABAJO"*.

PROCEDIMIENTO

- El Gerente de Cuenta o Jefe de Proyecto de la campaña realiza la solicitud mediante una petición de Ticketing Corporativo Digitex.
- La petición se asigna a un Técnico de Soporte Nivel I quien pasa puesto a puesto realizando el borrado, con la coordinación del Técnico de Nivel II a cargo de la actividad.
- Los funcionarios deben tener lista la carpeta que se va a borrar con la información de clientes o confidencial.
- El Técnico realiza el borrado con el software indicado, tomando las evidencias (Print Screen) y llenando un acta digital que se envía por correo al Gerente de Cuenta o Jefe de Proyecto quien luego las imprime y las hace firmar.
- Las Acta Borrado de Información son firmadas también por el Técnico de Soporte Nivel II que coordina la actividad de borrado.
- El Gerente de Cuenta o Jefe de Proyecto de la campaña realiza entrega de la documentación al cliente como prueba del borrado, entregando el Acta Borrado de Información y dejando una copia de archivo.

Procedimiento de borrado

a) El funcionario debe indicar la carpeta que se debe borrar con la documentación interna.

b) Configurar la aplicación ERASER con el método de borrado US DoD 5220.22-M (8-306./E, C & E) (7 passes)

c) Crear una nueva tarea para el borrado de los documentos o archivos

d) Ejecutar la tarea

LOG DE DESTRUCCION DE BACKUPS

a) Adjuntar log de destrucción, que especifica las fechas en la que se ha ejecutado la tarea de borrado.

b) Diligenciar el acta con los Print tomados y los datos de puesto para enviarlos al Responsable de Operaciones o gerente de Operaciones de la campaña.

7.1.2. Controles de Seguridad Lógicos

7.1.2.1. Control de Acceso

Se han creado estructuras de directorios compartidos para poder controlar y limitar los accesos a la información que corresponde a cada Área, los accesos se provisionan en base a grupos del Directorio Activo asociado al recurso compartido.

Figura 17 - Evidencia de Creación de Estructura en Servidor de Archivos.

Fuente: Digitex Perú SAC.

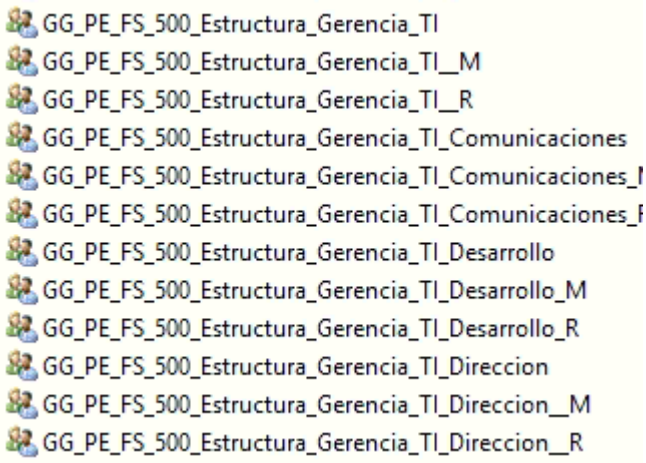
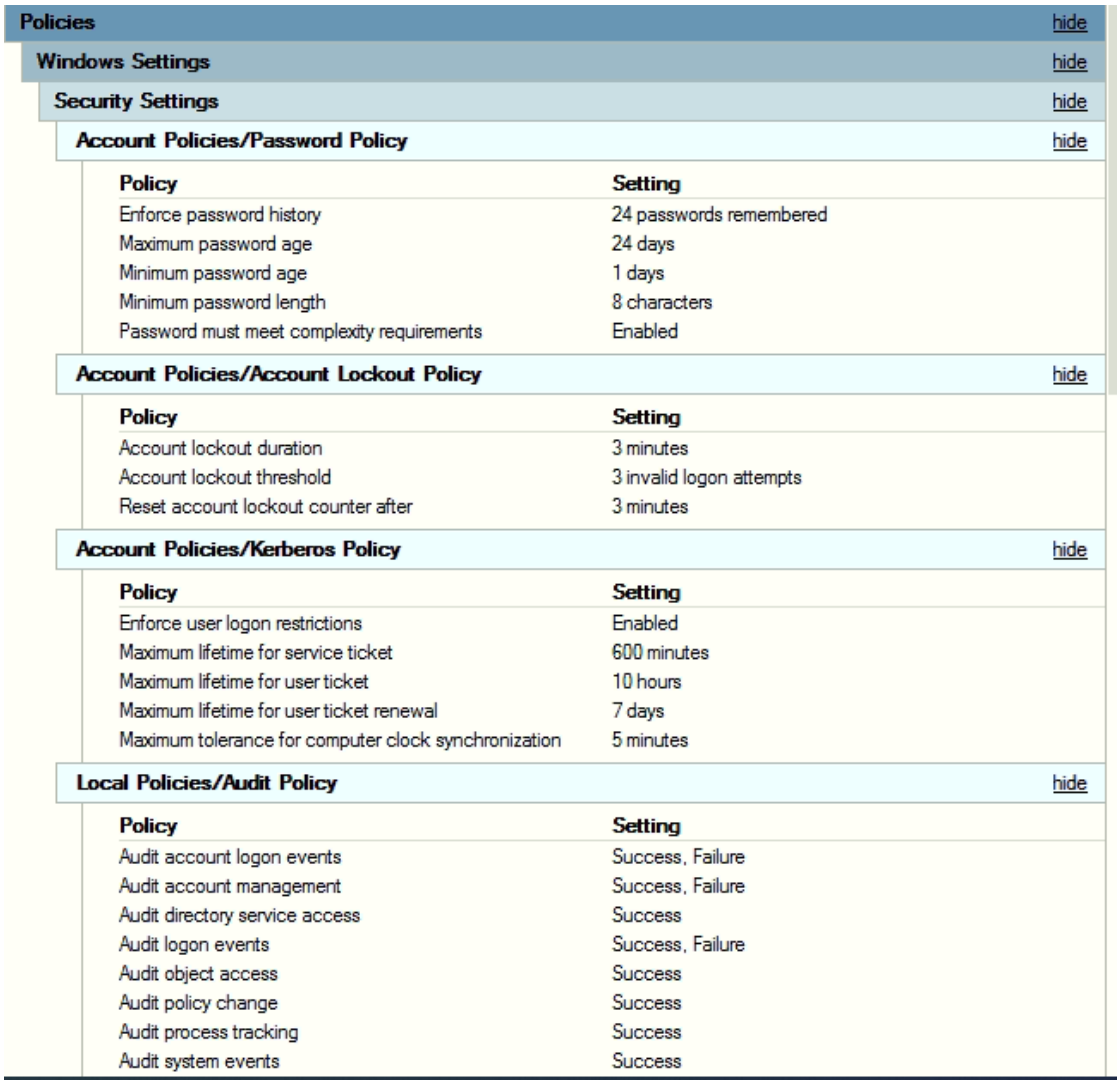


Figura 18 - Gestión de Permisos por Grupos en AD.

Fuente: Digitex Perú SAC.

Se han definido políticas de Contraseñas y Auditoria de Acceso en el Directorio Activo estructuras de directorios compartidos para poder controlar y limitar los accesos a la información que corresponde a cada Área.



Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	24 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout duration	3 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	3 minutes

Account Policies/Kerberos Policy hide

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy hide

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success
Audit logon events	Success, Failure
Audit object access	Success
Audit policy change	Success
Audit process tracking	Success
Audit system events	Success

Figura 19 - Evidencia de Políticas de Seguridad en Directorio Activo.

Fuente: Digitex Perú SAC.

Se creó política para que solo Soporte Técnico pueda tener privilegios de administrador en los equipos cliente.

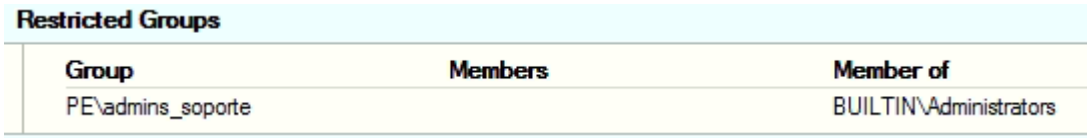


Figura 20 - Política de privilegios de Administrador.

Fuente: Digitex Perú SAC.

Se crearon políticas para restringir la instalación de Software en los equipos cliente asimismo para la ejecución con privilegios elevados.

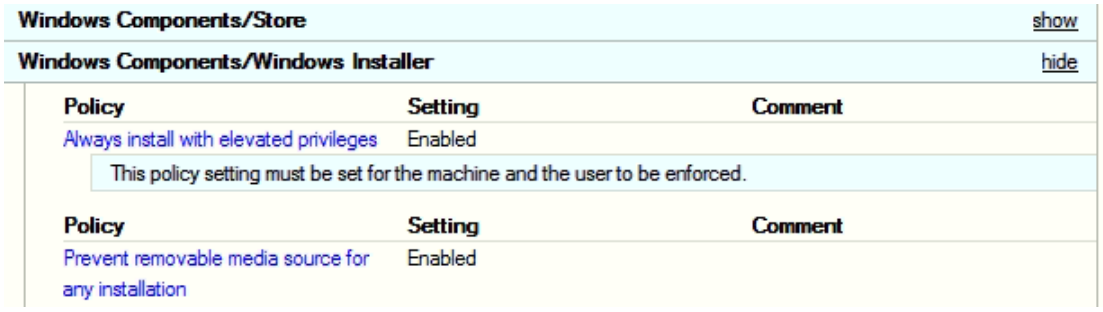


Figura 21 - Política de restricción de instalación de Software.

Fuente: Digitex Perú SAC.

Se habilitó la protección de acceso en el Anti Virus para prevenir cualquier intento de modificación o alteración de archivos o fuentes de los programas utilizados en los equipos cliente.

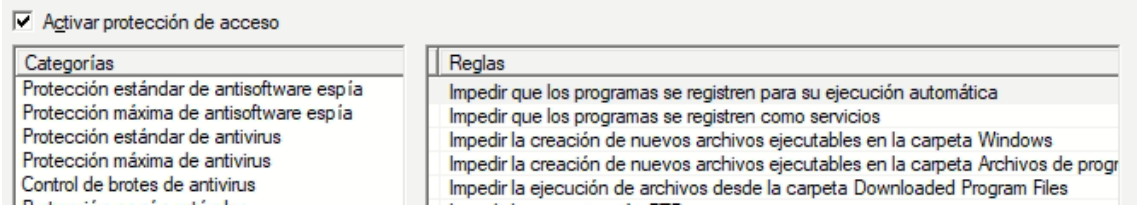


Figura 22 - Protección de Acceso en al Anti Virus.

Fuente: Digitex Perú SAC.

7.1.2.2. Criptografía

Se tiene definida en la Política un apartado correspondiente a contraseñas, pero en caso de contraseñas de accesos a los sistemas de información se propone el uso de un Gestor que garantice un cifrado robusto por ejemplo Team Password Manager). No se logró implementar ya que la aplicación tiene un Costo, la propuesta será evaluada por la Organización.

Figura 23 - Imagen de Software de Encriptación.

Fuente: teampasswordmanager.com

7.1.2.3. Seguridad física y del entorno

En la política se detalla que se deben bloquear los equipos de cómputo cuando se vayan a dejar de utilizar, se implementó un el control en el Directorio Activo para poder reforzar y garantizar el bloqueo del equipo cuando no está siendo utilizado.

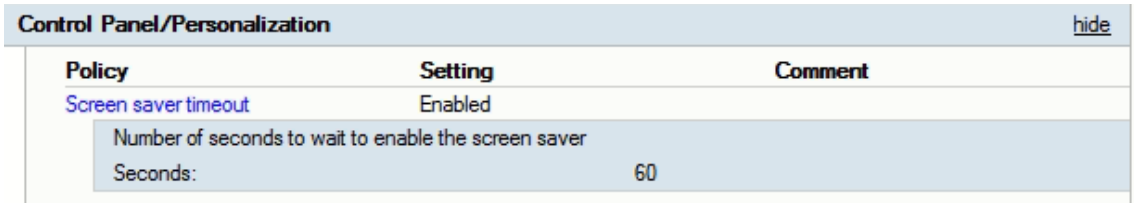


Figura 24 - Evidencia del control para equipos desatendidos.

Fuente: Digitex Perú SAC.

7.1.2.4. Seguridad de las operaciones

Se implementó una Herramienta Gratuita para monitoreo de capacidades para los servidores que soportan los sistemas de información (PRTG 100 Sensors)

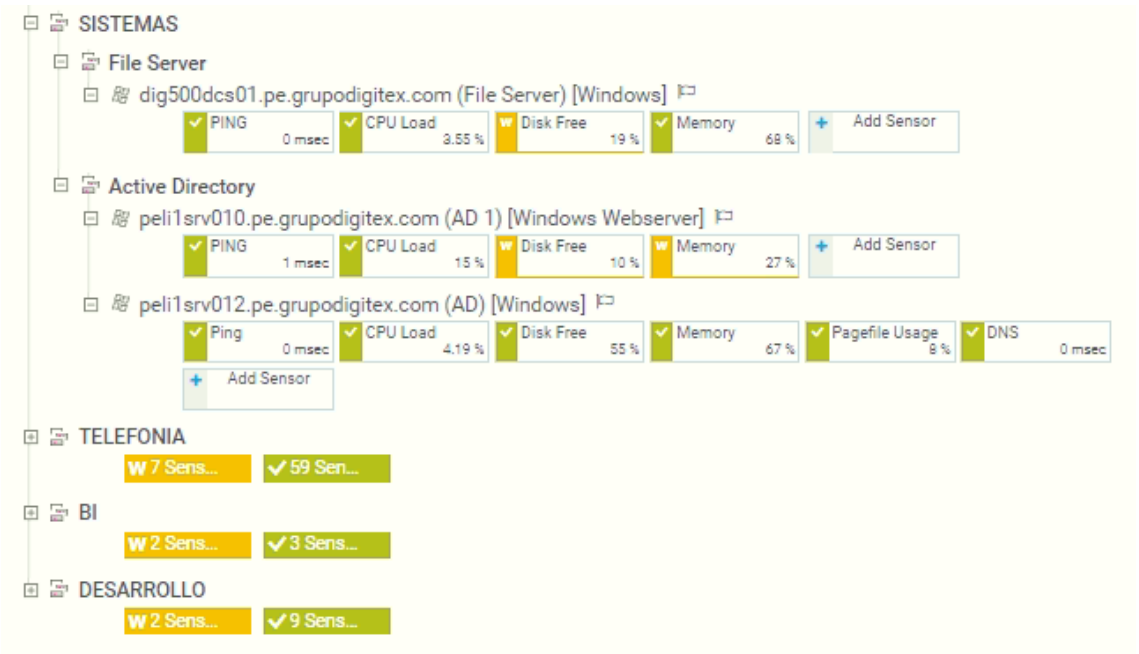


Figura 25 - Herramienta de Monitoreo de Capacidades.

Fuente: Digitex Perú SAC.

Se mejoró la sensibilidad del análisis en tiempo real del Anti Virus, se programaron tareas diarias para búsqueda de virus en los equipos de cómputo.

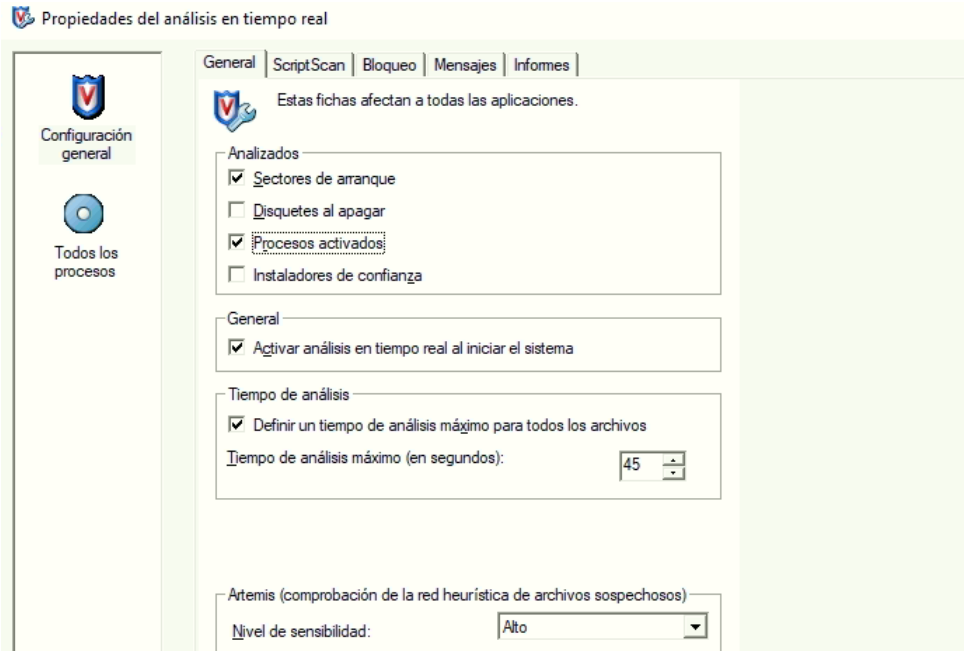


Figura 26 - Mejora de Sensibilidad de detección de Malware.

Fuente: Digitex Perú SAC.

En base a la Política de Backup se mejoraron las tareas automáticas de con Programaciones Semanales y Diarias de Tipo Full, Diferencial e Incremental en Cinta Magnética.

Nombre	Serv...	..	Tipo de trabajo	Es...	Estado de trabajo	Hora inicial
DIG500BKP01_PRIMAVERA_DESARROLLO_BD Copia de seguridad completa, Copia de seguridad completa, Copia de s...	DI...		Copia de seguridad	Pro g...	programado	13/01/2020 08:
DIG500BKP01_PRIMAVERA_SISTEMAS_FS Copia de seguridad completa, Copia de seguridad completa, Copia de s...	DI...		Copia de seguridad	Pro g...	programado	12/01/2020 10:
DIG500BKP01_PRIMAVERA_TELEFONIA_BD Copia de seguridad completa, Copia de seguridad diferencial, Copia de...	DI...		Copia de seguridad	Pro g...	programado	13/01/2020 05:
DIG500DCS01_PRIMAVERA_SISTEMAS_AD Copia de seguridad completa, Copia de seguridad completa, Copia de s...	DI...		Copia de seguridad	Pro g...	programado	13/01/2020 07:

Figura 27 - Tareas de Backup automáticas y programadas

Fuente: Digitex Perú SAC.

Se definió una tarea para archivado de LOGs de Auditoria del Directorio Activo manteniéndolos en línea por 30 días para que puedan ser revisados y respaldados en cinta.

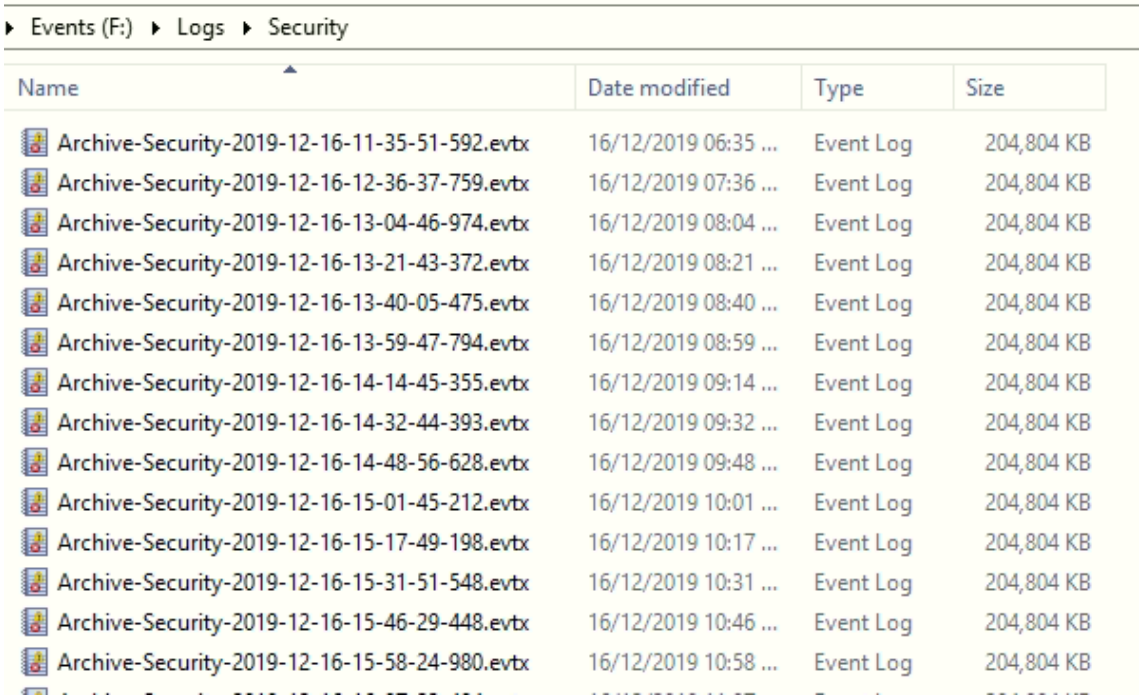


Figura 28 - Archivamiento de Logs del Directorio activo.

Fuente: Digitex Perú SAC.

Figura 29 - Tarea de Backup de archivos Log.

Fuente: Digitex Perú SAC.

Se realizó la sincronización de todos los servidores con el Servidor NTP, se habilitaron los servicios de Cliente NTP y se validó que el servidor NTP sincronice de forma regular con los NTP de Microsoft.

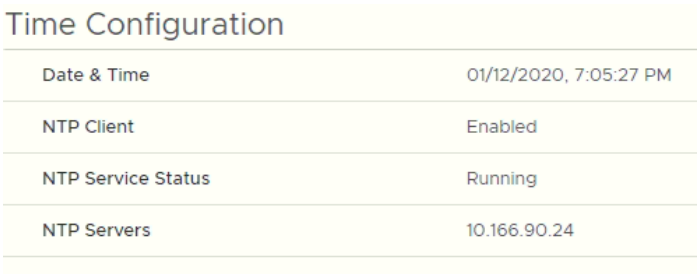


Figura 30 - Habilitación y uso de cliente NTP.

Fuente: Digitex Perú SAC.

Se recomienda el uso de un programa de Escaneo de Vulnerabilidades para una adecuada Gestión de estas. Se recomienda el uso de Nessus, al ser una herramienta que tiene un costo asociado la recomendación será evaluada por la organización.

Figura 31 - Top Soluciones para análisis de vulnerabilidades.

Fuente: www.tenable.com.

7.1.2.5. Seguridad de las comunicaciones

En coordinación en el Responsable de Redes y comunicaciones se definieron perfiles en el Directorio Activo asociados a las reglas del FW para tener un control centralizado de los permisos.

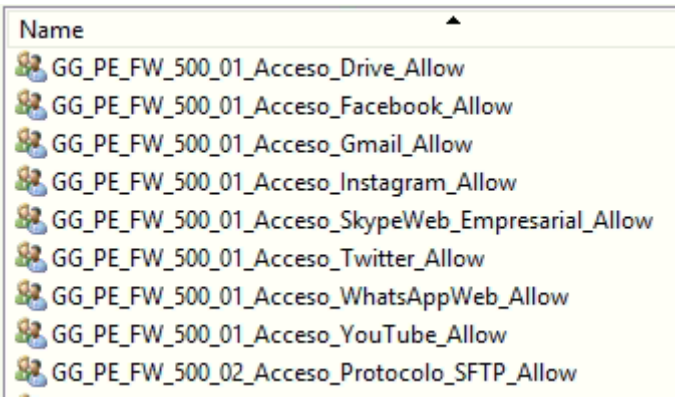


Figura 32 - Gestión de permisos el en Firewall por grupos de AD.

Fuente: Digitex Perú SAC.

Se creó una regla de filtrado SPAM estricto en la consola de GSUIT, que aplica a toda la sede de Perú.

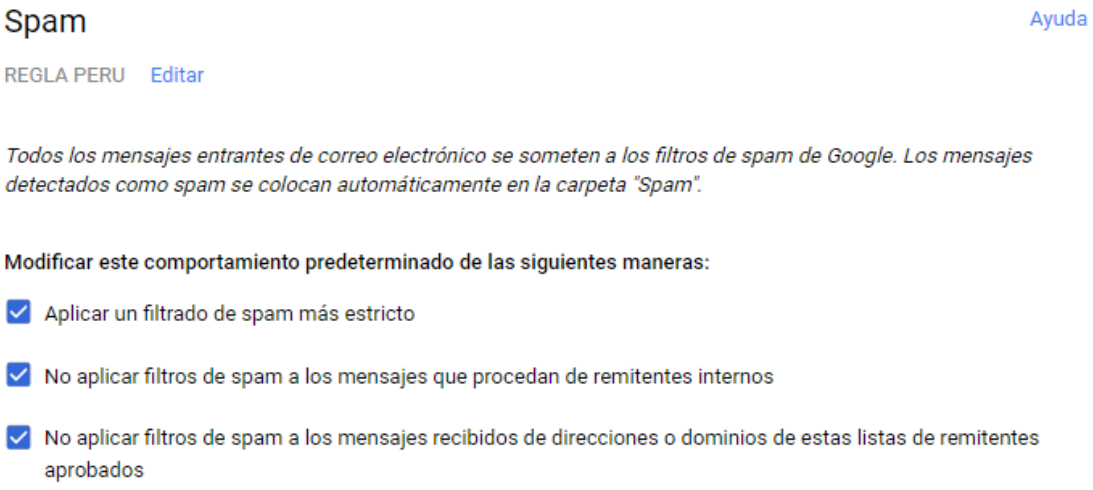


Figura 33 - Regla de filtrado estricto anti SPAM.

Fuente: Digitex Perú SAC.

7.1.3. Controles de Seguridad Físicos

7.1.3.1. Seguridad física y del entorno

Seguridad de oficinas, despachos y recursos.

Se tiene seguros los ambientes con cerraduras bajo llave, se recomienda la implementación de controles biométricos para las áreas donde se guardan información física confidencial.

Figura 34 - Control Físico biométrico.

Fuente: Foto tomada en Digitex Perú SAC.

Protección contra las amenazas externas y ambientales.
Se propuso la instalación de alarmas ante incendio y compra de extintores de acuerdo al tipo de recursos físicos que se tengan en cada ambiente.

Figura 35 - Control físico contra amenazas externas.

Fuente: Foto tomada en Digitex Perú SAC.

El trabajo en áreas seguras.

Se recomendó al responsable del área de Servicio Generales que implanten un procedimiento para el trabajo en las diferentes áreas de acuerdo al trabajo a realizar.

Emplazamiento y protección de equipos

Los equipos de cómputo que utilizan los usuarios se encuentran empernados a los muebles, adicional a esto se implementaron cadenas de seguridad para estos equipos.

Figura 36 - Control físico cadena de seguridad en equipos de cómputo.

Fuente: Foto tomada en Digitex Perú SAC.

Instalaciones de suministro

Se habilitaron los UPS para los equipos de cómputo del Data Center, se balancearon los equipos en los gabinetes para que cada equipo se mantenga conectado a ambos UPS, así se tiene redundancia de alimentación eléctrica.

Seguridad del cableado

El cableado interno se encontraba con canaletas y dentro delos muebles para prevenir accidentes, el cableado externo se ordenó con precintos de seguridad.

Figura 37 - Ordenamiento de Cableado y separación del circuito eléctrico.

Fuente: Foto tomada en Digitex Perú SAC.

Mantenimiento de los equipos

El mantenimiento físico de equipos no se realizaba, en coordinación con el Responsable de Soporte Técnico se propuso la programación del mantenimiento preventivo para el 2020 previa aprobación de la compra de los recursos necesarios:

- Equipos de Protección Personal
- Equipos técnicos para la limpieza de equipos.

8. VERIFICAR (CHECK)

En la tercera etapa del Ciclo PDCA se hizo la verificación de los controles implementados mediante la auditoria haciendo uso de la herramienta de recolección de datos utilizada en la presente investigación y así conocer el nuevo estado de madurez de los controles del SGSI.

8.1. Auditoria de Verificación

Al realizar la auditoria en el post test se obtuvieron los siguientes datos.

Tabla 45 - Resultados de la auditoria de verificación en el post test.

Fuente: Elaboración propia en base al instrumento de recolección de datos Anexo 5.

Sección	Controles de Seguridad de la Información	Estado	Resultado / Evidencia
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Administrado	Política de Seguridad de la Información. Establecer un marco genérico para toda la organización de obligado cumplimiento respecto a la seguridad de la información.
A5.1.2	Revisión de las políticas para la seguridad de la información	Administrado	Política de Seguridad de la Información. Adaptación a posibles cambios en el alcance de la política y en los requisitos de seguridad de la compañía.
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Administrado	Política de Seguridad de la Información. Dar a conocer las responsabilidades que

			tiene cada empleado en función de su cargo.
A6.1.2	Segregación de tareas	Administrado	Política de Seguridad de la Información. Repartir responsabilidades, cargas y conocimiento.
A6.1.3	Contacto con las autoridades	Limitado	Mantener los contactos apropiados con las autoridades relevantes. Se realiza pero se recomienda trabajar un procedimiento.
A6.1.4	Contacto con grupos de interés especial	Limitado	Se recomienda que el responsable de seguridad pertenezca a alguna entidad de seguridad de la información Ejemplo ISACA.
A6.1.5	Seguridad de la información en la gestión de proyectos	No aplicable	No aplicable para el alcance de la investigación.
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	Administrado	Política de Dispositivos Móviles. Se menciona en la Política de Seguridad de la Información.
A6.2.2	Teletrabajo	No aplicable	No aplicable para el alcance de la investigación.
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	No aplicable	No aplicable para el alcance de la investigación.
A7.1.2	Términos y condiciones del empleo	No aplicable	No aplicable para el alcance de la investigación.
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Limitado	Política de Seguridad de la Información
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Limitado	Política de Seguridad de la Información. Se recomienda capacitar al personal y evidenciarlo con Actas.
A7.2.3	Proceso disciplinario	Limitado	Política de Seguridad de la Información. Se recomienda implantar sanciones en base a la Política.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Definido	Evitar que el acceso a la información sea realizado por personal no autorizado.

			Procedimiento de Altas y Bajas de Usuarios.
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Definido	Documento de Inventario de Activos. Para la investigación se realizó un inventario.
A8.1.2	Propiedad de los activos	Definido	Documento de Inventario de Activos. Política de Seguridad de la Información.
A8.1.3	Uso aceptable de los activos	Definido	Documento de Uso aceptable de Activos y equipo de infraestructura
A8.1.4	Devolución de activos	Definido	Documento PSSGG_01 Gestión de Recursos Asignados al Personal.
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Definido	Documento de Inventario de Activos. Para la investigación se realizó una clasificación.
A8.2.2	Etiquetado de la información	Definido	Documento de Inventario de Activos.
A8.2.3	Manipulado de la información	Definido	Documento de Inventario de Activos. Documento de Uso aceptable de Activos y equipo de infraestructura
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	No aplicable	No aplicable para el alcance de la investigación.
A8.3.2	Eliminación de soportes	No aplicable	No aplicable para el alcance de la investigación.
A8.3.3	Soportes físicos en tránsito	No aplicable	No aplicable para el alcance de la investigación.
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Administrado	Política de Seguridad de la Información. Procedimiento de Altas y Bajas de Usuarios
A9.1.2	Acceso a las redes y a los servicios de red	Definido	Política de Seguridad de la Información.
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Administrado	Política de Seguridad de la Información.

			Procedimiento de Altas y Bajas de Usuarios.
A9.2.2	Provisión de acceso de usuario	Definido	Procedimiento de Altas y Bajas de Usuarios.
A9.2.3	Gestión de privilegios de acceso	Administrado	Procedimiento de Altas y Bajas de Usuarios. Gestión en Grupos de Directorio Activo.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Administrado	Política de gestión de contraseñas que además permita al usuario cambiarla según crea conveniente. Política de Seguridad de la Información.
A9.2.5	Revisión de los derechos de acceso de usuario	Administrado	Mantener los permisos de acceso actualizados ante cualquier cambio. Documento de Revisión de Permisos de Usuario.
A9.2.6	Retirada o reasignación de los derechos de acceso	Administrado	Política de Seguridad de la Información. Procedimiento de Altas y Bajas de Usuarios.
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Definido	Política de Seguridad de la Información.
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Definido	Gestión de permisos por Grupos de Directorio Activo.
A9.4.2	Procedimientos seguros de inicio de sesión	Definido	Políticas de Directorio Activo.
A9.4.3	Sistema de gestión de contraseñas	Definido	Política de Seguridad de la Información. Políticas de Directorio Activo.
A9.4.4	Uso de utilidades con privilegios del sistema	Definido	Políticas de Directorio Activo.
A9.4.5	Control de acceso al código fuente de los programas	Definido	Protección de Acceso activada en el Anti Virus.
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Administrado	Política de Cifrado Seguro
A10.1.2	Gestión de claves	Limitado	Se recomienda implementar una Herramienta de Gestión de Contraseñas.
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		

A11.1.1	Perímetro de seguridad física	No aplicable	No aplicable para el alcance de la investigación.
A11.1.2	Controles físicos de entrada	No aplicable	No aplicable para el alcance de la investigación.
A11.1.3	Seguridad de oficinas, despachos y recursos	Limitado	Oficinas aseguradas con cerraduras y Llaves. Se configuró el equipo Biométrico para el acceso al Data Center.
A11.1.4	Protección contra las amenazas externas y ambientales	Limitado	Se compraron extintores, se validó el funcionamiento de Alarmas. Se propone implementar detectores de humo, humedad y alarmas de temperatura.
A11.1.5	El trabajo en áreas seguras	Definido	Se colocaron avisos en las zonas restringidas solo al Personal Autorizado y se validó que las zonas estén aseguradas.
A11.1.6	Áreas de carga y descarga	No aplicable	No aplicable para el alcance de la investigación.
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Definido	Garantizar la seguridad del parque informático mediante pernos y cadenas de seguridad.
A11.2.2	Instalaciones de suministro	Definido	Se activaron y balancearon los UPS del Data Center, se recomendó adquirir generadores de Energía.
A11.2.3	Seguridad del cableado	Limitado	Protección del cableado de Energía y de Datos mediante canaletas u oculto como parte de la arquitectura del centro, se realizó un ordenamiento del cableado. Se recomienda que se diseñe una solución de cableado estructurado.
A11.2.4	Mantenimiento de los equipos	Limitado	Para conservar en buen uso los equipos.
A11.2.5	Retirada de materiales propiedad de la empresa	No aplicable	No aplicable para el alcance de la investigación.
A11.2.6	Seguridad de los equipos fuera de las instalaciones	No aplicable	No aplicable para el alcance de la investigación.
A11.2.7	Reutilización o eliminación segura de equipos	Administrado	Política de Seguridad de la información. Procedimiento de borrado seguro de la información.

A11.2.8	Equipo de usuario desatendido	Administrado	Política de Seguridad de la información. Política en Directorio Activo.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Administrado	Política de Seguridad de la información.
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	Definido	Documento PSSGG_01 Gestión de Recursos Asignados al Personal. Se recomienda documentar todos los procesos de la Organización.
A12.1.2	Gestión de cambios	No aplicable	No aplicable para el alcance de la investigación.
A12.1.3	Gestión de capacidades	Definido	Planificar la capacidad de los sistemas de información. Monitoreo de capacidades de los sistemas de información con alertas vía Email.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable	No aplicable para el alcance de la investigación.
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Administrado	Solución Antimalware de McAfee.
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Administrado	Se implementaron tareas automáticas y con programación periódica. Se creó documento para revisión de cumplimiento de Backups
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	Definido	Se almacenan los LOGs de Auditoria del Directorio Activo.
A12.4.2	Protección de la información del registro	Definido	Se tiene las tareas de backup de los LOGs.
A12.4.3	Registros de administración y operación	Definido	Todos los LOGs de Auditoria son guardados y respaldados.
A12.4.4	Sincronización del reloj	Definido	Se implementó un servidor NTP, todos los servidores locales sincronizan con el NTP.
A12.5	**Control del software en producción**		
A12.5.1	Instalación del software en producción	Administrado	Política de Seguridad de la información. Política de Directorio Activo.

A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Limitado	Se recomienda la implementación de una Herramienta de escaneo de vulnerabilidades.
A12.6.2	Restricción en la instalación de software	Definido	Política de Seguridad de la información. Política de Directorio Activo.
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Limitado	Se recomienda analizar el origen de problemas de seguridad cuya causa no está identificada y documentarla.
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Definido	Reglas en el Firewall, gestión de permisos mediante grupos de Directorio Activo.
A13.1.2	Seguridad de los servicios de red	No aplicable	No aplicable para el alcance de la investigación.
A13.1.3	Segregación en redes	No aplicable	No aplicable para el alcance de la investigación.
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	Administrado	Política de Seguridad de la información.
A13.2.2	Acuerdos de intercambio de información	No aplicable	No aplicable para el alcance de la investigación.
A13.2.3	Mensajería electrónica	Definido	Reglas estrictas de filtrado SPAM.
A13.2.4	Acuerdos de confidencialidad o no revelación	Limitado	Se recomienda que RRHH hagan firmar acuerdos de no divulgación de información a los empleados.
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No aplicable	No aplicable para el alcance de la investigación.
A14.1.3	Protección de las transacciones de servicios de aplicaciones	No aplicable	No aplicable para el alcance de la investigación.

A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	No aplicable	No aplicable para el alcance de la investigación.
A14.2.2	Procedimiento de control de cambios en sistemas	No aplicable	No aplicable para el alcance de la investigación.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No aplicable	No aplicable para el alcance de la investigación.
A14.2.4	Restricciones a los cambios en los paquetes de software	No aplicable	No aplicable para el alcance de la investigación.
A14.2.5	Principios de ingeniería de sistemas seguros	No aplicable	No aplicable para el alcance de la investigación.
A14.2.6	Entorno de desarrollo seguro	No aplicable	No aplicable para el alcance de la investigación.
A14.2.7	Externalización del desarrollo de software	No aplicable	No aplicable para el alcance de la investigación.
A14.2.8	Pruebas funcionales de seguridad de sistemas	No aplicable	No aplicable para el alcance de la investigación.
A14.2.9	Pruebas de aceptación de sistemas	No aplicable	No aplicable para el alcance de la investigación.
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	No aplicable	No aplicable para el alcance de la investigación.
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No aplicable	No aplicable para el alcance de la investigación.
A15.1.2	Requisitos de seguridad en contratos con terceros	No aplicable	No aplicable para el alcance de la investigación.
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No aplicable	No aplicable para el alcance de la investigación.
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	No aplicable	No aplicable para el alcance de la investigación.
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No aplicable	No aplicable para el alcance de la investigación.
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		

A16.1.1	Responsabilidades y procedimientos	Administrado	Política de Seguridad de la información.
A16.1.2	Notificación de los eventos de seguridad de la información	Administrado	Política de Seguridad de la información. Cartel de Difusión de Política.
A16.1.3	Notificación de puntos débiles de la seguridad	Limitado	Política de Seguridad de la información. Se recomienda difundir un procedimiento para cada Área.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	No aplicable	No aplicable para el alcance de la investigación.
A16.1.5	Respuesta a incidentes de seguridad de la información	Definido	Política de Seguridad de la información. El Responsable de Sistemas se encarga de responder y solucionar los Incidentes de seguridad.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Definido	Se recomienda tener documentación de soluciones de incidentes.
A16.1.7	Recopilación de evidencias	No aplicable	No aplicable para el alcance de la investigación.
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A17.1.2	Implementar la continuidad de la seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No aplicable	No aplicable para el alcance de la investigación.
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	No aplicable	No aplicable para el alcance de la investigación.
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Definido	Política de Protección de Datos Personales.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	No aplicable	No aplicable para el alcance de la investigación.
A18.1.3	Protección de los registros de la organización	No aplicable	No aplicable para el alcance de la investigación.
A18.1.4	Protección y privacidad de la información de carácter personal	No aplicable	No aplicable para el alcance de la investigación.

A18.1.5	Regulación de los controles criptográficos	No aplicable	No aplicable para el alcance de la investigación.
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Limitado	Se recomienda que se continúen con las revisiones con una auditoria externa.
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Limitado	Se recomiendan las auditorías internas de manera periódica. Para la investigación se hizo una auditoría.
A18.2.3	Comprobación del cumplimiento técnico	Limitado	Se recomienda verificar en las auditorías internas la conformidad con los estándares de implementación de la seguridad.

8.2. Interpretación de Auditoria de Verificación

Del total de 114 controles del Anexo A de la ISO 27001, teniendo en cuenta que 44 controles son No Aplicables para la investigación se identificaron:

- 70 controles Aplicables.
- 70 controles Implementados.

Es decir el 100% de controles aplicables fue implantado con el apoyo de los recursos brindados por la organización.

En los casos donde era necesario adquirir nuevos recursos y que demandará un costo se dejaron las recomendaciones para poder llegar a un mejor estado de madurez una vez que el área encarga gestione las adquisidores.

Basado en los estados de Madures se identificó la siguiente proporción de Controles de Seguridad tomando el 100% de los 114 Controles.

Estado de Madurez	Proporción de Controles de Seguridad de la Información
? Desconocido	0%
Inexistente	0%
Inicial	0%
Limitado	15%
Definido	27%
Administrado	18%
Optimizado	0%
No aplicable	38%

Tabla 46 - Proporción de controles en base a su estado de madurez

Fuente: Elaboración propia en base a los datos de la Tabla 45.

Podemos concluir en que el estado de Madurez de los Controles del Sistema de Gestión de Seguridad de la Información se encuentra en un estado Definido y Administrado, en la siguiente ilustración vemos la gráfica que nos ilustra el porcentaje de cumplimiento de controles implementados, no se considera los controles No Aplicables de acuerdo al alcance de la Investigación.

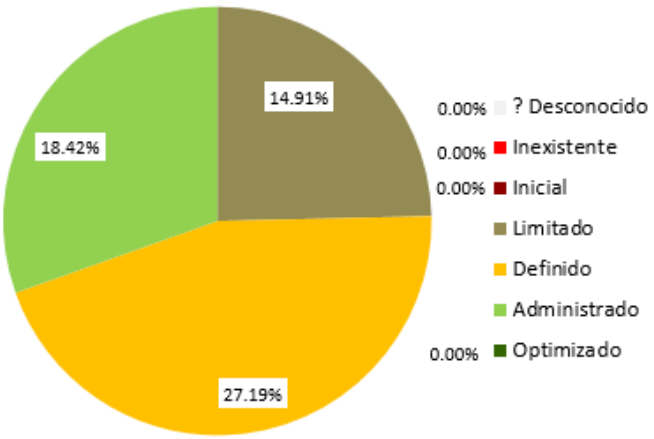


Figura 38 - Gráfica del estado de madurez de los 70 controles Aplicables.

Fuente: Elaboración proía en base a la Tabla 46.

9. ACTUAR (ACT)

En la cuarta y última etapa del Ciclo PDCA se debe de abordar las observaciones e implementar las recomendaciones encontradas en la etapa anterior ello para mejorar el nivel de madures de los controles implementados, se debería llegar mínimamente a un estado de madurez Definido por cada Control implementado para poder optar una certificación ISO.

Se recomienda la adquisición:

- Recursos físicos como Detectores de Humo, Grupo Electrógeno, CCTV Cámaras de seguridad, servicio de cableado estructurado.
- Recursos lógicos software escáner de vulnerabilidades, gestor de contraseñas.
- Recursos de gestión como documentación de procesos de todas las áreas, tercerización para auditoría externa y consultaría para mejorar el sistema de gestión.

ANEXO 2: MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	MARCO TEÓRICO	HIPÓTESIS	VARIABLES	METODOLOGÍA
PROBLEMA GENERAL:	**OBJETIVO GENERAL:**	**ANTECEDENTES:**	**HIPÓTESIS GENERAL:**		
¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima?	Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima.	**A NIVEL NACIONAL:** • (Atalaya Vásquez, 2016). *"Propuesta de un sistema de seguridad de la información para la oficina de admisión y registro académico de la Universidad Privada Antonio Guillermo Urrelo, 2016."* • *(Salinas y Valencia, 2017). "Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú."* • (Carranza y Gómez, 2018). *"Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001 para*	La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en la gestión de riegos de activos de información en la Empresa de BPO Contac Center Digitex, Lima.	**VARIABLE 1:** **Independiente** **Sistema de Gestión de Seguridad de la Información.** **DIMENSIONES**: Aplicabilidad de controles del SGSI	**MÉTODO DE INVESTIGACION:** ✓ Científico. **TIPO DE INVESTIGACION:** ✓ Aplicada. **NIVEL DE INVESTIGACION:** ✓ Explicativo **DISENO DE LA INVESTIGACION:** ✓ Experimental – Pre experimental
PROBLEMAS ESPECIFICOS:	**OBJETIVOS ESPECIFICOS:**		**HIPÓTESIS ESPECIFICO:**		
¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima?	Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.		La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad de Gestión en la Empresa de BPO Contac Center Digitex, Lima.		

¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima?	Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.	*el Hospital Nivel 2 - La Caleta"* • (Huanca Suaquita, 2018). *"La falsa percepción en la seguridad de los sistemas informáticos"* • (Cueva y Ríos, 2018). *"Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014"* **A NIVEL INTERNACIONAL:** • (Falivene, 2018). "Marco de Referencia Unificado en Seguridad de la Información" • (Yañez Caceres, 2017). "Sistema de Gestión de Seguridad de la Información para La Subsecretaria De Economía y Empresas De Menor Tamaño" • Changoluisa, 2017). "Optimización del Proceso de Alta y Baja De Usuarios a Través De La Implementación De Gestión De Seguridad	La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Lógicos en la Empresa de BPO Contac Center Digitex, Lima.	**VARIABLE 2:** **Dependiente** **Gestión de Riesgo en Activos de Información** **DIMENSIONES:** Controles de Seguridad de Gestión Controles de Seguridad Lógicos Controles de Seguridad Físicos	$G \quad O_1 \quad X \quad O_2$ **POBLACION:** ✓ 114 Controles del Anexo A de la ISO 27001. **MUESTRA:** ✓ 70 Controles Aplicables. **TECNICAS Y/O INSTRUMENTOS DE RECOLECCION DE DATOS:** ✓ Auditoria **TECNICAS DE PROCESAMIENTO Y ANALISIS DE DATOS:** ✓ Análisis Estadístico de Datos. ✓ Análisis GAP de Nivel de Madurez.
¿De qué manera influye la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima?	Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información a los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.		La implementación del Sistema de Gestión de Seguridad de la Información influye significativamente en los Controles de Seguridad Físicos en la Empresa de BPO Contac Center Digitex, Lima.		

		De La Información, Basado En La Norma ISO 27001:2013 En Una Empresa De Consultoría Para La Industria Petrolera" • (Álvarez, 2016). "Propuesta para La Gestión De La Seguridad de la Información en una Pequeña o Mediana Empresa" • (Nicasio, 2015). "Diseño e Implementación de un Sistemas de Gestión de Calidad en Seguridad de la Información (SGSI)"			

ANEXO 3: MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

DEFINICIÓN	DESCRIPCIÓN					
OPERACIONAL	Conjunto de elementos interrelacionados que nos permite medir y alcanzar los objetivos de control (Controles Anexo A SGSI) necesarios para una adecuada gestión de riesgo de los activos de información críticos para la organización.					
VARIABLE 1	DIMENSIONES	INDICADORES	ÍTEM	VALOR FINAL	TIPO DE VARIABLE	TÉCNICAS - INSTRUMENTOS
Independiente Sistema de Gestión de Seguridad de la Información.	Aplicabilidad de controles del SGSI	Cantidad de controles auditados del Anexo A de ISO 27001 de acuerdo al nivel de Madurez en el cual se encuentran. % de controles auditados del Anexo A de ISO 27001 de acuerdo al nivel de Madurez en el cual se encuentran. (1%-100%)	114 controles: Desde A5.1.1 hasta A18.2.3	0 Desconocido 1 Inexistente 2 Inicial 3 Limitado 4 Definido 5 Administrado 6 Optimizado 7 No aplicable	Ordinal	Instrumento: Auditoria Basada en los controles del Anexo A de ISO 27001. Métrica: Niveles de Madurez Continuo basado en la Metodología (CMMI) Análisis estadísticos de datos.

DEFINICIÓN	DESCRIPCION					
OPERACIONAL	Conjunto de actividades que permiten la selección y el cumplimiento de controles que puedan reducir el nivel de riesgo asociado a los activos de información.					
VARIABLE 2	DIMENSIONES	INDICADORES	ÍTEM	VALOR FINAL	TIPO DE VARIABLE	TÉCNICAS - INSTRUMENTOS
Dependiente Gestión de Riesgo en Activos de Información	Controles de Seguridad de Gestión	Cantidad de controles auditados del Anexo A de ISO 27001 de acuerdo al nivel de Madurez en el cual se encuentran. % de controles auditados del Anexo A de ISO 27001 de acuerdo al nivel de Madurez en el cual se encuentran. (1%-100%)	Controles: A5.1.1 - A5.1.2 A6.1.1 - A6.1.5 A6.2.1 - A6.2.2 A7.1.1 - A7.1.2 A7.2.1 - A7.2.3 A7.3.1 A8.1.1 - A8.1.4 A8.2.1 - A8.2.3 A8.3.1 - A8.3.3 A9.1.1 - A9.1.2 A9.2.1 - A9.2.6 A10.1.1 A11.2.7 - A11.2.9 A12.1.1 - A12.1.2 A12.5.1 A12.7.1 A13.1.2 - A13.1.3 A13.2.1 A13.2.2 A13.2.4 A14.1.1 - A14.1.3 A14.2.1 - A14.2.9 A14.3.1 A15.1.1 - A15.1.2 A15.1.3	0 Desconocido 1 Inexistente 2 Inicial 3 Limitado 4 Definido 5 Administrado 6 Optimizado 7 No aplicable	Ordinal	Instrumento: Auditoria Basada en los controles del Anexo A de ISO 27001. Métrica: Niveles de Madurez Continúo basado en la Metodología (CMMI) Análisis estadísticos de datos.

			A15.2.1 - A15.2.2 A16.1.1 - A16.1.7 A17.1.1 - A17.1.3 A17.2.1 A18.1.1 - A18.1.5 A18.2.1 - A18.2.3			
	Controles de Seguridad Lógicos		Controles: A9.2.3 A9.3.1 A9.4.1 - A9.4.5 A10.1.2 A11.2.8 A12.1.3 - A12.1.4 A12.2.1 A12.3.1 A12.4.1 - A12.4.4 A12.6.1 - A12.6.2 A13.1.1 A13.2.3			
	Controles de Seguridad Físicos		Controles: A11.1.1 - A11.1.6 A11.2.1 - A11.2.6			

ANEXO 4: INSTRUMENTO DE INVESTIGACIÓN.

Auditoría de los Controles del Sistema de Gestión de Seguridad de la Información

Adaptado y estandarizado por Miguel Angel Porras Ruiz.

Instrucciones:

Complete el campo Estado del formato de auditoria con el Estado de la tabla de métricas que más se aproxime al resultado del control de cada ITEM, los comentarios y evidencias de los resultados deben detallarse en el campo final (Resultados/Evidencias).

Tabla de Métricas para la Auditoria, basado en CMMI

VALOR	Estado	Significado
0	? Desconocido	No ha sido verificado
1	Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
2	Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
3	Limitado	La medida de seguridad se aplica de un modo informal (Con propuestas para un procedimiento formal). La responsabilidad es individual. No hay formación.
4	Definido	El control se aplica conforme a un procedimiento formal y verificado.
5	Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
6	Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
7	No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Formato de Auditoria, basado en el ANEXO A de la ISO 27001:2013

Sección	Controles de Seguridad de la Información	Estado	Resultado/ Evidencia
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información		
A5.1.2	Revisión de las políticas para la seguridad de la información		
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información		
A6.1.2	Segregación de tareas		
A6.1.3	Contacto con las autoridades		
A6.1.4	Contacto con grupos de interés especial		
A6.1.5	Seguridad de la información en la gestión de proyectos		
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles		
A6.2.2	Teletrabajo		
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes		
A7.1.2	Términos y condiciones del empleo		
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión		
A7.2.2	Concienciación, educación y capacitación en seguridad de la información		
A7.2.3	Proceso disciplinario		
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio		
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		

A8.1.1	Inventario de activos		
A8.1.2	Propiedad de los activos		
A8.1.3	Uso aceptable de los activos		
A8.1.4	Devolución de activos		
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información		
A8.2.2	Etiquetado de la información		
A8.2.3	Manipulado de la información		
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles		
A8.3.2	Eliminación de soportes		
A8.3.3	Soportes físicos en tránsito		
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso		
A9.1.2	Acceso a las redes y a los servicios de red		
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario		
A9.2.2	Provisión de acceso de usuario		
A9.2.3	Gestión de privilegios de acceso		
A9.2.4	Gestión de la información secreta de autenticación de los usuarios		
A9.2.5	Revisión de los derechos de acceso de usuario		
A9.2.6	Retirada o reasignación de los derechos de acceso		
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación		
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información		
A9.4.2	Procedimientos seguros de inicio de sesión		
A9.4.3	Sistema de gestión de contraseñas		
A9.4.4	Uso de utilidades con privilegios del sistema		
A9.4.5	Control de acceso al código fuente de los programas		
A10	**Criptografía**		

A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos		
A10.1.2	Gestión de claves		
A11	**Seguridad física y del entorno**		
A11.1	**Areas seguras**		
A11.1.1	Perímetro de seguridad física		
A11.1.2	Controles físicos de entrada		
A11.1.3	Seguridad de oficinas, despachos y recursos		
A11.1.4	Protección contra las amenazas externas y ambientales		
A11.1.5	El trabajo en áreas seguras		
A11.1.6	Areas de carga y descarga		
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos		
A11.2.2	Instalaciones de suministro		
A11.2.3	Seguridad del cableado		
A11.2.4	Mantenimiento de los equipos		
A11.2.5	Retirada de materiales propiedad de la empresa		
A11.2.6	Seguridad de los equipos fuera de las instalaciones		
A11.2.7	Reutilización o eliminación segura de equipos		
A11.2.8	Equipo de usuario desatendido		
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia		
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales		
A12.1.2	Gestión de cambios		
A12.1.3	Gestión de capacidades		
A12.1.4	Separación de los recursos de desarrollo, prueba y operación		
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso		
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información		
A12.4	**Registros y supervisión**		

A12.4.1	Registro de eventos		
A12.4.2	Protección de la información del registro		
A12.4.3	Registros de administración y operación		
A12.4.4	Sincronización del reloj		
A12.5	**Control del software en producción**		
A12.5.1	Instalación del software en producción		
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas		
A12.6.2	Restricción en la instalación de software		
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información		
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red		
A13.1.2	Seguridad de los servicios de red		
A13.1.3	Segregación en redes		
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información		
A13.2.2	Acuerdos de intercambio de información		
A13.2.3	Mensajería electrónica		
A13.2.4	Acuerdos de confidencialidad o no revelación		
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información		
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas		
A14.1.3	Protección de las transacciones de servicios de aplicaciones		
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro		
A14.2.2	Procedimiento de control de cambios en sistemas		
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		
A14.2.4	Restricciones a los cambios en los paquetes de software		

A14.2.5	Principios de ingeniería de sistemas seguros		
A14.2.6	Entorno de desarrollo seguro		
A14.2.7	Externalización del desarrollo de software		
A14.2.8	Pruebas funcionales de seguridad de sistemas		
A14.2.9	Pruebas de aceptación de sistemas		
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba		
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores		
A15.1.2	Requisitos de seguridad en contratos con terceros		
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones		
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor		
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor		
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos		
A16.1.2	Notificación de los eventos de seguridad de la información		
A16.1.3	Notificación de puntos débiles de la seguridad		
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información		
A16.1.5	Respuesta a incidentes de seguridad de la información		
A16.1.6	Aprendizaje de los incidentes de seguridad de la información		
A16.1.7	Recopilación de evidencias		
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información		
A17.1.2	Implementar la continuidad de la seguridad de la información		
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información		

A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		
A18.1.2	Derechos de Propiedad Intelectual (DPI)		
A18.1.3	Protección de los registros de la organización		
A18.1.4	Protección y privacidad de la información de carácter personal		
A18.1.5	Regulación de los controles criptográficos		
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información		
A18.2.2	Cumplimiento de las políticas y normas de seguridad		
A18.2.3	Comprobación del cumplimiento técnico		

ANEXO 6: VALIDACIÓN DEL INSTRUMENTO.

CONSTANCIA

Juicio de experto

Yo, _____, con documento nacional de identidad N° _____, certifico que realicé el juicio de experto del instrumento AUDITORÍA DE LOS CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, presentado por el bachiller Miguel Angel Porras Ruiz, en la investigación titulada SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE RIESGOS EN ACTIVOS DE INFORMACIÓN.

Huancayo, Diciembre 2019

……..
Sello y Firma del experto

CONSTANCIA

Juicio de experto

Yo, _____, con documento nacional de identidad N° _____, certifico que realicé el juicio de experto del instrumento AUDITORÍA DE LOS CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, presentado por el bachiller Miguel Angel Porras Ruiz, en la investigación titulada SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE RIESGOS EN ACTIVOS DE INFORMACIÓN.

Huancayo, Diciembre 2019

……..
Sello y Firma del experto

CONSTANCIA

Juicio de experto

Yo, _____, con documento nacional de identidad N° _____, certifico que realicé el juicio de experto del instrumento AUDITORÍA DE LOS CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, presentado por el bachiller Miguel Angel Porras Ruiz, en la investigación titulada SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE RIESGOS EN ACTIVOS DE INFORMACIÓN.

Huancayo, Diciembre 2019

……..
Sello y Firma del experto

ANEXO 7: LA DATA DE PROCESAMIENTO DE DATOS.

ITEM	Sección	INICIAL	FINAL
		Cuantitativo	Cuantitativo
1	A5.1.1	3	5
2	A5.1.2	3	5
3	A6.1.1	3	5
4	A6.1.2	3	5
5	A6.1.3	3	3
6	A6.1.4	1	3
7	A6.1.5	7	7
8	A6.2.1	1	5
9	A6.2.2	7	7
10	A7.1.1	7	7
11	A7.1.2	7	7
12	A7.2.1	1	3
13	A7.2.2	1	3
14	A7.2.3	1	3
15	A7.3.1	1	4
16	A8.1.1	1	4
17	A8.1.2	1	4
18	A8.1.3	3	4
19	A8.1.4	4	4
20	A8.2.1	1	4
21	A8.2.2	1	4
22	A8.2.3	1	4
23	A8.3.1	7	7
24	A8.3.2	7	7
25	A8.3.3	7	7
26	A9.1.1	1	5
27	A9.1.2	2	4
28	A9.2.1	1	5
29	A9.2.2	1	4
31	A9.2.4	1	5
32	A9.2.5	1	5
33	A9.2.6	1	5
40	A10.1.1	1	5
54	A11.2.7	3	5
56	A11.2.9	3	5

57	A12.1.1	3	4
58	A12.1.2	7	7
67	A12.5.1	1	5
70	A12.7.1	1	3
72	A13.1.2	7	7
73	A13.1.3	7	7
74	A13.2.1	3	5
75	A13.2.2	7	7
77	A13.2.4	1	3
78	A14.1.1	7	7
79	A14.1.2	7	7
80	A14.1.3	7	7
81	A14.2.1	7	7
82	A14.2.2	7	7
83	A14.2.3	7	7
84	A14.2.4	7	7
85	A14.2.5	7	7
86	A14.2.6	7	7
87	A14.2.7	7	7
88	A14.2.8	7	7
89	A14.2.9	7	7
90	A14.3.1	7	7
91	A15.1.1	7	7
92	A15.1.2	7	7
93	A15.1.3	7	7
94	A15.2.1	7	7
95	A15.2.2	7	7
96	A16.1.1	3	5
97	A16.1.2	1	5
98	A16.1.3	1	3
99	A16.1.4	7	7
100	A16.1.5	1	4
101	A16.1.6	1	4
102	A16.1.7	1	7
103	A17.1.1	7	7
104	A17.1.2	7	7
105	A17.1.3	7	7
106	A17.2.1	7	7
107	A18.1.1	1	4
108	A18.1.2	7	7

109	A18.1.3	7	7
110	A18.1.4	7	7
111	A18.1.5	7	7
112	A18.2.1	1	3
113	A18.2.2	1	3
114	A18.2.3	1	3
30	A9.2.3	1	5
34	A9.3.1	1	4
35	A9.4.1	1	4
36	A9.4.2	1	4
37	A9.4.3	1	4
38	A9.4.4	1	4
39	A9.4.5	1	4
41	A10.1.2	1	3
55	A11.2.8	3	5
59	A12.1.3	1	4
60	A12.1.4	7	7
61	A12.2.1	3	5
62	A12.3.1	3	5
63	A12.4.1	1	4
64	A12.4.2	1	4
65	A12.4.3	1	4
66	A12.4.4	1	4
68	A12.6.1	1	3
69	A12.6.2	1	4
71	A13.1.1	3	4
76	A13.2.3	1	4
42	A11.1.1	7	7
43	A11.1.2	7	7
44	A11.1.3	1	3
45	A11.1.4	1	3
46	A11.1.5	3	4
47	A11.1.6	7	7
48	A11.2.1	3	4
49	A11.2.2	1	4
50	A11.2.3	1	3
51	A11.2.4	1	3
52	A11.2.5	7	7
53	A11.2.6	7	7