FACULTAD DE INGENIERÍA

Carrera de Ingeniería Empresarial

“SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DOCUMENTAL DE LA ENTIDAD TÉCNICA L&M SEMINARIO GROUP S.A.C.”

Tesis para optar el título profesional de:

Ingeniera Empresarial

Autores:
Bach. Ana Paula Caiguaray Campos

Bach. Alicia Daniela Fernandez Diaz

Asesor:
Ing. Juan Miguel Deza Castillo

Trujillo - Perú

2020

ACTA DE AUTORIZACIÓN PARA SUSTENTACIÓN DE TESIS

El asesor Juan Miguel Deza Castillo, docente de la Universidad Privada del Norte, Facultad de Ingeniería, Carrera profesional de INGENIERÍA EMPRESARIAL, ha realizado el seguimiento del proceso de formulación y desarrollo de la tesis de los estudiantes:

- Caiguaray Campos, Ana Paula
- Fernández Díaz, Alicia Daniela

Por cuanto, **CONSIDERA** que la tesis titulada: Seguridad de la Información en la Gestión Documental de la Entidad Técnica L & M Seminario Group S.A.C para aspirar al título profesional de: Ingeniero Empresarial por la Universidad Privada del Norte, reúne las condiciones adecuadas, por lo cual, AUTORIZA al o a los interesados para su presentación.

_____

Ing. Juan Miguel Deza Castillo
Asesor

ACTA DE APROBACIÓN DE LA TESIS

Los miembros del jurado evaluador asignados han procedido a realizar la evaluación de la tesis de los estudiantes: Caiguaray Campos, Ana Paula & Fernández Díaz, Alicia Daniela para aspirar al título profesional con la tesis denominada: "Seguridad de la información en la gestión documental de la entidad técnica L & M Seminario Group S.A.C."

Luego de la revisión del trabajo, en forma y contenido, los miembros del jurado concuerdan:

( ) **Aprobación por unanimidad**

Calificativo:
( ) Excelente [20 - 18]
( ) Sobresaliente [17 - 15]
( ) Bueno [14 - 13]

( ) **Aprobación por mayoría**

Calificativo:
( ) Excelente [20 - 18]
( ) Sobresaliente [17 - 15]
( ) Bueno [14 - 13]

( ) Desaprobado

Firman en señal de conformidad:

Ing./Lic./Dr./Mg. Nombre y Apellidos
Jurado
Presidente

Ing./Lic./Dr./Mg. Nombre y Apellidos
Jurado

Ing./Lic./Dr./Mg. Nombre y Apellidos
Jurado

DEDICATORIA

A Dios, por brindarme sabiduría y fortaleza para alcanzar mis objetivos.
A mi familia, por ser mi soporte y compañía en el día a día. De forma muy especial, a mis padres, quienes me enseñaron a no rendirme y perseguir mis sueños desde pequeña y a mi abuela Teresa, por educarme en valores y apoyarme en cada uno de mis pasos.

Ana Paula Caiguaray Campos

A Dios, y a tres personas: mi madre, padre y abuela materna. Mamá, se la dedico por haberme enseñado la fortaleza y disciplina. Papá, porque en su paso por este mundo fue mi referencia de calidad e integridad profesional, me enseñó la importancia de trascender en la vida y a creer en que todo lo que aspire se consigue. Mey, porque sin tu guía, enseñanzas, paciencia y cuidados no sería la persona que soy ahora.

Alicia Daniela Fernández Díaz

AGRADECIMIENTO

Queríamos comenzar por agradecer a Dios, por guiarnos durante este camino de desarrollo profesional.

Agradecemos a nuestras familias por su apoyo incondicional y constante, sin el cual no hubiera sido posible concluir esta etapa.

A nuestro profesor, Nelson Angeles Quiñones por ser nuestro mentor y guía, gracias por la motivación y conocimientos brindados en los últimos años.

Tabla de contenidos

ÍNDICE DE TABLAS

Página

ÍNDICE DE FIGURAS

Página

RESUMEN

La presente investigación tuvo por finalidad determinar la influencia de la seguridad de información en la gestión documental de la entidad técnica L & M Seminario Group S.A.C. El diseño fue pre experimental de pre test y post test, para lo cual se hizo uso de técnicas como entrevista, cuestionario y análisis documental. La población y muestra fue conformada por los 8 colaboradores involucrados en la gestión documental. La prueba de hipótesis demuestra que existe un cambio significativo en la gestión documental, siendo $p = 0.024 < 0.05$ y en seguridad de la información $p= 0.038 < 0.05$. Los resultados obtenidos posteriormente a la implementación del procedimiento, basado en una propuesta de mejora continua y que consta de 15 etapas, fue una disminución de riesgos de seguridad de la información en un 56% los activos e incrementar un 83% los criterios evaluados para la concientización en seguridad de la información. De igual forma, en la gestión documental se logró proteger los activos con las pruebas de vulnerabilidad a un 100% de los ordenadores y conseguir accesibilidad a la documentación de hardware y software en un 96%. De igual forma, se obtuvo una proyección de VAN de S/. 40,773.05 soles, un TIR de 81.40 % y un índice costo beneficio de 1.90.

Palabras clave: Seguridad de la Información, Gestión Documental, Activo, Riesgos

ABSTRACT

The purpose of this investigation was to determine the influence of information security on the document management of the technical entity L & M Seminario Group S.A.C. The design was pre-experimental, pre-test and post-test, techniques such as interview, questionnaire and documentary analysis were used. The population and sample were the 8 collaborators involved in document management. The hypothesis test shows that there is a significant change in document management, with $p = 0.024 < 0.05$ and information security $p = 0.038 < 0.05$. The results obtained after the implementation was based on the continuous improvement plan, consisting of 15 stages; it was obtained from it a 56% decrease in the information security risks of the assets and an increases in 83% of the evaluated criterias from the information security conscientization program, in the document management a 100% of the computers were achieve after the vulnerabilities tests and it was obtained a 96% of accessibility in the hardware and software documentation. Likewise, a NPV projection of S /. 40,773.05 soles, an IRR of 81.40% and a cost benefit ratio of 1.9.

Keywords: Information Security, Document Management, Continuous Improvement, Asset, Risks

CAPÍTULO I. INTRODUCCIÓN

1.1. Realidad problemática

Las personas, ya sean miembros de la organización o stakeholders, siempre querrán que la información acerca de ellos sea gestionada y protegida apropiadamente; de igual manera las organizaciones buscan proteger sus procesos y asegurar las tecnologías de la información. Todos estos flujos de información procesados por las personas, tecnologías y procesos deben controlarse por el valor que ello representa. Una gestión efectiva del régimen de seguridad de la información puede proveer a la organización los cimientos para formar un modelo de gestión estratégica del conocimiento (Watkins, 2013); pues se sabe que todos los procesos son ejecutados por personas, las cuales usan tecnologías como productos basados en hardware y software para comunicar la información (Komisarczuk, 2019).

Muchas veces se minimiza el valor de la seguridad de la información física y digital. Sin embargo, se sabe que en el presente y con el incremento de la competencia se pueden usar diferentes técnicas como la ingeniería social para adquirir información confidencial de una empresa. Para una mayor comprensión, Watkins (2013) realiza una analogía de la seguridad de la información con el significado del dinero en una compañía en tres aspectos: nadie quiere que su dinero sea gastado sin permiso lo cual significa limitar el acceso manteniendo la confidencialidad; el segundo es que cada uno debe usar su dinero cuando lo desee y lo requiera, lo cual implica tener disponibilidad de este y por último todos quieren tener dinero verdadero al cambiarlo de moneda, es decir que se mantenga la integridad al recibir el dinero.

En España, el Instituto Nacional de Ciberseguridad indica que, a pesar de los avances tecnológicos en estos años y la aparición de dispositivos más rápidos, eficientes y sofisticados, sigue siendo el colaborador el principal elemento para respaldar la seguridad de la información de una organización pues se pueden implementar medidas; mas es el colaborador quien gestiona, modifica, transmite, procesa y elimina la información.

Asimismo, en Colombia la seguridad de la información es tomada como una necesidad en las organizaciones, las cuales cuentan con presupuesto para ello; no obstante, todos los integrantes de la organización deben ser concientizados de su valor y no solo las personas que laboran en el departamento de Tecnología de la Información (Dueñas, 2018). Un claro ejemplo de la falta de concientización en gestionar la seguridad de la información se presenta cuando un ex colaborador aún maneja datos y documentos de su antiguo empleo, se sabe de un estudio que 3 de cada 10 colaboradores que se han retirado de una empresa continua teniendo acceso a los mismos(Gestión, 2019).

Es por ello que, con el propósito de proteger la información en las empresas, se deben identificar los activos que presentan un impacto en ellas, hacer un análisis, realizar una evaluación de riesgo y definir el tratamiento de riesgo para minimizar la amenaza (Alexander, 2007). Lo anteriormente mencionado es de lo que trata un Sistema de Gestión de Seguridad de la Información, el cual está enfocados en preservar la confidencialidad, disponibilidad e integridad mediante la gestión y manejo de los riesgos integrando los procesos y sistema de gestión de la organización. Tal es su importancia que en el año 2016 en el Perú se dictó la Resolución Ministerial N° 004-2016-PCM en la que se convierte en uso obligatorio la NTP ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática; posteriormente,

en el año 2018 se aprueba la Política General de Seguridad de la Información en el Ministerio de Educación mediante la Resolución Ministerial N°664-2018-MINEDU.

De la mano con la seguridad de la información, se encuentra la gestión documental pues IsoTools (2017) asegura que un incorrecto control de la documentación puede afectar en la disponibilidad y fiabilidad de la información, ocasionando como consecuencia pérdidas monetarias en la organización; de igual manera, señala que, al digitalizar los documentos en físico, permite mejorar el tratamiento de datos personales, así como el establecimiento de autorizaciones de acceso.

En países de Latinoamérica como Colombia, existen empresas dedicadas a la administración de archivos ante la necesidad de gestionar su documentación. Tal es el caso de Transarchivos LTDA, la cual es la primera empresa dedicada a la gestión documental, utilizando tablas de valoración documental (TVD), tablas de retención documental (TRD) y la digitalización de documentos. Otro caso de éxito en Brasil es el de la empresa Macdata, su creador y director expresa que, en la gestión documental, la digitalización de documentos aumenta la productividad de las oficinas ya que permite brindar servicio en "home office", evitar el extravío de documentos y aprovechar al máximo los espacios físicos (Alvim, 2013).

En el Perú, se aprobó el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310, cuyo fin es la simplificación administrativa a través de la Plataforma de Interoperabilidad del Estado (PIDE) para el envío automático de documentos electrónicos. Cabe mencionar que esta norma es obligatoria solo para las entidades del poder ejecutivo; por otro lado, el Modelo de Gestión Documental se encuentra disponible para todas las entidades del sector público.

Sin embargo, también existen Normas Técnicas Peruanas basadas en la Organización Internacional de Normalización, las cuales sirven como referente para

todas las empresas que deseen aplicar buenas prácticas y de calidad aceptadas globalmente. Para la implementación de sistemas de gestión de seguridad de la información existe en concreto la familia de normas ISO/IEC 27000, esta proporciona un lenguaje universal y conceptos generales para la seguridad de la información, lo cual incrementa la cofianza entre los stakeholders en una organización (INACAL, 2018). Asimismo, dentro de esta familia de normas se encuentra la NTP ISO/IEC 27001:2014 la cual tiene por objetivo especificar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. A su vez, para complementar el establecimiento e implementación se toman las normas ISO 27002, 27003, 27004, 27005 y 27007 las cuales sirven como guía para implementar un sistema de gestón de seguridad de la información, incluyendo el código de práctica de controles, el monitoreo, medición, analisis y evalacion; asi como el análisis de riesgos y las guías para la auditoría.

El Ministerio de Vivienda, Construcción y Saneamiento del Perú cuenta con programas en pro del beneficio de los habitantes, tal es el caso de Techo Propio, el cual está dirigido a familias que cuentan con ingresos mensuales menores a S/ 3538 soles en la primera modalidad de compra denominada Adquisición de Vivienda Nueva; e ingresos de S/ 2627 soles para la modalidad de Construcción en Sitio Propio o Mejora de Vivienda.

En una empresa cuya actividad económica es la construcción y que a la fecha se desempeña para el Fondo MiVivienda como Entidad Técnica, la cual es quien promueve, desarrolla, construye y/o supervisa proyectos habitacionales para los Grupos Familiares Beneficiarios (Fondo Mivivienda, 2018) busca hoy en día realizar una correcta gestión de la seguridad de los datos que posee. L & M Seminario Group S.A.C. es una empresa trujillana constituida en el 2016 y trabaja bajo la modalidad de

Construcción en Sitio Propio, la cual busca satisfacer el déficit habitacional a nivel nacional de 500 000 viviendas mediante la construcción de Viviendas de Interés Social para las familias que cumplan algunos requisitos especificados en la Resolución Ministerial N° 236-2018-VIVIENDA (2018).

Asimismo, para lograr un Registro de Proyecto, la Entidad Técnica deberá realizar una serie de actividades, en el cual se manejan plazos y formatos establecidos por el Fondo Mivienda, los cuales son en su mayoría documentos en físicos, los que posteriormente a su presentación son almacenados dentro de cajas (ver anexo 01). Es por ello, que el principal argumento para realizar el presente estudio es tener un optimo registro de la documentación física pues ante algún reclamo de los stakeholder o de la Contraloría General, quien puede auditar hasta cinco años posterior a la entrega la obra, la organización deberá tener todos los documentos para poder objetar cualquier demanda.

De igual manera, la Entidad Técnica trabaja en conjunto con entidades financieras, estas son socios claves de la organización pues son quienes acreditan la oferta al Fondo Mivivenda y es el canal por el cual se desembolsa el bono familiar habitacional una vez aceptado el proyecto. En razón de ello, la organización requiere, como buena práctica, documentar la información técnica para la obtención de acreditaciones necesarias para el desarrollo de los proyectos. Por otro lado, cabe resaltar que durante el proceso y antes del desembolso del bono, existe la posibilidad que los beneficiarios calificados como elegibles sean contactados por otras Entidades Técnicas y que todos los recursos utilizados en la búsqueda hayan sido realizados para ser captados por la competencia. Asimismo, como en toda empresa, la entidad técnica busca generar rentabilidad mediante las actividades que desarrolla por lo que le interesa tener una buena gestión de los datos, información y documentos en sus proyectos.

Es así que, frente a los requerimientos de la organización analizada, el presente estudio se enfoca en la seguridad de la información en la gestión documental con el fin de actuar no solo de manera reactiva sino proactiva ante incidentes que puedan presentarse y asegurar una capacidad de servicio manteniendo a su vez la seguridad de la información. La implementación de la seguridad de la información resulta una decisión estratégica para la organización pues tiene como fin preservar la confidencialidad, disponibilidad y seguridad de la información mediante el desarrollo de buenas prácticas con respecto a la gestión de los datos e información procesada. Para ello, se aplicaron los linemientos de la NTP ISO/IEC 2700:2014 pues establece los requisitos genéricos para un sistema de gestión de seguridad de la información. Asimimo, la Entidad Técnica es consciente del impacto ambiental y social del entorno en el que se desarrollan. Es por ello que tomando una orientación hacia la seguridad de la información y un enfoque a la digitalización de documentos, se busca afirmar el compromiso con la reducción de huella de carbono en el planeta. Por último, se espera que la presente investigación brinde lineamientos trascendentes para organizaciones y estudios basados en desarrollar buenas prácticas enfocadas en la seguridad de la información.

1.1.1. Antecedentes

Lema, R. & Donoso, D. (2018) en su tesis para optar por título de magister en gerencia de sistemas en la Universidad de Las Fuerzas Armadas ESPE de Ecuador titulada **"Implementación de un sistema de gestión de seguridad de información basado en la norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa Lockers S.A."** concluye que según lo concertado en la norma ISO/IEC 27001:2013 se deben cumplir las

clausulas 4 a las 10 para la implementación de un Sistema de Gestión de Seguridad de la Información; se obtuvo que ayudó a identificar los riesgos de seguridad que vulneran la disponibilidad, integridad y confidencialidad de la empresa. Por último, recomienda realizar auditorías, cuyo tiempo está estipulado en la política de seguridad de la información, con el fin de cumplir con la mejora continua del sistema.

Suarez, S. (2015) en su tesis para optar por el título de especialista en seguridad informática en la Universidad Nacional Abierta y a Distancia de Bogotá D.C, Colombia. titulada **"Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suarez Padilla & CIA. LTDA. Que brinde una adecuada protección en seguridad informática de la infraestructura tecnolóca de la organización"** concluye que la información y los datos son el activo más importante de una empresa por lo que es vital contar con un Sistema de Gestión de Seguridad de la Información, el cual debe estar enfocado en la necesidades de la organización y basado en la norma ISO/IEC 27001:2013; asimismo afirma que el soporte de la alta dirección es esencial para la aprobación de toda la documentación generada en el sistema así como para la divulgación del mismo. Finalmente, recomienda que se realicen capacitaciones y sensibilización a los empleados con el de lograr mitigar riesgos de ataques de ingeniería social.

Justino, Z. (2015) en su tesis titulada **"Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013"** concluye que se necesita un compromiso de la

alta dirección para llevar a cabo el SGSI y la implementación de los controles, así como la difusión y conocimiento de la política a todo los colaboradores de la organización. De igual manera, enfatiza que los roles y responsabilidades del personal dentro del SGSI son fundamentales para que la política llegue a ser cumplidas y monitoreadas; a su vez, recomienda realizar capacitaciones permanentes con la finalidad de suscitar una cultura de seguridad en la organización el realizar auditorías periódicas del SGSI pues afirma que la seguridad total no existe.

Santos (2016) en su tesis para optar por el título de ingeniero informático en la Pontificia Universidad Católica del Perú titulada: **"Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software"** concluye que para las auditorías se debe tomar como guía la ISO 27002:2011, así como la ISO/IEC 27005:2008 para realizar la gestión de riesgos y por último la ISO 27004:2009 para obtener lineamientos con respecto a la elaboración las métricas para evaluar el sistema y los controles. De igual manera, se recomienda delimitar el alcance en los procesos críticos que manejen información y que posteriormente mediante la mejora continua se vayan agregando los procesos restantes.

Boca, V. (2016) en su artículo de investigación en la revista científica de la Universidad Señor de Sipán de Chiclayo titulada **"Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local Chiclayo"** sostiene que la seguridad de la información es un activo que no se compra, por el contrario, es un activo que debe gestionarse y

monitorearse. Concluye que el diseño de este sistema repercute en una efectiva dirección de la información mediante el estándar internacional de la ISO 27000, recalca que el recurso humano es el activo más importante por lo que debe estar concientización, capacitado y comprometido, así como saber las consecuencias procesales al atentar en contra de la disponibilidad, integridad y confidencialidad de los activos de información. Por último, señala que es esencial el establecimiento de un comité de seguridad de la información y la estipulación de un Oficial de Seguridad de la Información el cual mantendrá informado al comité acerca de los avances y velará por la ejecución de las políticas de seguridad de la información.

Mercado (2016) en su tesis para optar por el grado de magíster en ingeniería de sistemas con mención en gestión de la tecnología de información y comunicaciones en la Universidad Nacional Mayor de San Marcos titulada: **"Modelo de gestión de Seguridad de la información para el E-Gobierno"** concluye que se debe establecer una estructura organizacional con las funciones de los colaboradores definidas para poder gestionar la seguridad de la información. También, para medir el desempeño del SGSI estableció 6 distintos tipos de indicadores y métricas. Por otro lado, la elección de los controles de la ISO 27001:2014 a implementar se basó en un análisis y evaluación de riesgos previo.

Vilca (2017) en su tesis para optar por el título de ingeniería de sistemas e informática en la Universidad de Huánuco titulada: **"Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos**

humanos de la empresa GEOSURVEY de la ciudad de Lima" concluye que es fundamental tener las políticas de seguridad documentadas para generar conocimiento y concientización en los integrantes de la organización. Asimismo, luego de aplicar el SGSI se incrementó el control de acceso a los ordenadores de la empresa de un 21.2% a 60.6% protegiendo información sensible y el riesgo de la pérdida de esta.

Camargo (2017) en su tesis para optar por el grado de magíster en seguridad informática en la Universidad Nacional abierta y a distancia de Bogotá titulada: **"Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil – CNSC basada en la norma ISO 27000 e ISO 27001"** concluye que el riesgo más alto para la seguridad de la información en una organización es el recurso humano, es por eso que recomienda tener claro y cumplir con los procedimientos y políticas de seguridad partiendo desde el nivel gerencial. Por otro lado, se analizaron los riesgos y se realizó una declaración de aplicabilidad según el Anexo A de la ISO/IEC 27001.

Adriazola (2017) en su tesis para optar por el grado de magister en Procesamiento y Gestión de la Información en la Pontificia Universidad Católica de Chile titulada: **"Propuesta para la gestión documental de archivos escolares en Chile: El Instituto Nacional General José Miguel Carrera"** concluye que se realizó el esquema de la metodología DIRKS como orientación para implementar el sistema de gestión documental, se realizaron encuestas con preguntas abiertas para que los colaboradores indiquen qué

entendían por tratamiento documental y se propuso un manual de convivencia; de igual manera herramientas como el cuadro de clasificación y una tabla de retención documental (TRD) en la que se indica el tiempo de permanencia tanto en la oficina como en un archivo intermedio o/y en el Archivo Histórico Nacional. Finalmente señala que todos los cambios van de la mano con una modificación en la cultura organizacional, en la tecnología utilizada y el uso de normas.

Cabanaconza (2017) en su tesis para optar por el grado de maestro en Gestión Pública en la Universidad César Vallejo en Trujillo titulada: **"Procesos técnicos archivísco y gestión documental en la Oficina General de Administración de Recursos – Seguro Integral de Salud, Lima 2016"** sostiene que mediante la aplicación de cuestionarios con la escala de Likert para analizar los procesos técnicos archivísticos y la gestión documental, así como se determinó la correlación positiva entre ambas variables mediarte el uso del rho de Spearman.

Higa (2017) en su tesis para optar por el grado de ingeniero industrial en la Universidad Nacional Mayor de San Marcos titulada: **"Implementación de un sistema de gestión documental en el área de SSMA de una empresa del sector construcción"** concluye que para mejorar el trámite documentario en la organización es necesario aplicar las firmas electrónicas en los procesos administrativos que lo permiten legalmente. Para lograr eso, se realizaron estudios previos en organizaciones garantizando la seguridad de la información a través de una prueba previa. Asimismo, evalúo el VAN Y TIR del proyecto demostrando que es factible. Finalmente, recomienda a la empresa continuar con iniciativas para mejorar la gestión documental dentro de otras áreas.

Luyo (2018) en su investigación para optar por el grado de ingeniero de sistemas e informática en la Universidad Norbert Wiener titulada: **"Sistema digitalfile 1.0 para mejorar la gestión documental del tratamiento de datos personales en la empresa BBVA, Lima 2018"** concluye que el implementar el sistema Digitalfile acelerará la respuesta a la solicitud de sus clientes y entidades reguladores acerca de sus documentos, asegurando la confidencialidad de datos personales. Para lograr eso, se realizó una encuesta a los colaboradores para conocer la realidad problemática de la empresa, se mapearon los procesos y se realizó la simulación de escenarios reales de posibles resultados post implementación.

1.1.2. Marco teórico

1.1.2.1. Sistema de Gestión de Seguridad de la Información

"Conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base los riesgos a los que enfrente la organización." (p.13, Gómez & Fernández, 2018)

> "Preservar la confidencialidad. Integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos" (p.7, NTP ISO/IEC 27001:2016)

Activo

Definido por la ISO/IEC 27000:2018 como cualquier cosa con un valor en la organización, hay diferentes tipos de activos, incluyendo: activos de información, activos software (como programas de

computadora), activos físicos, activos servicios, activos personas (y sus títulos, habilidades, experiencia) y activos intangibles como la imagen y reputación.

Control

Establecido por la ISO/IEC 27000:2018 como el significado de manejar los riesgos, incluyendo políticas, procedimientos, pautas, estructuras organizacionales o prácticas, que pueden ser de naturaleza administrativas, técnicas, gerenciales o legales.

Seguridad de la Información

"Preservación de la confidencialidad, integridad y disponibilidad de la información" (p.3, ISO/IEC 27000:2018)

Práctica de defender la información de acceso o uso no autorizado, divulgación, interrupción, modificaciones, inspección, grabaciones o destrucción. Es un término en general que puede ser usado sin importar la forma de la data que tome, ya sea física o en una computadora (Komisarczuk, 2019).

Confidencialidad

Definida por la ISO/IEC 27000:2018 como la propiedad que la información no se encuentre disponible o sea revelada a personas, entidades o procesos carentes de autorización.

> "Grado en el que el acceso a la información está restringida a un cierto grupo autorizado a tener dicho acceso. Esto también incluye las medidas para proteger la privacidad" (Fundamentos de la seguridad de la información)

> "Solo los usuarios autorizados deberían tener acceso a la información"

Integridad

Establecida por la ISO/IEC 27000:2018 como la propiedad de estar completo y exacto. Asimismo, Komisarczuk (2019) señala que un sistema de seguridad debe estar completo, ser preciso y no presentar modificaciones no autorizadas, así como tener la capacidad de determinar que la información fue proporcionada según lo requerido y que se puede verificar su procedencia.

"Grado en el que la información está actualizada y sin errores" (Fundamentos de la seguridad de la información)

Disponibilidad

Definida por la ISO/IEC 27000:2018 como la propiedad de ser accesible y usable ante el requerimiento de un ente autorizado.

> "Grado en el que la información está disponible para el usuario y para el sistema de información que está operando en el momento que la organización lo requiere"
>
> "Disponible y operativo cuando sea requerido por cualquier usario autorizado" (Komisarczuk, 2019)

De acuerdo con la organización International Electrotechnical Commision es la habilidad de estar en un estado para desempeñarse

como es requerido; asimismo, establece que la disponibilidad depende de la combinación de características de confiabilidad, recuperabilidad, mantenibilidad de un ítem (objeto, articulo) y del desempeño del soporte de mantenimiento.

Figura 1. Triada de Seguridad de la Información
Fuente. Elaboración propia

Ciclo de mejora continua

La mejora continua está definida por la ISO/IEC 27000:2018 como la actividad recurrente para aumentar el desempeño. De acuerdo con Gómez & Fernández (2018) el ciclo de mejora continua se encuentra implícito en la composición de la norma.

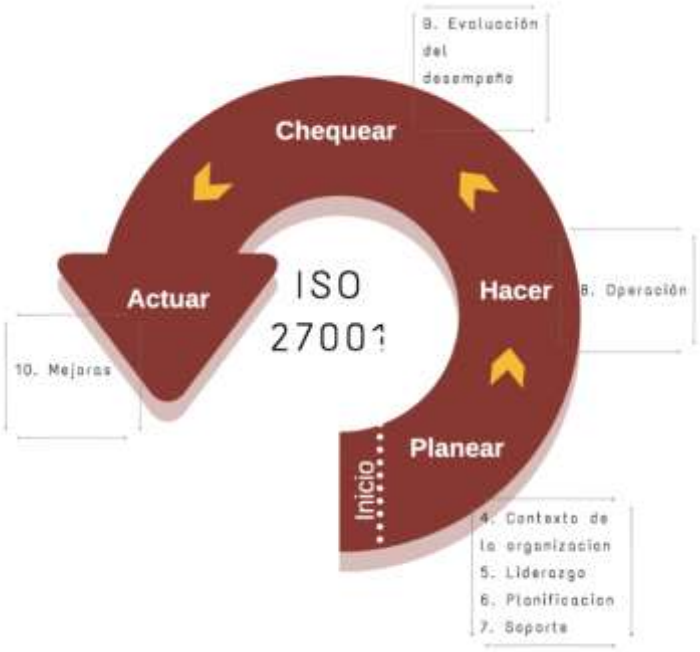


Figura 2. Mejora continua en la estructura de ISO 27001

Fuente. Elaboración propia

Planear

Para el planeamiento de la implantación del SGSI se utilizará los capítulos 4,5,6 y 7 de la norma ISO/IEC 27001:2014, a continuación, se mencionan y sus respectivas actividades:

Figura 3. Contexto de la organización. Capítulo 4 ISO 27001

Fuente. Elaboración propia

- Contexto de la organización (Capitulo 4 de NTP/ISO 27001)

Comprender la organización y su contexto

Es decir, reconocer los factores externos e internos de la organización; por ejemplo, para los de carácter internos se podría identificar las fortalezas, oportunidades, debilidades y amenazas, mientras que para los factores externos las políticas, economía, aspectos sociales, tecnología, aspectos ecológicos y legales con respecto a un sistema de gestión de seguridad de la información. Asimismo, fundamentalmente se debe conocer los objetivos del negocio.

Asimismo, Gómez & Fernández (2018) señalan que el conocimiento de la organización implica conocer los objetivos del negocio y todo el entorno externo e interno que pueda perjudicar o favorecer al logro de los mismos; indica también que el objetivo es que el sistema de gestión se encuentre alineado con los objetivos de negocio de manera que logre favorecer su desempeño.

Comprender las necesidades y expectativas de las partes interesadas

Siempre y cuando sean relevantes al sistema de gestión de seguridad de la información; como partes interesadas se toman los proveedores, usuarios, competencia y organismos que regulen legalmente.

Determinar el alcance del sistema de gestión de seguridad de la información

Es decir, se delimitará el objetivo que se alcanzará y los procesos más importantes para realizar la implementación del sistema de gestión de seguridad de la información, para lo cual se debe haber realizado un análisis de los dos primeros puntos, así como identificar las interacciones y dependencias con otras organizaciones.

Según Gomez & Fernández (2018), es fundamental dimensionar adecuadamente el proyecto para que este tenga éxito. De igual manera, la norma establece que este alcance se debe encontrar disponible como documento. Asimismo, la NTP ISO 27003:2012 indica que la salida del desarrollo del alcance preliminar del sistema de gestión de seguridad de la información es clarificar las prioridades de la organización para desarrollar el sistema de gestión de seguridad de la información.

Sistema de gestión de seguridad de la información

Según la norma técnica peruana ISO 27001 la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de seguridad de la información conforme a los requisitos establecidos en dicha norma.

- Liderazgo (Capitulo 5 de NTP/ISO 27001)

Figura 4. Liderazgo. Capítulo 5 ISO 27001
Fuente. Elaboración propia

Liderazgo y compromiso

Por parte de la dirección general, es decir esta debe estar involucrada en todo el proceso de la implementación de modo que se brinden tanto los recursos necesarios como el tener alineados los objetivos de seguridad de la información con los de la dirección estratégicas. La NTP ISO 27003:2012 sugiere que para obtener la aprobación de gerencia para dar inicio a un proyecto de SGSI se debería definir un caso de negocio y un plan de proyecto. De igual manera, la dirección deberá comprometerse con la comunicación del SGSI y la integración del mismo en los procesos de la organización de forma permanente para lograr una mejora continua.

A su vez, Gomez & Fernández (2018) enfatizan que las principales actividades en las que deberá involucrarse la dirección es en establecer la política y objetivos y en asegurar la integración de los requisitos de seguridad en los procesos de la organización para lograr el cambio de cultura organizacional.

Política

De acuerdo con la ISO/IEC 27000:2018, una política refleja las intenciones y dirección de la organización y formalmente comunicada por su más alta gerencia. Es así que Gomez & Fernández (2018) hacen hincapié en que debe ser establecida por la alta dirección, esta debe estar acorde al fin de la organización por lo que deberá incluir los objetivos orientados a la seguridad de la información y a prevalecer la confidencialidad, integridad y disponibilidad de la información de la empresa por lo cual se debe incluir un acuerdo de satisfacer las demandas de la organización y la mejora continua del sistema. Esta política deberá ser comunica y disponible para todos en la organización y partes interesadas como clientes, usuarios y proveedores. Asimismo, la NTP ISO 27003:2012 indica que al definir una política del sistema de gestión de seguridad de la información se debe entregar un documento en el que se describa la política documentada y aprobada por la dirección pues esta política de seguridad de la información documenta la posición estratégica con respecto a los objetivos de seguridad de la información de la misma.

Roles, responsabilidad y autoridades organizacionales

Las cuales deberán ser definidas por la alta dirección la misma que será responsable de que el SGSI esté de acuerdo con la NTP ISO/IEC 27001:2016. Gomez & Fernandez (2018) señalan que un error común al designar un encargado de la seguridad de la información es pensar que este debe ser un personal técnico, sin embargo, al ser el sistema basado en los

objetivos de la organización este comenzará por las áreas estratégicas para determinar los requisitos de seguridad los cuales luego serán implementados por el personal técnico, de igual manera indican que debería contemplar un responsable de seguridad y un comité de seguridad. Asimismo, la NTP ISO/IEC 27003:2012 señala que se debería definir y documentar la colaboración con especialistas del negocio, foros de seguridad de la información o algún medio parecido durante todo el proceso de desarrollar, implementar, operar y mantener el sistema de gestión de seguridad de la información.

- Planificación (Capitulo 6 de NTP/ISO 27001)

Figura 5. Planificación. Capítulo 6 ISO 27001
Fuente. Elaboración propia

Acciones para tratar los riesgos y las oportunidades

Como entrada se debe comprender el contexto y necesidades de la organización (puntos 4.1. y 4.2) para asegurar el logro de los resultados; se debe planificar cómo integrar e implementar las acciones que traten los riesgos en los procesos seleccionados del sistema de gestión al igual que

evaluar la efectividad de dichas acciones. Según la ISO/IEC 27000:2018 un riesgo es el efecto de incertidumbres los objetivos y dentro del contexto de los sistemas de gestión de seguridad de la información, un riesgo puede ser expresado como el efecto de incertidumbre en los objetivos de seguridad de la información.

Valoración del riesgo de seguridad de la información

La ISO/IEC 27000:2018 establece el análisis de riesgos como el proceso de comprender la naturaleza del riesgo y determinar el nivel del mismo. Es así que la NTP ISO/IEC 27001:2016 establece que:

> Se debe definir un proceso que establezca y mantengan los criterios de riesgo de seguridad de la información los cuales son los criterios de aceptación de riesgos.
>
> Se debe asegurar que las valoraciones repetitivas de riesgo de seguridad de la información produzcan resultados validos consisteses y comparables.
>
> Se debe identificar riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad para la información según lo establecido en el alcance del sistema de gestión de seguridad de la información
>
> Se debe analizar los riesgos valorando las consecuencias potenciales y probabilidad realista al materializarse, asignando un nivel de riesgo. De igual forma, toda la información acerca de la valoración de riesgos debe ser documentada.

La ISO 27005:2011 está dedicada especialmente a brindar lineamientos para los riesgos, definiendo la evaluación de riesgos como el proceso en general de identificación de riesgos, análisis de riesgo y evaluación de riesgos. Asimismo, en la NTP ISO 27003:2012 describe el objeto de realizar una evaluación de riesgo el establecer la metodología de evaluación del riesgo, identificación, análisis y evaluación de los riesgos de seguridad de la información para luego realizar la selección de opciones de tratamiento de riesgo y la selección de objetivos de control y controles.

Tratamiento de riesgos de seguridad de la información

El tratamiento de este tipo de riesgos es definido por la ISO/IEC 27000:2018 como el proceso para modificar los riesgos. La guía brindada por la NTP ISO/IEC 27001:2016 señala que se debe identificar un proceso de tratamiento de riesgo para determinar los controles necesario para realizar la implementación, los cuales se encuentran detallados en el anexo A de dicha norma.

De igual manera, la organización deberá realizar una Declaración de Aplicabilidad la cual detalle los controles y la justificación de su uso. Se deberá, de igual forma, realizar un plan de tratamiento de riesgos de seguridad de la información; así como conseguir la aprobación del propietario de riesgos y la aceptación de riesgos residuales. La información acerca del proceso de tratamiento de riesgos debe estar documentada en la organización.

En la ISO/IEC 27003:2012 se establece que el tratamiento de riesgos tiene como entrada una lista de riesgos prioritarios de acuerdo a un criterio de

evaluación de riesgo en relación a los escenarios de incidentes que pueden llevar a estos riesgos y la acción que se realiza mediante el tratamiento es la aplicación de controles para reducir, retener, evadir o compartir los riesgos debe ser seleccionado y un plan de tratamiento de riesgos debe ser definido.

Figura 6. Gestión de tratamiento de riesgos

Fuente. Adaptado de la figura The risk management process Iso/IEC 27005:2011 page 13

Objetivos de seguridad de la información y planificación para conseguirlos

Figura 7. Planificación para la obtención de objetivos de seguridad de la información

Fuente. Elaboración propia

Las informaciones acerca de los objetivos de seguridad de la información deben estar documentada en la organización.

Figura 8. Puntos a considerar en la planificación de objetivos

Fuente. Elaboración propia

De igual manera la NTP ISO/IEC 27000:2018 señala que los objetivos son los resultados a ser alcanzados, agrega que estos objetivos pueden ser estratégicos, tácticos u operativo.

- Soporte (Capitulo 7 de NTP/ISO 27001)

Figura 9. Soporte. Capítulo 7 ISO 27001

Fuente. Elaboración propia

Recursos

La organización debe brindar y gestionar los recursos necesarios para una efectiva implantación durante el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información. Gómez & Fernández (2018) sugieren que se debe incluir una previsión de costes de implantación de los recursos humanos y económicos necesarios.

Competencia

La ISO/IEC 27000:2018 define competencia como la habilidad para aplicar el conocimiento y las habilidades para conseguir los resultados esperados. En tanto, la NTP ISO/IEC 27001:2016 se refiere a las capacidades que debe

tener una persona con respecto a la experiencia y capacitaciones para cada puesto de trabajo; para ello la organización debe determinar la competencia necesaria, asegurar que el personal existente sea competente y si no lo es adquirir la competencia necesaria.

Concientización

Según la NTP ISO/IEC 27001:2016 todo el personal debe ser consciente acerca de la política de seguridad de la información y el rol que tiene para la efectividad del sistema. Tal es su importancia que dentro de los factores críticos para el éxito de un sistema de gestión de seguridad establecidos por ISO/IEC 27000:2018 se encuentra el realizar una efectiva concientización de seguridad de información, entrenamiento y educación informando a todos los colaboradores y partes relevantes sus obligaciones con respecto a las políticas y motivarlos para actuar acuerdo al mismo.

Comunicación

Tanto interna como externa (identificar las partes interesadas) acerca del sistema de gestión de seguridad de la información.

Qué, cuando, a quien y los procesos por los que la comunicación se efectuara

Información documentada

Es definida por la ISO/IEC 27000:2018 como la información que debe ser controlado y mantenida por la organización y por el medio en el que ha sido almacenada. Es así que la NTP ISO/IEC 27001:2016 significa registrar los

requerimientos de la norma técnica peruana, las actividades, los procesos y su complejidad, productos, servicios y competencias de las personas. Esta información debe estar correctamente identificada y descrita con la fecha, autor o el uso de un numero de referencia, de igual manera el formato debe ser el apropiado. Esta información documentada debe estar disponible para que toda la organización tenga acceso a ella cuando sea necesaria usarla y debe será protegida para que no sufra pérdida de confidencialidad, integridad o uso inapropiado. Para el control de la misma se debe realizar la distribución, acceso, recuperación y uso, almacenamiento y preservación, control de cambios (versiones), retención y disposición.

- Operación (Capitulo 8 de NTP/ISO 27001)

Figura 10. Operación. Capítulo 8 ISO 27001
Fuente. Elaboración propia

Planificación y control operacional, con el fin de lograr los objetivos de seguridad de la información determinados en la fase de planificación mediante el mantenimiento de información documentada, el control de los cambios planeados y la consecuencia de los mismos; así como el control de los procesos terciarizados previamente determinados.

Evaluación de riesgos de seguridad de la información, realizados por la organización en intervalos planificados o al ocurrir cambios significativos. Los datos de los resultados deberán ser documentados.

Tratamiento de riesgos de seguridad de la información, mediante un plan de tratamiento de riesgos, los resultados deberán documentase.

- Evaluación del desempeño (Capitulo 9 de NTP/ISO 27001)

Figura 11. Evaluación del desempeño. Capítulo 9 ISO 27001
Fuente. Elaboración propia

Monitoreo, medición, análisis y evaluación, para ello se debe determinar qué es necesario ser monitoreado y medido (incluir controles de seguridad de la información y procesos) y qué métodos se deben usar para obtener resultados válidos. De igual manera, determinar lo siguiente:

Figura 12. Monitoreo. Capítulo 9 ISO 27001

Fuente. Elaboración propia

Auditoría interna, se realiza para evaluar el cumplimento de los requisitos de la norma, la implantación de los procesos y la efectividad y eficacion de los controles. Para ello, la NTP ISO 27001:2016 establece que se deberá realizar un plan de auditoria el cual detalle el alcance, frecuencia, criterios a auditar, responsables. Una auditoría es definida por la ISO 27000:2018 como un proceso sistemático, independiente y documentado para objetar una evidencia auditada y evaluarla objetivamente para determinar cuál es su extensión respecto a lograr alcanzar el criterio de auditoría. Asimismo, el anexo A de la ISO/IEC 27007:2016 brinda una guía práctica en auditoría de sistemas de gestión de seguridad de la información, cuyo propósito es servir de referencia para el auditor ya sea interno o externo que realizará la auditoría.

Revisión por la gerencia, esta se realiza en transcursos planificados con el fin de garantizar la conveniencia, adecuación y efectividad del sistema de gestión mediante las identificaciones de oportunidades de mejora y necesidad de cambio.

- Mejoras (Capitulo 10 de NTP/ISO 27001)

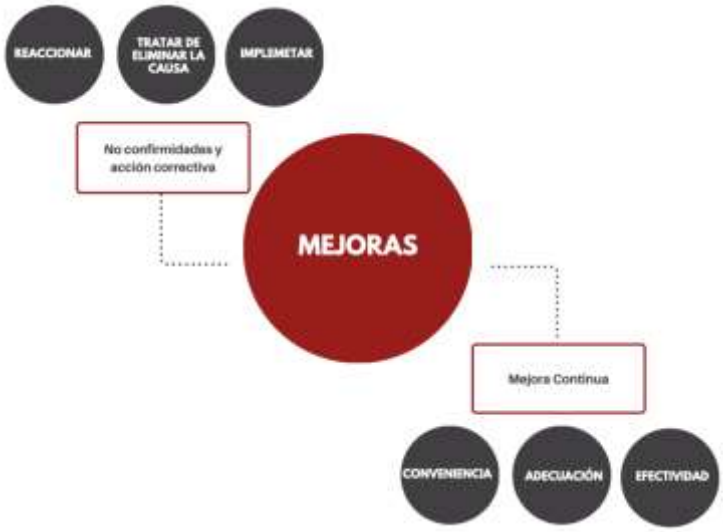


Figura 13. Mejoras. Capítulo 10 ISO 27001

Fuente. Elaboración propia

No conformidades y acción correctiva, al ocurrir esto la organización debe reaccionar y tomar acción para controlar y corregir. La ISO 27000:2018 define una no conformidad como el incumplimiento de un requerimiento.

Mejora continua, del sistema de gestión de seguridad de la información mediante la conveniencia, adecuación y efectividad.

1.1.2.2. Gestión Documental

"Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida… desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación"

Objetivo

Según Franklin (2014) la gestión documental es la manera por la cual se transmiten los datos e información de la organización de forma más sencilla, clara y funcional mediante el orden, sistematización y orientación de los recursos físicos o electrónicos.

Enfoques

Clásico

I. Importancia

Los documentos son usados para dejar en constancia su ejecución. Cuando las operaciones administrativas son numerosas y repetitivas es necesario utilizar formas impresas en las que se debe considerar lo siguiente:

- Contenido
- Cantidad
- Costo
- Grado y cohesión
- Confiabilidad

II. Análisis

Los requisitos que deben considerarse cuando se analizan las condiciones materiales de una forma impresa son los siguientes:

- Formas que no tienen el tamaño adecuado
- Duplicidad, al ser utilizadas para un mismo fin
- Exceso de formas que se utilizan con una baja frecuencia
- Formas con un número de copias innecesario
- Formas con un diseño ineficiente

- Sin forma o contenido requerido

III. Fuentes de información

Son diversas, pero las más utilizadas son:

- De uso interno
- Diseñadas para presentar resultados
- Producto de un consultor externo
- De uso comercial
- Elaboradas por una autoridad normativa
- Requeridas por una instancia externa
- Propuestas por un fabricante de papel o diseñador profesional

IV. Diseño

- **Identificación:** Logotipo de la empresa, Título, fecha, número de hoja.
- **Orden de los componentes:** secuencia de datos, flujo del trabajo, cuerpo, instrucciones al pie.
- **Condiciones para su llenado:**
  - ✓ **Manual:** Espacios adecuados para la cantidad de información
  - ✓ **Máquina:** El espaciado debe ser de acuerdo con una máquina de escribir**.**
  - ✓ **Impresoras de equipo:** Las formas se hacen en una computadora, por lo que es sencilla la impresión.
- **Clases de formas:**

- ✓ **De línea:** Es la más sencilla, los datos se anotan en líneas**.** Se utiliza al ser la información es mínima.
- ✓ **De columnas:** Contiene columnas y reglones que contienen datos fijos generalmente como encabezados.
- ✓ **De casillas:** Se utiliza cuando hay abundante información por registrar.
- ✓ **Combinado:** Incluye más de una presentación. Puede combinar casillas y bloques.
- ✓ **Visualización:** Una forma debe cumplir los requisitos de unidad, división modular, claridad, agrupación y jerarquización, saturación, movimiento, ritmo, imagen residual.

- **Elementos materiales:**
  - ✓ **Papel:** Se debe considerar el uso, el número de copias deseadas, la impresión y como se archivará.
  - ✓ **Tintas y Carbones:** Complementan el concepto y desarrollo de la imagen.
  - ✓ **De presentación:** Revisar su estructura según la funcionalidad y expresión.

- **Responsables de su manejo y control:**
  - ✓ **En forma especializada:**

A nivel directivo, conocen las formas ya que ellos aprueban cualquier cambio que se realice dentro de la empresa.

Las unidades de apoyo técnico son las áreas especializadas para el análisis, diseño y control de formas ya que poseen conocimientos técnicos.

Las unidades de administración de recursos son los responsables de manejar la papelería, reimpresión y almacenamiento de formas. Además, restituir formas en las áreas que lo necesiten.

- ✓ **Instrumentos de control:**

  Cuestionario para el análisis de formas para analizar y evaluar la funcionalidad de las formas.

  Catálogo de formas, que es un compendio con todas las formas que se utilizan en la organización.

  Tarjeta para el control interno de formas, que es un registro de las impresiones y reimpresiones de formas.

  Unidades de almacenamiento, son dispositivos en los que se puede preservar el inventario de todas las formas, permite la recuperación de estas en el caso de alguna pérdida.

Digital

Los archivos electrónicos es clave en la búsqueda del éxito de las empresas en la actualidad, debido a que:

- Reduce costos
- Mejora los tiempos de procesamiento
- Aumento de calidad
- Incremento de la productividad
- Acelera el manejo de documentos
- Potencia las inversiones en sistemas

Las herramientas más utilizadas debido a que su uso es sencillo y son estandarizadas a nivel mundial son:

- **Microsoft Excel:** Brinda un interfaz enfocado en el manejo de hojas de cálculo mediante celdas que se organizan en filas y columnas. La funcionalidad de este programa permite construir diversos formatos lo que permite gestionar listas o bases de datos.
- **Acrobat X Pro:** Herramienta para crear formularios, formatos y documentos administrativos. Permite crear formatos con espacios para rellenar con parámetros previamente establecidos.

Además, existen programas para poder generar formatos para la red, pero necesitan un mayor nivel de instrucción y son utilizados por diseñadores gráficos:

- **Adobe Flash:** Se utiliza para generar páginas web, presentaciones y animaciones. Se pueden elaborar formatos para subir a la red.
- **Adobe Dreamweaver:** Se utiliza para generar y administrar páginas web. Se pueden subir formatos y dar los lineamientos necesarios para mantener contacto entre empresa y usuario.
- **Adobe Fireworks:** Se utiliza para diseñar y generar prototipos de interfaces de sitios web, móviles y aplicaciones de forma rápida, así como optimizar gráficos móviles.
- **Opinio:** Aplicación web que permite diseñar formas, alojar un host y acceder a un dominio que puede ser protegido por contraseñas.
- **Lenguaje PHP:** Se utiliza para crear páginas web, pero requiere un programador que conozca el lenguaje y se debe contratar un servidor.
- **Question Writer:** Software que contiene plantillas personalizables para diseñar formas.
- **Google Docs:** Herramienta diseñada por Google para elaborar documentos con alojamiento en su propio Hosting.
- **Jot Form:** Aplicación web que permite diseñar y alojar formas para su aplicación posterior.

Metodología para analizar, diseñar y controlar

I. Determinar factibilidad del estudio

Indagar en base al contexto de aplicación que afecta el cual puede ser proceso o procedimiento para lo cual se establecen

características como el número de áreas que las utiliza, las operaciones y las formas que se usan. De igual manera, reconocer si él se cuenta con una persona preparada para la investigación, análisis, diseño y control (Franklin, 2014).

II. Investigación

a. Recopilación de las formas que se usan, de preferencia dos ejemplares, a considerar las usada con mayor frecuencia y relevantes.

b. Clasificación de las formas según los siguientes criterios:

Figura 14. Clasificación de las formas

Fuente. Elaboración propia

1.1.3. Marco normativo

1.1.3.1. ISO/IEC 27000:2018

Titulada "Tecnología de la Información. Técnicas de seguridad. Visión general y vocabularios" esta norma tiene como intención proveer una perspectiva general de un sistema de gestión de seguridad de la información y los términos relacionados utilizados.

1.1.3.2. NTP-ISO/IEC 27001:2014

Titulada "Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisitos" esta norma establece y especifica lo requerido para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI, lo cual permite a una organización certificarse internacionalmente en ISO/IEC 27001.

1.1.3.3. NTP-ISO/IEC 27002:2016

Titulada "Tecnología de la Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información" esta norma tiene como interés proporcionar los lineamientos para la selección, implementación y gestión de controles los cuales pueden ser tomados como guía para la gestión de la seguridad de la información y para el desarrollo de directrices.

1.1.3.4. NTP-ISO/IEC 27003:2012

Titulada "Tecnología de la Información. Técnicas de seguridad. Directrices para la implementación de un sistema de gestión de la

seguridad de la información" proporciona orientación práctica para el plan de implementación y diseño de un sistema de gestión de seguridad de la información; especificando las actividades que se deben realizar, las entradas como punto de partida de cada actividad, la guía para realizar las mismas y los resultados o entregables como salidas al finalizar las actividades. Se tomará como guía para el presente estudio el Anexo A, el cual es un informativo acerca de la lista de verificación de actividades requeridas para establecer e implementar un sistema de gestión de seguridad de la información.

1.1.3.5. ISO/IEC 27004:2016

Titulada "Tecnología de la Información. Técnicas de seguridad. Gestión de la seguridad de la información. Monitoreo, medición, análisis y evaluación" esta norma tiene como propósito apoyar a la organización en la evaluación del funcionamiento y efectividad del sistema de gestión de seguridad de la información con el fin de cumplir los requerimientos del punto 9.1 de la ISO/IEC 27001.

1.1.3.6. ISO/IEC 27005:2011

Titulada "Information technology – Security techniques – Information security risk management" (Tecnología de la Información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información) esta norma tiene como propósito una guía acerca del manejo de la seguridad de la información en una organización.

1.1.3.7. ISO/IEC 27007:2011

Titulada "Informatio Technology – Security Techniques – Guidelines for Information Security Management Systems Auditing" es una guía para realizar la gestión, conducción y competencias de las auditorías de seguridad de la información el cual debe implementarse de acuerdo con la ISO 27001; para ello establece en el anexo A, una Guía Práctica de Auditoría de un Sistema de Seguridad de la Información en la cual se toma nueve criterios a auditar.

1.1.3.8. Ley de protección de datos personales

1.1.3.8.1. Resolución Ministerial

A través de la resolución Ministerial N° 004-2016-PCM se aprobó el uso de la Norma Técnica Peruana ISO 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática, las cuales tendrán un plazo máximo de 2 años para implementarla.

Se debe asignar un comité de gestión de seguridad de la información. Asimismo, la alta dirección de la entidad debe demostrar liderazgo y compromiso con el SGSI, estableciendo una política de seguridad de la información, acciones para tratar los riesgos y oportunidades.

La entidad debe dar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. También, comunicar de manera interna y externa a los colaboradores y usuarios.

La implementación de esta norma incrementará la calidad en los procesos y servicios públicos que brinden las entidades del estado.

1.2. Formulación del problema

¿En qué medida la seguridad de la información influye en la gestión documental de la entidad técnica L & M Seminario Group S.A.C. en el año 2020?

1.3. Objetivos

1.3.1. Objetivo general

Determinar la influencia de la seguridad de la información en la gestión documental de la entidad técnica L & M Seminario Group S.A.C.

1.3.2. Objetivos específicos

- Analizar los requerimientos de seguridad de la información en la organización.
- Diseñar el sistema de seguridad de la información de influencia en la gestión documental.
- Implementar los controles y procedimientos aplicables según la norma técnica peruana de seguridad de la información.
- Demostrar el impacto económico de la seguridad de la información en la gestión documental.

1.4. Hipótesis

1.4.1. Hipótesis general

La seguridad de la información influye significativamente en la gestión documental de la entidad técnica L & M Seminario Group S.A.C. en el año 2020.

CAPÍTULO II. METODOLOGÍA

2.1. Tipo de investigación

Según el propósito: Aplicada

Según el diseño: Pre-experimental, como su nombre lo indica, este diseño es una especie de prueba o ensayo que se realiza antes del experimento verdadero (Arias, p.36).

$$G = O1 \quad X \quad O2$$

Aplicación del pre-test o medición inicial		Aplicación del estímulo o tratamiento	Aplicación del postest o medición final
G	O1	X	O2

Figura 15. Diseño de la investigación

Fuente. Elaboración propia

G: Entidad técnica L & M Seminario Group S.A.C.

O1: Pre test – Gestión Documental antes de la Seguridad de la Información.

X: Seguridad de la Información.

O2: Post test – Gestión Documental después de la Seguridad de la Información.

2.2. Población y muestra

En la presenta investigación la población es equivalente a la muestra, es decir, se tomó como muestra a los 8 colaboradores de la entidad técnica L & M Seminario Group S.A.C. El criterio a elegir la muestra fue por conveniencia. Específicamente, los colaboradores están subdivididos en personal administrativo (4) y operativo (4). El personal administrativo este compuesto por el gerente general, administrador, gestor de proyectos y contador. Por otro lado, el equipo operativo este compuesto por dos (2) ingenieros civiles, un gerente operativo y un residente de obra.

2.3. Técnicas e instrumentos de recolección y análisis de datos

Se ha diseñado una entrevista dirigida al gerente de la entidad técnica L & M Seminario Group S.A.C. para tener pleno conocimiento acerca de los procesos, así como de la información sensible que estos pueden manejar, la entrevista diseñada es a profundidad, de carácter semi estructurada pues a pesar de contar con un cuestionario estructurado de diez preguntas, se realizaran otras más de forma espontánea, de acuerdo a la flexibilidad en la consecución del diálogo. La validez estará dada por la veracidad de las respuestas proporcionadas por el señor Luis Hernando Seminario Narro, gerente general, así como por la confiabilidad del instrumento, las preguntas del cuestionario de la entrevista, validado por expertos en la materia.

La observación se efectuará directamente en la empresa L & M Seminario Group S.A.C., con la aprobación previa del gerente de la empresa, quien permite el reconocimiento de las instalaciones para poder identificar los procesos y gestionarlos. Asimismo, para el proceso operativo se realizó la visita de campo a la zona en donde la construcción de Viviendas de Interés Social está siendo ejecutadas, los cuales son los Centros Poblados de PayPay, La Florida y El Mango. La validez de lo observado se evidenciará con fichas de observación y de registro fotográfico, instrumentos validados por expertos, así como la firma del gerente, para demostrar la fiabilidad de la misma.

A su vez, se aplicó la revisión documental con el fin de examinar la documentación disponible y almacenada del proceso de negocio. Por último, se requirió de la técnica de encuestas, aplicando como instrumento un cuestionario dirigido a los colaboradores de la Entidad Técnica con el propósito de conocer la eficacia del programa de

entrenamiento y concientización en seguridad de la información. La validación de este fue realizada por el especialista Ing. Nelson Ángeles Quiñones. El cuestionario fue de carácter estructurado conformado por ocho preguntas cerradas; en cuanto al análisis de datos este fue descriptivo, a través del uso de Microsoft Excel precisando los resultados obtenidos en el pre y post test. Cabe señalar que los datos obtenidos de dichas encuestas fueron procesados haciendo de uso del software estadístico SPSS.

Tabla 1

Técnicas e Instrumentos de la investigación

Técnica	Justificación	Instrumentos	Materiales	Objeto / Sujeto de Aplicación
Observación	• Observar el entorno organizacional, asentar las actividades realizada por los colaboradores en oficina. Se centra en permitir corroborar la realidad problemática de la investigación.	• Ficha de Observación • Ficha de Registro Fotográfico	• Lapicero • Papel Bond A4 • Cámara fotográfica	• Actividades de la organización. • Los 8 colaboradores de la organización.
Entrevista	• La entrevista es el medio por el cual se le otorga a la alta dirección poner en manifiesto su percepción	• Cuestionario semi estructurado	• Grabadora de Voz • Lapicero	• Alta dirección

	respecto a la seguridad de la información.		• Papel Bond A4	
Revisión documental	• Comprobar la documentación existente y almacenada tanto en medios físicos como virtual de todas las actividades realizadas en el proceso de gestión documental.	• Ficha de Registro de Datos	• Activos físicos de la organización • Datos • Documentos Internos • Laptop	• Actividades del proceso de gestión documental
Encuesta	• Determinar si el programa de entrenamiento y concientización tuvo resultados positivos. Se aplicaron dos cuestionarios diferentes con 8 preguntas cerradas; uno precedente y otro posterior a la ejecución del programa.	• Cuestionario con preguntas cerradas	• Laptop	• A los 8 colaboradores de la organización especificados en la muestra.

Fuente. Elaboración propia

2.4. Procedimiento

Se realizaron las actividades propuestas teniendo como puntos de referencia las metodologías propuestas como la lista de verificación del anexo A de la NTP-ISO/IEC 27003 y la NTP-ISO/IEC 27001. En base a ellas, se plantean las siguientes actividades respectivamente agrupadas en fases de la siguiente manera:

Planificar

- Contexto de la organización: objetivos, necesidades, requerimientos y normas reglamentarias vinculadas con la seguridad de la información. Para ello, en primer lugar, se utilizó la técnica de entrevista al gerente general de la Entidad Técnica, para su desarrollo se hizo uso del instrumento de un cuestionario semi estructurado. Asimismo, la técnica de observación permitió conocer el estado actual, lo observado se documentó tanto en fichas de registro fotográfico como en las fichas de observación. Por último, para análisis del contexto se realizó la revisión documental para la cual se empleó un checklist y ficha de observación.
- Alcance preliminar, estableciendo limites organizacionales, físicos y de TI.
- Liderazgo y compromiso de la dirección de iniciar proyecto de SGSI con la política de seguridad.
- Política rectora y roles y responsabilidades del SGSI.
- Definición y aplicación de la valoración y tratamiento de riesgos.

Hacer

- Identificar activos del alcance del Sistema de Gestión de Seguridad de la Información.
- Evaluar riesgos de seguridad de la información.

- Tratamiento de riesgos de seguridad de la información.
- Comunicación.
- Programa de entrenamiento y concientización. Como parte del programa, se evaluaron los conocimientos de los colaboradores, tanto previos como posteriores al programa de entrenamiento y concientización en seguridad de la información.
- Preparar declaración de aplicabilidad

Verificar

- Evaluar el desempeño mediante monitoreo, medición y análisis.
- Propuesta de plan de auditoría para el sistema de seguridad de la información.
- Revisión por la gerencia.

Actuar

- Propuesta de mejora continua del sistema de seguridad de la información.

Figura 16. Procedimiento de Implementación de la Seguridad de la Información

Fuente: Elaboración propia

Matriz de Operacionalización de la Variable Independiente

Tabla 2

Matriz de Operacionalización de la Variable Independiente

TÍTULO	VARIABLE	DIMENSIONES	CATEGORÍA	INDICADOR	FÓRMULA	LEYENDA	INSTRUMENTO	VALOR OPTIMO	VALOR ACEPTABLE
Seguridad de la información en la gestión documental de la entidad técnica L&M Seminario Group S.A.C	Seguridad de la información	**Estratégico**	**Administración de riesgos**	Identificación de activos	$I_a = \frac{A_e}{A_i}$	Ia= Identificación de activos Ae= Activos etiquetados Ai= Activos inventariados	Ficha de Observación	1	0.8
				Aplicación de controles	$C_e = \frac{C1_e}{C_t}$	Ce= Controles ejecutados C1e= Nro de controles implementados Ct= Nro total de controles planificados	Matriz Declaración de Aplicabilidad de Controles	1	0.8
			Cumplimiento	Revisión de regulaciones nacionales	$R_r = \frac{R_e}{R_p}$	Rr= Revisión de regulaciones nacionales Re=Nro de revisiones ejecutadas Rp= Nro total de revisiones programadas	Checklist	1	0.7
			Objetivos de negocio	Significado de seguridad en presupuesto de negocio	$R_s = \frac{D_p}{T_p}$	Rs = Representación de la seguridad en el presupuesto del negocio Dp = Designación de presupuesto para la seguridad de la información Tp= Total de presupuesto para implementación	Revisión Documental	0.5	0.3
		Táctico	**Perímetro**	Licencias del antivirus	$L_a = \frac{O_{la}}{O_{la}+O_{lc}}$	La = Licencias del antivirus Olc= Ordenadores con licencia caducada Ola = Ordenadores con licencia activa	Ficha de Observación	0	0

		Servicios	Corrección de errores en backups	$C_e = \frac{O_s}{O_s+O_f}$	Ce = Corrección de errores en backups Os= Número de ordenadores examinados sin fallas Of= Número de ordenadores examinados con fallas	Ficha de Observación	1	0.8
	Operativo	**Confidencialidad**	Educación en seguridad de la información	$E = \frac{P1_a}{P1_a+P2_d}$	E = Educación en seguridad de la información P1a= Nro de colaboradores que aprobaron el examen luego de atender a las capacitaciones P2d = Nro de colaboradores que desaprobaron el examen luego de atender a las capacitaciones	Cuestionario con preguntas cerradas	1	0.75
			Autenticación	$Au = \frac{U_{ci}}{U_{ci}+U_{si}}$	Au = Autenticación Uci = *Número de usuarios con ID únicos* Usi = Número de usuarios sin ID	Ficha de Observación	1	0.875
		Integridad	Protección de los ordenadores	$PO = \frac{O_e}{O_t}$	PO= Protección de los ordenadores Oe= Número de ordenadores con capacidad de encriptación Ot = Número total de ordenadores	Ficha de Observación	5	5
		Disponibilidad	Disponibilidad de contacto con autoridades y grupos de interés	$D_c = D_{ca} + D_{cg}$	Dc= Disponibilidad de contacto Dca= Numero de contactos con autoridades establecidos Dcg= Número de contactos con grupos de interés establecidos	Checklist	5	4.00

Fuente. Elaboración propia

Matriz de Operacionalización de la Variable Dependiente

Tabla 3

Matriz de Operacionalización de la Variable Dependiente

TITULO	VARIABLE	DIMENSIONES	INDICADORES	FÓRMULA	LEYENDA	INSTRUMENTO	VALOR OPTIMO	VALOR ACEPTABLE
Implementación de la seguridad de la información en la gestión documental de la entidad técnica L&M Seminario Group S.A.C	Gestión Documental	Enfoque clásico	Eficiencia	$E = \frac{F_u}{F_p}$	E = Eficiencia Fu= Nro de formas utilizadas Fp= Nro de formas programadas	Checklist	1	0.83
			Protección de activos físicos	$PA_f = \frac{AR_{if}}{A_{if}}$	PAf= Protección de activos físicos ARif = Número de accesos restringidos a instalaciones físicas que contienen información sensibles. Aif = Número total de accesos a instalaciones físicas que contienen información sensibles.	Ficha de Registro Fotográfico	1	0.83
		Enfoque Digital	Planes de actualización y seguimiento	$Pl_s = \frac{Pl_e}{Pl_p}$	Pls= Planes de actualización y seguimiento Ple=Nro de planes ejecutados Plp=Nro total de planes programados	Revisión Dociumental	1	0.7
			Pruebas de vulnerabilidad de aplicaciones	$P_v = \frac{A_{ni}}{A_t}$	Pv = Prueba de vulnerabilidades de software Ani = Número de aplicaciones no infectadas Sa = Número total de aplicaciones analizadas	Ficha de Observación	1	0.80

Copias de respaldo	$C_r = C_{ra}$	Cr= Copias de respaldo Cra= Número de copias de respaldo realizadas anualmente	Revisión Documental	12	4
Grado de protección de los sistemas de información de sujetos no autorizados.	$G_s = S_a - \overline{P}_{sa}$	Gs = Protección de los sistemas de información de sujetos no autorizados. Sa= Softwares Analizados Psa= Número total de persona no autorizada que accede a los sistemas de información.	Ficha de Observación	7	6
Accesibilidad a la documentación de hardware/software	$A = \frac{A_d}{A_i}$	A = Accesibilidad a la documentación de hardware y software Ad = Numero de aplicaciones con documentación archivada Adi = Numero de aplicaciones inventariadas	Ficha de Observación	1	0.77
Capacitación	$C = \frac{C_c}{C_g}$	C= Capacitación del personal. Cc= Número de colaboradores capacitados en seguridad en gestión documental. Cg= Número de colaboradores dedicados a gestión documental.	Cuestionario	1	0.5

Fuente. Elaboración propia

2.5. Aspectos Éticos

La investigación se desarrolló siguiendo los lineamientos éticos de las regulaciones peruanas relevantes y lo establecido en la norma técninca NTP-ISO/IEC 27001 con el fin de proteger la confiabilidad e integridad de los datos e información de la Entidad Técnica L&M Seminario Group S.A.C.

Asimismo, alineados a ley N 29733 de 2011 de protección de datos personales, se desarrolló conforme a los siguientes principios:

- Manifestar detalladamente las garantías de seguridad que se le otorga a los participantes en las entrevistas aplicadas.

- Obtener el consentimiento informado de los involucrados en el muestreo.

- Garantizar a los involucrados en la investigación que la información recolectada será usada solo para los fines autorizados.

- Los datos e información recolectadas en la investigación no será transferida a terceros sin autorización previa.

- Se realizó una evaluación anti plagio con el fin de asegurar la originalidad de la investigación.

CAPÍTULO III. RESULTADOS

Según lo descrito en procedimientos, se obtuvo como resultado lo siguiente:

Se realizó una entrevista (ver anexo 02) al gerente general de L & M Seminario Group S.A.C. en la cual se identificó, según lo manifestado por el mismo, los procesos de la empresa los cuales fueron graficados en un mapa de procesos de la siguiente manera:

Figura 17. Mapa de Procesos de la entidad técnica L & M Seminario Group S.A.C.

Fuente. Elaboración propia

De igual manera, se logró identificar y describir cada proceso de negocio de la organización:

Tabla 4

Descripción de los procesos del negocio

ID	Procesos de negocio	Descripción
P01	Planificación Estratégica	Establecimiento de proyectos a mediano plazo.
P02	Gestión de Proyectos	Organización y desarrollo de los proyectos constructivos.
P03	Investigación y Desarrollo	Identificación y búsqueda de poblaciones prospecto para calificar como beneficiario del programa Techo Propio.
P04	Gestión Documental	Organización y trámite de los documentos solicitados principalmente por el Fondo MiVivienda.
P05	Gestión de Compras	Abastecimiento correcto de los materiales requeridos para obra y oficina.
P06	Ejecución de Obras	Construcción de Viviendas de Interés Social acorde a los estándares del Fondo MiVivienda.
P07	Control	Seguimiento y supervisión de los procesos administrativos y operativos de la empresa.
P08	Gestión Jurídica	Contratos con beneficiarios y personal de obra.
P09	Gestión de Recursos Humanos	Desarrollo de planilla y actividades relacionados con el ambiente laboral.
P10	Contabilidad	Declaración mensual de impuestos y balances.

Fuente. Elaboración propia

Asimismo, se expuso el significado e importancia de un sistema de gestión de seguridad de la información para la empresa, ante esto se realizó una matriz de selección de procesos en la cual se valoran tomando los criterios definidos como críticos por el gerente.

Tabla 5

Evaluación de criterios para obtener los procesos críticos del negocio

	CRITERIOS					
Procesos	C01	C03	C03	C04	C05	Puntuación
P01	4	4	3	3	3	3
P02	3	4	3	3	3	3
P03	4	4	2	3	3	3
P04	4	5	5	4	5	5
P05	4	4	4	4	4	4
P06	5	5	5	5	4	5
P07	4	4	3	3	4	4
P08	3	3	3	3	3	3
P09	3	4	3	3	3	3
P10	5	3	3	3	3	3

Fuente. Elaboración propia

En donde:

Tabla 6

Grado de impacto en el proceso por criterio a evaluar

Puntuación	Grado de Impacto en el proceso
1	Muy bajo
2	Bajo
3	Moderado
4	Alto
5	Muy alto

Fuente. Elaboración propia

Tabla 7

Criterios a evaluar

ID	Criterio
C01	Costos
C02	Calidad
C03	Tiempo de Entrega
C04	Satisfacción del cliente
C05	Seguridad

Fuente. Elaboración propia

De esta manera se obtuvo que los procesos críticos son el de gestión documental y ejecución de obra:

Descripción de los procesos seleccionados de la organización

Gestión documental

En la gestión documental se realiza todos los procedimientos de trámites documentarios establecidos por el Ministerio de Vivienda con el fin de obtener los permisos, códigos de proyecto y licencias necesarias para la construcción de viviendas de interés social (Ver anexo 03)

Ejecución de obras

Consiste en todas las actividades llevadas a cabo para realizar los módulos de Vivienda de Interés Social en el tiempo pactado y siguiendo los estándares mínimos de construcción dispuestos por el Fondo MiVivieinda (Ver anexo 04,05).

Sin embargo, para la presente investigación se tomó como alcance solo un proceso: la gestión documental.

Es así como se llegó a la primera fase del proyecto:

1. **Planificar**

Contexto de la organización: objetivos, necesidades, requerimientos y normas reglamentarias vinculadas con la seguridad de la información.

La empresa L & M Seminario Group S.A.C. está ubicada en la Mz. A Lote. 12 C.V. Urbanización El Paraíso, distrito de Moche, en la ciudad de Trujillo, La Libertad. La misma que está identificada bajo el número RUC 20601200091 y cuya actividad

económica principal es la Construcción de Edificios bajo la Clasificación Industrial Internacional Uniforme (CIIU) 4100. Actualmente, el gerente general de la organización y representante legal.

La empresa está registrada como Entidad Técnica del Fondo Mivivienda y al presente se centra en la modalidad de Construcción en Sitio Propio.

Visión

"Ser la Entidad Técnica con mayor cobertura en el programa Techo Propio reconocida por la calidad de Viviendas de Interés Social en el norte del Perú"

Misión

"Somos una empresa orientada a brindar servicios sociales bajo el programa Techo Propio realizando Vivivendas de Interés Social a familias peruanas y así contribuir con el déficit habitacional en el Perú"

Objetivos

- Contribuir a disminuir el deficit habitacional en el Perú.
- Consolidar la marca L & M Seminario Group S.A.C. como representante en el mercado actual de Construccion en Sitio Propio.
- Generar un impacto positivo en el entorno al ejecutar los proyectos sociales.
- Promover la mejora de la calidad de los materiales y mano de obra en la construcción de Viviendas de interés social.

Se identificó el modelo de negocio de la empresa de la siguiente manera:

Figura 18. Canvas del modelo de negocio

Fuente. Elaboración propia

Por otro lado, se determinó las siguientes partes interesadas relevantes al sistema de gestión de seguridad de la información:

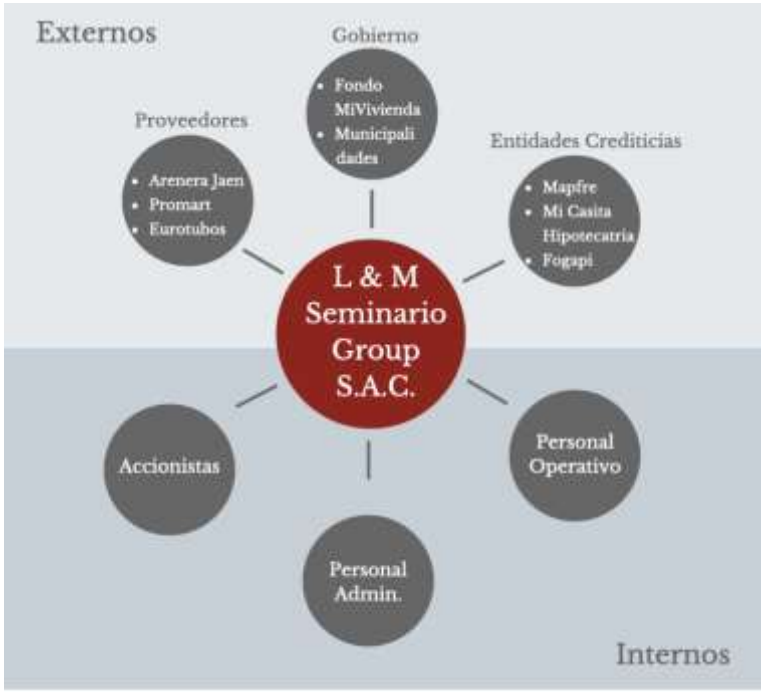


Figura 19. Stakeholders internos y externos

Fuente. Elaboración propia

De igual manera, con el fin de determinar el contexto externo con respecto a seguridad de la información, se realizó el siguiente análisis de los siguientes aspectos:

Tabla 8

Factores políticos, económicos, sociales, tecnologicos, ecologicos y legales de la entidad técnica L & M Seminario Group S.A.C.

Político	Económico
La oficina nacional de gobierno electrónico e informática (ONEIG) de Perú creó un manual de gestión de riesgos que se encuentra disponible en la página web del PCM. Existe una política nacional de ciberseguridad para todas las entidades de administración pública.	El crecimiento de inversión en ciberseguridad en el 2018 fue del 18% en las empresas peruanas. La inversión en seguridad de la información de los consumidores y clientes es del 0.07% del PBI. Se pierden 4 mil millones de dólares anualmente por delitos ante la seguridad de la información en Perú.

Social	Tecnológico
El 30 de noviembre se celebra en Perú el Día Internacional de la Seguridad Informática. Los ciberataques que más afectan a los usuarios y empresas peruanas son el ransomware, phishing y criptojacking. Los usuarios denuncian al menos 120 casos mensuales de ataques de ciberseguridad en Perú. Según el INEI, 19.5% de empresas peruanas declararon contar con áreas de soporte informático. Perú se encuentra en el puesto 58 del ranking de la National Cyber Security Index	Charlas sobre vulnerabilidades a las que se exponen los activos de información. Existen **maestrías** en dirección de tecnologías de la información. El consejo nacional de ciencia, tecnología e Innovación Tecnológica (CONCYTEC) se encarga de regular el soporte de las tecnologías en plataformas unificadas. Portal de Transparencia Estándar del Fondo MIVIVIENDA S.A. para la administración de información pública creado por Resolución de Gerencia General N° 094-2018-FMV/GG.
Ecológico	**Legal**
Plan de Ecoeficiencia MEF 2019 – 2021: Oportunidades de mejora en el uso eficiente del papel. Este plan promueve el uso de papel reciclado, reciclaje y escaneado de documentos para evitar el fotocopiado de documentos. Plan de Ecoeficiencia Senasa para el ahorro de papel, como el uso de ambas caras de papel, incidencia en el uso de correos electrónicos y uso del escáner. Guía de Ecoeficiencia para las Instituciones del Sector Público – Ministerio del Ambiente del Perú (MINAM)	Mediante el decreto supremo N° 050-2018-PCM aprueban la definición de seguridad de la información en el ámbito nacional Ley N° 29733 – Protección de datos personales del Perú, Decreto Supremo 019 – 2017 – JUS en cumplimiento con la ley N~29733 el cual pone a disposición del público en general la solicitud de los derechos ARCO, Resolución Ministerial N° 664- 2018 – Política General de Seguridad de la información en el Ministerio de Educación. Proyecto de Ley N~ 4029/2018 Ley que Promueve la Implementación Progresiva del Cero Papel en la Administración Pública. Decreto Legislativo 1412 – Decreto Legislativo que aprueba la Ley de Gobierno Digital.

	Ley N~27489 que regula las centrales privadas de información de riesgos y protección al titular de la información. Ley N~27806 de Transparencia y Acceso a la Información Pública. Ley N~27829 Ley que crea el Bono Familiar Habitacional y su reglamento

Fuente. Elaboración propia

A su vez, se identificó los siguientes aspectos internos relevantes a la seguridad de la información:

Tabla 9

Factores políticos, económicos, sociales, tecnológicos, ecológicos y legales de la entidad técnica L & M Seminario Group S.A.C.

	FORTALEZAS - El programa Techo Propio con el que trabaja la empresa está bajo el amparo de los derechos ARCO del Ministerio de Justicia.	**DEBILIDADES** - Alta rotación del personal operativo. - Desorganización de los expedientes en físico. - Falta de seguridad física de la oficina administrativa. - Fallas en el sistema integral Zona Segura. - No existe un responsable por cada activo.
OPORTUNIDADES - Contratos de no divulgación. - Orientación hacia la gestión de seguridad de la información. - Confianza de los beneficiarios con respecto a	ESTRATEGIAS FO - Capacitación del personal de la organización en el manejo del sistema integral. - Realizar un contrato de no divulgación con cada empleado.	ESTRATEGIAS DO - Capacitación al personal acerca de los riesgos de seguridad de la información.

la integridad del programa del Fondo Mivivienda.	- Proteger los documentos digitales importantes con una contraseña.	
AMENAZAS - Filtración de la información de los beneficiarios. - Filtración de los planos arquitectónicos. - Delincuencia en la zona de la oficina.	ESTRATEGIAS FA - Cifrar los planos para evitar robos o extracciones.	ESTRATEGIAS DA - Garantizar la seguridad física de la oficina mediante el uso de alarmas y/o cámaras de vigilancia.

Fuente. Elaboración propia

3.1. Funciones de la organización

Estructura divisional de la organización

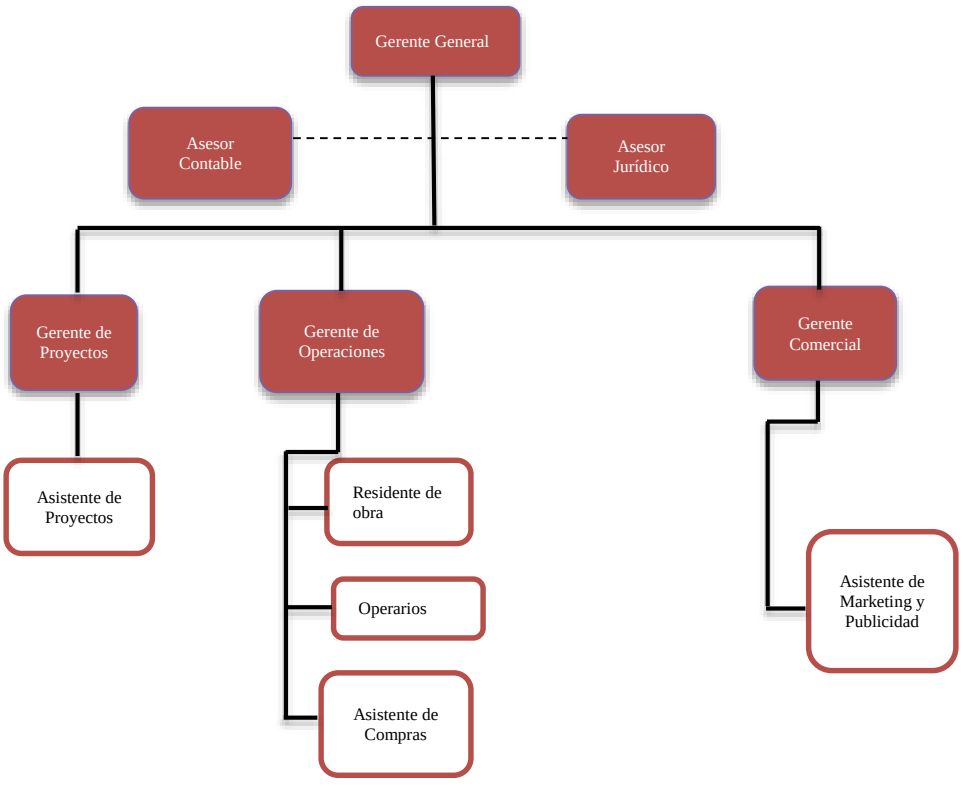


Figura 20. Estructura divisional de la organización

Fuente. Elaboración propia

a. Gerencia General.- El gerente compone este departamento y a su vez es responsable de los demás departamentos.

b. Gerencia de proyectos.- Un responsable es encargo de gestionar las actividades estratégicas de investigación y de la coordinación documental y control de las actividades de los proyectos en curso, cuenta con un practicante pre profesional para asistir sus funciones.

c. Gerencia de Operaciones.- Compuesto por la gerencia, dos residentes de obra, operarios en los que se incluye maestros de obra y albañiles, asi como un asistente de compras para las tareas logísticas en cuanto a la compra y distribución de materiales.

d. Gerencia Comercial.- Un director es el encargado de gestionar las actividades estratégicas concernientes al marketing y las ventas de la empresa, tiene a su cargo un jefe de ventas y un asistente de marketing y publicidad.

Objetivos de seguridad de** la **información de L & M Seminario Group. S.A.C.

El objetivo de L & M Seminario Group S.A.C., es que todos los tramite documentario se realicen y estén registrados para que la Entidad Técnica, pueda tener la información disponible que impactará principalmente en el proceso comercial, logístico, producción, de recursos humanos y financiero.

Necesidades L & M Seminario Group S.A.C.

Por otro lado, L & M Seminario Group S.A.C. tiene la necesidad de evaluar la seguridad de la información no solo de los documentos virtuales, sino también la circulante en físico dentro de la empresa, como las ideas o imágenes; es decir todos los activos de la información que participen en los procesos del negocio y que sean

objeto de amenazas. Para ello es necesaria la identificación de los riesgos y el tratamiento de estos a través de controles.

Requerimientos L & M Seminario Group S.A.C.

Se analizó los requerimientos de la organización referentes a confidencialidad, disponibilidad e integridad,

Tabla 10

Requerimiento de disponibilidad, confidencialidad e integridad de la entidad técnica L & M Seminario Group S.A.C.

Principios	**Requerimientos de la organización**
Confidencialidad	Se requiere inducir una cultura organizacional enfocada en resguardar la confidencialidad de la información manejada por la organización.
Disponibilidad	Se requiere disponibilidad de una manual de buenas prácticas de seguridad de la información de manera que los lineamientos se encuentren establecidos ante cualquier atentado contra la seguridad de la información.
Integridad	Se requiere capacitar al personal en cuanto al manejo de la información y de los datos para proteger la integridad de estos y que estos no sean modificados por terceros.

Fuente. Elaboración propia

Normas reglamentarias vinculadas con la seguridad de la información.

Para empezar, la constitución política del Perú contempla en el artículo 2, numeral 6 el derecho a la intimidad personal y familiar de la información manejada por los servicios informáticos, computarizados o no y públicos o privados. al buen nombre y a la obligación del estado de respetarlos como hacerlos respetar.

Por otro lado, la Ley N~ 29733 "Ley de Protección de Datos Personales" establece que se debe garantizar derechos de proteger lo descrito en el numeral 6 de la

constitución; y a su vez en el artículo N~9 titulado Principio de Seguridad, establece lo siguiente:

"El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales."

En este artículo se señala también que las medidas adoptadas para la seguridad tienen que caracterizarse por ser las idóneas y oportunas con respecto a estar alineadas al tratamiento y categoría con la que se califique los datos personales.

Esto significa que cada uno debe conocer la finalidad de la recopilación de sus datos personales, a quién será transferido y cómo ejercer los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) ante el tratamiento de los mismos. En la Guía practica para la observancia del "deber de informar" (Ministerio de Justicia y Derechos Humanos, 2019) afirma que "…toda información sobre las condiciones del tratamiento de los datos personales debe ser fácilmente identificable y accesible, lo que exige emplear un lenguaje sencillo…".

De esta manera, los derechos ARCO también son acatados por el Fondo Mivivienda, en cumplimiento a la ley N~29733 modificada por el DS 019 – 2017 – JUS el cual pone a disposición del público en general la solicitud de los derechos ARCO (Ver anexo 2) para el ejercicio de los mismos. A continuación, se especifica dichos derechos:

- Acceso a la obtención de información recopilada por los bancos de datos administrados por fuentes públicas o privadas.

- Rectificación es el derecho del propietario de datos personales de modificar los datos que sean inexactos, falsos o incompletos.
- Cancelación de los datos personales que haya vencido el plazo para su tratamiento, la revocación de consentimiento para el tratamiento y en cualquier otro caso que no haya sido tratado de acuerdo a la ley.
- Oposición, por algún motivo fundado y legítimo, de no aparecer en el banco de datos o el tratamiento de los mismo, siempre y cuando la ley no disponga lo contrario.

Asimismo, existe la ley N~27489 que regula las centrales privadas de información de riesgos y protección al titular de la información a la cual se debe regir la Entidad del Sistema Financiero con la que L & M Seminario Group opera para la emisión de cartas de acreditación, carta fianza bancaria de seriedad de oferta y carta fianza de fiel cumplimiento requeridas a la vez por el Fondo Mivivenda. Esta ley indica que las centrales privadas de información de riesgos están obligadas a brindar acceso a la información del titular de los datos una vez al año o cunado la información haya sido rectificada siempre y cuando se demuestre la identidad del solicitante.

Para finalizar, existe la ley N~27806 de Transparencia y Acceso a la Información Pública cuyo fin es la promoción de la transparencia en las acciones del Estado y así también respetar el numeral 5 del artículo segundo de la Constitución Política del Perú garantizando así la promoción de la transparencia en las actuaciones de las entidades de Administración Pública. Asimismo, señala que de no cumplirse se sancionará como una falta grave e incluso podrá denunciarse por Abuso de Autoridad según el artículo 377 del Código Penal. Según esta ley, recalca en el artículo 15 que

solo en caso de seguridad nacional la información calificada como secreta no podrá ser relevada.

Tabla 11

Normas reglamentarias vinculadas a la seguridad de la información

Normas reglamentarias Vinculadas a la Seguridad de la Información	Aplica a la organización	
	Si	No
Constitución Política del Perú, articulo 2 numeral 6. Toda persona tiene derecho: "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."	x	
LEY N~ 29733. "Ley de Protección de Datos Personales"*: " Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, perdida, tratamiento o acceso no autorizado."*	x	
LEY N~*29733 MODIFICADA POR EL DS 019 – 2017 – JUS. : Por la cual se pone a disposición del público en general la solicitud de los derechos ARCO.*	x	
LEY N~27489, Por la cual se regula las centrales privadas de información de riesgos y protección al titular de la información	x	
LEY N~27806 DE TRANSPARENCIA Y ACCESO A LA INFROMACIÓN PÚBLICA. Por la cual se promueve la transparencia en las acciones del Estado,	x	

Fuente. Elaboración propia

3.2. Alcance preliminar, estableciendo limites organizacionales, físicos y de TI.

Descripción de alcance preliminar del SGSI

L & M Seminario Group S.A.C., considerando los aspectos tanto internos como externos y los involucrados, ha definido el alcance del SGSI en: "Gestión de la seguridad de la información en los procesos de gestión documental y compras

siguiendo las normas internas según la ley y mediante la determinación de responsables del comité de seguridad. Así como, la protección de datos y la copia de seguridad de los mismos".

Limites organizacionales

Se tomó como límite la elaboración del Sistema de Gestión de Seguridad de la Información para los principales procesos críticos, los cuales son el de ejecución y gestión documental, tomando el intercambio de información de los colaboradores y activos dentro de los límites físicos establecidos.

Límites de las tecnologías de la información y las comunicaciones

Se consideró como límite a todas las TIC's utilizadas en los procesos gestión documental y compras de la empresa L & M Seminario Group S.A.C. en los que se almacenan y procesan información, teniendo como principal el sistema integral Zona Segura.

Límites físicos para el sistema de gestión de seguridad de la información.

Se limita el espacio de la oficina de la empresa ubicada en la ciudad de Trujillo, dirección Mz. X3 lote 5ª Urbanización Vista Hermosa.

Liderazgo y compromiso de la dirección de iniciar proyecto SGSI.

Según lo estipulada en la NTP ISO/IEC es de vital importancia obtener el compromiso documentado de la dirección (Ver anexo 06), para lo cual se realizó la siguiente acta de iniciación del plan de proyecto:

Tabla 12

Plan de proyecto presentado al gerente de la entidad técnica L & M Seminario Group S.A.C.

Componente	*Descripción*
Título del Proyecto	Proyecto de implantación de un SGSI en la empresa "L & M Seminario Group S.A.C." de la ciudad de Trujillo en el año 2019.
Director del Proyecto	Director del proyecto
Patrocinador del Proyecto	Luis Hernando Seminario Narro, gerente general de la empresa "L & M Seminario Group S.A.C."
Descripción del Proyecto	El presente proyecto se propone elaborar la implantación de un Sistema de Gestión de Seguridad de la Información para la empresa L & M Seminario Group S.A.C. con el fin de preservar la confidencialidad, integridad y disponibilidad de la información; Para la ejecución del proyecto se ha dividido en cuatro (4) fases, las cuales son: PLANIFICAR, HACER, VERIFICAR Y ACTUAR. En la primera fase se definirá el alcance o scoope del proyecto identificando los límites que tendrá el sistema de gestión de seguridad de la información. Así mismo se definirá la política rectora del SGSI, así como las políticas específicas. En la segunda fase se identificarán los requisitos de la seguridad de la información haciendo uso de las herramientas FODA y PESTEL para determinar los aspectos internos y externos relevantes para la organización, tomando en cuenta las partes interesadas. De igual manera, se realizará un listado de los activos de la información de los dos procesos definidos en el alcance. Finalmente se pondrán los resultados de la evaluación de la Seguridad de la información identificando los activos que contienen información sensible. En la tercera etapa se realizará la evaluación del riesgo comenzando con una nota escrita aprobada por la dirección para realizar la implantación del SGSI. Posteriormente, se realizará el plan de tratamiento de riesgos donde se realizará la valoración de los riesgos y se determinarán los controles que serán necesarios para el tratamiento de riesgos. Para finalizar, se redactará una declaración de aplicabilidad la cual debe contener los controles necesarios y el porqué de las inclusiones teniendo en cuenta los objetivos de control y los controles seleccionados. En la cuarta etapa se realizará el diseño del SGSI realizando el plan final de implementación del proyecto en la empresa. Finalmente se realiza la firma del acta y el cierre, para entregar el proyecto al patrocinador.
Justificación del Proyecto	Actualmente la empresa como proveedor de un servicio del Estado, deberá regirse a las leyes aprobadas con respecto a la ley de proteccion de datos personales y al modelo de Gestión de Seguridad de la Información y cumplimiento de los derechos

	ARCO; para estar alineado a ello, el presente proyecto propone una metodología que permite establecer un diseño de SGSI para la empresa L & M Seminario Group S.A.C.
Objetivos del proyecto y criterios de medición del éxito	Elaborar el diseño del SGSI para la empresa L & M Seminaario Group S.A.C. **Objetivos específicos:** • Realizar un (01) informe del alcance y políticas del SGSI. • Realizar un (01) informe del análisis interno y externo de la actual estructura organizacional. • Elaborar un (01) un informe de los activos de la información de los procesos de logística y comercial de la empresa L & M Seminario Group S.A.C. • Realizar un (01) informe de riesgos. • Realizar un (01) plan final de SGSI. • Elaborar un (01) NDA.
Requisitos de Alto Nivel del Proyecto	• Acceso a la información relevante de la empresa L & M Seminario Group S.A.C. • Disponibilidad de presupuesto • Disponibilidad de tiempo de los interesados del proyecto. • Compromiso con el patrocinador del proyecto
Riesgos de Alto Nivel	• Divulgación de la información. • Rechazo del patrocinador a la elaboración del diseño del SGSI. • Aumento de costos del proyecto. • Limitación del tiempo de los interesados del proyecto. • Retrasos de actividades de acuerdo al cronograma, debido a la falta de participación y compromiso del equipo de proyecto.
Criterios de aceptación del proyecto	• El plazo para la ejecución del no debe exceder los 3meses calendarios, contados a partir de la firma del acta de constitución del proyecto hasta la firma del acta de cierre del proyecto. • Cumplir con la satisfacción de los interesados. • El producto del proyecto debe entregarse dentro del plazo de tiempo y de acuerdo al alcance definido inicialmente.
Principales Interesados	• Director del proyecto • Patrocinador del proyecto: Luis Hernando Seminario Narro (Representante legal y gerente general de la empresa)

Fuente. Elaboración propia

De igual manera, se presentó un cronograma de plan de proyecto estipulando las actividades realizadas en cada fase de la metodología propuesta:

Tabla 13

Cronograma del proyecto en la seguridad de la información en la gestión documental

ACTIVIDADES POR FASES	INICIO	FIN	DURACIÓN	CICLO DE MEJORA CONTINUA
				PLANEAR / HACER / VERIFICAR / ACTUAR
				MES 1 / MES 2 / MES 3 / MES 4 / MES 5 / MES 6
				28/10 - 01/11 · 04/11 - 08/11 · 11/11 - 15/11 · 18/11 - 22/11 · 25/11 - 29/11 · 02/12 - 06/12 · 09/12 - 13/12 · 16/12 - 20/12 · 23/12- 27/12 · 30/12 - 03/01 · 06/01 -10/01 · 13/01 - 17/01 · 20/01 - 24/01 · 27/01 - 31/01 · 03/02 - 07/02 · 10/02 - 14/02 · 17/02 - 21/02 · 24/02 - 28/02 · 02/03 - 06/03 · 09/03 - 13/03 · 16/03 - 20/03 · 23/03 - 27/03 · 30/03 - 03/04 · 06/04 - 10/04 · 13/04 - 17/04 · 20/04 - 24/04 · 27/04 - 01/05
FASES DE PLANEAR	28/10/19	1/05/20	119 días	
1. CONTEXTO DE LA ORGANIZACION, OBJETIVOS, NECESIDADES, REQUERIMIENTO Y NORMAS REGLAMENTARIAS VINCULADAS CON LA SEGURIDAD DE LA INFORMACIÓN.	28/10/19	8/11/10	10 días	
1.1.REALIZAR INVESTIGACIÓN ACERCA DE LA DE REALIDAD PROBLEMÁTICA DE LA EMPRESA	28/10/19	30/10/19	3 días	
1.2.DETERMINAR PROCESO CRITICOS, MAPA DE PROCESOS, FUNCIONES, MISIÓN Y VISIÓN	31/10/19	31/10/19	1 día	
1.3.DETERMINAR REQUERIMIENTOS DE SEGURIDA DE LA INFORMACIÓN	4/11/19	6/11/19	3 días	
1.4.ESTABLECER LA NORMAS REGLAMENTARIAS VINCULADAS Y ACEPTADAS	7/11/19	8/11/19	2 días	
2.ALCANCE PRELIMINAR, LÍMITE ORGANIZACIONALES, FÍSICOS Y DE TI	11/11/19	15/11/19	5 días	
2.1.DESCRIBIR ALCANCE PRELIMINAR DE LA SEGURIDAD DE LA INFORMACIÓN	11/11/19	11/11/19	1 día	

2.2.ESTABLECER LÍMITES ORGANIZACIONALES DE LOS PROCESOS DEL ALCANCE	12/11/19	12/11/19	1 día
2.3.IDENTIFICAR LIMITES FÍSICOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	13/11/19	13/11/19	1 día
2.4.DETERMINAR LÍMITES DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	14/11/19	15/11/19	1 día
3.LIDERAZGO Y COMPROMISO DE LA DIRECCION DE INICIAR PROYECTO DE SGSI	18/11/19	22/11/19	5 días
3.1.REALIZAR INFORME DE DESCRIPCIÓN DEL PROYECTO	18/11/19	21/11/19	4 días
3.2.CONCERTAR COMPROMISO DE LA DIRECCIÓN CON EL PROYECTO	22/11/19	22/11/19	1 día
4.POLITICA RECTORA Y ROLES Y RESPONSABILIDADES DEL SGSI	25/11/19	6/12/19	10 días
4.1. DEFINIR POLÍTICA RECTORAY ALCANCE DE LA SEGURIDAD DE LA INFORMACIÓN	25/11/19	25/11/19	1 día
4.2. DETERMINAR OBJETIVOS Y PRINCIPIOS DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	25/11/19	25/11/19	1 día
4.3. DEFINIR ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN	26/11/19	27/11/19	2 días
4.4. REALIZAR SEGREGACIÓN DE FUNCIONES EN FUNCIÓN DE LOS ACTIVOS RELACIONADOS	28/11/19	28/11/19	1 día
4.5. DEFINIR CONTACTO CON AUTORIDADES DE SEGURIDAD DE LA INFORMACIÓN	29/11/19	29/11/19	1 día
4.6. DEFINIR CONTACTO CON GRUPOS ESPECIALES DE INTERÉS DE SEGURIDAD DE LA INFORMACIÓN	2/12/19	4/12/19	3 días
4.7. ESTABLECER OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	5/12/19	5/12/19	1 día

4.8. DEFINIR POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN	6/12/19	6/12/19	1 día
5.DEFINICIÓN DE LA VALORACIÓN Y TRATAMIENTO DE RIESGOS	9/12/19	9/12/19	1 día
5.1. INVESTIGAR Y REALIZAR DEL PROCESO DE VALORACIÓN Y TRATAMIENTO DE RIESGOS	9/12/19	9/12/19	1 día
FASES DE HACER	10/12/19	16/03/19	79 días
6. IDENTIFICAR ACTIVOS DEL ALCANCE Y ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN	10/12/19	13/12/19	4 días
6.1. DESCRIBIR ACTIVOS DEL ALCANCE DE SEGURIDAD DE LA INFORMACIÓN.	10/12/19	10/12/19	1 día
6.2. DETERMINAR NÚMERO, TIPO, UBICACIÓN Y FRECUENCIA DE USO DE CADA ACTIVO.	10/12/19	12/12/19	3 días
6.3. VALORAR ACTIVOS DE ACUERDO A LOS PRINICIPOS PARA DETERMINAR ESTADO ACTUAL.	13/12/19	13/12/19	1 día
7. EVALUAR RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.	16/12/19	27/12/19	15 días
7.1. IDENTIFICAR VULNERABILIDAD Y AMENAZA POR ACTIVO	16/12/19	26/12/19	14 días
7.2. REALIZAR CÁLCULO DE LA PROBABILIDAD POR IMPACTO EN LA SEGURIDAD DE LA INFORMACIÓN	27/12/19	27/12/19	1 día
8. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	30/12/20	10/01/20	10 días
8.1. DETERMINAR LOS CONTROLES APLICABLES DE LA ISO 27002	30/12/20	3/01/20	5 días
8.2. REALIZAR CÁLCULO DE RIESGO DESPUÉS DE MITIGAR	6/01/20	10/01/20	5 días
9. ACCIONES PARA EL TRATAMIENTO DE RIESGOS	13/01/20	31/01/20	15 días
9.1. DEFINIR LISTA DE ACCIONES ASOCIADOS CON LOS CONTROLES DE LA NTP-ISO/IEC 27002	13/01/20	15/01/20	3 días

9.2. DETERMINAR RESPONSIBLE, PLAZO, ACTIVOS AFECTADOS Y RECURSOS PARA CADA ACCIÓN	16/01/20	17/01/20	2 días
9.3. REALIZAR AVANCE DE LAS ACCIONES PARA EL TRATAMIENTO DE RIESGOS	20/01/20	31/01/20	10 días
10. COMUNICACIÓN	3/02/20	7/02/20	5 días
10.1. DETERMINAR PLAN DE COMUNICACIÓN EFECTIVA	3/02/20	4/02/20	2 días
10.2. REALIZAR EL MANUAL DE BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN	5/02/20	7/02/20	3 días
11. PROGRAMA DE ENTRENAMIENTO Y CONCIENTIZACIÓN	10/02/20	20/03/20	30 días
11.1. REALIZAR MANUAL DE BUENAS PRÁCTICAS PARA RECURSOS HUMANOS	10/02/20	12/02/20	5 días
11.2. REALIZAR EL PLAN DE CONCIENTIZACIÓN Y ACCIONES POR EJECUTAR	13/02/20	20/03/20	25 días
FASES DE VERIFICAR	23/03/20	17/04/20	20 días
12. EVALUAR DESEMPEÑO MEDIANTE MONITOREO, MEDICIÓN Y ANÁLISIS	23/03/20	3/04/20	10 días
12.1. DEFINIR INDICADORES PARA REALIZAR EL MONITOREO DE LOS CONTROLES IMPLEMENTADOS	20/01/20	24/01/20	5 días
12.2. REALIZAR MEDICIÓN PRE IMPLEMENTACIÓN DE CONTROLES	27/01/20	31/01/20	5 días
12.3. REALIZAR MEDICIÓN POST IMPLEMENTACIÓN DE CONTROLES	23/03/20	3/04/20	10 días
13. PROPUESTA DE PLAN DE AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN	6/04/20	10/04/20	5 días
13.1. REALIZAR MANUAL DE BUENAS PRÁCTICAS DE RECURSOS HUMANOS	6/04/20	8/04/20	3 días

13.2. DISEÑAR HERRAMIENTA PARA AUDITORÍA	9/04/20	10/04/20	2 días
14. REVISIÓN POR GERENCIA	13/04/20	17/04/20	5 días
14.1. ESTABLECER OBJETIVOS DE LA REVISIÓN POR GERENCIA	13/04/20	14/04/20	2 días
14.2. REALIZAR PLAN DE ACCIONES POR EJECUTAR PARA LA REVISIÓN POR GERENCIA	15/05/20	17/04/20	3 días
FASES DE ACTUAR	20/04/20	1/05/20	10 días
15. PROPUESTA DE MEJORA CONTINUA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	20/04/20	1/05/20	10 días
15.1. ESTABLECER TIPOLOGÍA DEL PLAN DE ACCIONES DE MEJORA	20/04/20	21/04/20	2 días
15.1. DISEÑAR HERRAMIENTA PARA LA MEJORA CONTINUA	22/04/20	24/04/20	3 días
15.3. REALIZAR DIAGRAMA DE PROCESOS DE LA MEJORA CONTINUA.	27/04/20	28/04/20	2 días
15.4. ENTREGAR CIERRE DE PROYECTO	29/05/20	1/05/20	2 días

Fuente. Elaboración propia

3.3. Política rectora y roles y responsabilidades del SGSI

La Política de Seguridad de la Información de la empresa L & M Seminario Group S.A.C. ha sido realizada tomando en cuenta la Norma Técnica Peruana ISO 27001:2013 y la Norma Técnica Peruana ENTP-ISO/IED 27002.

De igual manera, para la elaboración del mismo se toman en cuenta la ley 29733 Ley de Protección de Datos Personales y los derechos ARCO de la Autoridad Nacional de Protección de Datos Personales los cuales se dictan con la finalidad reglamentar el artículo 2 numeral 6 de la constitución política de Perú. Asimismo, se toman las leyes N~27806, de Transparencia y Acceso a la Información Pública cuyo fin es la promoción de la transparencia en las acciones del Estado; y la ley N~27489 que regula las centrales privadas de información de riesgos y protección al titular de la información a la cual se debe regir la Entidad del Sistema Financiero.

La política de seguridad de la información incluye los objetivos de seguridad de la información, la definición y principios para servir de guía en todas las actividades relacionadas con la seguridad de la información.

Alcance

- La presente política tiene como alcance a todas las personas que pertenecen al equipo de L & M Seminario Group S.A.C., directivo y colaborador en general que laboren en la empresa; así como a los proveedores y el comité de seguridad de la información.

- Abarca todos los requisitos de las partes interesadas relevantes a la seguridad de la información.
- La presente política está creada con el fin de proteger la información brindada por las partes interesadas de la empresa.

Objetivos

La Política de Seguridad de la Información tiene por objetivo regular la gestión de la seguridad de la información al interior de la entidad. De igual manera, tiene los siguientes objetivos específicos:

a) Crear un marco normativo de obligatorio cumplimiento, orientado a gestionar de manera apropiada la seguridad de información en la entidad técnica L & M Seminario Group S.A.C.
b) Establecer anualmente objetivos con relación a la seguridad de información.
c) Asegurar la disponibilidad, confidencialidad e integridad de la información.
d) Conseguir y mantener el nivel de seguridad requerido para garantizar de forma adecuada la continuidad del negocio, incluso en situaciones de riesgo.
e) Establecer las expectativas de la Dirección con respecto al correcto uso que el personal haga de los recursos de información de la entidad técnica L & M Seminario Group S.A.C, así como de las medidas que se deben adoptar para la protección de estos.
f) Establecer e implantar planes de formación y de no divulgación de seguridad para mejorar la formación del personal.
g) Proporcionar a L & M Seminario Group S.A.C. una herramienta que facilite a la alta dirección la toma de decisiones apropiada, en situaciones relacionadas con la preservación de la seguridad de la información.

Principios

a. Principio de Confiabilidad: propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

b. Principio de Integridad: busca proteger que se modifiquen los datos libres de forma no autorizada.

c. Principio de Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

Se sancionará conforme a la magnitud y característica no cumplido a todo aquel que viole lo dispuesto en las normas de las políticas de seguridad de la información que rigen al personal de L & M Seminario Group S.A.C.

Asimismo, según el artículo 39 y 40 de la ley 29733 Protección de datos personales del Perú, la sanción a los responsables del tratamiento de datos es:

- Infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
- Infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
- Infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).

Señala también que la multa impuesta no puede excederse del diez por ciento de los ingresos brutos anuales en el año anterior de cometida la infracción.

Responsabilidades

El Comité de Gestión de Seguridad de la Información de L & M Seminario Group S.A.C. vela por la existencia y cumplimiento de las medidas de seguridad de la información de la organización, propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan.

La junta directiva de la empresa mantiene las siguientes funciones:

- Mantener actualizada la agenda sobre los temas de seguridad del a información a tratar en las reuniones del comité de seguridad de la información de L & M Seminario Group S.A.C.
- Fijar las fechas para realizar las reuniones del comité.

Revisar y aprobar las actas del comité, previa rubrica de sus integrantes

El gerente general de la empresa L & M Seminario Group S.A.C. asume las siguientes funciones:

a) Realizar las coordinaciones de las reuniones del comité conforme al calendario del presidente de comité.

b) Realizar las actas de cada una de las reuniones

c) Convocar la firma del acta y realizara el respectivo archivo del documento

El gerente de operaciones de la empresa L & M Seminairo Group S.A.C. asume las siguientes funciones:

a) Plantear todas las modificaciones de las políticas de seguridad de información de L & M Seminario Group S.A.C. al Comité Gestión de Seguridad de Información, si en caso sea tan necesario.
b) Reorganizar y comunicar con la alta dirección y la administración de organización ante problemas que se puede causar en la seguridad de información, con el fin de

Definición de roles y responsabilidades del SGSI

Se definieron los siguientes roles:

a. Oficial de Seguridad de la Información (CISO)

Responsable del Sistema de Gestión de la Seguridad de la Información, reporta a la presidencia acerca de las políticas, los objetivos de las mismas y su cumplimiento en la organización. Tiene como responsabilidad:

- Definir y actualizar los activos de información.
- Realizar el análisis de riesgos de seguridad de la información.
- Planear el tratamiento de riesgos de seguridad de la información.
- Definir y difundir las políticas específicas del SGSI.
- Capacitar y sensibilizar a los colaboradores de L & M Seminario Group S.A.C. acerca de la seguridad de la información.
- Responsable de la definición del riesgo.

b. Comité de Seguridad de la información

Integrado por los principales, su objetivo es manejar los activos de información y tienen un rol de liderazgo dentro de la empresa, las responsabilidades de este comité son:

- Validar la documentación del SGSI con cada propietario del activo y responsable del riesgo.
- Sensibilizar a los colaboradores sobre seguridad de información
- Identificar y ayudar en la actualización de activos
- Identificar riesgos que afecten a la seguridad de la información
- Servir de apoyo en la selección de controles para mitigar los riesgos de seguridad de la información.
- Acudir a las reuniones para el establecimiento, implementación, mantención y mejora continua del SGSI
- Realizar un seguimiento a los controles aplicados en el tratamiento de riesgos.
- Proteger al activo con los controles definidos.
- Verificar el cumplimiento de la política
- Actualizar la información del activo.

3.4. Segregación de funciones

Se realiza el presente cuadro con el fin de minimizar las oportunidades de modificar activos de la organización sin la autorización de un responsable.

Tabla 14

Segregación de funciones

D01	SEGREGACIÓN DE FUNCIONES					
Proceso	**Responsable**	**Función**	**Activo relacionado**	**Facultades respecto a los activos**		
				Acceder	**Modificar**	**Utilizar**
P01	**Gerente General**	Establecimiento de proyectos a mediano plazo.	Ordenador	x	x	X
			Escritorio	x	x	X
		Establecimiento de nuevas líneas de negocio	Oficina	x	x	X
			Aire acondicionado	x		X
			Alarma de aire y de agua	X		x
P02	**Gerente de proyectos**	Organización y desarrollo de los proyectos constructivos.	Ordenador	x		X
			Escritorio	X		x
			Base de datos de beneficiarios por zona	x	x	X
		Realizar plan del alcance del proyecto, cronograma de actividades	Cronograma del proyecto	x	x	X
		Realizar informe de cierre de proyectos	Impresora	x		X
	Asistente de proyectos	Controlar las actividades programadas y costos del proyecto	Ordenador	x		X

		Realizar seguimiento a los proyectos mediante evidencias fotográficas	Cámara fotográfica	x	X	x
			Fotos de avances de obras	x		X
P03	**Gerente Comercial**	Identificación y búsqueda de poblaciones prospecto para calificar como beneficiario del programa Techo Propio.	Ordenador	x		X
	Gerente de operaciones	Investigar mejoras en la eficiencia de los procesos operativos de la empresa	Ordenador	X		x
	Asistente de marketing y publicidad	Desarrollar estrategias de diferenciación de la oferta en el mercado.	Ordenador	x		X
P04	**Gerente general**	Organización y trámite de los documentos solicitados principalmente por el Fondo MiVivienda.	Ordenador	X		x
			Sellos	x	X	X
			Agenda telefónica digital	x	X	x
			Carta solicitudes FMV	x	x	X
			Teléfono móvil	x	x	X
		Gestión de cartas de acreditación, seriedad de oferta y cartas fianzas con las entidades financieras.	Chequera	x	x	X

	Gerente de proyectos	Elaboración y gestión de expedientes y permisos municipales.	Expedientes técnicos	x	x	X
			Sellos	X		x
	Asistente de proyectos	Garantizar la disponibilidad de la información.	Ordenador	x		X
		Velar por la confidencialidad de los datos de los elegibles y beneficiarios.	USB	x		X
		Organizar y categorizar la información.	Impresora	X		x
P05	**Gerente de Operaciones**	Previsión de los materiales requeridos para obra y oficina.	Ordenador	x		X
	Asistente de Compras	Seleccionar y evaluar los proveedores de materiales de construcción.	Teléfono móvil	x		X
		Gestionar abastecimiento relación con los proveedores.	Facturas	x		
P06	**Operarios**	Construcción de Viviendas de Interés Social acorde a los estándares del Fondo MiVivienda.	EPP			X
	Residente de obras	Supervisar obra durante todo el proceso constructivo.	Planos arquitectónicos	x	X	x
		Controlar los materiales y	Ordenador	x	x	X

		cantidad repartidas, así como la mano de obra.				
		Realizar informes De avances de obra.	CD	X		
P07	**Gerente de Operaciones**	Seguimiento y supervisión de los procesos administrativos y operativos de la empresa.	Teléfono móvil	x	x	x
		Realizar informe de control de gestión para valorizaciones.	Correo electrónico	x	x	X
P08	**Asesor jurídico**	Contratos con beneficiarios y personal de obra.	Contratos	X		
P09	**Gerente General**	Realizar actividades relacionados con el ambiente laboral.	Personal	x	x	X
P10	**Asesor contable**	Declaración mensual de impuestos y PDT mensuales.	PDT mensuales	X		
		Realizar estados financieros y balances.	Estados financieros	X		
		Desarrollo de planillas	Planillas	X		

Fuente. Elaboración propia

Contacto con autoridades

El objetivo de tener establecido el contacto con las autoridades es dar a conocer los derechos ARCO (Acceso, Rectificación, Cancelación , Oposición) y cómo se debe reportar el incumplimiento de esta en la empresa L & M Seminario Group S.A.C. Es por ello que:

a. Los datos personales de todos los colaboradores de la empresa L&M Seminario Group S.A.C deberá controlarse por ellos a través de los derechos ARCO, los cuales permiten que se pueda exigir el correcto tratamiento de estos.
b. En caso de que los datos personales de los colaboradores se utilicen para motivos sin previa autorización, se podrá generar una solicitud para restringir el uso de estos (Anexo #).
c. El encargado de informática deberá explicar el proceso de solicitud para restringir el uso de datos personales.
d. Los colaboradores de L & M Seminario Group S.A.C. deberán ingresar al banco de datos del Fondo MIVIVIENDA para asegurarse que sus datos personales se encuentren utilizados correctamente. Los colaboradores deberán solicitar el origen de sus datos personales dentro del banco de datos del Fondo MIVIVIENDA.

Contacto con grupos especiales de interés

El objetivo es de conocer e involucrarse con grupos de personas que velen por la seguridad de la información dentro de una organización. Para lo cual se realizará:

a. La constante capacitación los colaboradores de la empresa L&M Seminario Group S.A.C acerca de seguridad de la información deberá realizarse a través de CERTIPRO, el cual es un centro de certificación en tecnología de información.
b. El foro "Wilders Security" es una página web de fácil en la que los colaboradores de la empresa L&M Seminario Group S.A.C podrán acceder para visualizar el control de seguridad de la información de distintas organizaciones.

c. El encargado de informática es responsable de informar a todos los colaboradores acerca de las capacitaciones que brindará CERTIPRO. Por otro lado, deberá hacer simulaciones de posibles ataques contra la seguridad de la organización.

d. Los colaboradores de L & M Seminario Group S.A.C. son responsables de asistir a las capacitaciones que brindará CERTIPRO. De igual forma, deberán actualizar constantemente sus conocimientos acerca de seguridad de la información.

Seguridad de la información en la gestión de proyectos

Al realizar cualquier proyecto o expediente se deberá tener en cuenta los siguientes objetivos de seguridad de la información:

- Evaluar riesgos de seguridad de la información en la evaluación de factibilidad del proyecto.
- Velar por los activos de seguridad utilizados en las fases de inicio, planificación, ejecución, control y cierre del proyecto.
- Asignar un responsable de los activos implicados dentro del equipo de gestión de proyecto.

3.5. Políticas relacionadas

a) Adhesión a la política:

(i) La política actual debe ser cumplida por todo el personal de L & M Seminario Group S.A.C.

(ii) El Comité de Seguridad de la Información debe mantener el control y el seguimiento en el cumplimiento de la política actual, reportando constantemente los resultados y desarrollos a los Directivos Generales de la empresa.

b) Gestión de Riesgos:

(i) El Oficial de Seguridad de la Información de L & M Seminario Group S.A.C. tiene como funciones:

- Apoyar a los demás miembros del equipo en la identificación, cuantificación y priorización de riesgos de seguridad de la información.
- Tomar decisiones de seguridad corporativa (Seguridad física, seguridad de las instalaciones e investigaciones).
- Junto a la Directiva de la empresa, puede tomar decisiones sobre qué hacer con los riesgos.

(ii) El Comité de Seguridad de Seguridad de la Información aprueba los resultados de la evaluación y tratamiento de riesgos.

c) Protección de la información:

(i) La empresa L & M Seminario Group S.A.C. sabe que la información que poseen y conoce el personal, es fundamental para el funcionamiento de la misma por lo cual le dan un alto valor lo que conlleva a considerar de suma importancia la seguridad de la información y la plantean como un objetivo institucional.

(ii) Se conoce que todos los riesgos no se pueden eliminar, solo mitigar a partir de controles que definirá la empresa para proteger la información en base al previo análisis de los riesgos.

(iii) La seguridad de la información se dará tanto en el plano informático como en el plano personal empleando acuerdos dentro de los contratos, como por ejemplo el de no divulgación, para mantener la información protegida.

d) Clasificación de la información:

(i) La información debe ser clasificada de acuerdo al nivel de importancia para L & M Seminario Group S.A.C., de acuerdo a sus necesidades o relevancias dentro del desarrollo de la empresa.

e) Uso de activos de información:

(i) Los activos de información deben ser utilizados de acuerdo a lo que L & M Seminario Group S.A.C. tenga como objetivos de acuerdo a las políticas de la empresa.

En la relación con otras empresas, L & M Seminario Group S.A.C. debe establecer convenios o contratos que tengan cláusulas o disposiciones para mantener protegida la información.

3.6. Políticas específicas

Política de dispositivos móviles

Objetivos

a. Crear un marco normativo acerca de las condiciones de manejo de los dispositivos móviles (celulares, tablets, etc) de la empresa y personales.
b. Garantizar el uso responsable de los dispositivos móviles proporcionados por la e mpresa.
c. Gestionar los riesgos derivados del uso de dispositivos móviles.

Política

a. Los equipos personales no tendrán acceso a los servicios de la empresa. Se separa el uso privado y de negocio de los dispositivos.

b. Se debe evitar conectar los equipos de la empresa a redes inalámbricas de uso público, se deberá evitar conectar los equipos móviles por puesto USB a cualquier equipo público.
c. Se deberá tener un registro de los dispositivos móviles institucionales. Asimismo, se deberá registrar al ingresar los dispositivos móviles personales que entran a la empresa.
d. Se deberá redactar y entregar junto a los equipos un acuerdo de usuario final de acuerdo al proveedor del equipo.
e. Se tiene el deber de configurar en todos los equipos pertenecientes a la empresa la opción de borrado remoto de datos en caso de pérdida o hurto.
f. Los equipos brindados a los colaboradores deberán ser configurado con contraseñas y con bloque de pantalla automático después de pasado un tiempo de inactividad de un minuto.
g. Los colaboradores solo recibirán los dispositivos proporcionados por la empresa después de haber firmado el acuerdo de usuario final.
h. Los colaboradores usarán los equipos de la empresa para fines del negocio, no se almacenarán material fotográfico o información personal en los mismos.

Política de teletrabajo

Objetivos

a. Crear un marco normativo acerca de las condiciones trabajo desde casa o lugares remotos a las oficinas de la organización.
b. Definir las restricciones cuando se haga uso del teletrabajo.
c. Alinear la política de teletrabajo de la organización a la ley promulgada por el congreso de la República del Perú N~30036 que regula el teletrabajo.

Política

a. Se debe asegurar que el ambiente físico en el que se realice el teletrabajo sea seguro, así como del entorno. De lo contrario, la pérdida de la información o del equipo estará a cargo del usuario.
b. Se deberá procurar trabajar sobre un escritorio o superficie limpia, en la cual solo se encuentre el equipo, papeles en físico y útiles de escritorio a utilizar.
c. Evitar el uso del mismo ambiente en el que se realiza el teletrabajo a familiares o amigos; cuando el material no sea utilizado deberá almacenarse en una zona segura.
d. La organización se compromete a enviar semanalmente boletines informativos sobre las buenas prácticas para el teletrabajo.
e. La organización evaluará el desempeño del colaborador que hace uso del teletrabajo de manera mensual.
f. La organización podrá prohibir el uso de la modalidad de teletrabajo si se presenta algún riesgo que atente contra la seguridad de la información o de comprobarse que el colaborador no alcanza con los objetivos propuestos.
g. El colaborador se compromete a hacer uso y gestionar el material a su disposición de manera responsable y a tener la capacidad de autogestión del tiempo, gestión de la comunicación, sistematicidad, disciplina y orden.
h. El colaborador deberá asegurarse y velar para que el material no sea utilizado por terceros.

Política de Control de Acceso

Objetivos

a. Crear un marco normativo de obligatorio cumplimiento orientado a gestionar de manera adecuada el control de acceso.

b. Establecer los límites de acceso a la información e instalaciones de procesamiento de la información en la oficina donde se almacenan todos los documentos en físico de la gestión documental.

a. Establecer los lineamientos para el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.

Política:

a. Adhesión a la Política:

   (i) La presente política debe ser cumplida por todo el personal de L & M Seminario Group S.A.C., sin excepción.

   (ii) El Comité de Gestión de Seguridad de la Información debe monitorear el cumplimiento de la presente política.

b. Revisión de derechos de acceso de usuarios:

   L & M Seminario Group S.A.C. deberá revisar y asignar privilegios de accesos a cada colaborador que ingrese a la empresa. Los mismos que serán revisados en intervalos regulares de tres meses o cada que el contrato sea renovado, de ser el caso de un ascenso o descenso se realizará una revisión de sus derechos, los cuales se especificaran en el nuevo contrato a firmar. El comité de seguridad de la información llevará un registro de todas las cuentas privilegiadas para una revisión periódica mensual.

c. Acceso a redes y servicios de red:

   Los colaboradores de L & M Seminario Group S.A.C. deberán tener acceso solo a la red y servicios de red inalámbrica del área de trabajo a la que pertenecen, autorización la cual será especificada el día de inducción a la empresa.

Para el acceso a la red inalámbrica se proporcionará una contraseña al usuario la cual es intransferible y confidencial del área de trabajo en el que se desempeña.

d. Registro y baja de usuarios

L & M Seminario Group S.A.C., debe mantener los registros de cada uno de los integrantes de los procesos que hayan sido autorizados en el sistema.

Cada usuario que acceda al sistema de información de la organización deberá utilizar la identificación única de usuario (ID) con el fin de que ellos sean vinculados y responsables de sus acciones en el sistema.

El uso de ID compartidos solo deberá ser permitido cuando sea necesario por razones de negocio y deberá ser plasmado en un documento en el cual todos los involucrados se comprometen a asumir las responsabilidades.

Política de seguridad de la información para las relaciones con los proveedores

Objetivo:

a. Asegurar protección a los activos de la organización que son accesibles por los proveedores.

Política:

a. La empresa L & M Seminario Group S.A.C. identifica los tipos de proveedores a los que permitirá el acceso a su información.
b. Los proveedores no cuentan con acceso a toda la información de la empresa y tienen un constante monitoreo y control.
c. Los proveedores reciben la información sobre los tipos de obligaciones que deben realizar para garantizar la seguridad de la información de la empresa.

d. Los proveedores conocen los requisitos y procedimientos de gestión de incidentes.
e. La empresa L & M Seminario Group S.A.C. realiza auditorías internas o independientes a los proveedores y el seguimiento de problemas identificados
f. La empresa L & M Seminario Group S.A.C. garantiza que sus proveedores cuentan con la capacidad de servicio junto con los planes realizables diseñados para garantizar que los niveles de continuidad de servicio acordado se mantendrán después de fallas importantes en el servicio o desastres.

Política de escritorio limpio y pantalla limpia

Objetivo:

a. Establecer las disposiciones con respecto al uso de las computadoras y terminales cuando estas se encuentran desatendidas en las instalaciones de procesamiento de la información.
b. Establecer los lineamientos que faciliten el almacenamiento tanto electrónico como de papeles para mantener la seguridad de la información.

Política:

a. Toda información en papel, es decir en físico, que no sea usada y que sea de carácter sensible o crítico para el negocio deberá ser asegurada bajo llave en el cubículo del colaborador que maneje dicha información, el cual será responsable de la llave y de velar por su seguridad especialmente cuando la oficina se encuentre desocupada; dejando al finalizar el día su mesa de trabajo sin ningún papel en ella.
b. Se debe utilizar el mecanismo de bloqueo de pantalla y de teclado con una contraseña; la contraseña de bloqueo es personal. Todas las computadoras contarán con restricción de tiempo de sesión desatendida.

c. Las impresoras deberán ser usadas solo cuando sean necesarias, de tratarse de información sensible y para obtener las impresiones utilizará el código de uso PIN y estará ubicado al lado de la impresora, retirando los documentos inmediatamente.

Responsabilidades

a. Responsabilidades del área de informática

   Deberá programar un código PIN para el funcionamiento de la impresora.

   Deberá establecer un manual de usuario en el que se indique las características que cada trabajador debe poner en sus contraseñas, la cual debe contener números y símbolos cuando no esté en uso el equipo.

b. Responsabilidades del colaborador

   Deberá guardar todo equipo portátil guardado bajo llave al finalizar la jornada laboral.

   Deberá utilizar el mecanismo de bloqueo de pantalla y de teclado cada que la computadora este desatendida.

   Debe desconectar todos los equipos que estén bajo su responsabilidad al finalizar la jornada laboral.

Políticas y procedimientos de transferencia de la información

Objetivo:

a. Establecer los lineamientos para la transferencia adecuada de información sensible de la empresa L & M Seminario Group S.A.C.

Política:

a. La información digital transportada físicamente a otro lugar deberá protegerse del acceso no autorizado haciendo uso de mensajeros fiables, todo equipo trasladado físicamente deberá embalarse y protegerse contra impactos.
b. Si es necesario el uso de dispositivos móviles se deberá eliminar inmediatamente después de utilizada la información. La información trasladada en dispositivos USB deberá cifrarse.

Responsabilidades:

a. Responsabilidades del área de informática

   El encargado de informática deberá realizar cifrado de documentos que contenga información sensible.

   Deberá encargarse de redactar el acuerdo sobre transferencia de información.

b. Responsabilidades del colaborador

   Los colaboradores de L & M Seminario Group S.A.C. no deberán comunicar información sensible mediante medios telefónicos, con el fin de prevenir interpretaciones de terceros que escuchen dicha conversación.

   Los colaboradores deberán evitar entablar conversaciones confidenciales en espacios públicos o abiertos. Ningún mensaje deberá ser dejado desatendido en contestadores.

   Al iniciar sus actividades laborales en la empresa y al finalizarlas, los colaboradores deberán aceptar y firmar el acuerdo de confidencialidad o no divulgación.

Definición de la valoración y tratamiento de riesgos

Se estableció un conjunto de actividades a seguir para realizar la valoración y tratamiento de riesgos en la organización el cual se basa en el procedimiento brindado por la ISO/IEC 27005;2011 (Ver anexo 05).

3.7. Hacer

Identificar activos del alcance del SGSI

Tabla 15

Identificación de activos de gestión documental

D02	IDENTIFICAR ACTIVOS					
ID	**ACTIVO**	**DESCRIPCIÓN**	**CANTIDAD**	**TIPO DE ACTIVO**	**UBICACION**	**FRECUENCIA DE USO**
A01	Servidor	Equipo del cual se almacena la información, aplicaciones y acceso a redes de la empresa	1	ST	Ubicación Física	Diaria
A02	Teléfono móvil	Utilizado para realizar llamadas al Fondo Mivivienda, Financieras y nexo de comunicación con el personal y beneficiarios	3	AF	Ubicación Física	Diaria
A03	Facturas	Comprobante de pago en el que se detallan los productos y/o servicios que adquiere la empresa y el cual sirve para sustentar las actividades de la misma.	15	AF	Ubicación Física	Mensual
A04	Impresoras	Objeto que permite transferir documentos de una computadora a un papel	2	AF	Ubicación Física	Semanal
A05	Sellos	Objeto que permite reflejar signos y/o figuras en un documento o papel	6	AF	Ubicación Física	Diaria
A06	Chequera	Documento contable de la empresa para autorizar el retiro de dinero de la cuenta corriente al portador del cheque	2	AF	Ubicación Física	Mensual
A07	Expedientes técnicos	Conjunto de documentos en el cual se establece el presupuesto, licencias, memorias descriptivas, planos y detalles para la ejecución de la obra	5	AF	Ubicación Física	Diaria
A08	CD	Disco para almacenar datos en forma digital, especificamente los planos	12	AF	Ubicación Física	Mensual

		catastrales brindados por COFOPRI				
A09	Escritorio	Es un tipo de mueble que se utiliza frecuentemente en un lugar de trabajo y cuenta con un tablero para escribir	2	AF	Ubicación Física	Diaria
A10	Ordenadores	Ordenador portátil usado para la gestión documental de la empresa, así como para la elaboración de planos y presupuestos	5	AF	Ubicación Física	Diaria
A11	Adobe	Aplicación que permite visualizar, crear y modificar archivos con formato pdf.	1	AT	Ubicación Lógica	Diaria
A12	Paquete autodesk	Paquete de aplicaciones de autodesk que incluyen autocad y civil 3D	1	AT	Ubicación Lógica	Diaria
A13	Fotos de avances de obra	Imagen visual captada digitalmente para obtener como evidencia y registro de los avances realizados en obra.	84	AI	Ubicación Lógica	Semanal
A14	Ms Office	Paquete de aplicaciones, para oficina desarrollado por Microsoft	ND	AT	Ubicación Lógica	Diaria
A15	Correo electrònico	Es un servicio de red que permite el intercambio de mensajes entre usuarios	2	AI	Ubicación Lógica	Diaria
A16	Estados financieros, balance general y PDT	Reportes que reflejan la situación financiera de una organización	ND	AI	Ubicación Lógica	Mensual
A17	Bases de datos de beneficiarios por zona	Conjunto de datos organizados y almacenados de los beneficiarios que pertenecen a la entidad pública	1	AI	Ubicación Lógica	Diaria
A18	Agenda telefònica digital	Es un conjunto de números telefónicos de usuarios que se tiene en un dispositivo móvil	1	AI	Ubicación Lógica	Diaria
A19	Cartas solicitudes FMV	Constancias físicas de recepción de documentos	91	AF	Ubicación Física	Diaria
A20	USB	Es un pequeño dispositivo que se utiliza para almacenar información digital	2	AF	Ubicación Física	Semanal
A21	Planos arquitectònicos, de ubicacion y localizacion	Es la representación gráfica del diseño de un futuro proyecto	287	AI	Ubicación Lógica	Diaria
A 22	Personal	Compuesto por los 12 colaboradores de la empresa L & M Seminario Group S.A.C.	1	AH	Ubicación Física	Diaria
A23	Servicio de Anti-Virus	Programa para detectar y eliminar virus informáticos	1	AT	Ubicación Lógica	Diaria
A24	Proceso de Ejecución de Obra	Conjunto de actividades a realizar para obtener la construcción de viviendas finalizadas	1	AP	Ubicación Lógica	Semanal
A25	Proceso de Gestión Documental	Conjunto de actividades realizadas para poder desarrollas las obras	1	AP	Ubicación Lógica	Trimestral

A26	Cámara fotográfica	Es un objeto que sirve para capturar imágenes o fotografías	1	AF	Ubicación Física	Semanal
A27	Oficina	Espacio físico donde se realizan las actividades de trabao	1	AF	Ubicación Física	Diaria
A28	Servicio de Red	Servicio que facilita la comunicación entre dos o más ordenadores	1	AT	Ubicación Lógica	Diaria
A29	Servicio de Internet	Es un servicio de red que permite compartir recursos, acceder a información y comunicarse.	1	AT	Ubicación Lógica	Diaria

Fuente. Elaboración propia

Tabla 16

Tipos de activos

Leyenda:

Tipo de activo	
Abreviatura	**Tipo de Activo**
AI	Activos de Información Pura
AF	Activos Físicos
AT	Activos de Servicio de TI
AH	Activos Humanos

Fuente. Elaboración propia

Asimismo, después del registro de los activos existentes se realizó una valoración del activo con el fin de determinar los activos sensibles con respecto a la seguridad de la información:

Tabla 17

Valoración de los activos identificados.

VALORACIÓN DEL ACTIVO					
ID	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Nivel**	**Valoración Total**
A01	3	0	3	MEDIO	2
A02	1	1	3	MEDIO	2
A03	3	1	3	MEDIO	2
A04	1	0	3	BAJO	1
A05	3	1	3	MEDIO	2
A06	3	2	3	ALTO	3
A07	3	2	3	ALTO	3
A08	2	2	1	MEDIO	2
A09	0	0	2	BAJO	1

A10	3	2	3	ALTO	3
A11	0	1	2	BAJO	1
A12	0	1	3	BAJO	1
A13	2	2	2	MEDIO	2
A14	2	2	3	ALTO	3
A15	3	2	3	ALTO	3
A16	2	2	3	MEDIO	2
A17	3	2	3	ALTO	3
A18	3	1	3	MEDIO	2
A19	3	1	2	MEDIO	2
A20	3	2	3	ALTO	3
A21	3	1	3	MEDIO	2
A22	3	2	3	ALTO	3
A23	3	3	2	ALTO	3
A24	0	1	2	BAJO	1
A25	2	1	1	BAJO	1
A26	1	1	2	BAJO	1
A27	3	2	3	ALTO	3
A28	2	3	3	ALTO	3
A29	2	3	3	ALTO	3

Fuente. Elaboración propia

Leyenda:

Valor	
0	No aplicable
1	La pérdida de seguridad en el principio no impediría la actividad de la organización.
2	La pérdida de seguridad en el principio causaría trastornos leves en la actividad normal de la organización.
3	La pérdida de seguridad en el principio causaría trastornos graves en la actividad normal de la organización.

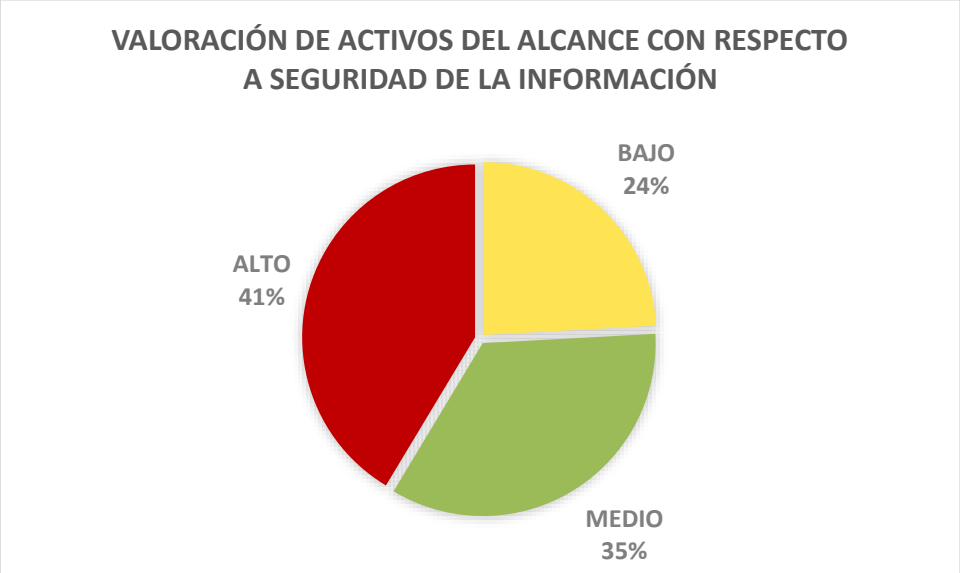


Figura 21. Gráfico de valoración de activos del alcance con respecto a seguridad de la información

Fuente. Elaboración propia

3.8. Pruebas Pre Test

Variable Independiente

La variable independiente de la investigación es la seguridad de la información, se tomó como dimensiones los objetivos estratégicos, tácticos y operativos. Los resultados por cada dimensión serán analizados a continuación:

Estratégico

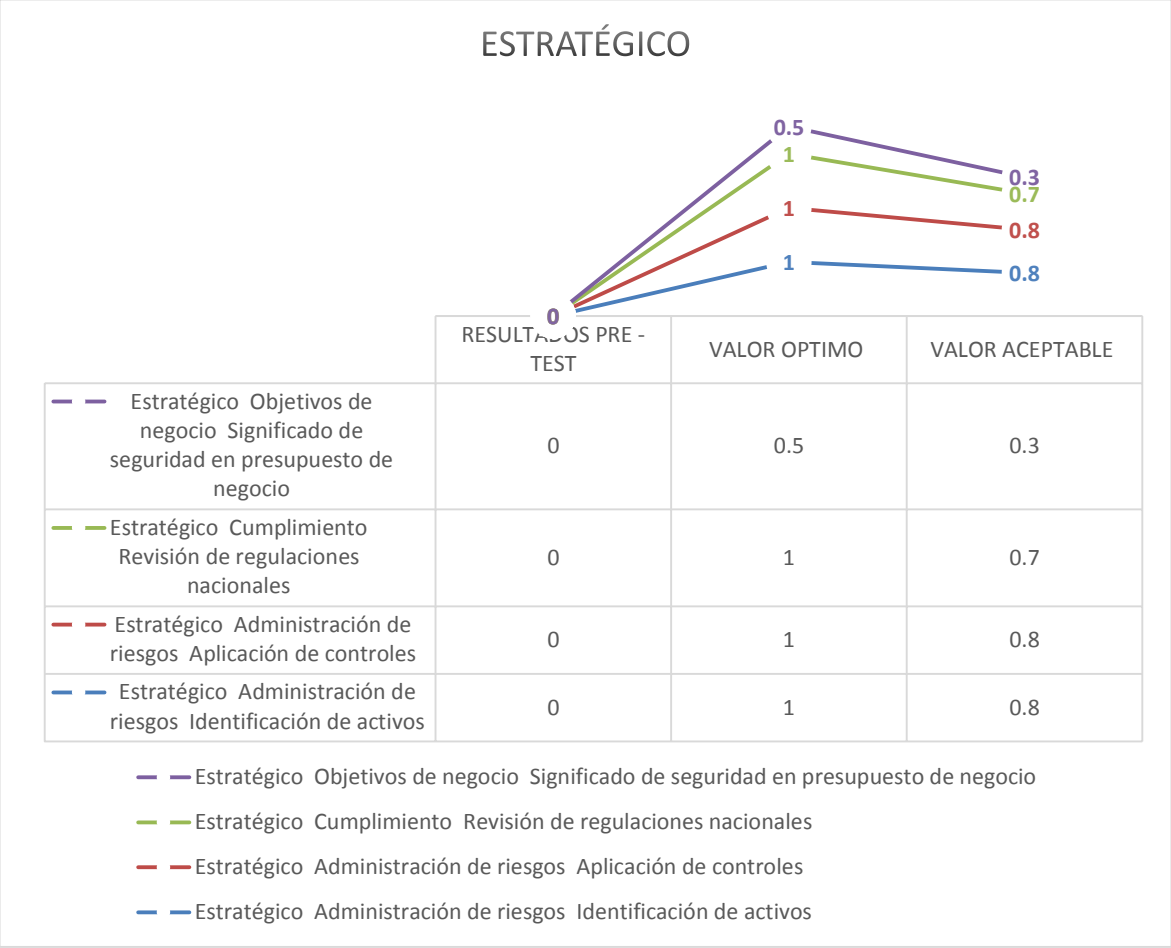
Dentro de los objetivos estratégicos se consideraron las categorías administración de riesgos, cumplimiento y objetivos de negocio. Dentro de la primera categoría de administración de riesgos se establecieron los siguientes tres indicadores:

El indicador de identificación de activos se obtuvo de la división entre los activos etiquetados y los activos inventariados; teniendo como dato inicial que existen 29 activos dentro del alcance del proyecto de los cuales ninguno se encontraba etiquetado, obteniendo así un índice nulo.

Con respecto al indicador de aplicación de controles, se encontró que la existencia de tanto la planificación como la implementación de controles de seguridad de la información era nula.

La segunda categoría de la dimensión de los objetivos estratégicos es la de cumplimiento, teniendo como indicador la revisión de regulaciones nacionales ejecutadas entre las programadas para así tener conocimiento de lo reglamentado por el gobierno peruano sobre lo concerniente a la seguridad de la información.

La tercera y última categoría de la dimensión estratégica es la de objetivos de negocio, para lo cual se consideró analizar el indicador del significado de seguridad en presupuesto de negocio, tomando como dato de entrada el presupuesto asignado para implementaciones el cual es de S/ 45, 000 soles, de los cuales ningún porcentaje se destina a la seguridad de la información, teniendo como resultado de la fórmula el índice 0.



	RESULTADOS PRE - TEST	VALOR OPTIMO	VALOR ACEPTABLE
Estratégico Objetivos de negocio Significado de seguridad en presupuesto de negocio	0	0.5	0.3
Estratégico Cumplimiento Revisión de regulaciones nacionales	0	1	0.7
Estratégico Administración de riesgos Aplicación de controles	0	1	0.8
Estratégico Administración de riesgos Identificación de activos	0	1	0.8

Figura 22. Resultados pre test de la dimensión estratégica

Fuente. Elaboración propia

Táctico

En esta dimensión se consideraron dos categorías: perímetro y servicios. Dentro de la primera categoría se analizó el indicador de licencias del antivirus, este se obtuvo

de la división de lo entre los ordenadores con licencia activa y los ordenadores con licencia caducada más los con licencia activa, se tenía que 5 ordenadores contaban con licencia caducada por lo que el índice de este indicador es nulo (ver anexo 09).

La tercera categoría de servicios se analizó la tasa de corrección de errores de backups, obtenido de la división del número de ordenadores examinados sin fallas encontradas entre la sumatoria de los ordenadores examinados con fallas y los ordenadores sin fallas; obteniendo un índice nulo. Asimismo, se documentación las fallas más frecuentes en la restauración de la data las cuales fueron 14 en promedio de los cinco (5) ordenadores evaluados.

Tabla 18

Identificación de fallas encontradas

ID	Identificación de fallas encontradas	Tipo
F001	Falla en programas internos	Software
F002	Falla en la data de trabajo de los archivo	Software
F003	Falla de inicio de sesión	Software
F004	Falla de configuraciones establecidas	Software
F005	Falla en archivo de arranque en Office 365	Software
F006	Falla en archivo de arranque del navegador	Software
F007	Falla en el arranque del sistema operativo	Software
F008	Falla en el rendimiento del sistema	Software
F009	Falla en el disco duro por sobre calentamiento	Hardware
F010	Falla en el disco duro por tiempo de vida	Hardware
F011	Falla en la placa madre por falta de mantenimiento	Hardware
F012	Falla en el procesador por falta de mantenimiento	Hardware
F013	Falla en la memoria RAM por falta de mantenimiento	Hardware
F014	Falla en el tiempo de respuesta del sistema operativo	Software

Fuente. Elaboración propia

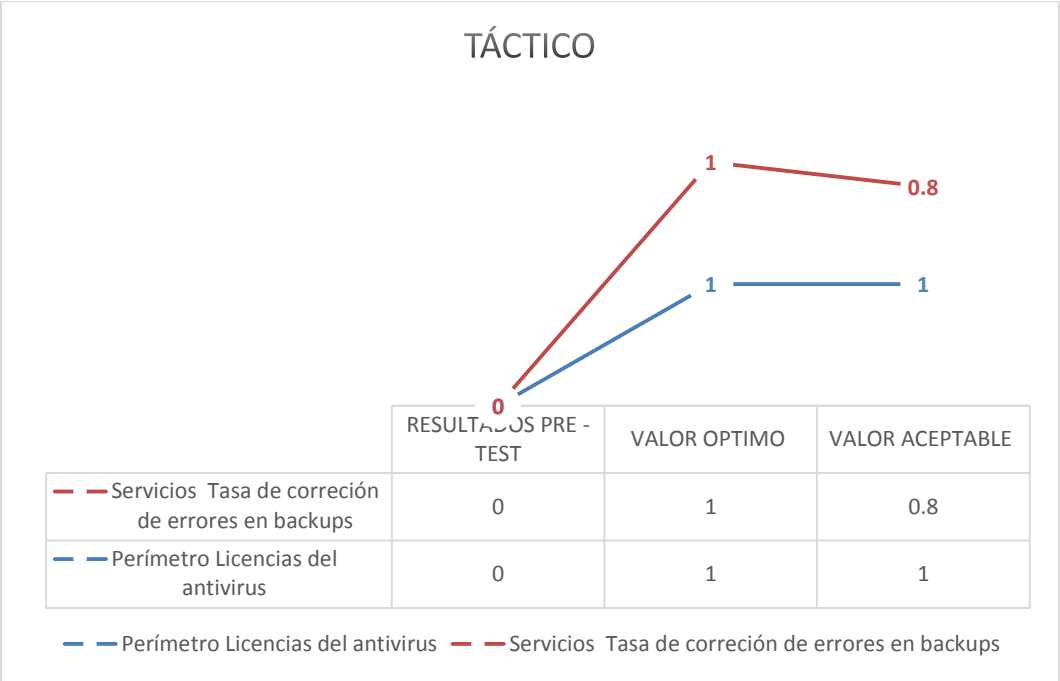


Figura 23. Resultados pre test de la dimensión táctica

Fuente. Elaboración propia

Operativo

En esta dimensión se tomaron los principios de la seguridad de la información los cuales son la confidencialidad, integridad y disponibilidad.

En la primera categoría se establecieron tres indicadores, protección de activos físicos, educación en seguridad de la información y autenticación.

El primer indicador de confidencialidad fue el de educación en seguridad de la información obtenido de la división del número de colaboradores que aprobaron el cuestionario (anexo 13 & 14) luego de atender a las capacitaciones entre la sumatoria de los que aprobaron y los que no aprobaron el examen. El segundo indicador evaluado en esta categoría evaluado fue la autenticación, obtenida del número de usuarios con ID únicos entre la sumatorio del número de usuarios con ID y los usuarios sin ID.

En la categoría de integridad se evalúa la protección de los ordenadores, obtenido del número de ordenadores con capacidad de encriptación entre el número total de ordenadores; se obtuvo que de los cinco (5) ordenadores ninguno tenía la capacidad de encriptación debido a que los equipos no habían tenido mantenimiento.

La última categoría es de disponibilidad teniendo como indicador la disponibilidad para el contacto con autoridades y grupos de interés, esta se obtiene de la sumatoria del número de contactos con autoridades establecidos más el número de contactos con grupos de interés; anterior a la implementación se encontró que estos contactos eran nulos.

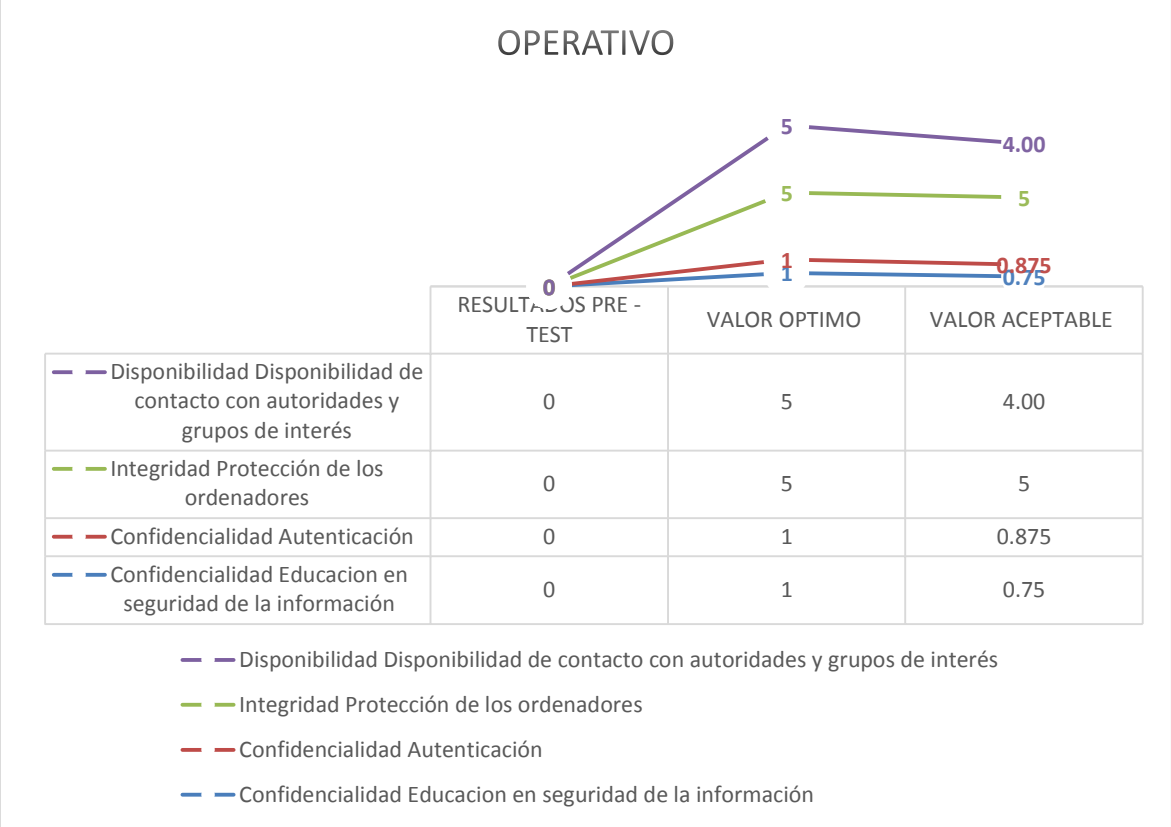


Figura 24. Resultados pre test de la dimensión operativa

Fuente. Elaboración propia

Variable Dependiente

La variable dependiente de la investigación es la gestión documental, se tomó como dimensiones los enfoques clásicos y digital. Los resultados por cada dimensión serán analizados a continuación:

Enfoque Clásico

Se analizaron dos indicadores: la eficiencia y la protección de activos físicos. El primero se obtuvo del número de formas utilizadas entre el número de formas programadas, como resultado se encontró que no existe ninguna forma programada de las utilizadas, por lo que el índice es 0.

Por otro lado, el resultado del indicador de protección de activos físicos se halló de la división del número de acceso restringidos a las instalaciones físicas que contienen información sensible (nulo) entre el número total de acceso a las instalaciones físicas que contiene información sensible, que en el caso de la oficina principal es seis (6) accesos físicos. Obteniendo como índice 0.

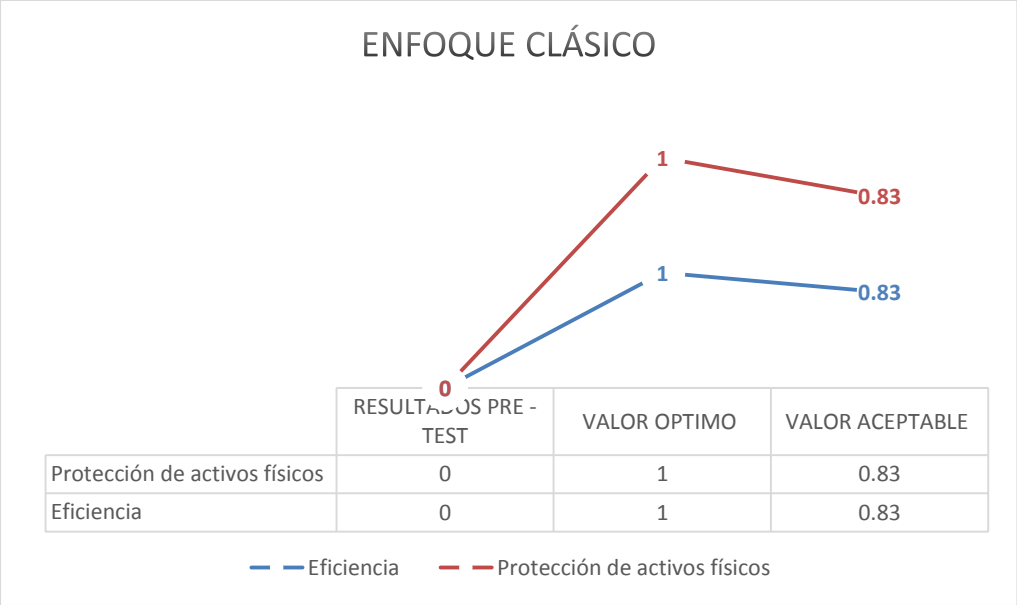


Figura 25. Resultados pre test de la dimensión enfoque clásico

Fuente. Elaboración propia

Enfoque Digital

Dentro del enfoque digital se evaluaron seis indicadores. El primero es el indicador de planes de actualización y seguimiento se obtuvo de la división del número de planes ejecutados entre el número total de planes programados, los cuales eran inexistentes en materia de seguridad de la información.

En segundo lugar, se tomó como indicador las pruebas de vulnerabilidad de software, hallado de la división de softwares no infectados entre el número total de softwares analizados; se analizaron diez softwares en los cinco ordenadores de la empresa, de los cuales 20 fueron infectados por alguna clase de virus, obteniendo el índice 0.60. A continuación se muestra el listado de los diez softwares analizados.

Tabla 19

Aplicaciones encontradas en evaluación pre test

ID	Identificación de aplicaciones encontradas	Tipo
APP001	Microsoft Word	Software
APP002	Microsoft Excel	Software
APP003	Microsoft Power Point	Software
APP004	Microsoft Project	Software
APP005	Adobe	Software
APP006	Autocad	Software
APP007	Autodesk	Software
APP008	Civil 3D	Software
APP009	Outlook	Software
APP010	Microsoft teams	Software

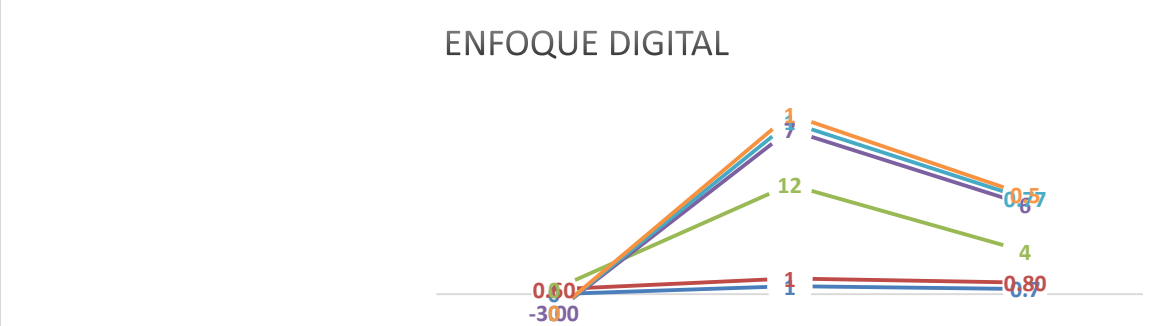
Fuente. Elaboración propia

Asimismo, el indicador de copias de respaldo se obtuvo del índice de las copias de respaldo realizadas anualmente, las cuales eran nulas.

Respecto al indicador de grado de protección de los sistemas de información de sujetos este se obtuvo de la sustracción de los softwares analizados, los cuales fueron 10, menos el número total de personas no autorizadas que acceden a los sistemas de información, las cuales fueron trece (13); obteniendo así un índice negativo de menos 3.

El indicador de accesibilidad a la documentación del hardware y software de la organización, es decir a los manuales de los equipos. Este resultado se obtiene de la división del número de aplicaciones con documentación archivada entre el número de aplicaciones inventariadas. Se encontraron 10 aplicaciones inventariadas, sin embargo, ninguna contaba con documentación archivada por lo que el resultado del índice es 0.

Por último, el indicador de capacitación fue obtenido del número de colaboradores capacitados en gestión documental entre el número de colaboradores dedicados a la gestión documental (cinco); el resultado fue nulo.



	RESULTADOS PRE - TEST	VALOR OPTIMO	VALOR ACEPTABLE
Enfoque Digital Capacitación	0	1	0.5
Enfoque Digital Accesibilidad a la documentación de hardware/software	0	1	0.77
Enfoque Digital Grado de protección de los sistemas de información de sujetos no autorizados.	-3.00	7	6
Enfoque Digital Copias de respaldo	0	12	4
Enfoque Digital Pruebas de vulnerabilidad del software	0.60	1	0.80
Enfoque Digital Planes de actualización y seguimiento	0	1	0.7

Figura 26. Resultados pre test de la dimensión enfoque digital

Fuente. Elaboración propia

Evaluar riesgos de seguridad de la información.

La evaluación del riesgo se realizó tomando como entradas los activos de los procesos ejecución de obra y gestión documental, calificados como sensible con respecto a la seguridad de la información de la organización:

Tabla 20

Evaluación de los riesgos de seguridad de la información

D03	EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN				
			RIESGO		
ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD	IMPACTO	RESULTADO
Chequera	Los cheques se encuentran firmados y sellados en unos compartimientos sin llave	Hurto o pérdida del cheque	1	3	3
Expedientes técnicos	Se encuentran accesibles a cualquier persona a pesar de ser una información confidencial	Pérdida de la información	2	3	6
Ordenador	Los ordenadores no cuentan con usuarios y contraseñas de inicio y estas son transportadas interprovincialmente.	Robo de equipo	1	2	2
Ms Office	Vencimiento de licencias	Errores de actualización	1	2	2
Correo electrònico	Falta de robustez en la contraseña de acceso al correo corporativo	Hurto de detalles de la información de la empresa	2	3	6
Impresora	Mantenimiento insuficiente	Falla técnica de la impresora	1	1	1
Bases de datos de beneficiarios por zona	Inexistencia de control de acceso	Extracción no autorizada de datos	1	3	3
USB	Acceso a equipos no verificados	Pérdida de archivos por virus	2	3	6
Personal	Falta de concientización en seguridad de la información	Fuga de información	2	3	6
Servicio de Anti-Virus	Licencias desactivadas en los ordenadores	Ataques	2	3	6
Oficina	Desorganización del espacio de trabajo, falta de seguridad en la locación.	Robo	2	3	6
Servicio de Red	Falta de autenticación al ingreso	Filtración de información fuera de la compañía	1	2	2
Servicio de Internet	Dependencia de su funcionamiento. Canal vulnerable a ataques cibernéticos.	Ciber ataque	2	3	6

Fuente. Elaboración propia

Tratamiento de riesgos de seguridad de la información:

Se realizó el tratamiento como parte del proceso de gestión de riesgos (Ver anexo 07), se tuvo como entrada la evaluación del riesgo resultado de los factores probabilidad por impacto, y a su vez todos los controles de la NTP ISO/IEC 27002:2016 los cuales fueron evaluados individualmente para identificar cuáles son aplicables para la mitigación del riesgo (Ver anexo 08). Para lograr el tratamiento de riesgos se extrajo datos de la probabilidad de ocurrencia de la amenaza de la valoración de amenazas y el valor de impacto de los niveles de impacto enfocados en las dimensiones de confidencialidad, disponibilidad e integridad de cada riesgo.

Tabla 21

Tratamiento de los riesgos de seguridad de la información

D04	TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN									
ACTIVO	VULNERABILIDAD	AMENAZA	RIESGO			Control ISO27002 Aplicable	DESPUÉS DE MITIGAR			VARIACIÓN
			PROB.	IMP.	RSL.		PROB.	IMP.	RSL.	
Expedientes técnicos	Se encuentran accesibles a cualquier persona a pesar de ser una información confidencial	Pérdida de la información	2	3	6	6.1.5. Seguridad de la información en la gestión de proyectos 8.2.1. Clasificación de la información 8.2.2. Etiquetado de la información 8.2.3. Manejo de activos	1	2	2	67%
Correo electrónico	Falta de robustez en la contraseña de acceso al correo corporativo	Hurto de detalles de la información de la empresa	2	3	6	9.1.1. Política de control de acceso. 9.4.3. Sistema de gestión de contraseñas. 11.2.8. Equipo de usuario desatendido 11.2.9. Política de escritorio limpio y pantalla limpia 13.2.1. Políticas y procedimientos de transferencia de información	1	2	2	67%

USB	Acceso a equipos no verificados	Pérdida de archivos por virus	2	3	6	6.2.1. Política de dispositivos móviles. 8.3.1. Gestión de medios removibles 8.3.2. Disposición de medios 8.3.3. Transferencia de medios físicos 11.2.5. Remoción de activos	1	3	3	50%
Personal	Falta de concientización en seguridad de la información	Fuga de información	2	3	6	5.1.1. Políticas para la seguridad de la información. 6.1.1. Roles y responsabilidades en seguridad de la información 6.1.2. Segregación de funciones 6.1.3. Contacto con autoridades 6.1.4. Contacto con grupos de interés especial 7.1.1. Selección. 7.1.2. Términos y condiciones del empleo 7.2.1.Responsabilidades de gestión 7.2.2. Concientización, educación y capacitación en seguridad de la información. 7.2.3. Proceso disciplinario	1	3	3	50%
Oficina	Desorganización del espacio de trabajo, falta de seguridad en la locación.	Robo	2	3	6	11.1.1. Perímetro de seguridad física 11.1.2. Controles físicos de entrada 11.1.3. Seguridad de oficinas, despachos y recursos	1	3	3	50%
Servicio de antivirus	Licencias desactivadas en los ordenadores	Ataques	2	3	6	8.2.3. Manejo de activos	1	3	3	50%
Servicio de Internet	Dependencia de su funcionamiento. Canal vulnerable a ataques cibernéticos.	Ciber ataque	2	3	6	6.2.2. Teletrabajo	1	3	3	50%

Fuente. Elaboración propia

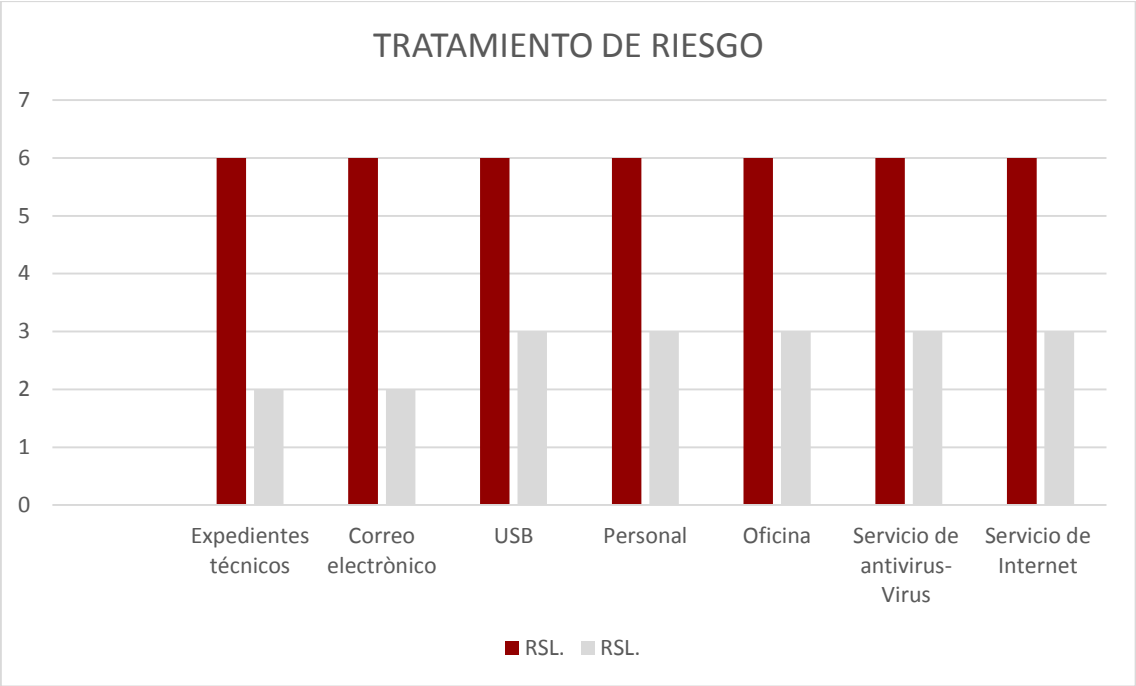


Figura 27. Mitigación de los riesgos

Fuente. Elaboración propia

Acciones para el tratamiento de riesgos

A continuación, se realizó una lista de las acciones realizadas para tratar cada riesgo y minimizar de tal manera su riesgo.

Tabla 22

Acciones a tomar para el tratamiento de los riesgos de seguridad de la información

D05	ACCIONES PARA EL TRATAMIENTO DE RIESGOS					
ID	Acción	Control Asociado NTP-ISO/IEC 27002	Responsable	Plazo	Activos afectados	Recursos
AC1	Crear un manual de buenas prácticas con las políticas de seguridad de la información	5.1.1. Políticas para la seguridad de la información 6.2.1. Política de dispositivos móviles. 6.2.2. Teletrabajo 9.1.1. Política de control de acceso 11.2.8. Equipo de usuario desatendido 11.2.9. Política de escritorio limpio y pantalla limpia 15.1.1. Política de seguridad de la información en relaciones con los proveedores	Oficial de seguridad de la información	3 meses	Todos los activos de seguridad de la información de la organización	Horas responsable de seguridad
AC2	Realizar etiquetado de activos de la información	8.2.1. Clasificación de la información 8.1.1. Inventario de activos	Comité de seguridad de la información	2 semanas	Todos los activos de seguridad de la información de la organización	Horas responsable de seguridad
AC3	Establecer lineamiento para la auditoría y revisión periódica de las polïticas de seguridad de la información.	5.1.2. Revisión de las políticas para la seguridad de la información.	Oficial de seguridad de la información	1 semana	Todos los activos de seguridad de la información de la organización	Horas responsable de seguridad
AC4	Establecer los roles del comite de seguridad de la información, oficial de seguridad de la información, usuario de activo y del responsable del riesgo.	6.1.1. Roles y responsabilidades en seguridad de la información	Oficial de seguridad de la información	1 mes	Colaboradores de la organización	Horas responsable de seguridad
AC5	Elaborar segregación de funciones de facultades con respecto a cada activo	6.1.2. Segregación de funciones	Oficial de seguridad de la información	1 Semana	Colaboradores de la organización	Horas responsable de seguridad

AC6	Elaborar indicaciones de a quién y cómo actuar en caso de necesitar apoyo de autoridades y/o grupos de interés	6.1.3. Contacto con autoridades 6.1.4. Contacto con grupos de interés especial	Oficial de seguridad de la información	1 Semana	Manual de políticas de seguridad de la información	Horas responsable de seguridad
AC7	Incluir en el manual de buenas prácticas los lineamientos que se deben incluir en los objetivos para la gestión de los proyectos en la empresa.	6.1.5. Seguridad de la información en la gestión de proyectos	Oficial de seguridad de la información	1 Semana	Manual de políticas de seguridad de la información	Horas responsable de seguridad
AC8	Elaborar un manual de recursos humanos que sirva de apoyo en el proceso de selección y guía de las acciones a tomar durante el empleo en caso de cometerse faltas en las políticas de seguridad de la información	7.1.1. Selección. 7.1.2. Términos y condiciones del empleo 7.2.1. Responsabilidades de gestión 7.2.3. Proceso disciplinario	Oficial de seguridad de la información	1 Mes	Información	Horas responsable de seguridad
	Realizar un programa de capacitación en seguridad de la ingotmación	7.2.2. Concientización, educación y capacitación en seguridad de la información.	Oficial de Seguridad de la Información	6 Semanas	Personal	Capacitador especialista en seguridad de la información.
	Realizar un procedimiento de medios removibles	8.3.1. Manejo de medios removibles	Comité de Seguridad de la Información	2 Semanas	Equipos & Personas	Horas del responsable de seguridad de la información
AC9	Instalar cámaras de seguridad	9.1.1. Política de control de acceso	Comité de Seguridad de la Información	2 Semanas	Oficina	Uso de presupuesto asignado para la seguridad de la Informacion
AC10	Instalación de Blackouts en las ventanas con vista el exterior	11.1.3. Seguridad de oficinas, despachos y recursos	Comité de Seguridad de la Información	1 Mes	Oficina	Uso de presupuesto asignado para la seguridad de la Información
AC11	Realizar mantenimiento anual a equipos	11.2.4. Mantenimiento de equipos	Comité de Seguridad de la Información	1 Mes	Equipos	Uso de presupuesto asignado para la seguridad de la Información

Fuente. Elaboración propia

Comunicación

Para este programa se establecieron las responsabilidades con respecto a la seguridad de la información, las cuales fueron descritas para cada puesto de la estructura organizacional de la empresa, descritas en la guía propuesta en la presente investigación y titulada "Manual de Buenas Prácticas de Seguridad de la Información de L & M Seminario Group S.A.C.". (Ver anexo 07)

El documento de la política de seguridad de la información fue revisado y aprobado por el gerente general y de operaciones de la empresa, de igual manera se incluyó en el Manual de Buenas Prácticas enfocado en la Seguridad de la información para que esté a disposición de todos los colaboradores.

Por último, se definieron las siguientes acciones para lograr una comunicación efectiva:

Tabla 23

Plan de comunicaciones de la seguridad de la información

D08	PLAN DE COMUNICACIONES						
ID	ETAPA	MENSAJE (QUÉ)	CONTEXTO (CUÁNDO)	EMISOR (QUIÉN)	RECEPTOR (A QUIÉN)	PROCESOS PARA EFECTUAR LA COMUNICACIÓN (CÓMO)	RESULTADO
C01	Etapa de Planificación- Fase 03	Inicio del proyecto	A comunicar cuando se haya iniciado la etapa de planificar.	Oficial de Seguridad de la Información	Gerente General L & M Seminario Group S.A.C.	1. Presentar análisis del contexto de la organización. 2. Explicar las etapas del plan de proyecto.	Firmar Carta de Aceptación del proyecto
C02	Etapa Planificar- Fase 04	Políticas de Seguridad de la Información	A comunicar cuando se haya establecido la política rectora	Oficial de Seguridad de la Información	Gerente General y Gerente de Operaciones de L & M Seminario Group S.A.C.	1. Reunión para presentar y dialogar acerca política rectora. 2. Difundir documento a los interesados.	Manual de Buenas Prácticas de Seguridad de la Información.
CO3	Etapa Hacer – Fase 10	Acciones para el tratamiento de riesgo	A comunicar al finalizar el tratamiento de riesgos y contar con las acciones para mitigar.	Oficial de Seguridad de la Información	Comité de Seguridad de la Información.	1. Realizar cuadro de acciones y controles. 2. Reunión para presentar propuesta.	Cuadro de acciones para tratamiento de riesgos.
CO4	Etapa Hacer – Fase 12	Programa de Entrenamiento y Concientización.	A comunicar las actividades a realiza y plan de comunicación	Oficial de Seguridad de la Información	Comité de Seguridad de la información.	1. Realizar lista de actividades. 2. Reunir a comité y establecer fechas para actividades.	Manual de Buenas Prácticas enfocado en Recursos Humanos.

			mediante charlas, boletines y afiches.			3. Enviar comunicado a participantes.	
CO5	Etapa Verificar – Fase 13	Comunicar monitoreo, medición y análisis	A comunicar los indicadores y resultados de la medición.	Comité de Seguridad de la Información	Gerente General	1. Solicitar permiso y datos para realizar los indicadores. 2. Comunicar los resultados a gerencia	Informe de resultado de la evaluación de la seguridad de la información.
CO6	Etapa Verificar – Fase 14	Comunicar plan de auditoría	A comunicar el plan de auditoría	Oficial de Seguridad de la Información	Comité de Seguridad de la Información	1. Realizar reunión para explicar plan de auditoría a implementar a futuro.	Manual de plan de auditoría
C07	Etapa Verificar – Fase 15	Comunicar la revisión por gerencia	Comunicar formato de revisión de gerencia periódica o al ocurrir algún incidente de seguridad.	Oficial de Seguridad de la Información	Gerente General	1. Realizar reunión para brindar lineamientos y formato a implementar a futuro.	Formato de revisión por gerencia
CO8	Etapa Actuar – Fase 16	Comunicar mejoras propuestas	A comunicar cuando se aprueben planes de mejora.	Comité de Seguridad de la Información	Gerente General	1. Reunión con los responsables de cada acción propuesta.	Formato de plan de acciones de mejora.

Fuente. Elaboración propia

Programa de entrenamiento y concientización

El programa de entrenamiento propuesto está conformado por dos etapas, en la primera se realizó el manual de buenas prácticas para recursos y en la segunda se realizó el plan de concientización y acciones por ejecutar.

Manual de Buenas Prácticas

Se encuentra enfocado en los Recursos Humanos para que este sirva de guía a la gerencia de operaciones, el cuál va desde la selección del personal hasta la terminación o cambio de empleo del colaborador. que hace las veces del área recursos humanos; dicho manual se estructuró en antes, durante y después del empleo.

En el capítulo titulado Antes se especifica el procedimiento para realizar la selección del personal, identificando también los actores del mismo; de igual manera, se propuso la implementación y firma del acuerdo de No Divulgación de la Información (NDA) como estrategia y respaldo ante cualquier filtración de información por parte del colaborador, pues mediante este documento acepta su responsabilidad y obligación de mantener la confidencialidad de la información y la devolución y cuidado de los equipos de la organización.

A continuación, en el capítulo Durante se establece las responsabilidades de gerencia y el plan de concientización. Asimismo, en este capítulo se especifica en proceso disciplinario las medidas que la organización tomará medidas en caso incumplirse las políticas internas. Por último, en el capítulo "Después" se brindan puntos guías a tomar en cuenta al terminar o finalizar el contrato y al cambiar de funciones. (Ver Anexo 08).

Plan de concientización y acciones para ejecutar

Este plan se dividió en cinco fases: diagnóstico de necesidades de concientización, establecer el programa de concientización, ejecutarlo y evaluación del programa. El resultado de la primera fase se obtuvo aplicando un cuestionario a los ocho colaboradores de la entidad técnica; de este análisis se logró identificar los temas a cubrir en la capacitación en materia de seguridad de la información, los cuales fueron: escritorio limpio y pantalla limpia, remoción de medios y contraseñas.

En la fase del programa de concientización se realizó una capacitación acerca de la seguridad de la información (ver anexo), posteriormente se enviaron boletines informativos al correo electrónico y se colocaron afiches alusivos a los temas tratados para generar una retroalimentación. Finalmente, se realizó una evaluación (ver anexo) para poder evaluar la efectividad de la capacitación realizada.

A continuación, una síntesis de las actividades con respecto al plan de concientización se definieron las siguientes actividades:

Tabla 24

Plan de concientización de la seguridad de la información

PLAN DE CONCIENTIZACIÓN									
ID	ETAPA	ACCIÓN POR TOMAR	TIPO	ESTADO	RESPONSABLES	RECURSOS	ACTIVIDADES	INICIO	FIN
CN01	Etapa Implementar – Fase 12	Observar desempeño de los colaboradores	Capacitación	Diagnóstico de necesidades de concientización.	Comité de Seguridad de la Información	Ficha de observación.	1. Observar al personal realizar sus funciones cotidianas. 2. Registrar lo observado.	17/02/2020	19/02/2020
CN02	Etapa Implementar – Fase 12	Realizar examen sobre seguridad de la información	Evaluación	Diagnóstico de necesidades de concientización.	Oficial de la Seguridad de la información.	Cuestionario estructurad de diez preguntas.	1. Reunión con el comité para coordinaciones. 2. Aplicar cuestionario en el día planificado. 3. Realizar informe de resultados. 4. Analizar causas que llevan a necesidad de capacitación.	20/02/2020	21/02/2020
CN03	Etapa Implementar – Fase 12	Establecer temas a cubrir	Capacitación	Programa de concientización	Comité de seguridad de la información.	Informe de programa de capacitación	1. Realizar lista de temas a capacitar. 2. Realizar un cronograma para los temas.	24/02/2020	24/02/2020
CN04	Etapa Implementar – Fase 12	Realizar búsqueda de especialistas y asignación de recursos.	Capacitación	Programa de concientización	Oficial de seguridad de la información.	Informe de recursos a utlizar en capacitación.	1. Realizar búsqueda de especialista en seguridad la información. 2. Realizar recursos a utilizar como boletines y afiches.	25/02/2020	28/02/2020
CN05	Etapa Implementar – Fase 12	Realizar charlas de concientización.	Capacitación.	Ejecución de la concientización.	Oficial de Seguridad de la Información.	Informe de la capacitación.	1. Anunciar una semana antes la capacitación mediante correo corporativo. 2. Colocar afiche del primer tema a tratar en la	2/03/2020	16/03/2020

							oficina. 3. Realizar ponencia del especialista. 4. Enviar retroalimentación mediante un boletín semanal sobre el tema.		
CN06	Etapa Implementar – Fase 12	Analizar resultados post capacitación.	Evaluación.	Evaluación de la concientización.	Oficial de Seguridad de la Información.	Informe de cierre.	1. Aplicar cuestionario estructurado de diez preguntas. 2. Datar resultados y compararlos con el estado inicial. 3. Analizar si se logró el resultado y registrar puntos débiles a considerar en la próxima capacitación para lograr mejora continua.	17/03/2020	20/03/2020

Fuente. Elaboración propia

Asimismo, se realizó un cronograma para realizar estas actividades:

Tabla 25

Cronograma del plan de concientización de la seguridad de la información

ACTIVIDADES DEL PLAN	INICIO	FIN	DURACIÓN	PLAN DE ENTRENAMIENTO Y CONCIENTIZACIÓN
				SEMANA 1 (10/02 - 14/02) · SEMANA 2 (17/02 - 21/02) · SEMANA 3 (24/02 - 28/02) · SEMANA 4 (02/03 - 06/03) · SEMANA 5 (09/03 - 13/03) · SEMANA 6 (16/03 - 20/03)
				L M X J V L M X J V L M X J V L M X J V L M X J V L M X J V
11. PROGRAMA DE ENTRENAMIENTO Y CONCIENTIZACIÓN	10/02/20	20/03/20	30 días	
11.1. REALIZAR MANUAL DE BUENAS PRÁCTICAS PARA RECURSOS HUMANOS	10/02/20	14/02/20	5 días	
11.1.1. REALIZAR CAPÍTULO ANTES DE SER CONTRATADOS	10/02/20	12/02/20	3 días	
11.1.1.1. REALIZAR PROCEDIMIENTO DE SELECCIÓN DE PERSONAL	10/02/20	10/02/20	1 día	
11.1.1.2. REALIZAR ACUERDO DE NO DIVULGACIÓN NDA	10/02/20	11/02/20	2 días	
11.1.1.3. REALIZAR DECLARACIÓN JURADA DE INTERESES	11/02/20	11/02/20	2 días	
11.1.1.1. REALIZAR PROCEDIMIENTO DE SELECCIÓN DE PERSONAL	12/02/20	12/02/20	1 día	

11.1.2. REALIZAR CAPITULO DURANTE EL TRABAJO	13/02/20	13/02/20	1 día	
11.1.2.1 COMPROMISO POR PARTE DE LAS GERENCIA PARA EL ENTRENAMIENTO	13/02/20	13/02/20	1 día	
11.1.2.2. ESTABLECER LINEAMIENTOS DEL PLAN DE CAPACITACIÓN	13/02/20	13/02/20	1 día	
11.1.2.2. ESTABLECER LINEAMIENTOS DEL PLAN DE CAPACITACIÓN	13/02/20	13/02/20	1 día	
11.1.3. REALIZAR CAPÍTULO DESPUÉS DEL TRABAJO	14/02/20	14/02/20	1 día	
11.1.3.1. DEFINIR DIRECCIONAMIENTO AL FINALIZAR O TERMINAR CONTRATO	14/02/20	14/02/20	1 día	
11.1.3.2. DEFINIR DIRECCIONAMIENTO AL CAMBIAR DE FUNCIONES	14/02/20	14/02/20	1 día	
11.2. REALIZAR EL PLAN DE CONCIENTIZACIÓN Y ACCIONES POR EJECUTAR	17/02/20	20/03/20	25 días	
11.2.1. DIAGNOSTICAR NECESIDADES DE CONCIENTIZACIÓN	17/02/20	21/02/20	5 días	
11.2.1.1. OBSERVAR DESEMPEÑO DE LOS COLABORADORES	17/02/20	19/02/20	3 días	
11.2.1.2. REALIZAR EXAMEN SOBRE SEGURIDAD DE LA INFORMACIÓN	20/02/20	20/03/20	1 día	

11.2.1.3. ANALIZAR RESULTADOS DEL EXAMEN DE SEGUIRDA DE INFORMACIÓN	21/02/20	21/02/20	1 día
11.2.2. ESTABLECER PROGRAMA DE CONCIENTIZACIÓN	24/02/20	28/02/20	5 días
11.2.1.2. ESTABLECER TEMAS A CUBRIR	24/02/20	24/02/20	1 día
11.2.1.2. REALIZAR BÚSQUEDA DE ESPECIALISTAS Y ASIGNACIÓN DE RECURSOS	25/02/20	28/02/20	4 días
11.2.3. EJECUTAR PROGRAMA DE CONCIENTIZACIÓN	2/03/20	16/03/20	11 días
11.2.3.1. REALIZAR CHARLA DE CONCIENTIZACIÓN: LA SEGURIDAD DE LA INFORMACIÓN.	2/03/20	2/03/20	1 día
11.2.3.1.1. COLOCAR AFICHE ALUSIVO AL TEMA ESCRITORIO LIMPIO	3/03/20	3/03/20	1 día
11.2.3.1.2. ENVIAR BOLETÍN INFORMATIVO SOBRE ESCRITORIO LIMPIO	6/03/20	6/03/20	1 día
11.2.3.1.1. COLOCAR AFICHE ALUSIVO AL TEMA MEDIOS REMOVIBLES	9/03/20	9/03/20	1 día
11.2.3.1.2. ENVIAR BOLETÍN INFORMATIVO SOBRE MEDIOS REMOVIBLES	12/03/20	12/03/20	1 día

11.2.3.1.1. COLOCAR AFICHE ALUSIVO AL TEMA CONTRASEÑAS	13/03/20	13/03/20	1 día	
11.2.3.1.2. ENVIAR BOLETÍN INFORMATIVO SOBRE CONTRASEÑAS	16/03/20	16/03/20	1 día	
11.2.4. EVALUAR EL PROGRAMA DE CONCIENTIZACIÓN	17/03/20	20/03/20	4 días	
11.2.1.2. REALIZAR EVALUACIÓN POST PROGRAMA DE CONCIENTIZACIŒN	17/03/20	17/03/20	1 día	
11.2.1.2. ANALIZAR RESULTADOS POST CAPACITACIÓN	18/03/20	18/03/20	1 día	

Fuente. Elaboración propia

3.9. Verificar

Prueba Post test

Para verificar el cumplimiento de los objetivos de la presente investigación se ha realizado una prueba post test en base a los indicadores propuestos para las variables de investigación.

Variable Independiente – Seguridad de la Información

Estratégico

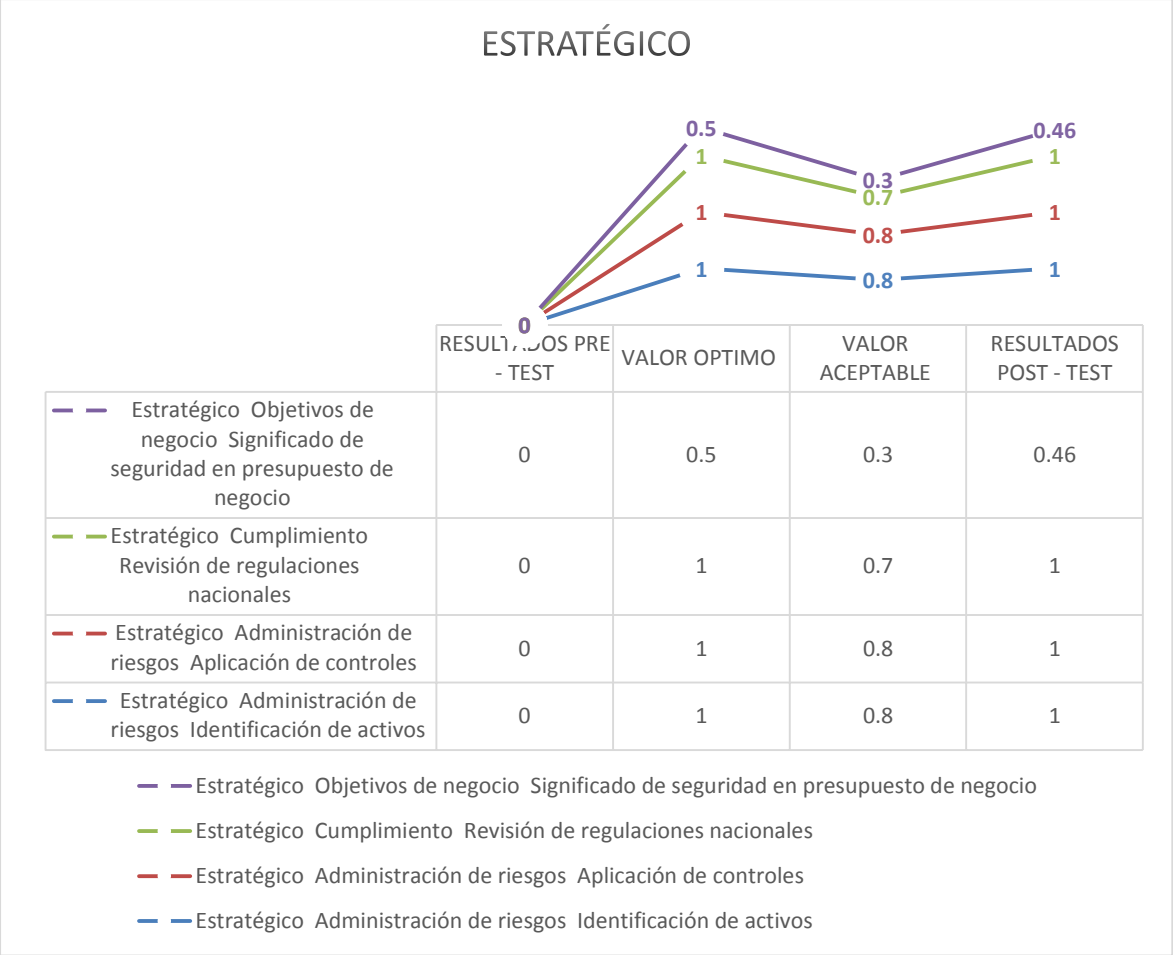
Dentro de las categorías administración de riesgos, se encontró los resultados de los siguientes tres indicadores:

Identificación de activos: Se realizó el etiquetado, de los 29 activos identificados, además de asignarles un propietario, se obtuvo un índice de 1, logrando así alcanzar el valor óptimo.

Aplicación de controles: De los 25 controles planificados en esta investigación, se implementaron todos en su totalidad, alcanzando el índice óptimo, es decir 1.

En la categoría de cumplimiento se obtuvo que el número de revisiones que debería realizarse son seis, es decir una mensualmente; se obtuvo un índice 1, logrando entonces ejecutar las seis revisiones mensuales.

En la categoría de objetivos de negocio, se logró la aprobación para hacer uso de S/ 20 780 soles de los S/ 45 000 que la empresa tenía asignado para implementaciones de mejora, logrando alcanzar un resultado de 0.46.



	RESULTADOS PRE - TEST	VALOR OPTIMO	VALOR ACEPTABLE	RESULTADOS POST - TEST
Estratégico Objetivos de negocio Significado de seguridad en presupuesto de negocio	0	0.5	0.3	0.46
Estratégico Cumplimiento Revisión de regulaciones nacionales	0	1	0.7	1
Estratégico Administración de riesgos Aplicación de controles	0	1	0.8	1
Estratégico Administración de riesgos Identificación de activos	0	1	0.8	1

Estratégico Objetivos de negocio Significado de seguridad en presupuesto de negocio
Estratégico Cumplimiento Revisión de regulaciones nacionales
Estratégico Administración de riesgos Aplicación de controles
Estratégico Administración de riesgos Identificación de activos

Figura 28. Resultados post test de la dimensión estratégica

Fuente. Elaboración propia

Táctico

Se obtuvo como resultado del indicador licencias del antivirus, cero infecciones luego de poner en marcha el antivirus en todos los ordenadores de la empresa (Ver anexo). Se obtuvo también que con la implementación del antivirus, ninguna de las diez aplicaciones evaluadas fueron infectadas, logrando así disminuir la vulnerabilidad de los mismos.

En la categoría servicios, el indicador de corrección de errores de backups, se obtuvo como resultado 0 fallas encontradas en los 5 ordenadores evaluados en la segunda

prueba de restauración de la data, a diferencia de las catorce encontradas en la primera prueba realizada a los 5 ordenadores.

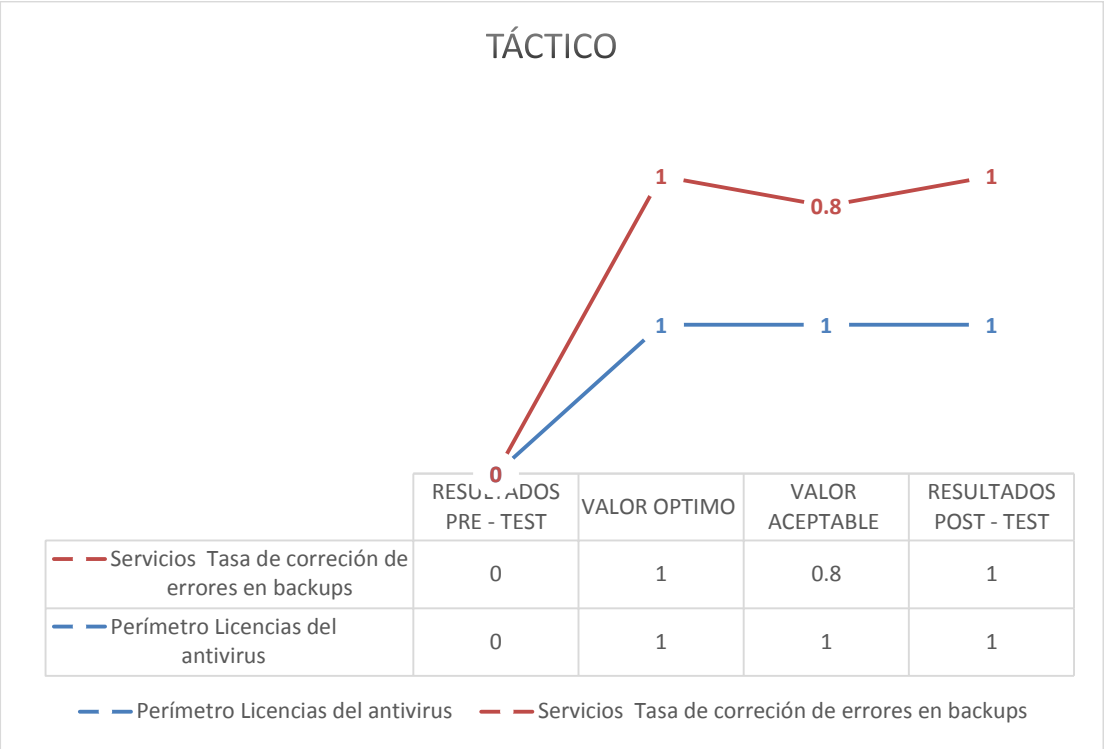


Figura 29. Resultados post test de la dimensión táctica

Fuente. Elaboración propia

Operativo

En la categoría de confidencialidad, el indicador de educación en seguridad de la información se midió aplicando un cuestionario (ver anexo 19) a todos los colaboradores después de realizar el programa de capacitación en seguridad de la información, encontrando que los colaboradores en su totalidad lo aprobaron (ver anexo 20).

A continuación, se presenta una síntesis de las preguntas englobandolas según criterios críticos encontrados en el pre – test, los cuales fueron tratados en la capacitación; por consiguiente, en el post test se realizaron tres preguntas para

evaluar la efectividad de la capacitación para cada criterio, plasmado en el siguiente cuadro comparativo entre los resultados pre y post test:

Tabla 26

Resultados post test de los criterios evaluados en el cuestionario aplicado a los colaboradores acerca de la seguridad de la información.

Criterio evaluado	Alternativa	Pre-test	Post - test	Variación
Escritorio limpio y pantalla limpia	Incorrectas	100%	17%	-83%
	Correctas	0%	83%	0%
Remoción de medios	Incorrectas	75%	25%	-67%
	Correctas	25%	75%	200%
Contraseñas	Incorrectas	100%	8%	-92%
	Correctas	0%	92%	0%
Media total	**Incorrectas**	**92%**	**17%**	**-82%**
	Correctas	**8%**	**83%**	**900%**

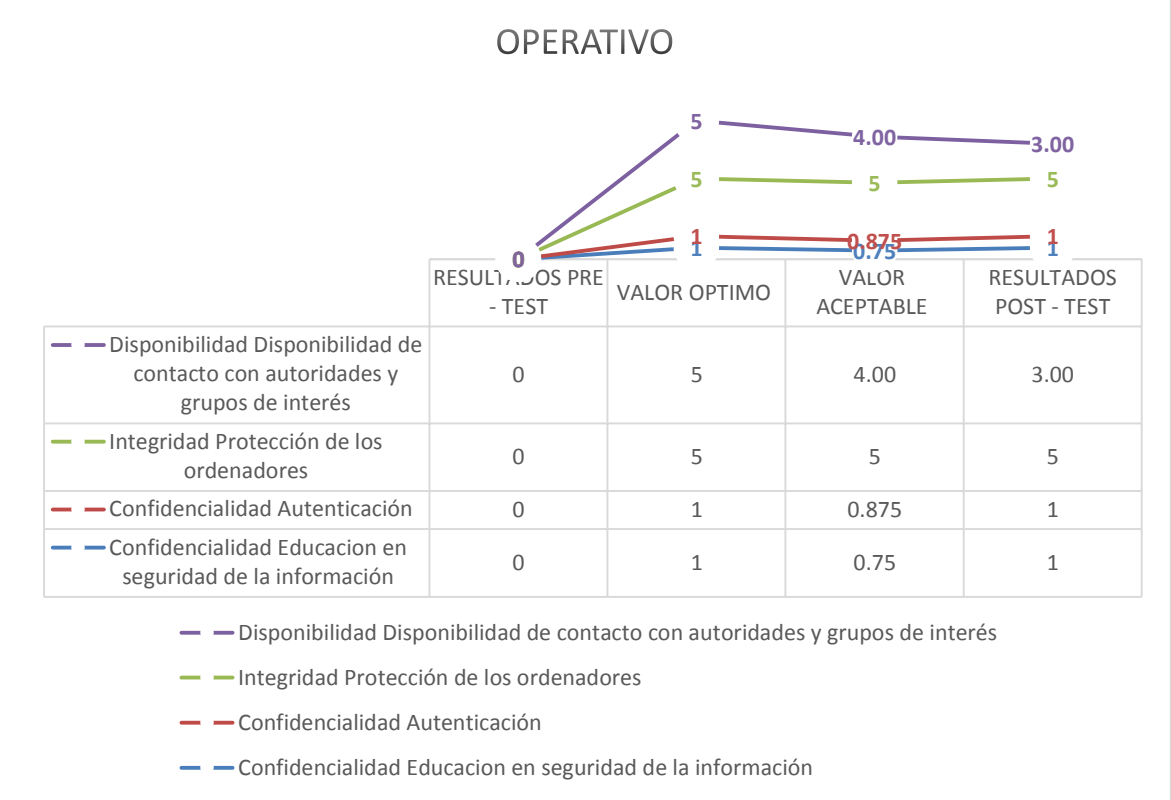
Fuente. Elaboración propia

Por último, en el indicador autenticación se obtuvo que los 8 colaboradores de la empresa cuentan ahora con un ID único, por lo tanto, se alcanzó el índice óptimo de uno (1). Asimismo, se realizó una guía práctica para crear usuario de Windows, la cual fue proporcionada al CISO (ver anexo 21)

Dentro de la categoría de integridad, en el indicador protección de los ordenadores se logró que los cinco equipos cuenten con capacidad de encriptación, obteniendo un índice perfecto. Además, se proporcionó al CISO un manual para encriptar el disco duro de los ordenadores (ver anexo 23)

En la última categoría de disponibilidad, para el indicador la disponibilidad para el contacto con autoridades y grupos de interés, se establecieron tres contactos: los

derechos ARCO, CERTIPRO y el foro de seguridad de la información "Wilders Security".



	RESULTADOS PRE - TEST	VALOR OPTIMO	VALOR ACEPTABLE	RESULTADOS POST - TEST
Disponibilidad Disponibilidad de contacto con autoridades y grupos de interés	0	5	4.00	3.00
Integridad Protección de los ordenadores	0	5	5	5
Confidencialidad Autenticación	0	1	0.875	1
Confidencialidad Educacion en seguridad de la información	0	1	0.75	1

Figura 30. Resultados post test de la dimensión operativa

Fuente. Elaboración propia

Variable Dependiente – Gestión Documental

Enfoque Clásico

Se obtuvo en el primer indicador de eficiencia que las 12 formas propuestas listadas a continuación, se utilizaron en su totalidad; logrando así un índice de 1.

Tabla 27

Formatos identificados en post test del enfoque clásico

ID	Formatos identificados	Aplicada Sí	Aplicada No
D01	Formato para segregación de funciones	X	
D02	Formato para identificar activos	X	
D03	Formato para evaluar los riesgos	X	
D04	Formato para tratamiento de riesgos	X	
D05	Formato de acciones para el tratamiento de riesgos	X	

D06	Cuadro de registro de control de acceso	X
D07	Formato de remoción de activos	X
D08	Formato de examen de conocimientos	X
D09	Formato para plan de comunicaciones	X
D10	Formato para auditoría	X
D11	Formato para revisión por gerencia	X
D12	Fomato para las acciones de mejora	X

Fuente. Elaboración propia

Se logró implementar controles para el acceso a las instalaciones físicas, instalando cámaras de seguridad y alarmas en las ventanas, logando proteger los puntos de acceso.

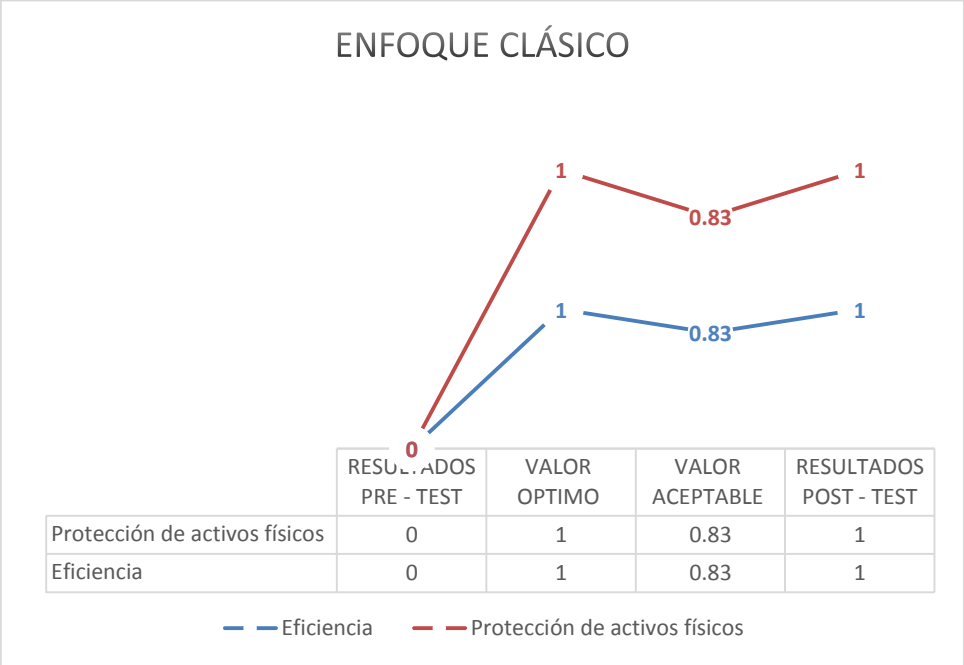


Figura 31. Resultados post test del enfoque clásico

Fuente. Elaboración propia

Enfoque Digital

En el indicador de planes de actualización y seguimiento: Se propusieron tres planes de actualización y seguimiento y los tres fueron ejecutados. De esta manera se obtuvo un índice de uno.

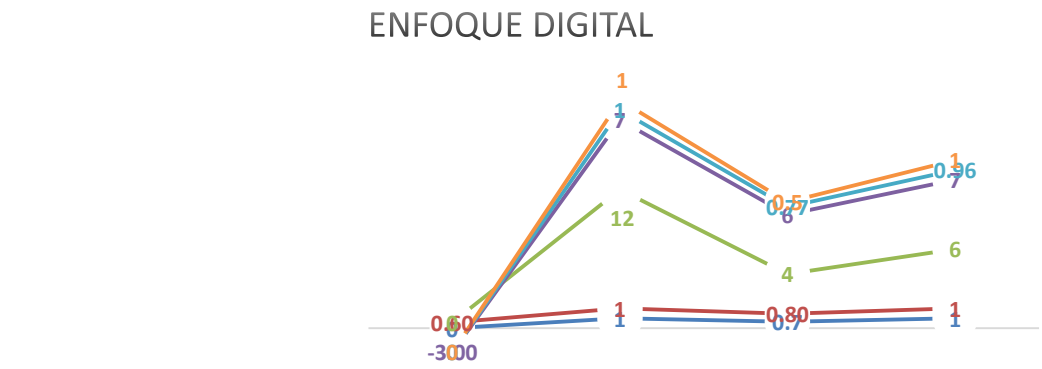
Asimismo, se halló del indicador titulado pruebas de vulnerabilidad de software que, de los diez softwares en los cinco ordenadores de la empresa, ninguno presentó vulnerabilidad, obteniendo un índice de uno.

Se identificó que se debería realizar una copia de respaldo mensualmente. Tomando como datos que se realizaron 6 copias de respaldo en los seis meses de la investigación se logró alcanzar el índice óptimo de 1. De igual manera, se documentó el procedimiento para realizar una copia de seguridad, el cual se le proporcionó a cada usuario de los equipos (ver anexo 22)

Por otro lado, en el indicador grado de protección de los activos se obtuvo que ninguna persona no autorizada pudo acceder a los sistemas de información, esto fue logrado estableciendo un usuario y contraseña para acceder al equipo.

En el indicador de accesibilidad a la documentación de hardware y software, se logró identificar y archivar 25 manuales de usuarios de los 26 productos, obteniendo un índice de 0.96.

Para finalizar, el indicador de capacitación se logró instruyendo al personal encargado de gestión documental con herramientas digitales para el almacenamiento de los archivos, es así como se obtuvo un índice 1.



	RESULTADOS PRE - TEST	VALOR OPTIMO	VALOR ACEPTABLE	RESULTADOS POST - TEST
Enfoque Digital Capacitación	0	1	0.5	1
Enfoque Digital Accesibilidad a la documentación de hardware/software	0	1	0.77	0.96
Enfoque Digital Grado de protección de los sistemas de información de sujetos no autorizados.	-3.00	7	6	7
Enfoque Digital Copias de respaldo	0	12	4	6
Enfoque Digital Pruebas de vulnerabilidad del software	0.60	1	0.80	1
Enfoque Digital Planes de actualización y seguimiento	0	1	0.7	1

Figura 32. Resultados post test del enfoque digital

Fuente. Elaboración propia

Herramienta propuesta para monitoreo interno

En cuanto a la medición del desempeño de los controles implantados, se buscó la forma de llevar un registro y dirección de estos. Para ello, se calificó el porcentaje de importancia dentro de cada objetivo de control implementado, asignándole un peso y definiendo los criterios óptimos, aceptable y no aceptable. Se recomienda que sea el CISO quien realice este monitoreo de manera semestral.

Tabla 28

Rúbrica para monitoreo interno de los indicadores

Objetivo de Control NTP ISO/IEC 27002:2016	Controles	ID	PESO	CRITERIO OPTIMO (PESO TOTAL)	CRITERIO ACEPTABLE (PESO PARCIAL)	NO ACEPTABLE
5.1. DIRECTRICES EN SEGURIDAD DE LA INFORMACIÓN	5.1.1. Políticas para la seguridad de la información	PS1	70%	Implementación total de las políticas planificadas	Implementación del 50% de las políticas planteadas	No haber implementado las políticas establecidas
	5.1.2. Revisión de las políticas para la seguridad de la información.	PS2	30%	Haber realizado tres revisiones anuales	Haber realizado una revisión anual	No haber realizado ninguna revisión
6.1. ORGANIZACIÓN INTERNA	6.1.1. Roles y responsabilidades en seguridad de la información	OI1	20%	Haber establecido roles y responsabilidades para todos los integrantes del comité	Haber establecido roles y responsabilidades para el CISO	No haber realizado ninguna revisión
	6.1.2. Segregación de funciones	OI2	10%	Implementar la segregación de funciones en los 8 colaboradores	Implementar la segregación de funciones en administrativos	No poner en práctica la segregación de funciones
	6.1.3. Contacto con autoridades	OI3	5%	Haber identificado tres autoridades para comunicación de temas relaciones a IS	Haber identificado dos autoridades para comunicación de temas relaciones a IS	No haber implementado las políticas establecidas
	6.1.4. Contacto con grupos de interés especial	OI4	5%	Haber identificado cinco grupos de interés en IS	Haber identificado tres grupos de interés en IS	No haber identificado grupos de interés en IS
	6.1.5. Seguridad de la información en la gestión de proyectos	OI5	10%	Haber cumplido los 3 objetivos para la gestión de proyectos	Haber cumplido con 2 objetivos para la gestión de proyectos	Haber cumplido con 1 objetivo para la gestión de proyectos

6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO	6.2.1. Política de dispositivos móviles	DM1	25%	Haber cumplido los 8 lineamientos de la política de dispositivos móviles	Haber cumplido 6 lineamientos de la política de dispositivos móviles	Haber cumplido 2 lineamientos de la política de dispositivos móviles
	6.2.2. Teletrabajo	DM2	25%	Haber cumplido los 8 lineamientos de la política de teletrabjo	Haber cumplido 6 lineamientos de la política de teletrabjo	Haber cumplido 2 lineamientos de la política de teletrabjo
7.1. ANTES DE LA CONTRATACIÓN	7.1.1. Selección.	AC1	60%	Haber implementado el procedimiento de selección	Haber implementado los lineamientos del procedimiento de selección	No haber implementado el procedimiento de selección
	7.1.2. Términos y condiciones del empleo	AC2	40%	Haber comunicado a los 8 colaboradores los términos y condiciones del empleo y haber enviado por correo documento informativo	Haber comunicado a los 8 colaboradores los términos y condiciones del empleo	No haber comunicado a los colaboradores en su totalidad los términos y condiciones del empleo
7.2. DURANTE LA CONTRATACIÓN	7.2.1. Responsabilidades de gestión	DC1	25%	El Gerente General ha asistido a reuniones y enviado compromiso con la seguridad de la información	El Gerente General ha asistido a reuniones de seguridad de la información	El Gerente General no ha asistido a reuniones de seguridad de la información
	7.2.2. Concientización, educación y capacitación en seguridad de la información.	DC2	50%	Haber realizados tres programas de capación al año	Haber realizado dos programas de capacitación al año	No haber realizado ningún programa de capacitación
	7.2.3. Proceso disciplinario	DC3	25%	Haber comunicado de manera escrita y verbal el proceso disciplinario a los colaboradores	Haber comunicado de manera escrita el proceso disciplinario	No haber comunicado el proceso disciplinario
8.1. RESPONSABILIDAD POR LOS ACTIVOS	8.1.1. Inventario de activos	RA1	50%	Haber inventariado todos los activos de la organización	Haber inventariado los activos críticos de la organización	No haber realizado inventario de activos
	8.1.4. Retorno de activos	RA2	50%	Haber seguido el procedimiento para retorno de activos al finalizar el contrato	Haber registrado solo la salida y entrada de activo mas no el estado	No haber seguido el procedimiento para retorno de activos
8.2. CLASIFICACIÓN DE LA INFORMACIÓN	8.2.1. Clasificación de la información	CI1	40%	Haber clasificado información en término de confidencialidad, disponibilidad e integridad. Así como identificar tipo de activo, ubicación y frecuencia de uso.	Haber clasificado información en término de confidencialidad, disponibilidad e integridad	No haber clasificado información en término de confidencialidad, disponibilidad e integridad
	8.2.3. Manejo de activos	CI2	60%	Protección de la información original, teniendo los antivirus activos.	Protección de la información original, teniendo los antivirus activos.	No tener la protección de la información original,

						teniendo las licencias de antivirus caducadas.
8.3. MANEJO DE MEDIOS	8.3.1. Gestión de medios removibles	MM1	100%	Seguir el procedimiento de remoción de activos y hacer uso del equipo fuera de la compañía en ambiente seguro	Seguir el procedimiento de remoción de activos y hacer uso del equipo fuera de la compañía en ambiente seguro	No haber seguido el procedimiento para remoción de medios removibles
9.1. REQUISITOS DE NEGOCIO PARA CONTROL DE ACCESO	9.1.1. Política de control de acceso	CA1	100%	Haber revisado derechos de acceso de usuarios, acceso a redes y servicios de red y registro y baja de usuarios.	Haber revisado derechos de acceso de usuarios, así como registro y baja de usuarios	No haber revisado la política de control de accesos
11.1. AREAS SEGURAS	11.1.3. Seguridad de oficinas, despachos y recursos	AS1	100%	Haber asegurado los 8 accesos a las instalaciones físicas	Haber asegurado 6 accesos a las instalaciones físicas	No haber asegurado accesos a las instalaciones físicas
11.2. SEGURIDAD DE LOS EQUIPOS	11.2.4. Mantenimiento de equipos	SE1	40%	Haber realizado 2 mantenimientos anuales a todos los equipos de la organización	Haber realizado 1 mantenimiento anual a todos los equipos de la organización	No haber realizado mantenimiento anual a equipos de la organización
	11.2.8. Equipo de usuario desatendido	SE2	20%	Los 8 colaboradores bloquean sus equipos cuando no están haciendo uso de ellos	Seis (6) colaboradores bloquean sus equipos cuando no están haciendo uso de ellos	Tres colaboradores bloquean sus equipos cuando no están haciendo uso de ellos
	11.2.9. Política de escritorio limpio y pantalla limpia	SE3	40%	Los 8 colaboradores ponen en práctica los 4 lineamientos de la política	Los 8 colaboradores ponen en práctica los 2 lineamientos de la política	No haber revisado la política de control de accesos
15. RELACIONES CON PROVEEDORES	15.1.1. Política de seguridad de la información en relaciones con los proveedores	RP1	100%	Se siguen los 6 lineamientos de la política en las relaciones con los proveedores	Se siguen 4 lineamientos de la política en las relaciones con los proveedores	No se siguen los lineamientos de la política en las relaciones con los proveedores

Fuente. Elaboración propia

Propuesta de plan de auditoría para el sistema de seguridad de la información.

Se realizó un "Manual de Buenas Prácticas. Auditoría enfocada en la seguridad de la información" en la cual se utilizó los lineamientos de la ISO/IEC 27007 y específicamente la guía de auditoría para los sistemas de seguridad de la información del anexo A. Es así que se propuso un cuadro guía por cada punto a auditar, señalando en cada uno de ellos las entradas que debe tener el auditor como "Evidencias del Auditor" y las principales actividades que debe realizar en este seguimiento. (Ver anexo 12).

Revisión por la gerencia

La revisión por gerencia se realizará teniendo como objetivo encontrar oportunidades de mejora o necesidades de cambio en la seguridad de la información, esto incluye la verificación de los siguientes documentos:

Tabla 29

Plan de revisión por gerencia

D10	PLAN DE REVISIÓN POR GERENCIA				
ID	ETAPA	ACCIÓN POR TOMAR	FUENTE	RESPONSABLES	ACTIVIDADES
RE01	Etapa Verificar– Fase 15	Revisar política de seguridad de la información.	Política de Seguridad de la Información.	Gerente General	1. Revisar alcance y lineamientos de la política, verificar si estos han cambiado. 2. Revisar políticas específicas. 3. Revisar roles y responsabilidades en las políticas específicas.

RE02	Etapa Verificar – Fase 15	Revisar resultados del plan de tratamiento de riesgos.	Informe de tratamiento de riesgos	Gerente General.	1. Revisar metodología usada para la evaluación de riesgos. 2. Revisar controles propuestos para tratar los riesgos verificándolos con ISO/IEC 27002:2013.
RE03	Etapa Verificar – Fase 15	Revisar resultados de programa de capacitación	Informe de cierre de plan de capacitación.	Gerente General.	1. Revisar temas tratados en la concientización 2. Revisar resultados obtenidos después de realizada la capacitación. 3. Verificar los recursos utilizados para su ejecución.
RE04	Etapa Verificar– Fase 15	Revisar resultados de evaluación de desempeño de la seguridad de la información.	Informe de evaluación de desempeño. Informe de objetivos de seguridad de la información.	Gerente General.	1. Revisar la metodología de medición. 2. Revisar resultados de las métricas de seguridad de la información implementadas.
RE05	Etapa Verificar– Fase 15	Revisar plan de mejora continua.	Informe de objetivos de Seguridad de la Información. Informe de auditoría.	Gerente General.	1. Analizar los resultados de todos los esfuerzos realizados. 2. Proponer acciones para la mejora continua.

Fuente. Elaboración propia

Actuar

En la fase de actuar se propuso un proceso de mejora continua (Ver anexo 25) y un formato para el plan de acciones de mejora, el cual se determinó que su tipología puede ser acciones de mejora o correctivas. Las primeras se hallan de las oportunidades de mejora identificadas en las auditorías o en la revisión por gerencia; mientras que las acciones correctivas nacen de las no conformidades halladas. Para ambas se describirán el estado actual o justificación por las que se han identificado la no conformidad o la oportunidad de mejora, de igual manera se determinarán los responsables, recursos y actividades a tomar (Ver anexo 24).

Prueba de hipótesis

Comparación de Resultado de la Variable Dependiente

La investigación aplicada a la gestión documental de la entidad técnica L & M Seminario Group S.A.C. es de tipo longitudinal, a continuación, se describe el establecimiento de hipótesis.

Establecimiento de la hipótesis nula – alternativa:

H0: No existe un cambio significativo en la gestión documental antes ni después de la implementación de la seguridad información en la entidad técnica L & M Seminario Group S.A.C. de la ciudad de Trujillo.

H1: Existe un cambio significativo en la gestión documental antes y después de la implementación de la seguridad información en la entidad técnica L & M Seminario Group S.A.C. de la ciudad de Trujillo.

Tabla 30

Regla de decisión y nivel de significancia

Nivel de confianza	95% = 0.95	
Nivel de significancia	5% = 0.05	
Regla de decisión	p < 0.05	Se rechaza Hipótesis Nula (H0)
	p > 0.05	Se acepta Hipótesis Nula (H0)

Fuente. Elaboración propia

Teniendo como entrada estos datos, se realizó la prueba T- Student a los 8 indicadores evaluados en la matriz de operacionalizacion de la variable gestión documental. Se pudo afirmar que sí existe una diferencia significativa en la misma pues se obtuvo como resultado que p = 0.024 < 0.05, rechazando la hipótesis nula y aceptando que sí existe un cambio significativo de la gestión documental entre el antes y después de la implementación de la seguridad información en la entidad técnica L & M Seminario Group S.A.C. de la ciudad de Trujillo.

Tabla 31

Prueba estadística T-student de la variable gestión documental

Estadísticas de grupo					
Estado		N	Media	Desviación estándar	Media de error estándar
Indicador_Gestion_Documental	1,00	8	-.3000	1.11098	.39279
	2,00	8	2.3625	2.56790	.90789

Fuente. Elaboración propia

Tabla 32

Prueba estadística de muestras independientes de la variable gestión documental

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Indicador_ Gestion_ Documental	Se asumen varianzas iguales	6.431	.024	-2.692	14	.018	-2.66250	.98922	-4.78416	-.54084
	No se asumen varianzas iguales			-2.692	9.532	.024	-2.66250	.98922	-4.88137	-.44363

Fuente. Elaboración propia

Comparación de Resultado de la Variable Independiente

La investigación aplicó la seguridad de la información al proceso de gestión documental de la entidad técnica L & M Seminario Group S.A.C., a continuación, se realiza la prueba t para determinar si los datos pre y post test dieron como resultado cambios significativos.

H0: La seguridad de la información no presenta cambios significativos antes ni después de su implementación en la entidad técnica L & M Seminario Group S.A.C. de la ciudad de Trujillo.

H1: La seguridad de la información presenta cambios significativos después de su implementación en la entidad técnica L & M Seminario Group S.A.C. de la ciudad de Trujillo.

Tabla 33

Prueba estadística T-student de la variable seguridad de la información

Estadísticas de grupo

Estado		N	Media	Desviación estándar	Media de error estándar
Indicador_Seguridad_Informacion	1,00	10	0.0000	0.00000	0.00000
	2,00	10	6.1000	14.08269	4.45334

Fuente. Elaboración propia

Tabla 34

Prueba estadística de muestras independientes de la variable seguridad de la información

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Indicador_ Seguridad_ Informacion	Se asumen varianzas iguales	4.992	.038	-1.370	18	.188	-6.10000	4.45334	-15.45612	3.25612
	No se asumen varianzas iguales			-1.370	9.000	.204	-6.10000	4.45334	-16.17415	3.97415

Fuente. Elaboración propia

En la tabla se comprueba que el valor de p=0.038 < 0.05 por lo que se rechaza la hipótesis nula y se acepta la hipótesis que la seguridad de la información presenta cambios significativos después de su implementación en la entidad técnica L & M Seminario Group S.A.C. de la ciudad de Trujillo.

Análisis económico

ITEMS	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
INVERSIÓN DE ACTIVOS TANGIBLES						
UTILES DE ESCRITORIO						
Hoja bond A4	S/387	S/129	S/129	S/129	S/129	S/129
Lapiceros	S/50	S/30	S/30	S/30	S/30	S/30
Separador Divisiones A4	S/73	S/44	S/44	S/44	S/44	S/44
Archivadores	S/15	S/15	S/15	S/15	S/15	S/15
Perforador	S/15	S/15	S/15	S/15	S/15	S/15
Folder A4	S/22	S/22	S/22	S/22	S/22	S/22
Sobres A4	S/20	S/20	S/20	S/20	S/20	S/20
EQUIPOS DE OFICINA						
Computadora	S/2,500					
Impresora Multifuncional	S/1,200					
Cámaras de seguridad	S/1,500					
Disco duro externo 2 TB	S/350					
USB 16 GB	S/100					
Tóner de impresora	S/250					
Escritorio	S/500					
Silla de escritorio	S/250					
Chapa para estanterías	S/60					
Depreciación		S/1,040	S/1,040	S/1,040	S/1,040	S/1,040
SERVICIOS						
Asesoría de sistemas	S/1,200					
Mantenimiento de equipos	S/1,500	S/1,500	S/1,500	S/1,500	S/1,500	S/1,500
Capacitador IS	S/2,000					
Afiches de IS	S/100					
Diseño de boletines informativos	S/170					
Instalación de Cámaras de Seg	S/200					
Antivirus	S/150	S/150	S/150	S/150	S/150	S/150
Internet	S/80	S/80	S/80	S/80	S/80	S/80
Telefonía	S/100	S/100	S/100	S/100	S/100	S/100
EQUIPO operativos						
Cámara fotográfica	S/1,500					
Depreciación		S/750	S/750	S/750	S/750	S/750
OTROS GASTOS						
Refrigerio	S/400	S/400	S/400	S/400	S/400	S/400
Movilidad	S/800	S/800	S/800	S/800	S/800	S/800
Investigadoras de IS	S/4,000	S/2,000	S/2,000	S/2,000	S/2,000	S/2,000
TOTAL DE GASTOS	**S/19,492**	**S/7,094**	**S/7,094**	**S/7,094**	**S/7,094**	**S/7,094**

Tabla Resumen de Ahorro Proyectado Anualmente

CONCEPTO DEL AHORRO	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Eficiencia en la gestión de activos confidenciales	S/ 18,432.00	S/ 18,432.00	S/ 18,432.00	S/ 18,432.00	S/ 18,432.00
Eficiencia operativa de los ordenadores por mantenimientos correctivo	S/ 1,500.00	S/ 1,500.00	S/ 1,500.00	S/ 1,500.00	S/ 1,500.00
Eficiencia operativa de colaboradores concientizados en seguridad de la información	S/ 2,880.00	S/ 2,880.00	S/ 2,880.00	S/ 2,880.00	S/ 2,880.00
Eficiencia en el control de acceso	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00
TOTAL	**S/ 23,812.00**	**S/ 23,812.00**	**S/ 23,812.00**	**S/ 23,812.00**	**S/ 23,812.00**

Flujo de Caja

FLUJO DE CAJA LIBRE INCREMENTAL						
DESCRIPCION	**año 0**	**año 1**	**año 2**	**año 3**	**año 4**	**año 5**
Ingresos		S/. 23,812.00	S/. 23,812.00	S/. 23,812.00	S/. 23,812.00	S/. 23,812.00
Costos		S/. 7,094.00	S/. 7,094.00	S/. 7,094.00	S/. 7,094.00	S/. 7,094.00
UTILIDAD BRUTA		S/16,718.00	S/16,718.00	S/16,718.00	S/16,718.00	S/16,718.00
Gasto de Administración y Venta						
UTILIDAD O PERDIDAD OPERATIVA		S/16,718.00	S/16,718.00	S/16,718.00	S/16,718.00	S/16,718.00
Impuesto a la Renta						
Inversiones	**S/19,492.00**					
Activo Fijo						
Intangible						
Capital de Trabajo						
FLUJO DE CAJA LIBRE	**-S/19,492.00**	**S/16,718.00**	**S/16,718.00**	**S/16,718.00**	**S/16,718.00**	**S/16,718.00**
FLUJO DE CAJA DESCONTADA		**S/15,479.63**	**S/14,332.99**	**S/13,271.29**	**S/12,288.23**	**S/11,377.99**

Flujo Neto de Efectivo

Año de	Ingresos	Egresos totales	Inversiones para el proyecto		Cap de trab.	Valor de Rescate Valor Residual	Recup. De cap. De Trab.	Flujo Neto de Efectivo
			Fija	Diferida				
0		S/19,491.60						-S/19,491.60
1	S/23,812.00	S/7,094.00	S/0.00	S/0.00	S/0.00			S/16,718.00
2	S/23,812.00	S/7,094.00						S/16,718.00
3	S/23,812.00	S/7,094.00						S/16,718.00
4	S/23,812.00	S/7,094.00						S/16,718.00
5	S/23,812.00	S/7,094.00				S/0.00	S/0.00	S/16,718.00

Cálculo del VAN, TIR Y B/C

Año de operación	Costos totales (S/)	Beneficios totales (S/)	Factor de actualización 12.00%	Costos actualizados (S/)	Beneficios actualizados (S/)	Flujo neto de efectivo act. (S/)
0	S/19,491.60	S/0.00	S/1.00	S/19,491.60	S/0.00	-S/19,491.60
1	S/7,094.00	S/23,812.00	S/0.89	S/6,333.93	S/21,260.71	S/14,926.79
2	S/7,094.00	S/23,812.00	S/0.80	S/5,655.29	S/18,982.78	S/13,327.49
3	S/7,094.00	S/23,812.00	S/0.71	S/5,049.37	S/16,948.91	S/11,899.54
4	S/7,094.00	S/23,812.00	S/0.64	S/4,508.37	S/15,132.96	S/10,624.59
5	S/7,094.00	S/23,812.00	S/0.57	S/4,025.33	S/13,511.57	S/9,486.24
Total	**S/47,867.60**	**S/119,060.00**		**S/45,063.88**	**S/85,836.93**	**S/40,773.05**

Los indicadores financieros que arroja el proyecto son:

VAN=	**40,773.05**	**Se acepta**
TIR =	**81.40%**	**Se acepta**
B/C =	**1.90**	**Se acepta**

El resultao del valor actual neto, teniendo como base una tasa de descuento del 12% aplicable en función del tipo de interés del mercado, es de S/ 40, 773.05, lo cual significa que la implementación de la seguridad de la información en la gestión documental representa una propuesta rentable para la entidad técnica. De igual manera, la tasa interna de retorno señala un rentabilida de la inversión del 81.40%, el cual superó las expectativas de los interesados del proyecto. A su vez, el indicador de Beneficio Costo es de 1.90, el cual superó el parámetro de 1, confirmando nuevamente la rentabilidad del proyecto pues por cada sol invertido en el proyecto se obtiene una ganancia de 0.90 cétimos.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1. **Discusión**

La presente investigación tuvo como propósito determinar la influencia de la seguridad de la información en la gestión documental de la entidad Técnica L & M Seminario Group S.A.C. Para ello, como punto de partida se realizó el análisis de los requerimientos de seguridad de la información para la protección de los activos sensibles. Esto concuerda con la investigación de Suarez (2015) la cual indica que la información y datos son el activo más imperante de una organización por lo que es importante la implementación de un sistema de gestión de seguridad de la información orientado a las necesidades del negocio y fundamentado en las buenas prácticas de la ISO/IEC 27001:2013. Para la determinación de estas necesidades se aplicaron dos técnicas, la entrevista a la alta dirección; así como los cuestionarios a los colaboradores de la organización. Esta última técnica coincide con Vilca (2017) en donde se encuestó a los 33 colaboradores de la empresa, la misma que determinó la falta de concientización en seguridad de la información, evidenciando la existencia de esta necesidad.

Además, para el diseño de seguridad de la información se tomó en cuenta la investigación de Lema & Donoso (2018) quienes implementaron 6 fases basándose en las cláusulas 4 a la 10 de ISO/IEC 27001. Desde otra perspectiva, Suárez (2015) propuso 7 fases las cuales son la definición de la situación actual, el análisis de riesgos, la identificación y valoración de activos corporativos, la identificación, evaluación y clasificación de amenazas, la evaluación de controles de la ISO/IEC 27003, un esquema documental del sistema y la definición de políticas. Ambos diseños difieren de la presente tesis pues si bien es cierto se tomó como referencia el modelo de mejora

continua de la ISO 27001, también se propuso integrar los lineamiento de la ISO 27003 para el desarrollo de la seguridad de la información en 15 fases.

Por otra parte, fue necesario realizar la aplicación de 25 controles para minimizar los riesgos. En el análisis Lema & Donoso (2018) obtuvieron como resultado que la implementación de un sistema de gestión de seguridad de la información en una empresa de control físico y digital de documentos ayudó a identificar los riesgos de seguridad que vulneran la integridad, confidencialidad y disponibilidad de la información; al igual que en la presente investigación, se realizó el cálculo de la probalidad por el impacto para hallar el riesgo. Esta fórmula también fue usada en la presente investigación para hallar el riesgo y posteriormente lograr reducirlo en un 55% mediante las acciones del tratamiento de riesgos.

A su vez, fue esencial la evaluación económica a largo plazo de la inversión realizada para la investigación. Relativo a ello, Chávez & Sánchez (2016) manifestaron la viabilidad de aplicar la seguridad de la información; esta generó un VAN de S/ 10,527.76, con una TIR de 58% lo cual evidencia la viabilidad económica de la propuesta en el horizonte de cinco año. Esto guarda relación con la presente investigación en donde se demuestra la factibilidad debido a que se obtuvo un VAN positivo de S/ 40,773.05 y TIR igual a 81,40% demostrando su rentabilidad.

Por consiguiente y según lo anteriormente descrito, los resultados obtenidos permiten confirmar la hipótesis de la investigación " La seguridad de la información influye significativamente en la gestión documental de la entidad técnica L & M Seminario Group S.A.C. en el año 2020", afianzando las afirmaciones de los autores considerados en la presente investigación los mismos que en su totalidad afirman que repercute efectivamente en las organizaciones.

4.2. **Conclusiones**

- Se concluye que la seguridad de la información representa una influencia significativamente en la gestión documental de la entidad técnica L & M Seminario Group S.A.C., pues se logró determinar que el impacto de la propuesta en el ahorro es de S/ 23,812.00 soles; esto fue comprado al hallar un incremento significativo en la seguridad de la informacion $P = 0.038 < 0.05$ y en la gestión documental $P = 0.024 < 0.05$ después de aplicar el procedimiento propuesto basado en el ciclo de mejora continua y en los lineamientos de las normas NTP-ISO/IEC 27001:2014 para lograr la seguridad de la información en la gestión documental de la organización.
- El análisis de los requerimientos de seguridad de la información en la organización permitió identificar el modelo de negocio, procesos y funciones con el fin de comprender las necesidades y de igual manera las expectativas de las partes interesadas.
- El diseño de seguridad de la información se basó en el ciclo de Deming y contempló 15 fases basadas en las ISO 27001:2014 y en el anexo A de la ISO 27003:2012. A traves de estas etapas se buscó perserverar los prinicipios de confianilidad, disponibilidad en integridad de la información.
- Se logró proteger los 7 activos valorados como sensibles mediante la aplicación de 25 controles de la NTP-ISO 27002:2016 como medida para mitigar los riesgos de seguridad de la información vinculados a estos activos; logrando reducir en un 55% el impacto por la probabilidad de ocurrencia después de aplicar las acciones asociadas al tratamiento de riesgos.

- Se evaluó el impacto económico y se concluye que la propuesta es viable, puesto que el VAN resultó positivo e igual a S/ 40,773.05; en cuanto a la TIR este fue de 81.40%, siendo superior a la tasa de descuento usada. Asimismo, se obtuvo un B/C de 1.90 lo cul indica que por cada sol invertido existe una ganancia de 0.90 centimos/soles.
- Se precisa que existió limitaciones en cuanto a la disponibilidad de la alta dirección para involucrarse en la investigación, ello llevó a los involucrados a acordar un horario pertinente para las visitas, aplicación de los cuestionarios y capacitación a los colaboradores. Asimismo, otra limitante fue la escaza información enfocada al rubro de la investigación; por una parte esto significó tomar como referencia investigaciones de otros rubros; y por otro lado, ello representó una oportunidad para una investigación futura de la seguridad de la información en el sector constructivo.

REFERENCIAS

Adriazola, A. (2017). Propuesta para la gestión documental de archivsos escolares en Chile: El Instituto Nacional General José Miguel Carrera (Tesis de especialización). Pontificia Universidad Católica de Chile. Recuperado el 07 de mayo de 2019 de **https://repositorio.uc.cl/handle/11534/21380**

Adriazola, A. (2017). Propuesta para la Gestión Documental de Archivos Escolares en Chile: El Instituto Nacional General José Miguel Carrera. (Tesis de grado). Pontificia Universidad Católica de Chile. [En línea] recuperado el 17 marzo del 2019 de https://repositorio.uc.cl/bitstream/handle/11534/21380/Tesis%20MPGI%20Ana%20Maria%20Adriazola%202017.pdf?sequence=1

Angarita, J. (2014). Diseño de un sitema de gestión de la seguridad de la información ISO 27001 para la alcaldía de Floridablanca y plan de acción para su implementación segú la guía PMBOK. (Tesis de especialización). Universidad Industrial de Santander, Colombia. [En línea] recuperado el 15 de mayo de 2019 de http://tangara.uis.edu.co/biblioweb/tesis/2014/151285.pdf

Arias, F. (2006). El proyecto de Investigación. Introducción a la metodología científica. [En línea] recuperado el 15 de mayo de 2019 de https://ebevidencia.com/wp-content/uploads/2014/12/EL-PROYECTO-DE-INVESTIGACI%C3%93N-6ta-Ed.-FIDIAS-G.-ARIAS.pdf

Boca, V. (2016). Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local – Chiclayo. (Articulo de investigación) Universidad Señor de Sipán, Perú. [En línea]. Recuperado el 20 de mayo de 2019 de http://revistas.uss.edu.pe/index.php/ING/article/view/357/346

Cabanaconza, P. (2017). Procesos técnicos archivísticos y gestión documental en la Oficina General de Adminastración de Recursos – Seguro Integral de Salud, Lima 2016. (Tesis de grado). Universidad Cesar Vallejo. [En línea] recuperado el 17 marzo del 2019 de http://repositorio.ucv.edu.pe/bitstream/handle/UCV/9013/Cabanaconza_TPA.pdf?sequence=1&isAllowed=y

Chávez & Sánchez (2016). *Implementación de un plan de seguridad basado en iso 27002 y su impacto en la fiabilidad de la información en sabrisa s.a.c.* (Tesis de grado). Universidad Privada del Norte.

Consejos para mejorar la gestión documental en las empresas [Web log post]. (2017, November 22). Retrieved February 12, 2020, from https://www.isotools.org/2017/11/22/8-consejos-para-mejorar-la-gestion-documental/

Dueñas, J. (2018, July 17). Colombia es más consciente frente a la seguridad de la información • ENTER.CO. Retrieved February 12, 2020, from https://www.enter.co/especiales/empresas/colombia-seguridad-informacion/

Franklin, E. (2014). Organización de Empresas. Editorial Mc Graw Hill. Cuarta Edición.

Higa, T. (2017). Implementación de un sistema de gestión documental en el área de SSMA de una empresa del sector construcción. (Tesis de licenciatura). Universidad Nacional Mayor de San Marcos de Perú. [En línea] recuperado el 18 de enero del 2020 de http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/6391/Higa_ct.pdf?sequence=1&isAllowed=y

INACAL. (2018). *NTP – ISO / IEC 2021: 2014 Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos*. [En línea] recuperado el 01 de mayo de 2019 de https://www.inacal.gob.pe/inacal/files/27001-Carlos_Hornafinal.pdf

Justino, Z. (2015*). Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013*. (Tesis de grado). Pontificia Universidad Católica del Perú. [En línea] Recuperado el 01 de mayo de 2019 de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/6045/JUSTINO_ZULLY_DISEÑO_SISTEMA_GESTION_SEGURIDAD.pdf?sequence=1&isAllowed=y

Komisarczuk, P. (2020). An introduction to knowledge areas in Information Security - Introduction to Information Security. Retrieved June 04, 2020, from https://www.coursera.org/learn/information-security-data/lecture/7mqjI/an-introduction-to-knowledge-areas-in-information-security

Lema, R. & Donoso, D. (2018). Implementación de un sistema de gestión de seguridad de información basado en la norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa Lockers S.A.. (Tesis de grado). [En línea].

Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador. Recuperado el 20 de mayo de 2019 de http://repositorio.espe.edu.ec/bitstream/21000/14397/1/T-ESPE-057876.pdf

Luyo, J. (2018). Sistema digitalfile 1.0 para mejorar la gestión documental del tratamiento de datos personales en la empresa BBVA, Lima 2018. (Tesis de licenciatura). Universidad Norbert Wiener de Perú. [En línea] recuperado el 18 de enero del 2020 de http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/2501/TESIS%20Luyo%20Jean.pdf?sequence=1&isAllowed=y

Santos, D. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basdo en la ISO/IEC 27001:2013 para una empresa de consultoría de software*. (Tesis de grado). Pontificia Universidad Católica del Perú. [En línea] Recuperado el 01 de marzo del 2019 de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/7616/SANTOS_DANIEL_SISTEMA_GESTIÓN.pdf?sequence=1&isAllowed=y&fbclid=IwAR14DIkQzGBzxVXYez9FxwJ_wUjDGexECmeG-wtV7GnaQrK990fhpFB81I4

Suarez, S. (2015). *Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suarez Padilla & CIA. LTDA. Que brinde una adecuada protección en seguridad informática de la infraestructura tecnolóca de la organización*. (Tesis de especialización). Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas, Tecnología e Ingeniería Bogotá D.C. [En línea] Recuperado el 07 de marzo de 2019 de https://core.ac.uk/download/pdf/47279965.pdf

Vilca (2017). *Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa GEOSURVEY de la ciudad de Lima*. (Tesis de grado). Universidad de Huánuco. [En línea] Recuperado el 07 de marzo de 2019 de http://repositorio.udh.edu.pe/bitstream/handle/123456789/809/T_047_43087253_T.pdf?sequence=1&isAllowed=y

Yañez, N. (2017). *Sistema de Gestión de Seguridad de la Información para la susbsecretaria de economía y empresas de menor tamaño*. (Tesis de grado). Universidad de Chile. [En línea] recuperado el 17 marzo del 2019 de http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y

Watkins, S. G. (2013). An introduction to information security and ISO27001:2013: A pocket guide (2nd ed.). Cambridgeshire: It Governance Publishing.

ANEXOS

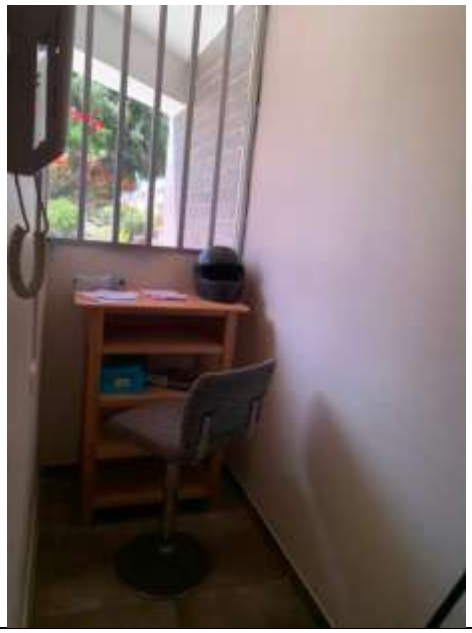
ANEXO n.° 01. Ficha de registro de observación oficina principal

FICHA DE REGISTRO FOTOGRÁFICOS	
CODIGO:	**RF001**
FECHA:	10/03/20
LUGAR:	OFICINA L & M SEMINARIO GROUP S.A.C. TRUJILLO
DESCRIPCIÓN DE LO OBERVADO	**IMAGEN**
IMAGEN DE PUERTA DE INGRESO PRINCIPAL POR AMBOS LADOS DE LA OFICINA	 
ESCRITORIO PRINCIPAL DE LA OFICINA	

COMPUTADORA PRINCIPAL POR AMBOS LADSO	 
CAJONES DEL ESCRITORIO PRINCIPAL	

ESTANTE SIN PUETAS Y COMPARTIMENTOS INFERIORES SIN LLAVE	
EXPEDIENTES DE AÑOS ANTERIORES EN CAJAS	

SEGUNDA IMPRESORA DE USO PARA TODO EL PERSONAL	
GAVETAS INFERIORES SIN LLAVE	

SEGUNDA ESTANTERÍA SIN PUERTAS, SELLOS EXPUESTOS	
OFICINA DE VIGILANCIA SIN USO	

ANEXO n.° 02. Transcripción de entrevista al gerente general

ENTREVISTA AL GERENTE GENERAL

Datos de identificación

Nombre del entrevistado:	Luis Hernando Seminario Narro	
Empresa:	L & M Seminario Group S.A.C.	
Nombre del entrevistador:	Ana Paula Caiguaray Campos	
Fecha:	Lugar:	Mz X3 lote 2 Urbanización Vista Hermosa, Trujillo.

Presentación:

Buenos días, soy Ana Paula Caiguaray Campos, de la carrera ing. Empresarial de la Universidad Privada del Norte, la presente entrevista es con fines académicos, asimismo quisiera empezar agradeciéndole por el tiempo que se tomará para esta entrevista. Para comenzar, quisiera recalcar el fin académico de la presente investigación por lo que la información brindada será confidencial.

Guía de entrevista:

1. Para comenzar me gustaría conocer cómo se constituyó la empresa, sus inicios
2. ¿Cuál es el rubro y los servicios que brinda?
3. ¿Cuáles son los actividades que realiza para cumplir con los servicios?
4. ¿Considera que es necesario mantener protegida la información de su empresa? ¿Por qué?
5. ¿Cómo se registra la información de sus clientes? ¿Considera que podría existir alguna pérdida de esta?
6. ¿Cómo se maneja la información recopilada dentro de su empresa?

Transcripción

E: Muchas gracias por su atención, nos gustaría empezar conociendo un poco acerca de los inicios de la empresa, cómo es que se constituyen como una entidad técnica.

G: No, muchas gracias a ustedes por realizar su investigación sobre esta empresa familiar, la que mi padre fundó hace 4 años, dando inicio a la gestión administrativa en la ciudad de Trujillo, y bueno un poco acerca de la reseña histórica, la empresa fue creada por mi (Luis

Hernando Seminario Narro) como gerente general y representante legal en el año 2016, contando con solo el gerente operativo de la empresa. En el año 2017, se inició la sub contrata de obras para empresas que trabajaban como Entidades Técnicas del Fondo Mivivienda, donde nos encargamos exclusivamente del proceso constructivo de módulos de viviendas de interés social. Nuestra empresa comenzó con la subcontratación de 7 módulos en la ciudad de Chiclayo, posteriormente en octubre del 2018 ejecutó 18 viviendas en la localidad de Tembladera. A finales del 2018 empezamos con la última terciarización del año, la cual fue de 140 viviendas en el departamento de Lambayeque. Paralelamente, y al ya contar con experiencia en la construcción de viviendas de interés social bajo la modalidad de construcción en sitio propio, comenzamos con el registro de la empresa como Entidad Técnica autorizada por el Fondo MiVivienda. Este expediente se aprobó en Enero del 2019, otorogandole el codigo de ET. LIB – 826 – 19 – 1N – 19, con el cual nuestra empresa se convertió en una Entidad Técnica autorizada para registrar proyectos bajo las tres diferentes modalidades del programa Techo Propio.

E: Justo mi siguiente preguntaba iba a enfocada a lo que me acaba de decir, quería que me comente un poco más acerca del rubro y los servicios que brindan

G: Sí claro con respecto al rubro de la construcción y específicamente como entidad técnica del fondo mivivienda nosotros nos enfocamos en beneficiar a los sectores económicos B, C y D brindando el servicio de construcción de viviendas de interés social para grupos familiares que cumplan con los requisitos establecidos por el fondo, los cual es que este conformado por un jefe de familia y una carga familiar, esta puede ser padres, cónyuge, hermanos discapacitados, hijos y abuelos. Qué más … con respecto al bono familiar habitacional esto es un subsidio directo del Estado que si mal no me equivoco decretado por la ley 27829 y cuyo objetivo es que más peruanos cuenten Con una vivienda digna con servicios básicos de agua potable luz y desagüe.

E: y con respecto a las actividades que realiza para cumplir con su servicio ¿Cuáles?

G: Bueno podríamos decir que nuestra actividad como entidad técnica empieza por determinar la zona con mayor número posible de beneficiarios, recogemos información de los prospectos y vemos si es que es un número aceptable, entonces empezamos a pedir documentos como el DNI del jefe familiar y el de la carga familiar así como una copia literal

para ingresarlos en el sistema llamado zona segura y así poder saber si es que estos califican para ser beneficiarios del bono una vez que los hemos registrado tenemos que llenar un formulario de registro y ellos nos tienen quedar una carta poder de representación; nosotros les damos el formato y ellos la firman y con esos dos documentos podemos armar el expediente de un grupo familiar estos expedientes los escaneamos y un encargado del fondo mivivienda valida la información recibida y la filtra teniendo en cuenta si el grupo familiar ha recibido apoyo habitacional del Estado, si es que no ha recibido ayuda, publica la lista del grupo familiar en la página si es que ha recibido algún tipo de ayuda aún cabe la posibilidad de calificar si es que el apoyo recibido fue antes de declararse en estado de emergencia, si es que fuese así se acepta como grupo familiar excepcional de acuerdo al artículo 14.3, otro filtro es que el grupo familiar debe contar sólo con una propiedad Y si no es titular exclusivo de la propiedad el copropietario se tiene que evaluar el copropietario también si es que éste es parte del grupo familiar y si es que no es parte del grupo familiar y copropietario no será elegible una vez terminado el filtro se publica para todos el que quiera ingresar a la página del fondo mivivienda es decir en el portal institucional la lista de grupos familiares sólo con el jefe solo con la información del jefe de familia es ahí donde empezamos elaborar el expediente presentamos el expediente al fondo mi vivienda con los planos y el formulario único edificación Y este tiene un plazo de 20 días calendario para revisar si está conforme y si no está conforme nosotros tenemos un plazo de 15 días calendarios para levantar las observaciones; una vez que es conforme nos otorgan el código de proyecto con el código del proyecto nosotros contamos con 45 días calendarios más para presentar el expediente en el cual se presente el formulario solicitud de registro del proyecto, la copia de auto valúo, el contrato de ejecución de obra, la carta de seriedad oferta por el 2.5% del monto a afianzar, la memoria descriptiva y el juegos de planos de arquitectura. Con todos estos documentos se realiza el registro del proyectos y se solicita la asignación y desembolso del bono familiar habitacional el cual se desembolsa a través de la entidad financiera con la que se tramitó la seriedad de oferta, Para esta solicitud de desembolso el fondo mi vivienda tiene 30 días calendarios máximo para verificar que cumplimos con toda la documentación requerida y en caso de nosotros tener alguna observación tenemos 15 días calendarios para subsanarlo sino después de haberse aprobado el fondo cuenta con 5 días hábiles para realizar el desembolso del bono familiar habitacional a través de la financiera elegida.

Ahora con respecto a nuestro proceso constructivo nosotros iniciamos informando a la municipalidad con una carta de inicio de obra, esta la realiza nuestro gerente operativo. Una

vez enviada esta carta a nuestro ingeniero civil se realiza el reconocimiento de área es decir junto con los obreros se realiza el trazado y limpieza del área, los obreros habilitarán el fierro, realizarán el zanjeo y luego el armado de columnas y zapatas; nuestro ingeniero civil o también llamado residente de obra estará en constante supervisión del avance de obra para ver si existe alguna observación. Si es que así fuese tendrían que realizar la actividad anterior nuevamente o corregir sus errores, sino se procede a vaciar cimientos y zapatas luego se le van los muros luego se seguiría con el encofrado de columnas y estas alturas estaríamos al 40% de la obra entonces nuestro ingeniero civil nos arma un informe de avance de obra con el cual nuestro gerente de operaciones puede solicitar la valorización de la obra. Esta valorización le realizará un perito enviado por la financiera, el perito nos va a solicitar información como la lista de beneficiarios, los planos de ubicación de los módulos y está documentación la tenemos que enviar a ellos. Asimismo, tenemos que realizar el deposito de viáticos para que nos agente en una supervisión. En el día asignado se realiza la visita a la obra y este perito emite un informe, junto a este informe nos van a alcanzar unos documentos que tenemos que llenar, una carta de solicitud de la supervisión, el detalle de requerimientos y el cronograma de obra. Luego el perito tiene 5 a 7 días para enviar toda la documentación a la financiera. Esta realiza el informe interno, entonces nos informa para ir a cobrar este cheque en la caja con la copia de DNI y la vigencia de poder de la empresa este proceso o conjunto de pasos se vuelve a realizar al solicitar otra valorización. Generalmente las solicitamos al 60 u 80% y al cerrar la obra. Cabe resaltar que se solicitan estas valorizaciones con el objetivo de que nos desembolse dinero de los bonos y contar con efectivos para realizar la obra.

E: ¿Considera que es necesario mantener protegida la información de su empresa? ¿Por qué?

G: Si, si considero que es importante mantener protegida la información de la empresa porque manejamos documentos personales de los beneficiarios y también documentos de valor para nosotros como son los planos y nuestras listas de beneficiarios o prospectos de beneficiarios encontrados. Los cuales, si son filtrados, otra entidad técnica podría coger estos beneficiarios y realizar el procedimiento antes que nosotros y todos nuestros esfuerzos realizados para la búsqueda de estos prospectos y todos los recursos utilizados para esto, eh no habrían valido de nada. De igual manera hemos presentado problemas con las fotos publicadas en las redes sociales las cual es en las usan para publicitar otras empresas haciéndose pasar por nosotros.

E: ¿Cómo se registra la información de sus clientes? ¿Considera que podría existir alguna pérdida de esta?

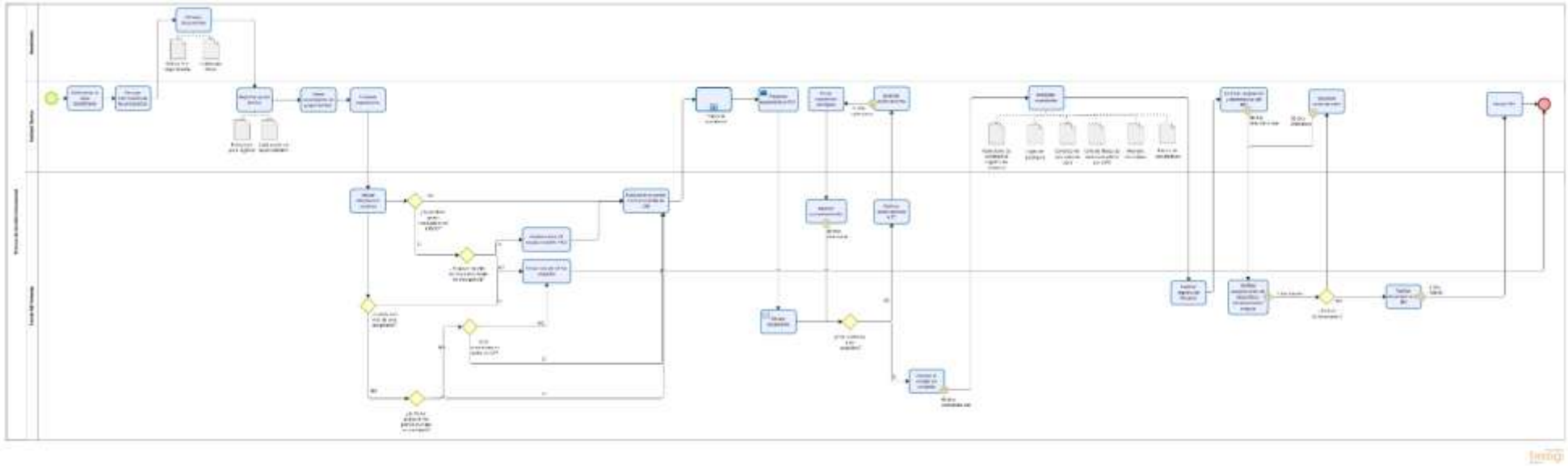
G: Debo de admitir que no llevamos un registro muy ordenado que digamos de nuestros datos de los expedientes registrados y esto muchas veces nos causa perder tiempo buscando todos estos expedientes en físicos porque en algún momento vamos a realizar el procedimiento de solicitar una carta nuevamente y yo teníamos el formato de cómo llenar la documentación pero no la tenemos a disponible en el momento que la necesitamos porque no sabemos dónde está eh entonces esta falta de gestión podría decirse nos lleva a perder tiempo generalmente la información de nuestros clientes o beneficiarios la registramos tanto en Un Excel como en físico Pero el primer registro que se realiza en físico porque se hace que este beneficiario firme el formato entonces en el camino en el transcurso se puede perder estos documentos si es que no son correctamente almacenados.

E: ¿Cómo se maneja la información recopilada dentro de su empresa?

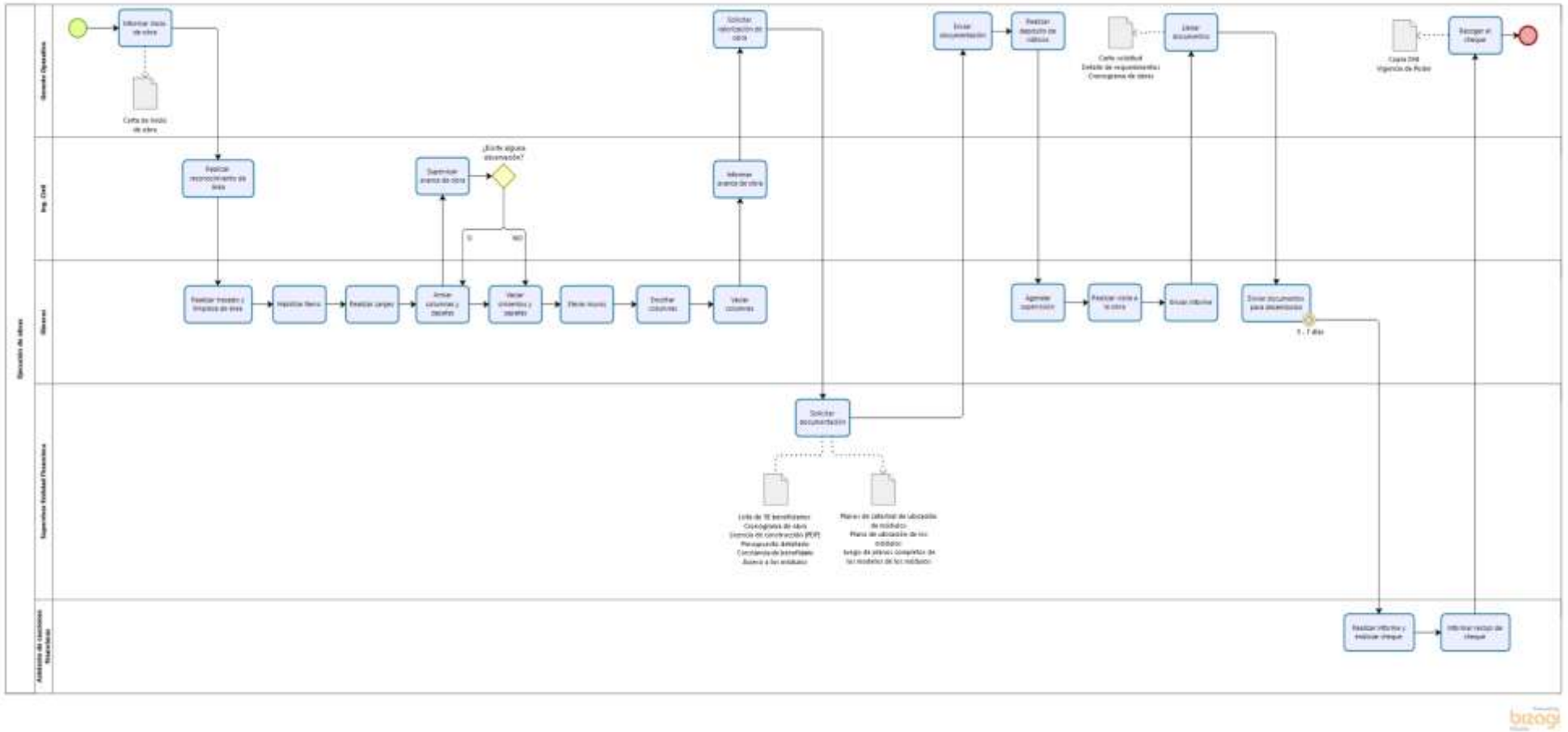
G: Claro, bueno la mayor parte de nuestra información la tenemos en documentos en físico ya que como te había explicado anteriormente nosotros llegamos a los beneficiarios y hacemos que ellos nos llenen unas fichas las cual es las tienen que firmar y posteriormente nosotros pasamos se registró un Excel para realizar solicitudes como nuestra carta de seriedad oferta. Asimismo, existen más trámites burocráticos que se tienen que presentar eh en mesa de partes del fondo mi vivienda y todos son documentos en físicos los cual es después nos quedamos con un cargo como prueba de que este documento ha sido ingresado.

E: Gracias por el tiempo brindado, que tenga un buen día.

ANEXO n.° 03. Diagrama del proceso de Gestión Documental



ANEXO n.° 04. Diagrama del proceso de Ejecución de Obra



ANEXO n.° 05. Ficha de registro observación obra – guía de observaicon

FICHA DE REGISTRO FOTOGRÁFICOS	
CODIGO:	**RF002**
FECHA:	10/03/20
LUGAR:	OBRA CONSTRUCCIÓN DE 17 MODULOS DE INTERÉS SOCIAL
DESCRIPCIÓN DE LO OBERVADO	**IMAGEN**
ALMACÉN DE MATERIALES PARA LA OBRA	
REPARTO DE MATERIAL	

OBREROS EN PROCESO DE LEVANTAMIENTO DE MUROS	
CASA MODELO DE MÓDULO DE INTERÉS SOCIAL	

ANEXO n.° 06. Documento de compromiso de la dirección con el proyecto

L & M Seminario Group S.A.C.

Mza. A. LT 12. Urb. El Paraíso - Moche
Trujillo - La Libertad

"Año de la lucha contra la corrupción e impunidad".

Trujillo, 21 de agosto de 2019

CARTA 0090 - 2019

Asunto : Aceptación del proyecto de creación de un sistema de gestión de seguridad de la información.

Yo, **Luis Hernando Seminario Narro**, con documento de identidad **Nº 71494828**, en mi calidad de representante legal de la empresa **L & M Seminario Group S.A.C.** con Código de Entidad Técnica **Nº LIB – 826 – 19 – 1N -19**, tengo el agrado de dirigirme a usted, con la finalidad de informarles que su solicitud para realizar el proyecto de creación de un sistema de gestión de seguridad de la información en nuestra empresa ha sido aceptada, con el fin de gestionar los posibles riesgos con respecto a la seguridad de la información. Para la ejecución del mismo, esta carta tiene una vigencia de tres (03) meses durante los cuales nos comprometemos a brindar a su equipo de investigación el apoyo e información necesaria para garantizar el éxito del proyecto.

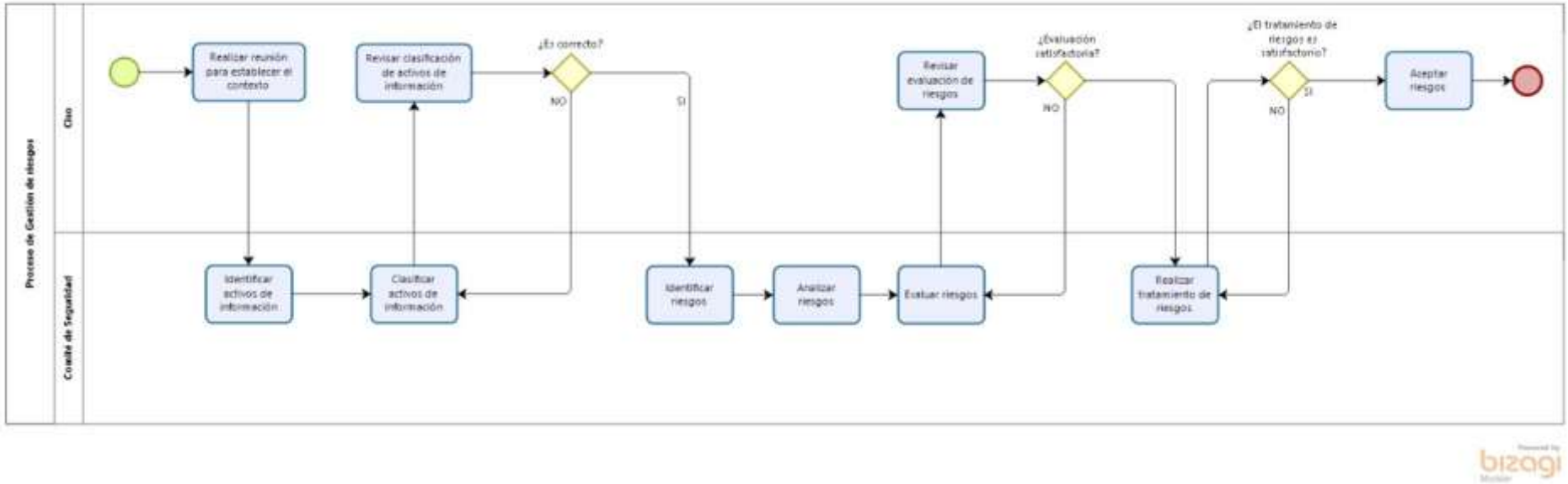
Sin otro particular, quedamos de ustedes,

Atentamente,

L&M SEMINARIO GROUP SAC
LUIS HERNANDO SEMINARIO NARRO
GERENTE GENERAL

941 975 193 / 982 016 530

ANEXO N 07. Diagrama de proceso de gestión de riesgos



ANEXO n.° 08. Declaración de aplicabilidad de controles

Seccion	Objetivo	Control	Estado	Justificación
A.5	**Políticas de seguridad de la información**			
A.5.1.	**Directrices de gestión de seguridad de la información**	5.1.1. Políticas para la seguridad de la información	Aplicar	Para la persente investigación se usó los lineamiento de la NTP-ISO/IEC 27001, la cual indica que la alta dirección debe establecer politica de seguridad de la información.
		5.1.2. Revisión de las políticas para la seguridad de la información.	Aplicar	Los lineamientos de la NTP-ISO/IEC 27001 indican que deberá realizarse una evaluación del desempeño de las políticas a implementar.
A.6	**Organización de la seguridad de la información**			
A.6.1.	**Organización interna**	6.1.1. Roles y responsabilidades en seguridad de la información	Aplicar	Los lineamientos de la NTP-ISO/IEC 27001 indica que deberá establecerse roles, responsabilidades y autoridades organizacionales.
		6.1.3. Contacto con autoridades	Aplicar	Debido a que la organización es una Entidad Técnica del Fondo MiVivienda del Gobierno Peruano, se establecerán procedimientos de comunicación con la autoridad pertinente ante atentados contra la seguridad de la información.
		6.1.5. Seguridad de la información en la gestión de proyectos	Aplicar	La organización trabaja con proyectos de construcción de viviendas de interés social en diversas partes del país, por lo que es necesario salvaguardar la información confidencial de la misma, incluyendo objetivos de seguridad de la información conjuntamente a los del proyectos.

A.6.2.	**Los dispositivos móviles y el teletrabajo**	6.2.1. Política de dispositivos móviles	Aplicar	La organización utiliza dispositivos móviles para el escaneo de documentos, asi como la agenda de contactos por lo que es importante una copia de seguridad.
		6.2.2. Teletrabajo	Aplicar	La organización permite a los colaboradores trabajar desde casa y/o lugar donde se ejecute la obra para lo cual es necesario tener control de la información sensible.
A.7	**Seguridad de los recursos humanos**			
A.7.1.	**Antes del empleo**	7.1.1. Selección	Aplicar	La organización deberá investigar los antecedentes del candidato a fin de que se compruebe su ética e información proporcionada por el candidato.
		7.1.2. Términos y condiciones del empleo	Aplicar	La organización debe proteger la seguridad de la información mediante la implementación de un Acuerdo de No Divulgación, especificando las acciones a tomar en caso se incumpla.
A.7.2.	**Durante el empleo**	7.2.1. Responsabilidades de gestión	Aplicar	Se precisa que la gerencia sea la responsable de comunicar los roles, responsabilidades y motive a los colaboradores con respecto a la seguridad de la información de manera que minimice los incidentes de seguridad de la información.
		7.2.2. Concientización, educación y capacitación en seguridad de la información	Aplicar	El personal de la organización no se encuentra informado sobre la importancia de mantener un nivel optimo de seguridad de la información por lo que se requiere material y charlas para crear una cultura de seguridad.
		7.2.3. Proceso disciplinario	Aplicar	Tanto en la política de seguridad de la información como en el Acuerdo de No Divulgación se informará acerca del proceso disciplinario ante el incumplimiento de alguna política, el cual servirá de igual

				manera para disuadir que los colaboradores violen alguna política.
A.7.3.	**Terminación y cambio de empleo**	7.3.1. Terminación o cambio de responsabilidades del empleo	Aplicar	La organización debe definir los deberes y responsabilidades vigentes con respecto a la confidencialidad posterior al finalizar el contrato de trabajo.
A.8.	**Gestión de activos**			
A.8.1.	**Responsabilidad sobre los activos**	8.1.1. Inventario de activos	Aplicar	La organización debe mantener un catálogo de activos para poder controlar y estar informado del estado de los mismos.
		8.1.2. Propiedad de los activos	Aplicar	Cada activo debe tener un propietario o responsable que se encargue de la correcta gestión del activo.
		8.1.3. Uso aceptable de los activos	Aplicar	La organización debe tener un conjunto de reglas para el uso aceptable de información y de las instalaciones de forma documentada.
		8.1.4. Retorno de activos	Aplicar	Se debe incluir en el proceso de finalización del contrato o renuncia el retorno de activos físicos, electrónicos.
A.8.2.	**Clasificación de la información**	8.2.1.Clasificación de la información	Aplicar	La información manejada por la organización debe ser clasificada en términos del análisis de confidencialidad, integridad y disponibilidad
		8.2.2. Etiquetado de la información	Aplicar	Se debe etiquetar la información de manera que facilite la identificación al usuario.
		8.2.3. Manejo de activos	Aplicar	La organización debe tener procedimientos para manejar, procesar y almacenar la información.
A.8.3.	**Manejo de los medios**	8.3.1. Gestión de medios removibles	Aplicar	Debido a que se utiliza dispostivos USB en la organización es necesario estipular directrices para el correcto uso del mismo.

		8.3.2. Disposición de medios	Aplicar	Es necesario establecer la mejor manera de eliminar la información cuando esta ya no sea requerida.
		8.3.3. Transferencia de medios físicos	Aplicar	La organización envía documentación a Lima constantemente por lo que es necesario identificar el servicio de courrier mas confiable.
A.9	**Control de acceso**			
A.9.1.	**Requisitos de la empresa para el control de acceso**	9.1.1. Política de control de acceso	Aplicar	La organización debe tener una política de control de acceso tanto físico como lógico, identificando las restriccciones y derechos de acceso de los usuarios.
		9.1.2. Acceso a las redes y a los servicios de red	No aplicar	
A.9.2.	**Gestión de acceso de usuario**	9.2.1. Registro y baja de usuario	Aplicar	La organización debe tener un proceso de registro y baja de usuarios.
		9.2.2. Aprovisionamiento de acceso de usuario	Aplicar	Establecer proceso por el cual se le asigne el acceso a los colaboradores.
		9.2.3.Gestión de derechos de acceso privilegiado	Aplicar	Se debe asignar el acceso de uso privilegiados basado en la necesidad de uso y en la política de control de acceso
		9.2.4. Gestión de la información de autentificación secreta de los usuarios	Aplicar	La organización debe brindar contraseñas a cada usuario para iniciar sesión en las laptops.
		9.2.5. Revisión de los derechos de acceso de usuario	Aplicar	Establecer en la política un intervalo de tiempo en el que se debe revisar los accesos, asi como después de realizarse algún cambio interno.
		9.2.6. Remoción o ajuste de derechos de acceso	Aplicar	Incluir en la política para respaldar la confidencialidad de los derechos una vez finalizado el contrato o renuncia.
A.9.3	**Responsabilidades de los usuarios**	9.3.1. Uso de información de autentificación secreta	Aplicar	Es necesario informar a los usuario el correcto uso de información secreta como son las contraseñas para que estos tengan

				noción de cómo salvaguardar la información.
A.9.4	**Responsabilidades de los usuarios**	9.4.1. Restricción del acceso a la información		aplicar
		9.4.2. Procedimientos de ingreso seguro	Aplicar	Establecer pautas para ingreso seguro con el fin de minimizar el riesgo de acceso no autorizado.
		9.4.3. Sistema de gestión de contraseñas	Aplicar	Un control de la gestión de contraseñas brindado a todo el personal es necesario para asegurar la confidencialidad y disponibilidad de la información.
		9.4.4. Uso de programas utilitarios Privilegiados	No aplicar	Pertenece a la seguridad informática
		9.4.5. Control de acceso al código fuente de los programas	No aplicar	Pertenece a la seguridad informática
A.10	**Criptografía**			
A.10.1.	**Controles criptográficos**	10.1.1. Política de uso de los controles criptográficos	No aplicar	Pertenece a la seguridad informática
		10.1.2.Gestión de claves	No aplicar	Pertenece a la seguridad informática
A.11	**Seguridad física y del entorno**			
A.11.1.	**Áreas seguras**	11.1.1. Perímetro de seguridad física	Aplicar	No existe alarma o vigilante que proteja el edificio en el que se ubica la oficina donde realizan las operaciones de la organización.
		11.1.2. Controles físicos de entrada	Aplicar	Llevar un control de las personas que ingresan a la oficina es necesario para saber quienes estuvieron presente en caso de produzca algún atentado contra la información.
		11.1.3. Seguridad de oficinas, despachos y recursos	Aplicar	Las actividades de la oficina no deberían ser audibles o visibles al exterior.
		11.1.4. Protección contra las amenazas externas y ambientales	No aplicar	
		11.1.5. Trabajo en áreas seguras	Aplicar	Se debe evitar el trabajo no supervisado

		11.1.6. Áreas de carga y descarga	No Aplicar	Se tiene como límite físico la oficina ubicada en Trujillo.
A.11.2.	**Seguridad de los equipos**	11.2.1. Emplazamiento y protección de equipos	Aplicar	El equipo de la compañía debe estar en una sala segura, de igual manera se redactara un manual de buenas practicas para el uso del equipo.
		11.2.2. Servicio de suministros	No aplicar	
		11.2.3. Seguridad del cableado	Aplicar	Se realizará la colocación de canaletas a todos los cables sueltos en la oficina de la organización.
		11.2.4. Mantenimiento de equipos	Aplicar	Realizar mantenimiento externo de los equipos en un periodo determinado del año, el cual deberá ser especificada en el manual de buenas prácticas.
		11.2.5. Remoción de activos	Aplicar	Se llevará un registro de los datos de la persona, así como la fecha y hora que los equipos fueron extraidos y retornados a la empresa.
		11.2.6. Seguridad de los equipos y activos fuera de las instalaciones	Aplicar	Aplicar a los activos que se encuentran fuera de la oficina, siempre que estos tengan el permiso de gerencia
		11.2.7. Reutilización o eliminación segura de equipos	Aplicar	Se estipulara en la politica un procedimiento de eliminación de los equipos en obsolescenia, verificando su contenido antes de eliminar o reutilizar el equipo.
		11.2.8. Equipo de usuario desatendido	Aplicar	Se especificará en la política el uso de bloqueo de pantallas con contraseñas cada que no se haga uso del equipo.

		11.2.9. Política de escritorio limpio y pantalla limpia	Aplicar	Incluir política de escritorio limpio y pantalla limpia, estipulando el uso de gabinetes con llave para los documentos con información sensible o crítica del negocio.
A.12	**Seguridad de las operaciones**			
A.12.1	**Procedimientos y responsabilidades operacionales**	12.1.1. Procedimientos operativos documentados	Aplicar	Se incluirá en el manual de buenas practicas el procedimiento de reinicio y recuperación para usar en caso de fallo en el sistema.
		12.1.2. Gestión del cambio	Aplicar	Realizar una lista con los posibles cambios que pueden realizarse en la organización y su efecto que estos tendrían en la seguridad de la información, asi como establecer un procedimeinto formal para la aprobación de los cambios propuestos, incluyendo el responsable de aceptar los cambios.
		12.1.3. Gestión de la capacidad	Aplicar	Se aplicará una política que establezca la eliminación de datos obsoletos para obtener mayor capacidad en el disco, asi como el retiro de aplicaciones y/o bases de datos que ya no sean de utilidad.
		12.1.4. Separación de los recursos de desarrollo, prueba y operación	No aplicar	Pertenece a la seguridad informática
A.12.2.	**Protección contra el software malicioso (malware)**	12.2.1. Controles contra el código malicioso	Aplicar	Establecer en la política prohibir el uso de software no autorizado, asi como establecer un software de respaldo en caso de perder la información. Incluir tambien en los boletines informativos informacion de como identificar este tipo de software.
A.12.3.	**Respaldo**	12.3.1. Respaldo de la información	Aplicar	Verificar el medio de respaldo mensualmente.
A.12.4.	**Registro y supervisión**	12.4.1. Registro de eventos	No aplicar	Pertenece a la seguridad informática

		12.4.2. Protección de la información del registro	No aplicar	Pertenece a la seguridad informática
		12.4.3. Registro de administración y operación	No aplicar	Pertenece a la seguridad informática
		12.4.4. Sincronización del reloj	No aplicar	Pertenece a la seguridad informática
A.12.5.	**Control del software en explotación**	12.5.1. Instalación del software en explotacion	No aplicar	Pertenece a la seguridad informática
A.12.6.	**Gestión de la vulnerabilidad técnica**	12.6.1. Gestión de las vulnerabilidades técnicas	No aplicar	Pertenece a la seguridad informática
		12.6.2. Restricción en la instalación de software	No aplicar	Pertenece a la seguridad informática
A.12.7.	**Consideraciones sobre la auditoría de sistemas de información**	12.7.1. Controles de auditoría de sistemas de información	No aplicar	Pertenece a la seguridad informática
A.13	**Seguridad de las comunicaciones**			
A.13.1.	**Gestión de la seguridad de redes**	13.1.1 Controles de red	No aplicar	Pertenece a la seguridad informática
		13.1.2. Seguridad de los servicios de red	No aplicar	Pertenece a la seguridad informática
		12.1.3. Segregación en redes	No aplicar	Pertenece a la seguridad informática
A.13.2.	**Intercambio de información**	13.2.1. Políticas y procedimientos de transferencia de información	Aplicar	Establecer un procedimiento para proteger la información enviada como archivo adjunto, estableciendo la responsabilidad del usuario que envia el mensaje a que no comprometa la confidencialidad de la información; asi como los lineamientos para conservar y eliminar los correos de manera pertinente.
		13.2.2. Acuerdos de intercambio de información		
		13.2.3. Mensajería electrónica		
		13.2.4. Acuerdos de confidencialidad o no revelación		

A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A.14.1.	**Requisitos de seguridad en los sitemas de información**	14.1.1. Análisis de requisitos y especificaciones de seguridad de la información		
		14.1.2. Asegurar los servicios de aplicaciones en rdes públicas	No aplicar	Pertenece a la seguridad informática
		14.1.3. Protección de las transacciones de servicios de aplicaciones	No aplicar	Pertenece a la seguridad informática
A.14.2.	**Seguridad en el desarrollo y en los procesos de soporte**	14.2.1. Política de desarrollo seguro	No aplicar	Pertenece a la seguridad informática
		14.2.2. Procedimiento de control de cambios en sistemas	No aplicar	Pertenece a la seguridad informática
		14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en ele sistema operativo	No aplicar	Pertenece a la seguridad informática
		14.2.4. Restricciones a los cambios en los paquetes dde software	No aplicar	Pertenece a la seguridad informática
		14.2.5. Principio de ingeniería de sistemas seguros	No aplicar	Pertenece a la seguridad informática
		14.2.6. Entorno de desarrollo seguro	No aplicar	Pertenece a la seguridad informática
		14.2.7. Externalización del desarrollo de software	No aplicar	Pertenece a la seguridad informática
		14.2.8. Pruebas funcionales de seguridad de sistemas	No aplicar	Pertenece a la seguridad informática
		14.2.9. Pruebas de aceptación de sistemas	No aplicar	Pertenece a la seguridad informática
A.14.3.	**Datos de prueba**	14.3.1. Protección de los datos de prueba	No aplicar	Pertenece a la seguridad informática
A.15	**Relación con proveedores**			
A.15.1.	**Seguridad en las relaciones con proveedores**	15.1.1. Política de seguridad de la información en relaciones con los proveedores	Aplicar	Realizar una politica de seguridad de información para las relaciones con los proveedores en la cual se especifique como será el tratamiento de de información entre ambos, asi como registrar los

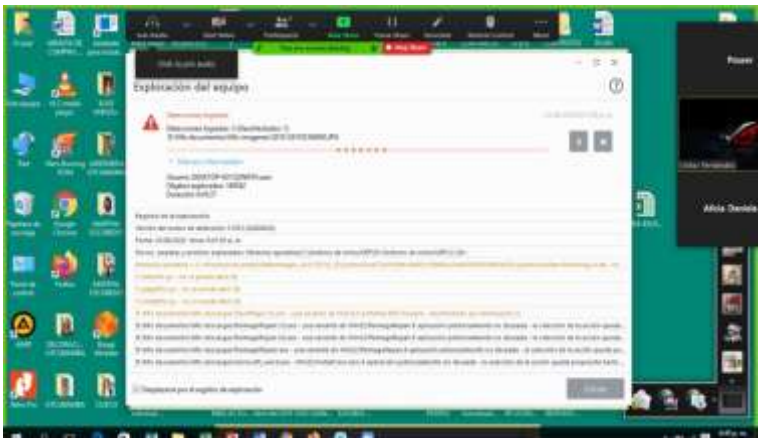
				proveedores, un procedimiento, definir el tipo de acceso de información, todas estas condiciones se deben
		15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores	Aplicar	Documentar y guardar todos los acuerdos firmados con los proveedores con el fin de evitar malentendidos, especificando las obligaciones contractuales y el uso aceptable de la información.
		15.1.3. Cadena de suministros de tecnología de la información y de las comunicaciones	No aplicar	
A.15.2	**Gestión de entrega de servicios del proveedor**	15.2.1. Monitore y revisión de servicios del proveedor	Aplicar	Se especificará en la politica las auditorias qeue se realizaran para medir el desempeño del servicio brindado por parte de los proveedores, asi como anotar cualquier incidente en caso de presentarse.
		15.2.2 Gestión de cambios ea los servicios de proveedores	Aplicar	Tener presente como realizar los cambios tanto en los acurdos como en la organzación y llevar un registro de los mismos.
A.16	**Gestión de incidentes de seguridad de la información**			
A.16.1.	**Gestión de incidentes de seguridad de la información y mejoras**	16.1.1. Responsabilidades y procedimientos	Aplicar	Establecer un responsablde en caso existan un incidente de seguridad de la información, asi como definir el procedimiento para planificar y preparar la respuesta ante el incidente y los procedimientos de monitorización, detección, análisis y reporte de los mismos; también se llevará un registro de las actividades realizadas para la gestión de los mismos y los procedimientos para la evaluación, decisión y respuestas.

		16.1.2. Reporte de eventos de seguridad de la información	Aplicar	Especificar en la política de seguridad de la información las situaciones puntuales en las cuales se considera reportar eventos de seguridad de la información.
		16.1.3. Reporte de debilidades de seguridad de la información	Aplicar	Especificar en la política que todos los colaboradores y proveedores que identifiquen alguna debilidad en el sistema de gestión de seguridad de la Información deberá comunicarlo mediante un reporte, cuya plantilla será especificada en el manual de manera que este disponible.
		16.1.4. Evaluación y decisión sobre eventos de seguridad de la información	Aplicar	Se realizará la evaluación de los eventos de seguridad de la información siguiendo el formato especificado para la clasificación y nivel del incidente con el find e saber el impacto y la extensión del mismo. Todos los resultado y decisiones tomadas deberán registrarse.
		16.1.5. Respuesta a incidentes de seguridad de la información	Aplicar	Establecer un procedimiento documentado para las respuestas a incidentes de seguridad, el cual deberá tener evidencias, análisis y actividades de respuestas.
		16.1.6. Aprendizaje de los incidentes de seguridad de la información	Aplicar	Se deberá analizar a profundidad los incidentes de seguridad de la información con la finalidad de mejorar o agregar cpontroles para no incidir en los mismos incidentes.
		16.1.7. Recolección de evidencias	Aplicar	Se aplicará un estandar para el procedimiento de identificación, recolección, adquisición y conservación de evidencia, tratando de que el personal o alguna herramienta las certifique.

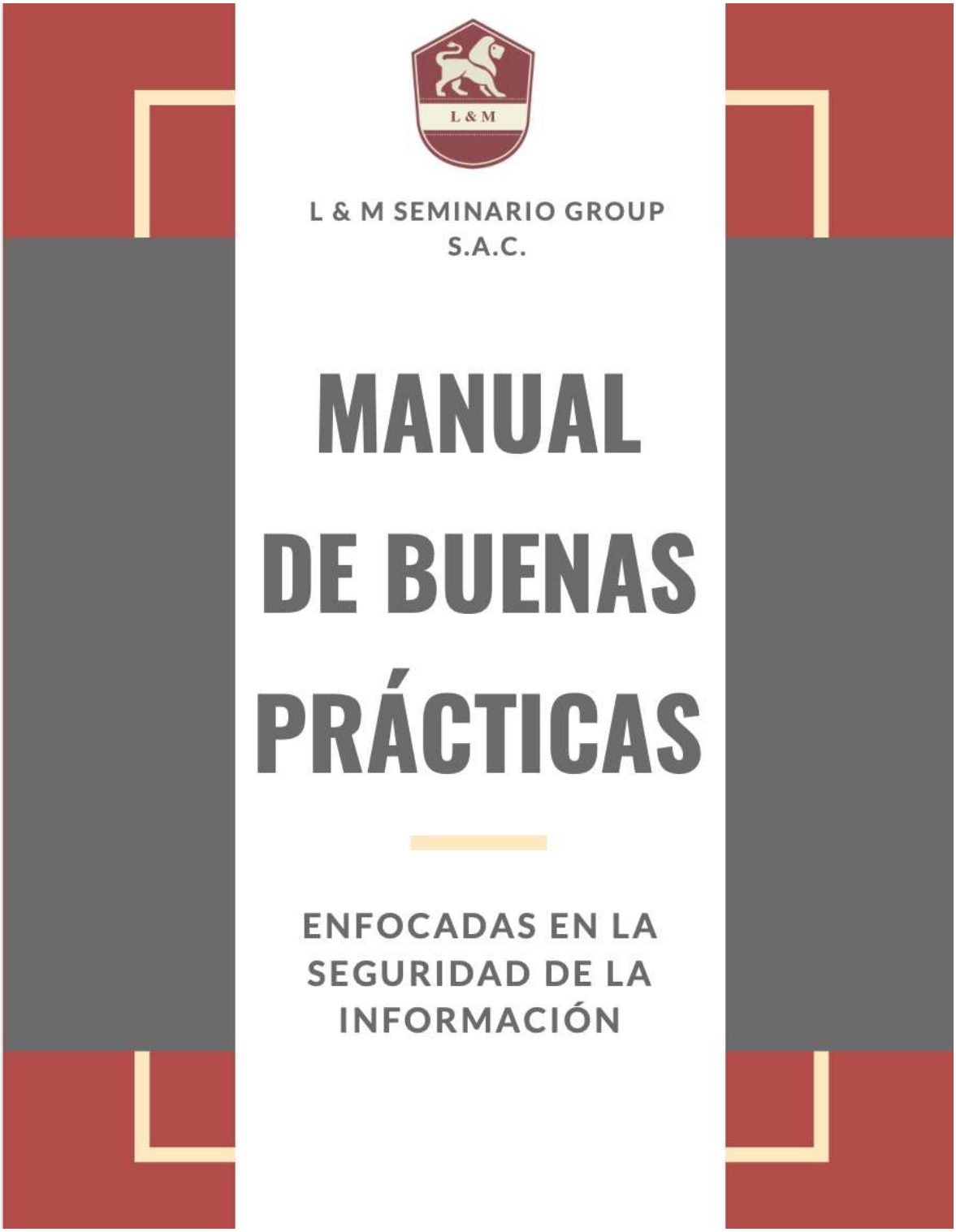
A.17	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**			
A.17.1.	**Continuidad de seguridad de la información**	17.1.1. Planificación de continuidad de la seguridad de la información	Aplicar	Incluir en la gestión de continuidad del negocio los requisitos para la continuidad de la seguirdad de la información.
		17.1.2. Implementar la continuidad de la seguridad de la información	No aplicar	
		17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No aplicar	
A.17.2.	**Redundancias**	17.2.1. Instalaciones de procesamiento de la información	No aplicar	Pertenece a la seguridad informática
A.18	**Cumplimiento**			
A.18.1.	**Cumplimiento de los requisitos legales y contractuales**	18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales	Aplicar	Especificar en la politica de seguridad de la información los requisitos legales del gobierno peruano que debe cumplir la organización.
		18.1.2. Derechos de propiedad intelectual	Aplicar	Establecer una politica en la cual se describan los lineamientos para proteger toda propiedad intelectual de la organización, asi como la de los recursos que se utilizan en la misma.
		18.1.3. Protección de los registros de la organización	Aplicar	Se adoptarán medidas para proteger los registros fíiscos de información asi como los virtuales para que estos puedan ser conservados satisfactoriamente.
		18.1.4. Privacidad y protección de datos personales	Aplicar	Establecer un política de datos personales, la cual deberá ser comuinicada a todo el personal.
		18.1.5. Regulación de los controles criptográficos	No aplicar	Pertenece a la seguridad informática
A.18.2.	**Revisiones de la seguridad de la información**	18.2.1. Revisión independiente de la seguridad de la información	Aplicar	Establecer intervalos de tiempo definidos para la revisión de la seguirdad de la información por parte de la gerencia, con el fin de identificar las oportunidades de

				mejora y/o la identificación de alguna necesidad de cambio.
		18.2.2. Cumplimiento de las políticas y normas de seguridad	Aplicar	Revisión, por parte de la gerencia, el cumplimiento del procesamiento de la información.
		18.2.3. Comprobación del cumplimiento técnico	No aplicar	Pertenece a la seguridad informática

ANEXO n.° 09. Infecciones detectadas por el antivirus

FICHA DE OBSERVACIÓN	
CODIGO:	**RE001**
FECHA:	10/03/20
DESCRIPCIÓN DE LO OBERVADO	**IMAGEN**
ESTADO INICIAL DE LOS ORDENADORES SIN LICENCIAS ACTUALIZADAS	
Opción de licencia gratuita elegida para evaluar el número de infecciones	
INFECCIONES DETECTADAS AL INSTALAR LA LICENCIA DEL ANTIVIRUS	

ANEXO n.° 10. Manual de Buenas Prácticas de la Seguridad de la Información



CONTENIDO

MANUAL DE BUENAS PRACTICAS

L & M SEMINARIO GROUP S.A.C.


GUÍA
PRÁCTICA
Este manual fue realizado como guía para la aplicación de la seguridad de la información dentro de la empresa L & M Seminario Group S.A.C., incluyendo las políticas de seguridad de la información y los procedimientos básicos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información de la empresa L & M Seminario Group S.A.C. ha sido realizada tomando en cuenta la Norma Técnica Peruana ISO 27001:2013 y la Norma Técnica Peruana ENTP-ISO/IED 27002.

De igual manera, para la elaboración del mismo se toman en cuenta la ley 29733 Ley de Protección de Datos Personales y los derechos ARCO de la Autoridad Nacional de Protección de Datos Personales los cuales se dictan con la finalidad reglamentar el artículo 2 numeral 6 de la constitución política de Perú. Asimismo, se toman las leyes N~27806, de Transparencia y Acceso a la Infromación Pública cuyo fin es la promoción de la transparencia en las accioneas del Estado; y la ley N~27489 que regula las centrales privadas de información de riesgos y protección al titular de la información a la cual se debe regir la Entidad del Sistema Financiero.

La política de seguridad de la información incluye los objetivos de seguridad de la información, la definición y principios para servir de guía en todas las actividades relacionadas con la seguridad de la información.

ALCANCE

- Todas las personas que pertenecen al equipo de L & M Seminario Group S.A.C., directivo y colaborador en general que laboren en la empresa; así como a los proveedores y el comité de seguridad de la información.
- Abarca todos los requisitos de las partes interesadas relevantes a la seguridad de la información.
- La presente política está creada con el fin de proteger la información brindada por las partes interesadas de la empresa.

CONTROL 5.1.1.
NTP ISO/IEC 27002:2016

PÁGINA 02

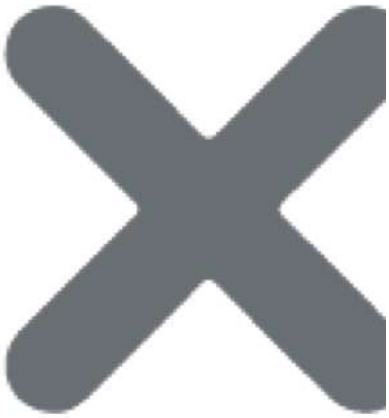
OBJETIVOS

La Política de Seguridad de la Información tiene por objetivo regular la gestión de la seguridad de la información al interior de la entidad. De igual manera, tiene los siguientes objetivos específicos:

a) Crear un marco normativo de obligatorio cumplimiento, orientado a gestionar de manera apropiada la seguridad de información en la entidad técnica L & M Seminario Group S.A.C.

b) Establecer anualmente objetivos con relación a la seguridad de información.

c) Asegurar la disponibilidad, confidencialidad e integridad de la información.



d) Conseguir y mantener el nivel de seguridad requerido para garantizar de forma adecuada lacontinuidad del negocio, incluso en situaciones de riesgo.

e) Establecer las expectativas de la Dirección con respecto al correcto uso que el personal haga de los recursos de información de la entidad técnica L & M Seminario Group S.A.C, así como de las medidas que se deben adoptar para la protección de estos.

f) Establecer e implantar planes de formación y de no divulgación de seguridad para mejorar la formación del personal.

g) Proporcionar a L & M Seminario Group S.A.C. una herramienta que facilite a la alta direcciónla toma de decisiones apropiada, en situaciones relacionadas con la preservación de la seguridad de la información.

PAGINA 03

PRIN CIPIOS &

a. Principio de Confiabilidad: propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

b. Principio de Integridad: busca proteger que se modifiquen los datos libres de forma no autorizada.

c. Principio de Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

SANCIONES

Se sancionará conforme a la magnitud y característica no cumplido a todo aquel que viole lo dispuesto en las normas de las políticas de seguridad de la información que rigen al personal de L & M Seminario Group S.A.C. Asimismo, según el artículo 39 y 40 de la ley 29733 Proteccion de datos personales del Perú, la sanción a los responsables del tratamiento de datos es:

- Infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).

- Infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).

- Infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).

Señala también que la multa impuesta no puede excederse del diez por ciento de los ingresos brutos anuales en el año anterior de cometida la infracción.

PAGINA 04

RESPONSABILIDADES

La junta directiva de la empresa mantiene las siguientes funciones:

- Mantener actualizada su agenda sobre los temas de seguridad del a información a tratar en las reuniones del comité de seguridad de la información de L & M Seminario Group S.A.C.
- Fijar las fechas para realizar las reuniones del comité.
- Revisar y aprobar las actas del comité, previa rubrica de sus integrantes.

El Comité de Gestión de Seguridad de la Información de L & M Seminario Group S.A.C. vela por la existencia y cumplimiento de las medidas de seguridad de la información de la organización, propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan.solucionarlo rápidamente

El gerente general de la empresa L & M Seminario Group S.A.C. asume las siguientes funciones

Realizar las coordinaciones de las reuniones del comité conforme al calendario del presidente de comité.

Realizar las actas de cada una de las reuniones.

Convocar la firma del acta y realizara el respectivo archivo del documento.

El gerente general de operaciones de la empresa L & M Seminairo Group S.A.C. asume las siguientes funciones:

Plantear todas las modificaciones de las políticas de seguridad de información de L & M Seminario Group S.A.C. al Comité Gestión de Seguridad de Información, si en caso sea tan necesario.

Reorganizar y comunicar con la alta dirección y la administración de organización ante problemas que se puede causar en la seguridad de información, con el fin de solucionarlo rápidamente.

PAGINA 05

Políticas Relacionadas

a) Adhesión a la política:

(i) La política actual debe ser cumplida por todo el personal de L & M Seminario Group S.A.C.

(ii) El Comité de Seguridad de la Información debe mantener el control y el seguimiento en el cumplimiento de la política actual, reportando constantemente los resultados y desarrollos a los Directivos Generales de la empresa.

b) Gestión de Riesgos:

(i) El Oficial de Seguridad de la Información de L & M Seminario Group S.A.C. tiene como funciones:

- Apoyar a los demás miembros del equipo en la identificación, cuantificación y priorización de riesgos de seguridad de la información.
- Tomar decisiones de seguridad corporativa (Seguridad física, seguridad de las instalaciones e investigaciones).
- Junto a la Directiva de la empresa, puede tomar decisiones sobre qué hacer con los riesgos.

(ii) El Comité de Seguridad de Seguridad de la Información aprueba los resultados de la evaluación y tratamiento de riesgos.

c) Protección de la información:

(i) La empresa L & M Seminario Group S.A.C. sabe que la información que poseen y conoce el personal, es fundamental para el funcionamiento de la misma por lo cual le dan un alto valor lo que conlleva a considerar de suma importancia la seguridad de la información y la plantean como un objetivo institucional.

(ii) Se conoce que todos los riesgos no se pueden eliminar, solo mitigar a partir de controles que definirá la empresa para proteger la información en base al previo análisis de los riesgos.

(iii) La seguridad de la información se dará tanto en el plano informático como en el plano personal empleando acuerdos dentro de los contratos, como por ejemplo el de no divulgación, para mantener la información protegida.

d) Clasificación de la información:

(i) La información debe ser clasificada de acuerdo al nivel de importancia para L & M Seminario Group S.A.C., de acuerdo a sus necesidades o relevancias dentro del desarrollo de la empresa.

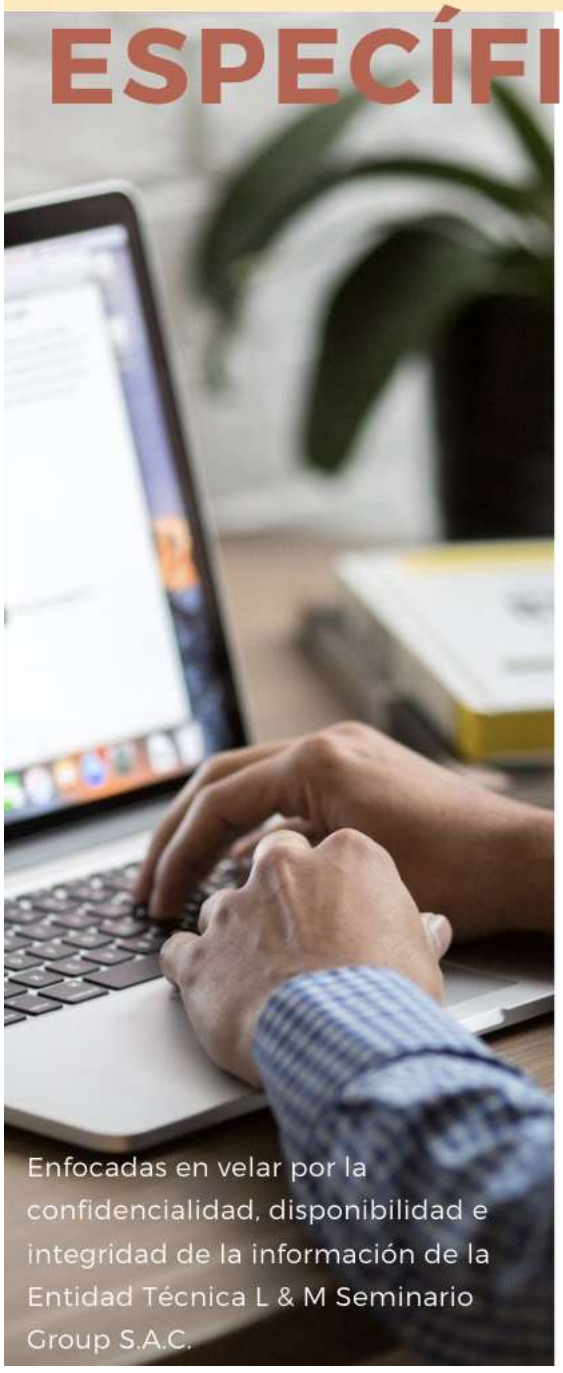
e) Uso de activos de información:

(i) Los activos de información deben ser utilizados de acuerdo a lo que L & M Seminario Group S.A.C. tenga como objetivos de acuerdo a las políticas de la empresa.

En la relación con otras empresas, L & M Seminario Group S.A.C. debe establecer convenios o contratos que tengan cláusulas o disposiciones para mantener protegida la información.

PAGINA 06

POLÍTICAS ESPECÍFICAS



POLÍTICA DE DISPOSITIVOS MÓVILES

OBJETIVOS DE ESTA POLÍTICA:

a. Crear un marco normativo acerca de las condiciones de manejo de los dispositivos móviles (celulares, tablets, etc) de la empresa y personales.

b. Garantizar el uso responsable de los dispositivos móviles proporcionados por la empresa.

c. Gestionar los riesgos derivados del uso de dispositivos móviles.

a. Los equipos personales no tendrán acceso a los servicios de la empresa. Se separa el uso privado y de negocio de los dispositivos.

b. Se debe evitar conectar los equipos de la empresa a redes inalámbricas de uso público, se deberá evitar conectar los equipos móviles por puesto USB a cualquier equipo público.

c. Se deberá tener un registro de los dispositivos móviles institucionales. Asimismo, se deberá registrar al ingresar los dispositivos móviles personales que entran a la empresa.

d. Se deberá redactar y entregar junto a los equipos un acuerdo de usuario final de acuerdo al proveedor del equipo.

e. Se tiene el deber de configurar en todos los equipos pertenecientes a la empresa la opción de borrado remoto de datos en caso de pérdida o hurto.

f. Se tiene el deber de configurar en todos los equipos pertenecientes a la empresa la opción de borrado remoto de datos en caso de pérdida o hurto.

g. Los equipos brindados a los colaboradores deberán ser configurado con contraseñas y con bloque de pantalla automático después de pasado un tiempo de inactividad de un minuto.

h. Los colaboradores solo recibirán los dispositivos proporcionados por la empresas después de haber firmado el acuerdo de usuario final.

i. Los colaboradores usarán los equipos de la empresa para fines del negocio, no se almacenarán material fotográfico o información personal en los mismos.

CONTROL 6.2.1.
NTP ISO/IEC 27002:2016

PAGINA 07

POLÍTICA DE TELETRABAJO

OBJETIVOS DE ESTA POLÍTICA:

a. Crear un marco normativo acerca de las condiciones trabajo desde casa o lugares remotos a las oficinas de la organización.

b. Definir las restricciones cuando se haga uso del telebrajo.

c. Alinear la política de teletrabajo de la organización a la ley promulgada por el congreso de la República del Perú N~30036 que regula el teletrabajo.

a. Se debe asegurar que el ambiente físico en el que se realice el teletrabjo sea seguro, así como del entorno. De lo contrario, la pérdida de la información o del equipo estará a cargo del usuario.

b. Se deberá procurar trabajar sobre un escritorio o superficie limpia, en la cual solo se encuentre el equipo, papeles en físico y útiles de escritorio a utilizar.

c. Evitar el uso del mismo ambiente en el que se realiza el teletrabajo a familiares o amigos; cuando el material no sea utilizado deberá almacenarse en una zona segura.

d. La organización se compromete a enviar semanalmente boletines informativos sobre las buenas práticas para el teletrabajo.

e. La organización evaluará el desempeño del colaborador que hace uso del teletrabjo de manera mensual.

f. La organización podrá prohibir el uso de la modalidad de teletrabajo si se presenta algún riesgo que atente contra la seguridad de la información o de comprobarse que el colaborador no alcanza con los objetivos propuestos

g. El colaborador se compromete a hacer uso y gestionar el material a su disposicion de manera responsable y a tener la capacidad de autogestión del tiempo, gestión de la comunicación, sistematicidad, disciplina y orden.

h. El colaborador deberá asegurarse y velar para que el material no sea utilizado por terceros.

CONTROL 6.2.2.
NTP ISO/IEC 27002:2016

PAGINA 08

POLÍTICA DE CONTROL DE ACCESO

a. Adhesión a la Política:

(i) La presente política debe ser cumplida por todo el personal de L & M Seminario Group S.A.C., sin excepción.

(ii) El Comité de Gestión de Seguridad de la Información debe monitorear el cumplimiento de la presente política.

b. Revisión de derechos de acceso de usuarios:

L & M Seminario Group S.A.C. deberá revisar y asignar privilegios de accesos a cada colaborador que ingrese a la empresa. Los mismos que serán revisados en intervalos regulares de tres meses o cada que el contrato sea renovado, de ser el caso de un ascenso o descenso se realizará una revisión de sus derechos, los cuales se especificaran en el nuevo contrato a firmar. El comité de seguridad de la información llevará un registro de todas las cuentas privilegiadas para una revisión periódica mensual.

c. Acceso a redes y servicios de red:

Los colaboradores. deberán tener acceso solo a la red y servicios de red inalámbrica del área de trabajo a la que pertenecen, autorización la cual será especificada el día de inducción a la empresa. Para el acceso a la red inalámbrica se proporcionará una contraseña al usuario la cual es intransferible y confidencial del área de trabajo en el que se desempeña.

d. Registro y baja de usuarios

L & M Seminario Group S.A.C., debe mantener los registros de cada uno de los integrantes de los procesos que hayan sido autorizados en el sistema. Cada usuario que acceda al sistema de información de la organización deberá utilizar la identificación única de usuario (ID) con el fin de que ellos sean vinculados y responsables de sus acciones en el sistema. El uso de ID compartidos solo deberá ser permitido cuando sea necesario por razones de negocio y deberá ser plasmado en un documento en el cual todos los involucrados se comprometen a asumir las responsabilidades.

OBJETIVOS DE ESTA POLÍTICA:

a. Crear un marco normativo de obligatorio cumplimiento orientado a gestionar de manera adecuada el control de acceso.

b. Establecer los límites de acceso a la información e instalaciones de procesamiento de la información en la oficina donde se almacenan todos los documentos en físico de la gestión documental

c. Establecer los lineamientos para el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.

CONTROL 9.1.1.
NTP ISO/IEC 27002:2016

PAGINA 09

RELACIONES CON LOS PROVEEDORES

OBJETIVO DE ESTA POLÍTICA:

a. Asegurar protección a los activos de la organización que son accesibles por los proveedores

a. La empresa L & M Seminario Group S.A.C. identifica los tipos de proveedores a los que permitirá el acceso a su información.

b. Los proveedores no cuentan con acceso a toda la información de la empresa y tienen un constante monitoreo y control.

c. Los proveedores reciben la información sobre los tipos de obligaciones que deben realizar para garantizar la seguridad de la información de la empresa.

d. Los proveedores conocen los requisitos y procedimientos de gestión de incidentes.

e. La empresa L & M Seminario Group S.A.C. realiza auditorías internas o independientes a los proveedores y el seguimiento de problemas identificados.

f. La empresa L & M Seminario Group S.A.C. garantiza que sus proveedores cuentan con la capacidad de servicio junto con los planes realizables diseñados para garantizar que los niveles de continuidad de servicio acordado se mantendrán después de fallas importantes en el servicio o desastres.

CONTROL 15.1.1.
NTP ISO/IEC 27002:2016

PAGINA 10

POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

OBJETIVOS DE ESTA POLÍTICA:

a. Establecer las disposiciones con respecto al uso de las computadoras y terminales cuando estas se encuentran desatendidas en las instalaciones de procesamiento de la información.

b. Establecer los lineamientos que faciliten el almacenamiento tanto electrónico como de papeles para mantener la seguridad de la información.

a. Toda información en papel, es decir en físico, que no sea usada y que sea de carácter sensible o crítico para el negocio deberá ser asegurada bajo llave en el cubículo del colaborador que maneje dicha información, el cual será responsable de la llave y de velar por su seguridad especialmente cuando la oficina se encuentre desocupada; dejando al finalizar el día su mesa de trabajo sin ningún papel en ella.

b. Se debe utilizar el mecanismo de bloqueo de pantalla y de teclado con una contraseña; la contraseña de bloqueo es personal. Todas las computadoras contarán con restricción de tiempo de sesión desatendida.

c. Las impresoras deberán ser usadas solo cuando sean necesarias, de tratarse de información sensible y para obtener las impresiones utilizará el código de uso PIN y estará ubicado al lado de la impresora, retirando los documentos inmediatamente.

a. Responsabilidades del área de informática

Deberá programar un código PIN para el funcionamiento de la impresora.

Deberá establecer un manual de usuario en el que se indique las características que cada trabajador debe poner en sus contraseñas, la cual debe contener números y símbolos cuando no esté en uso el equipo.

b. Responsabilidades del colaborador

Deberá guardar todo equipo portátil guardado bajo llave al finalizar la jornada laboral.

Deberá utilizar el mecanismo de bloqueo de pantalla y de teclado cada que la computadora este desatendida. Debe desconectar todos los equipos que estén bajo su responsabilidad al finalizar la jornada laboral.

CONTROL 11.2.9.
NTP ISO/IEC 27002:2016

PAGINA 11

POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE LA INFORMACIÓN

OBJETIVO DE ESTA POLÍTICA:

a. Establecer los lineamientos para la transferencia adecuada de información sensible de la empresa L & M Seminario Group S.A.C.

a. Responsabilidades del área de informática

El encargado de informática deberá realizar cifrado de documentos que contenga información sensible.

Deberá encargarse de redactar el acuerdo sobre transferencia de información.

b. Responsabilidades del colaborador

Los colaboradores de L & M Seminario Group S.A.C. no deberán comunicar información sensible mediante medios telefónicos, con el fin de prevenir interpretaciones de terceros que escuchen dicha conversación.

Los colaboradores deberán evitar entablar conversaciones confidenciales en espacios públicos o abiertos. Ningún mensaje deberá ser dejado desatendido en contestadores.

Al iniciar sus actividades laborales en la empresa y al finalizarlas, los colaboradores deberán aceptar y firmar el acuerdo de confidencialidad o no divulgación.

a. La información digital transportada físicamente a otro lugar deberá protegerse del acceso no autorizado haciendo uso de mensajeros fiables, todo equipo trasladado físicamente deberá embalarse y protegerse contra impactos.

b. Si es necesario el uso de dispositivos móviles se deberá eliminar inmediatamente después de utilizada la información. La información trasladada en dispositivos USB deberá cifrarse.

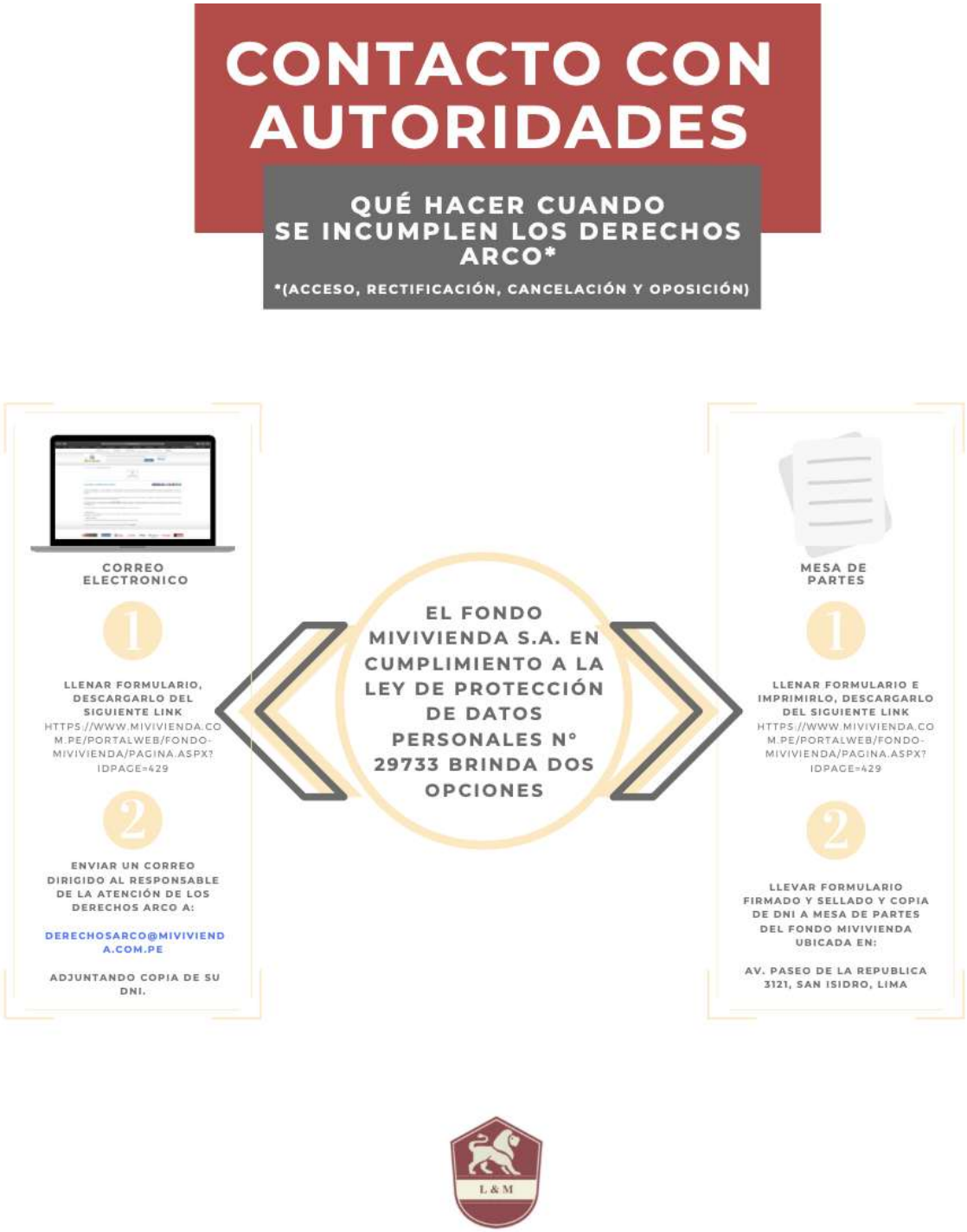
CONTROL 8.3.1.
NTP ISO/IEC 27002:2016

PAGINA 10


PROCEDIMI
ENTOS
A SEGUIR
por todos los colaboradores de L &
M Seminrio Group S.A

CONTROL 9.1.1.
NTP ISO/IEC 27002:2016

PAGINA 11


CONTACTO CON AUTORIDADES
QUÉ HACER CUANDO SE INCUMPLEN LOS DERECHOS ARCO*
*(ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN)
CORREO ELECTRONICO
1
LLENAR FORMULARIO, DESCARGARLO DEL SIGUIENTE LINK HTTPS://WWW.MIVIVIENDA.COM.PE/PORTALWEB/FONDO-MIVIVIENDA/PAGINA.ASPX?IDPAGE=429
2
ENVIAR UN CORREO DIRIGIDO AL RESPONSABLE DE LA ATENCIÓN DE LOS DERECHOS ARCO A:
DERECHOSARCO@MIVIVIENDA.COM.PE
ADJUNTANDO COPIA DE SU DNI.
EL FONDO MIVIVIENDA S.A. EN CUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS PERSONALES N° 29733 BRINDA DOS OPCIONES
MESA DE PARTES
1
LLENAR FORMULARIO E IMPRIMIRLO, DESCARGARLO DEL SIGUIENTE LINK HTTPS://WWW.MIVIVIENDA.COM.PE/PORTALWEB/FONDO-MIVIVIENDA/PAGINA.ASPX?IDPAGE=429
2
LLEVAR FORMULARIO FIRMADO Y SELLADO Y COPIA DE DNI A MESA DE PARTES DEL FONDO MIVIVIENDA UBICADA EN:
AV. PASEO DE LA REPUBLICA 3121, SAN ISIDRO, LIMA
L & M
CONTROL 6.1.3.
NTP ISO/IEC 27002:2016
PAGINA 12

TELETRABAJO

CÓMO ENVIAR ARCHIVOS CON INFORMACIÓN SENSIBLE

CON EL FIN DE EVITAR CONFLICTOS ACERCA DE LA AUTORIZACIÓN Y DERECHOS DE PROPIEDAD

1 ASEGÚRATE DE ESTAR CONECTADO A UNA RED SEGURA ANTES DE ENVIAR EL ARCHIVO, RECUERDA QUE ERES RESPONSABLE DE TU ACTIVO,

HAZ CLICK EN GUARDAR COMO, LUEGO EN OPCIONES Y CREA LA CONTRASEÑA DE ACCESO, LA CUAL DEBERÁ CONTENER LETRAS, NÚMEROS Y UN CARÁCTER ESPECIAL EN ESTE PASO PODRÁS ELEGIR SI TIENE ACCESO AL DOCUMENTO O ES SOLO DE LECTURA. 2

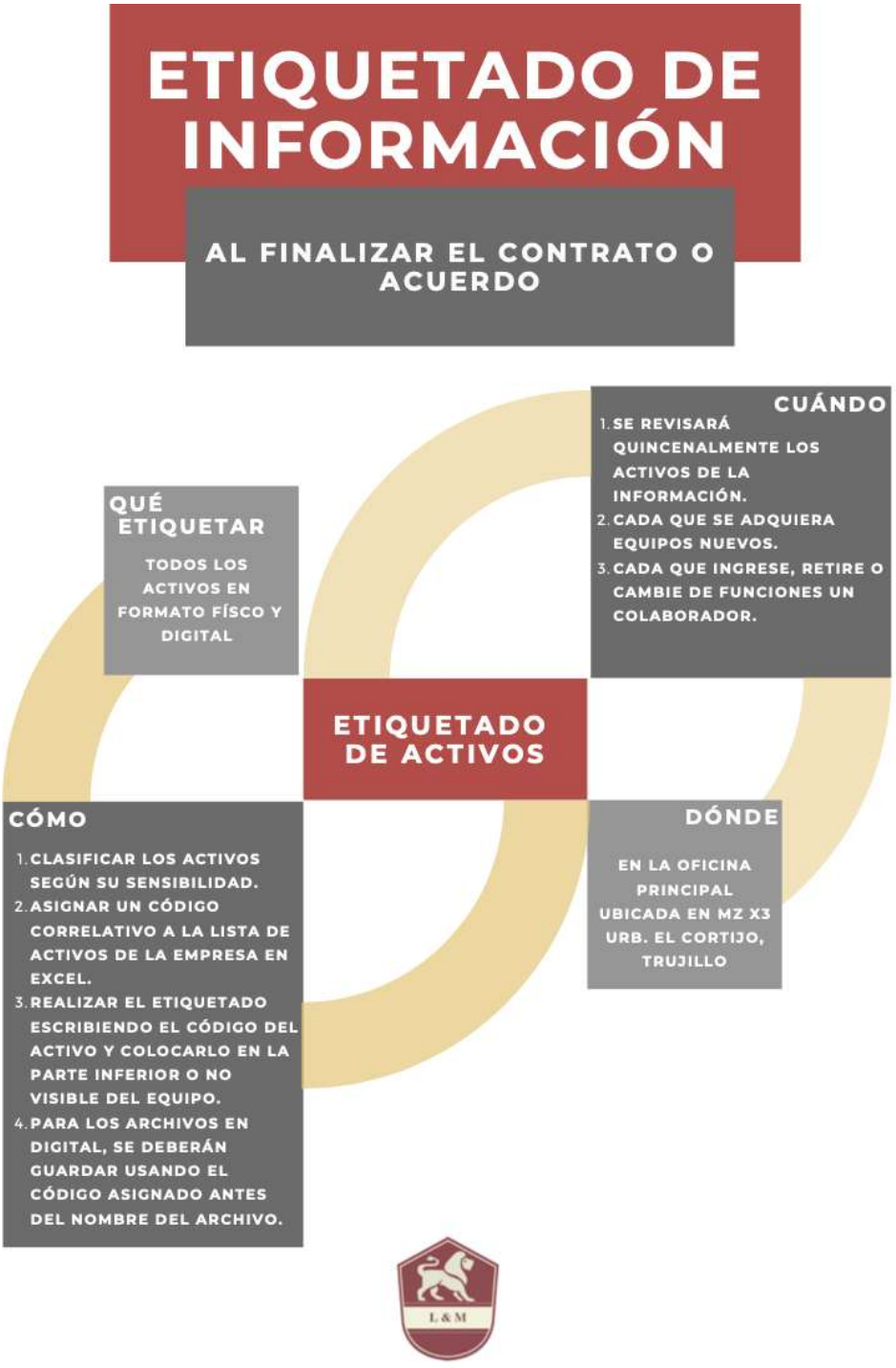
3 ENVÍA EL ARCHIVO MEDIANTE EL CORREO ELÉCTRONICO CORPORATIVO Y LA CONTRASEÑA DE ACCESO AL NÚMERO MÓVIL DEL DESTINATARIO.

L & M

CONTROL 6.2.2.
NTP ISO/IEC 27002:2016

PAGINA 13


RETORNO DE ACTIVOS
AL FINALIZAR EL CONTRATO O ACUERDO
L&M
SI EL EQUIPO ES DE LA COMPAÑÍA
• ENTREGAR EL EQUIPO AL GERENTE GENERAL CON TODA LA INFORMACIÓN, NO ELIMINAR NADA POR CUENTA PROPIA.
• EL GERENTE GENERAL VERIFICARÁ SU CONTENIDO ANTES DE LA ELIMINACIÓN O REUTILIZACIÓN DEL EQUIPO.
SI HACÍAS USO DE EQUIPO PROPIO
• ENTREGAR EL EQUIPO AL PARA VERIFICAR, EXTRAER Y POSTERIORMENTE ELIMINAR LA INFORMACIÓN DEL EQUIPO PERSONAL.
• RECUERDA QUE ESTE PERMISO LO FIRMASTE EN EL ACUERDO NDA AL INICIAR EL CONTRATO.
L&M
CONTROL 8.1.4.
NTP ISO/IEC 27002:2016
PAGINA 14

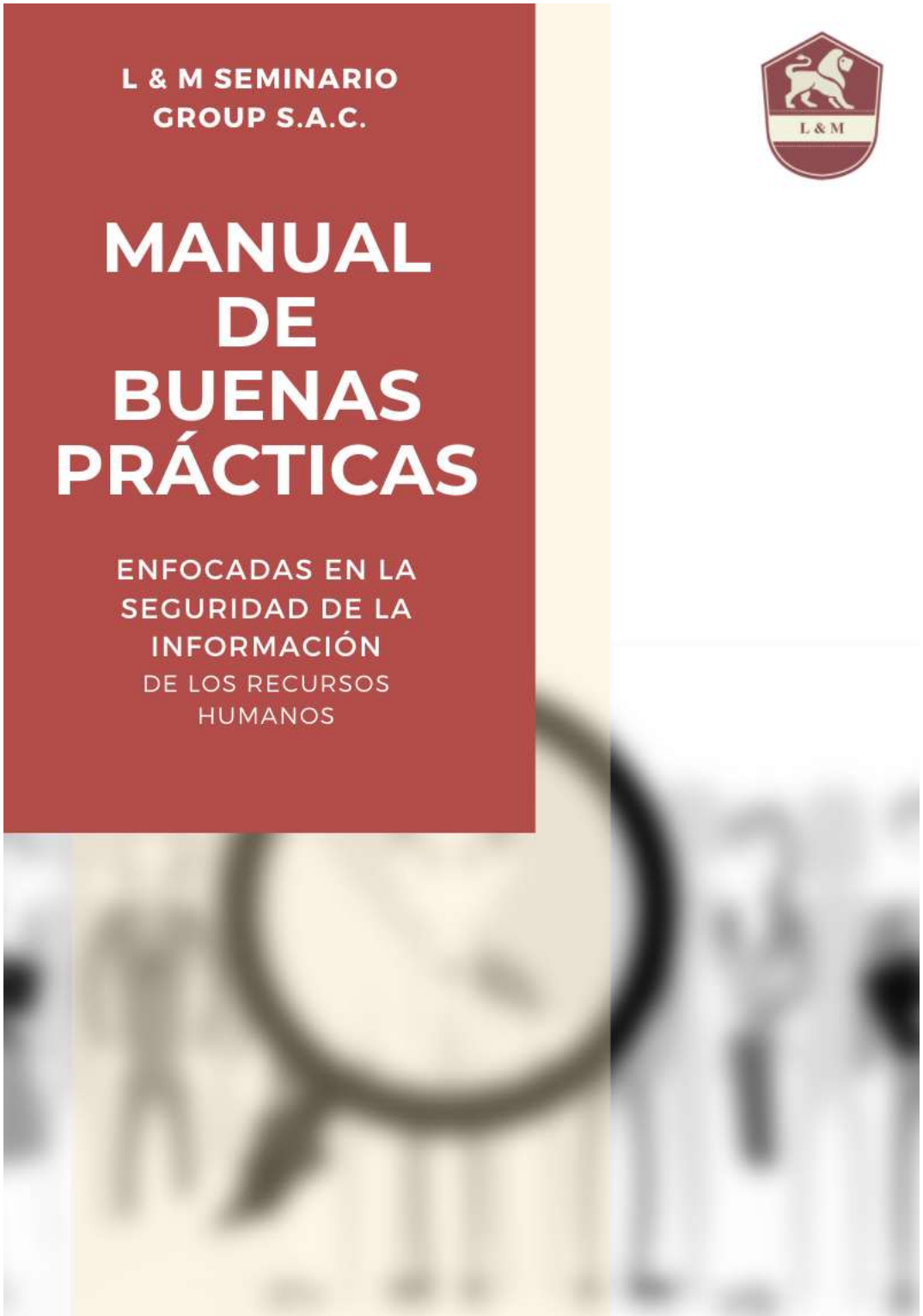


CONTROL 8.1.1.
NTP ISO/IEC 27002:2016

PAGINA 15


MEDIOS REMOVIBLES
CÓMO TRATAR CON MEDIOS REMOVIBLES
Autorizar salida
El gerente general deberá autorizar la salida y llevar registro de la fecha y hora de salida
Firmar registro
El colaborador deberá firmar la ficha de registro de autorización de salida del equipo
Colaborador
Gerente General
Uso del equipo fuera de la compañía
Una vez puesto a disposición del colaborador este deberá hacer uso del equipo en un ambiente seguro y protegido.
REMOCIÓN DE EQUIPOS
De la oficina central de la empresa L & M Seminario Group.
Verificar equipo
El gerente general verificará y registrará el equipo, una vez conforme firmará la ficha de entrada y almacenará el mismo en una zona segura bajo llave.
Retorno del equipo
El colaborador deberá retornar el equipo en perfectas condiciones y firmar la fecha de entrada del equipo.
L & M
CONTROL 8.3.1.
NTP ISO/IEC 27002:2016
PAGINA 16

ANEXO n.° 11. Manual de Buenas Prácticas enfocado en los Recursos Humanos



SEGURIDAD DE LA INFORMACIÓN ENFOCADA EN LOS RECURSOS HUMANOS

Se ha considerado la elaboración del presente manual como guía para los resposnsables del recurso humano en la organización desde la selección del nuevo personal, los términos y condiciones del empleo, hasta la terminación del contrato o cambio de responsabilidades dentro de nuestra organización. El uso de este manual o guía es de carácter obligatorio.

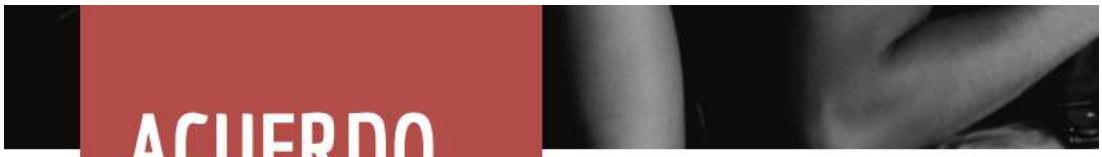
ANTES

SELECCIÓN Y FIRMA DE ACUERDO NDA

Se debe garantizar la comprensión de las responsabilidades, la elección de las personas adecuadas para el rol y los términos y condiciones del empleo antes de empezar a laborar en la organización.

CONTROL 7.1.1.
NTP ISO/IEC 27002:2016

PÁGINA 02



ACUERDO DE NDA

COMUNICAR Y FIRMAR AL CONTRATAR UN NUEVO COLABORADOR.

ACUERDO DE NO DIVULGACIÓN DE LA INFORMACIÓN

Entre L & M SEMINARIO GROUP S.A.C., con domicilio en Mz. X3 lote 5 Urbanización Vista Hermosa, dedicada a la construcción, representada en este acto por Luis Hernando Seminario Narro en su carácter de gerente general y representante legal, en adelante LA EMPRESA, por una parte y por la otra parte, el señor (NOMBRE DEL COLABORADOR), documento (DNI) , domicilio (DIRECCIÓN), en adelante COLABORADOR, en lo sucesivo se denominaran en forma conjunta e indistinta LAS PARTES, quienes declaran:

a) Que (NOMBRE DEL COLABORADOR) se desempeña para LA EMPRESA cumpliendo funciones de (PUESTO)

b) Que de acuerdo con el Art. 2 de la Constitución Política del Perú y a la Ley 29733, ley de Protección de Datos Personales, se considera necesario especificar a más amplio alcance lo siguiente.

Por medio de la presente, LAS PARTES acuerdan lo siguiente:

A mantener confidencialidad respecto de toda la información obtenida, a no divulgar ningún material o información a terceras personas sin la previa autorización escrita del Comité de Seguridad de L & M Seminario Group S.A.C., a no utilizar la información para ningún otro propósito que no esté relacionado con la empresa L & M Seminario Group S.A.C., en la seguridad de información; y a no utilizar la información de cualquier manera que pudiera generar conflictos con los intereses de la empresa.

Primero. Confidencialidad

- EL COLABORADOR se obliga en forma irrevocable ante LA EMPRESA a devolver cualquier documentación, equipo y antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente Acuerdo en el supuesto de que cese la relación entre las partes por cualquier motivo.

- EL COLABORADOR asume la obligación de confidencialidad acordada por todo el plazo de la relación laboral. Asimismo, asume la responsabilidad de velar por la integridad de la información brindada dentro de su empresa, un proveedor con inadecuada gestión de seguridad de la información puede poner en riesgo la información.

- Se deja constancia que la violación o el incumplimiento de la obligación de confidencialidad a cargo del COLABORADOR, así como la falsedad de la información que pudiere brindar a terceros, podrá dejarlo incurso en el delito de violación de secreto, siendo facultad de LA EMPRESA formular la denuncia del caso y constituirse en parte querellante.

Segundo. Compensación. Resarcimiento.

- Queda expresamente aclarado que la remuneración que EL COLABORADOR percibe de LA EMPRESA, compensa a las obligaciones de confidencialidad, aclaradas en este documento.

- De igual forma, queda expresamente convenido que todo incumplimiento total y/o parcial imputable al COLABORADOR con relación a las obligaciones de confidencialidad asumidas por el presente, facultará a LA EMPRESA para disponer la extinción del contrato de trabajo con justa causa. Asimismo LA EMPRESA queda facultada para accionar por los daños y prejuicios efectivamente ocasionados, así como para constituirse en parte querellante en denuncia penal contra EL COLABORADOR.

Lugar y fecha: ....., ... de ..... de 2020.

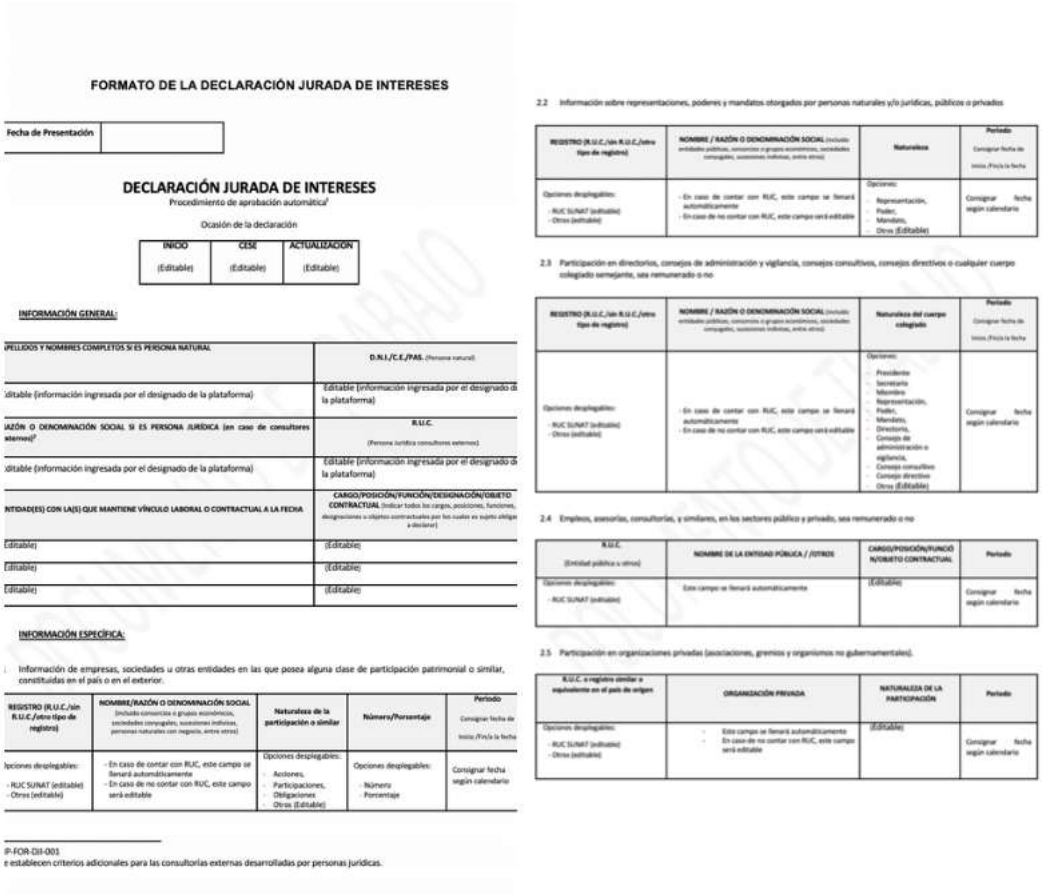
Colaborador	Gerente General L & M Seminario Group S.A.C.

CONTROL 7.1.2.
NTP ISO/IEC 27002:2016

PÁGINA 03

DECLARACION JURADA DE INTERESES

COMUNICAR Y FIRMAR AL CONTRATAR UN NUEVO COLABORADOR.



FORMATO DE LA DECLARACIÓN JURADA DE INTERESES

Fecha de Presentación

DECLARACIÓN JURADA DE INTERESES

Procedimiento de aprobación automática[1]

Ocasión de la declaración

INICIO	CESE	ACTUALIZACIÓN
(Editable)	(Editable)	(Editable)

INFORMACIÓN GENERAL:

APELLIDOS Y NOMBRES COMPLETOS SI ES PERSONA NATURAL	D.N.I./C.E./PAS. (Persona natural)
Editable (información ingresada por el designado de la plataforma)	Editable (información ingresada por el designado de la plataforma)
RAZÓN O DENOMINACIÓN SOCIAL SI ES PERSONA JURÍDICA (en caso de consultores externos)[2]	R.U.C. (Persona jurídica consultores externos)
Editable (información ingresada por el designado de la plataforma)	Editable (información ingresada por el designado de la plataforma)
ENTIDAD(ES) CON LA(S) QUE MANTIENE VÍNCULO LABORAL O CONTRACTUAL A LA FECHA	CARGO/POSICIÓN/FUNCIÓN/DESIGNACIÓN/OBJETO CONTRACTUAL (Indicar todos los cargos, posiciones, funciones, designaciones u objetos contractuales por los cuales es sujeto obligado a declarar)
Editable)	(Editable)
Editable)	(Editable)
Editable)	(Editable)

INFORMACIÓN ESPECÍFICA:

Información de empresas, sociedades u otras entidades en las que posea alguna clase de participación patrimonial o similar, constituidas en el país o en el exterior.

REGISTRO (R.U.C./sin R.U.C./otro tipo de registro)	NOMBRE/RAZÓN O DENOMINACIÓN SOCIAL (Incluido consorcios o grupos económicos, sociedades conyugales, sucesiones indivisas, personas naturales con negocio, entre otros)	Naturaleza de la participación o similar	Número/Porcentaje	Periodo (Consignar fecha de Inicio/Fin/a la fecha
Opciones desplegables: - RUC SUNAT (editable) - Otros (editable)	- En caso de contar con RUC, este campo se llenará automáticamente - En caso de no contar con RUC, este campo será editable	Opciones desplegables: - Acciones, - Participaciones, - Obligaciones - Otros (Editable)	Opciones desplegables: - Número - Porcentaje	Consignar fecha según calendario

P-FOR-DJI-001
e establecen criterios adicionales para las consultorías externas desarrolladas por personas jurídicas.

2.2 Información sobre representaciones, poderes y mandatos otorgados por personas naturales y/o jurídicas, públicos o privados

REGISTRO (R.U.C./sin R.U.C./otro tipo de registro)	NOMBRE / RAZÓN O DENOMINACIÓN SOCIAL (incluido entidades públicas, consorcios o grupos económicos, sociedades conyugales, sucesiones indivisas, entre otros)	Naturaleza	Periodo (Consignar fecha de Inicio /Fin/a la fecha
Opciones desplegables: - RUC SUNAT (editable) - Otros (editable)	- En caso de contar con RUC, este campo se llenará automáticamente - En caso de no contar con RUC, este campo será editable	Opciones: - Representación, - Poder, - Mandato, - Otros (Editable)	Consignar fecha según calendario

2.3 Participación en directorios, consejos de administración y vigilancia, consejos consultivos, consejos directivos o cualquier cuerpo colegiado semejante, sea remunerado o no

REGISTRO (R.U.C./sin R.U.C./otro tipo de registro)	NOMBRE / RAZÓN O DENOMINACIÓN SOCIAL (incluido entidades públicas, consorcios o grupos económicos, sociedades conyugales, sucesiones indivisas, entre otros)	Naturaleza del cuerpo colegiado	Periodo (Consignar fecha de Inicio /Fin/a la fecha
Opciones desplegables: - RUC SUNAT (editable) - Otros (editable)	- En caso de contar con RUC, este campo se llenará automáticamente - En caso de no contar con RUC, este campo será editable	Opciones: - Presidente - Secretario - Miembro - Representación, - Poder, - Mandato, - Directorio, - Consejo de administración o vigilancia, - Consejo consultivo - Consejo directivo - Otros (Editable)	Consignar fecha según calendario

2.4 Empleos, asesorías, consultorías, y similares, en los sectores público y privado, sea remunerado o no

R.U.C. (Entidad pública u otros)	NOMBRE DE LA ENTIDAD PÚBLICA / /OTROS	CARGO/POSICIÓN/FUNCIÓN/OBJETO CONTRACTUAL	Periodo
Opciones desplegables: - RUC SUNAT (editable)	Este campo se llenará automáticamente	(Editable)	Consignar fecha según calendario

2.5 Participación en organizaciones privadas (asociaciones, gremios y organismos no gubernamentales).

R.U.C. o registro similar o equivalente en el país de origen	ORGANIZACIÓN PRIVADA	NATURALEZA DE LA PARTICIPACIÓN	Periodo
Opciones desplegables: - RUC SUNAT (editable) - Otros (editable)	- Este campo se llenará automáticamente - En caso de no contar con RUC, este campo será editable	(Editable)	Consignar fecha según calendario

*Formato DJI D.U. 020-2019 DE LA PLATAFORMA DE DECLARACIONES JURADAS DE INTERESES DE LA PRESIDENCIA DE CONSEJO DE MINISTROS

PÁGINA 03

PLAN DE CONCIENCIACIÓN

A SER DESARROLLADO POR LA ORGANIZACIÓN

ESTADO	GUÍA
Diagnóstico de necesidades de concienciación	Analizar la causas que llevan a la necesidad de capacitación. Realizar un test a los colaboradores para identificar sus conocimientos iniciales.
Programa de de concienciación	Determinar los temas a cubrir. Elegir y coordinar el especialista para cubrir las necesidades identficadas.
Ejecución de la concienciación	Implementar el programa de concienciación en las oficina principal de la organización.
Evaluación de la concienciación	Analizar los resultado comparándolos con el conocimiento incial para evaluar si se logro el objetivo. Los puntos débiles deberán ser tomados en cuenta en el próximo programa a fin de lograr la mejora continua.

ASPECTOS GENERALES A CUBRIR EN LOS PROGRAMAS

- Familiarizar a los colaboradores con las normas, acuerdos, leyes, manual de buenas prácticas y políticas respecto a la seguridad de la información.
- Dar a conocer la responsabilidad de las acciones y omisiones de los colaboradores.
- Incidir en los procedimientos de seguridad de la información.

DURACIÓN

El plan de concienciación tendrá una duración total de dos meses (02) teniendo cada fase una duración de una semana a excepción de la ejecución la cual tomará como mínimo (04) semanas.

Actividades de sensibilización:

Campaña

Anunciar la campaña una semana antes de la ejecución.

Boletines Informativos

Enviar un boletín informativo diferente semanalmente durante las 04 semanas de ejecución.

Afiches

Colocar 03 afiches en la oficina durante las 04 semanas de ejecución.

CONTROL 7.2.2.
NTP ISO/IEC 27002:2016

PÁGINA 05

PROCESO DISCIPLINARIO

La organización tomará medidas en caso incumplirse las políticas internas. De igual forma, L & M Seminario Group S.A.C. se rige bajo el decreto legislativo N° 728, Ley de Productividad y Competitividad Laboral, detallado a continuación:

CAUSAS DE DESPIDO RELACIONADAS CON LA CONDUCTA DEL TRABAJADOR (ART.24)

a) La comisión de falta grave.

b) La condena penal por delito doloso.

c) La inhabilitación del trabajador.

Las faltas graves se comprueban objetivamente en el procedimiento laboral, excluyendo las connotaciones de carácter penal o civil que tales hechos pudieran revestir. (Art.26)

FALTAS GRAVES (ART.25)

a) Incumplimiento de sus obligaciones, reiterada resistencia a las órdenes laborales o paralización intempestiva, la inobservancia del Reglamento Interno.

b) Disminuir deliberada y reiterada en el rendimiento de las labores.

c) Apropiación, retención de bienes o servicios del empleador o utilización indebidas de los mismos, en beneficio propio o de terceros.

d) Uso o entrega a terceros de infor**mación reservada del** empleador; sustracción o utilización no autorizada de documentos; la información falsa al empleador con la intención de causarle perjuicio u obtener una ventaja; y la competencia desleal.

e) La concurrencia reiterada en estado de embriaguez o bajo influencia de drogas o sustancias estupefacientes.

f) Los actos de violencia, grave indisciplina, injuria y faltamiento de palabra verbal o escrita en agravio del empleador.

g) Daño intencional a los edificios, instalaciones y demás bienes de propiedad de la empresa.

h) Abandono de trabajo por mas de 03 días consecutivos, ausencias injustificadas por mas de 05 días en un período de 30 días calendario o mas de 15 en un período de 180 días calendario,

i) Hostigamiento sexual cometido por los representantes del empleador o quien ejerza autoridad sobre el trabajador, así como el cometido por un trabajador cualquiera sea la ubicación de la víctima del hostigamiento en la estructura jerárquica del centro de trabajo.

CONTROL 7.2.3.
NTP ISO/IEC 27002:2016

PÁGINA 06

DESPUES

TERMINACIÓN Y CAMBIO DE EMPLEO O CAMBIO DE RESPONSABILIDADES

Se debe garantizar la protección de los intereses de la organización una vez el colaborador cambie sus funciones o termine con el contrato.

QUÉ HACER AL TERMINAR O FINALIZAR CONTRATO

Aplicar el procedimiento Retorno de activos en el "Manual de Buenas Prácticas enfocado en la Seguridad de la Información"

Las responsabilidades y deberes definidos por la organización una vez terminado el empleo son las siguientes:

Se prohibe la divulgación de la información de los beneficiarios del programa del Fondo MIVIVIENDA.

Se prohibe el uso de los planos de arquitectura y estructuras en otras organizaciones del mismo rubro.

QUÉ HACER AL CAMBIO DE FUNCIONES

Los cambios de responsabilidades serán comunicados.

Se actualizará el inventario de propietario de activos.

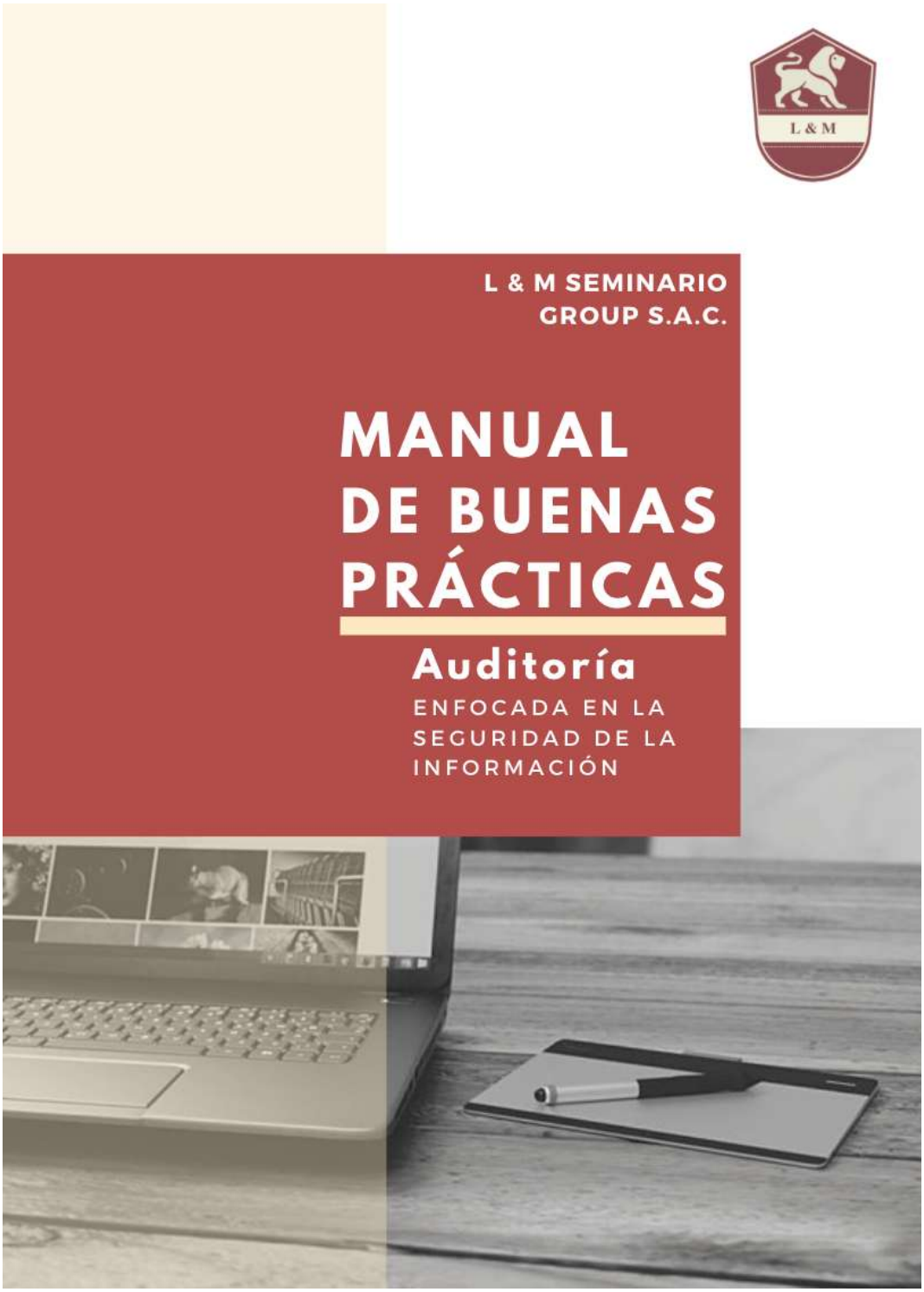
Se evaluará los activos requeridos para el cumplimiento de las nuevas funciones.

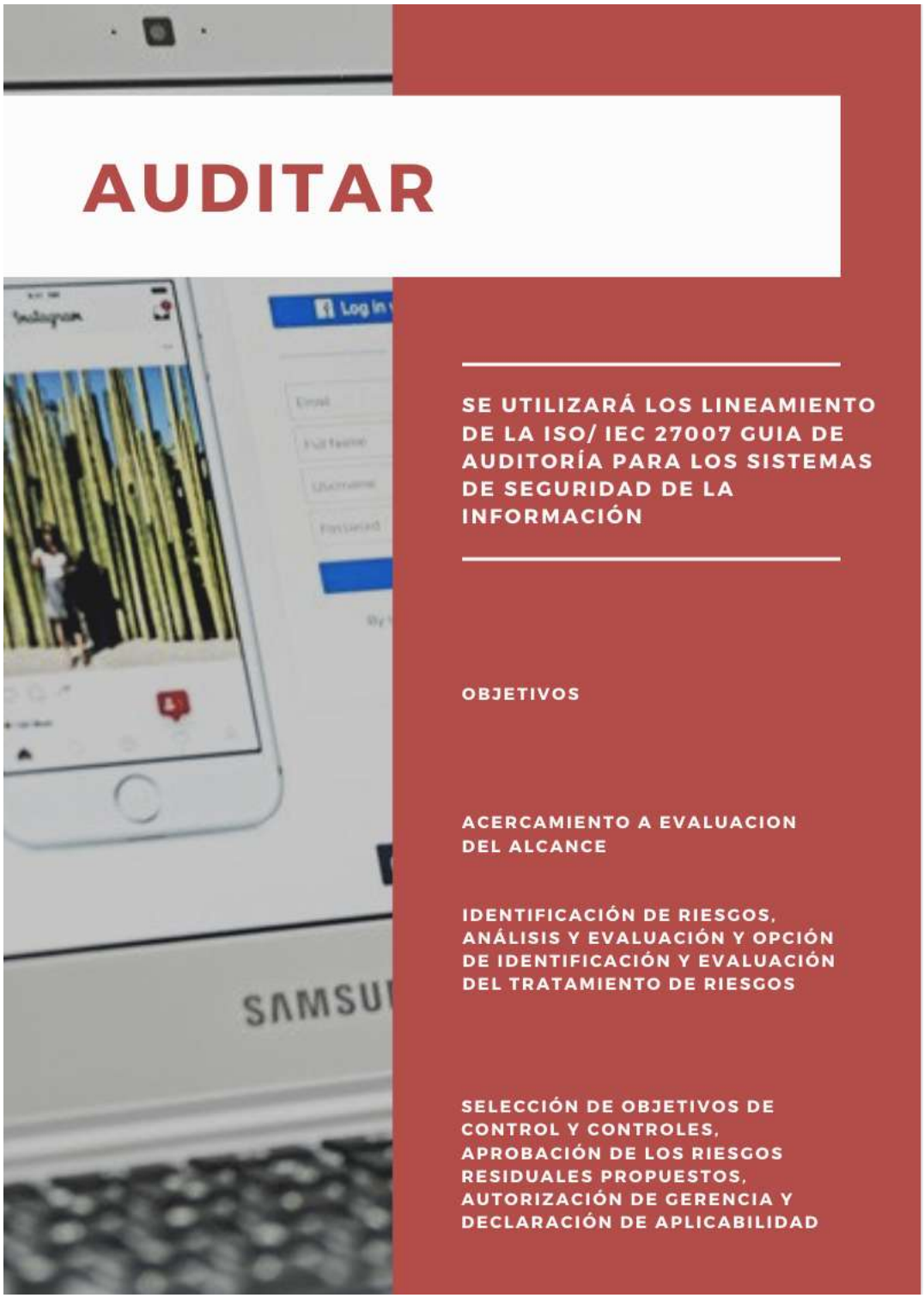
CADA ROL DESEMPEÑADO Y FUNCIONES SON DIFERENTES Y ALGUNAS INVOLUCRAN INFORMACIÓN MÁ SENSIBLE POR LO QUE ES IMPORTANTE QUE RECURSOS HUMANOS TRABAJE EN CONJUNTO CON EL JEFE DIRECTO DEL COLABORADOR A RETIRARSE PARA DETERMINAR LOS PUNTOS DE SEGURIDAD DE INFORMACIÓN A INCLUIR EN LA DESVINCULACIÓN LABORAL.

CONTROL 7.3.1.
NTP ISO/IEC 27002:2016

PÁGINA 07

ANEXO n.° 12. Manual de Buenas Prácticas de Auditoría




AUDITAR
SE UTILIZARÁ LOS LINEAMIENTO DE LA ISO/ IEC 27007 GUIA DE AUDITORÍA PARA LOS SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN
OBJETIVOS
ACERCAMIENTO A EVALUACION DEL ALCANCE
IDENTIFICACIÓN DE RIESGOS, ANÁLISIS Y EVALUACIÓN Y OPCIÓN DE IDENTIFICACIÓN Y EVALUACIÓN DEL TRATAMIENTO DE RIESGOS
SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES, APROBACIÓN DE LOS RIESGOS RESIDUALES PROPUESTOS, AUTORIZACIÓN DE GERENCIA Y DECLARACIÓN DE APLICABILIDAD

ESTABLECER LOS OBJETIVOS

PARA EL PROGRAMA DE AUDITORÍA

LOS OBJETIVOS PUEDEN DEPENDER DE:

- Identifica los requerimientos de seguridad de la información.
- Requerimientos de la ISO/IEC 27001.
- Nivel de desempeño de las personas auditoras, reflejado en la ocurrencia de errores de seguridad de la información, incidentes y efectividad en las mediciones.
- Auditar los riesgos de seguridad de la información en la organización.

LOS OBJETIVOS PARA EL PROGRAMA DE AUDITORÍA DEBEN SER ESTABLECIDOS PARA DIRIGIR EN PLANEAMIENTO Y CONDUCIR LAS AUDITORÍAS, ASÍ COMO PARA ASEGURAR QUE EL PROGRAMA DE AUDITORÍA SE IMPLEMENTE EFECTIVAMENTE.

PÁGINA 1

GUÍ PRÁCTICA PARA AUDITORÍA

1. ACERCAMIENTO A EVALUACIÓN DEL ALCANCE, POLÍTICIAS Y RIESGOS DEL SGSI

EVIDENCIA DEL AUDITOR	GUÍA PRÁCTICA
• ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (4.3 ISO 27001). • ORGANIGRAMA. • ESTRATEGIA ORGANIZACIONAL. • DECLARACIÓN DE LA POLÍTICA DEL NEGOCIO. PROCESOS Y ACTIVIDADES DEL NEGOCIO. • DOCUMENTACIÓN DE LOS ROLES Y RESPONSABILIDAD. • CONFIGURACIÓN DE LA RED. • SITIOS DE INFORMACIÓN, LISTA DE SUCURSALES, NEGOCIOS, OFICINAS Y FACILIDADES Y DISTRIBUCIÓN DEL ESPACIO EN FÍSICO. • INTERFACES Y DEPENDENCIAS QUE TIENEN LAS ACTIVDADES DEL NEGOCIO INCLUIDAS EN EL ALCANCE DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON LAS QUE NO ESTÁN INCLUIDAS EN EL ALCANCE. • LEYES RELEVANTES, REGULACIONES Y CONTRATOS. • ACTIVOS DE LA INFORMACIÓN RELEVANTES. • DOCUMENTO DE LA POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.	EL AUDITOR DEBERA CONFIRMAR QUE EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ES: - ORGANIZADO Y EJECUTADO CONFORME AL CONTEXTO DE LAS ACTIVIDADES DE LA ORGANIZACIÓN EN CONJUNTO Y A LOS RIESGOS QUE ENFRENTA. - DOCUMENTAR PARA SATISFACER LOS REQUERIMIENTOS DE DOCUMENTACIÓN. EL AUDITOR DEBERA REVISAR Y CONFIRMAR QUE TANTO EL **ALCANCE** Y LOS LÍMITE DE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN TOMANDO EN CUENTA SUS ESTRATEGIAS, OBJETIVOS, PROCESO, FUNCIONES, ESTRUCTURA ORGANIZACIONAL, ACTIVOS RELEVANTES, LOCACIONES GEOGRAFICAS, EXPECTATIVAS DE LOS INTERESADOS, ENTORNO SOCIO-CULTURAL, LEGAL, REQUERIMIENTOS CONTRACTUALES E INTERFACES. EL AUDITOR DEBERÁ CONFIRMAR QUE LA **POLÍTICA** ESTA ESPECIFICAMENTE DESCRITA EN TÉRMINOS Y CARACTERÍSTCAS DEL NEGOCIO, DE LA ORGANIZACIÓN, DE SU UBICACIÓN, DE LOS ACTIVOS Y DE LA TECNOLOGÍA. PODRÁ CONFIRMARLO MEDIANTE LOS DOCUMENTOS EN DONDE SE ESTABLECEN LOS PROCEDIMIENTOS DE LA POLÍTICA Y LAS REGLAS DEFINIDAS Y DOCUMENTADAS. EL AUDITOR DEBERÁ VERIFICAR QUE EL PRIMER ACERCAMIENTO A LA EVALUACIÓN DE RIESGOS ESTA IMPLEMENTADO PARA IDENTIFICAR LOS RIESGOS EN LOS PROCESOS Y ACTIVIDADES DEL NEGOCIO. ADICIONALMENTE, SE DEBE DEMOSTRAR QUE EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN HA SIDO ESTABLECIDO, IMPLEMENTADO, EJECUTADO, MONITOREADO, REVISADO, MANTENIDO Y MEJORADO. POR EJEMPLO: LA ORGANIZACIÓN DEBE DEMOSTRAR QUE TIENE LA CAPACIDAD DE LLEVAR A CABO ESTOS PROCESOS

PÁGINA 2

2. Identificación de riesgos, análisis y evaluación y opción de identificación y evaluación del tratamiento de riesgos

EVIDENCIA DEL AUDITOR	GUÍA PRÁCTICA
• IINVENTARIO DE ACTIVOS • DOCUMENTOS DE LA METODLOGÍAA DE EVALUACIÓN DE RIESGOS. • REPORTES DE EVALUACIÓN DE RIESGOS	EL AUDITOR DEBE REVISAR EL INVENTARIO DE ACTIVOS PARA CONFIRMAR QUE TODOS LOS ACTIVOS IMPORTANTES Y RELEVANTES EN EL ALCANCE ESTAN INCLUIDOS EN EL INVENTARIOS. EL AUDITOR DEBE REVISAR LA **IDENTIFICACIÓN DE AMENAZAS** RELACIONADAS CON LOS ACTIVOS, LAS VULNERABILIDADES EXPLOTADAS POR LAS AMENAZAS Y LAS FALLAS EN LA SEGURIDAD DE INFORMACIÓN CAUSADAS POR LAS MISMAS (INCIDENTES). EL AUDITOR DEBE REALIZAR EL **ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS** CHEQUEANDO QUE LA EVALUACIÓN DE RIESGOS SE DIRIJA A LOS ACTIVOS IMPORTANTES EN EL ALCANCE Y QUE LA EVALUACIÓN DE LAS AMANEZAS Y VULNERABILIDADES EN RELACIÓN A LOS ACTIVOS ESTA ADAPTADAS A LA ORGANIZACIÓN Y QUE NO SE USE UNA LISTA PRE-DEFINIDA DE AMANENAZAS O VULNERABILIDADES. TAMBEIN DE CONFIRMAR QUE TODA LA LISTA DE ACTIVOS IMPORTANTES ESTAN INCLUIDAS EN EL INVENTARIO Y QUE EN LA EVALUACIÓN DE RIESGOS SE HAN REFLEJADO LOS ESCENARIOS DE INCIDENTES DE ACUERDO A LAS NECESIDADES DEL NEGOCIO Y QUE HA IMPACTADO POSITIVAMENTE. EL AUDITOR DEBE REVISAR LAS OPCIONES DE **TRATAMIENTO DE RIESGOS** DE LA ORGANIZACIÓN, REVISANDO SI LOS TRATAMIENTOS (CONTROLES) SON APROPIADOS Y ESPECIFICASO POR CADA RIESGO IDENTIFICADO. EL AUDITOR DEBE BUSCAR VACÍOS Y OTRAS ANOMALÍAS Y SI SE REALIZARON CAMBIOS RECIENTES CHEQUEAR SI SE HAN INCORPORADO A LA EVALUACIÓN Y TRATAMIENTO DE RIESGOS.
ADICIONALMENTE. SE DEBE TENER EN CUENTA EL PUNTO 4.2 DE LA ISO/IEC 27001 QUE EXPLICA ACERCA DE COMPRENDER LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS. Y EL PUNTO 8.2, 8.3, 9 Y 10 DE LA ISO/IEC 27005	

PÁGINA 3

3. SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES, APROBACIÓN DE LOS RIESGOS RESIDUALES PROPUESTOS, AUTORIZACIÓN DE GERENCIA Y DECLARACIÓN DE APLICABILIDAD

EVIDENCIA DEL AUDITOR

- DOCUMENTOS DE LA METODOLOGÍA DE EVALUACIÓN DE RIESGOS.
- REPORTES DE EVALUACIÓN DE RIESGOS.
- DOCUMENTOS DESCRIBIENDO LA MAGNITUD DE LA REDUCCIÓN DE RIESGOS POR LOS CONTROLES ADOPTADOS (ES DECIR EL RESULTADO DE LA EVALUACIÓN DE RIESGOS).
- REGISTROS INDICANDO LA APROBACIÓN DE RIESGOS RESIDUALES POR GERENCIA.
- REGISTROS QUE DEMUESTREN LA AUTORIZACIÓN POR GERENCIA DE LA IMPLEMENTACIÓN Y OPERACIÓN DEL SISTEMA DE GESTIOS DE SEGURIDAD DE LA INFORMACIÓN.
- LA DECLARACIÓN DE APLICABILIDAD.

GUÍA PRÁCTICA

PARA AQUELLOS REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DERIVADOS DE LA EVALUACIÓN DE RIESGOS Y DE LAS OPCIONES SELECCIONADAS PARA LOS REQUERIMIENTOS DE TRATAMIENTO DE RIESGOS.

EL AUDITOR DEBE REVISAR QUE LOS CONTROLES **SELECCIONADOS Y LOS OBJETIVOS DE CONTROL** HAYAN ALCANZADO EL IMPACTO PLANFICADO, REALIZANDO MUESTRAS ADECUADAS. EL AUDITOR DEBE REVISAR QUE LOS CONTROLES SELECCIONADO Y LOS OBJETIVOS CONFORMAN LOS REQUERIMIENTOS DE SEGURIDAD DE INFORMACION EN VISTA DE LOS REQUERIMIENTOS DE CONTROL DEFINIDOS EN EL ANEXO A DE LA ISO/IEC 27001. DE IGUAL MANERA.

EL AUDITOR DEBE CHEQUEAR QUE LAS MEJORES PRACTICAS COMUNMENTE ADOPTADAS POR LOS NEGOCIOS RELEVANTES DEL SECTOR HAYAN SIDO CONSIDERADAS EN EL PROCESO DE SELECCIÓN DE CONTROLES.

EL AUDITOR DEBE CHEQUEAR QUE CUALQUIER REQUERIMIENTO DE SEGURIDAD DE INFORMACION EXPLICITAMENTE MANDADO POR LAS POLÍTICAS DE LA ORGANIZACIÓN, REGULACIONES O LEYES SE VEA PROPIAMIENTE REFLEJADO EN LOS OBJETIVOS DE CONTROL Y CONTROLES DOCUMENTADOS Y QUE LOS RIESGOS HAYAN SIDO REDUCIDOS PARA ACLARECER EL CRITERIO PARA LA ACEPTACIÓN DE RIESGOS.

EL AUDITOR DEBE CONFIRMAR QUE EL TRATAMIENTO DE RIESGOS ESTA APLICADO REPETITIVAMENTE SI ES QUE EL RIESGO RESIDUAL NO HA SATISFACIDADO EL CRITERIO PARA LA ACEPTACIÓN DE RIESGOS INCLUSO DESPUÉS DE LA ADOPCIÓN DE CONTROLES.

EL AUDITOR DEBE EVALUAR LA **APROBACIÓN DE LOS RIESGOS RESIDUALES** PROPUESTOS PARA CONFIRMAR QUE LA ORGANIZACIÓN A OBTENIDO APROBACIÓN DE LA GERENCIA CONSIDERANDO Y ACEPTADO CADA RIESGO RESIDUAL.

EL AUDITOR DEBE REVISAR LOS DOCUMENTOS DE **DECLARACIÓN DE APLICABILIDAD** EL CUAL DEBE DEMOSTRAR LA CONEXIÓN ENTRE LOS RIESGOS IDENTIFICADO Y LOS OBJETIVOS DE CONTROL Y LOS CONTROLES QUE HAN SIDO SELECCIONADO LOS REDUZCAN.

EL AUDITOR DEBE CONFIRMAR QUE EXISTAN ENTRADAS ADECUADAS PARA CADA OBJETIVO DE CONTROL Y CONTROLES LISTADOS EN LA ISO/IEC 27001.

EL AUDITOR DEBE REVISAR QUE LA DECLARACIÓN DE APLICABILIDAD INCLUYA LOS CONTROLES EXISTENTES. ES NECESARIO QUE LA DECLARACIÓN DE APLICABILIDAD HAYA SIDO REVISADA Y AUTORIZADA POR UN NIVEL DE GERENCIA APROPIADO CON REGISTROS DE HISTORIAL DE HABER CREADO, APROBADO, REVISADO COMO EVIDENCIA.

4. IMPLEMENTACIÓN Y OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

EVIDENCIA DEL AUDITOR

- PLAN DE TRATAMIENTO DE RIESGOS Y REGISTRO DEL PROGENSO EN LOS PLANES DEL PROYECTO.
- PROCEDIMIENTO DOCUMENTADOS Y REGISTROS DE CONTROL DE LA EFECITIVIDAD DE LA MEDICIÓN.

CUANDO SE AUDITAN LAS MEDICIONES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SE DEBE RESALTAR QUE LA MEDICIONES PUEDEN SER ALCANZADAS DE DIFERENTES MANERAS, ALGUNAS MAS COMPLEJAS QUE OTRAS; POR LO QUE EL AUDITOR NECESITA SER ADVERTIDO QUE SIN IMPORTAR QUE EXISTE UNA GUIA DISPONIBLE PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, LOS REQUERIMIENTO DE LA ISO/IEC 27001 SOLO SERAN ALCANZADO SIEMPRE Y CUANDO EL CRITERIO DE PRODUCIR Y REPRODUCIR RESULTADOS COMPARABLES PARA LA EVALUACIÓN DE CONTROLES DE EFECTIVIDAD HAN SIDO ACEPTADOS POR LA GERENCIA Y QUE ESTOS ALCANCEN LOS REQUERIMIENTOS DEL NEGOCIO TOMANDO EN CUENTA LOS RESULTADOS DE LOS PROCESOS DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS.

GUÍA PRÁCTICA

EL AUDITOR DEBE CONFIRMAR QUE LA ORGANIZACIÓN HA FORMULADO E IMPLEMENTADO EL PLAN DE TRATAMIENTO DE RIESGOS CON LAS OPCIONES IDENTIFICADAS PARA EL TRATAMIENTO DE RIESGOS. ES IMPORTANTE QUE EL AUDITOR CONFIRME QUE:

- EL PLAN DE TRATAMIENTO DE RIESGOS HA SIDO IMPLEMENTADO TOMANDO EN CUENTA LAS PRIORIDADES Y RESPONSABILIDADES DEFINIDAS.

- SE TIENE LOS RECURSOS SUFICIENTES DESIGNADOS PARA APOYAR LAS OPERACIONES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

- SE HAN IDENTIFICADO CLARAMENTE LA PRIORIDADES Y EL TIEMPO DE IMPLEMENTACIÓN DE CADA RIESGO RESPECTIVAMENTE.

- SE HAN IDENTIFICADO LOS FONDOS, ROLES Y RESPONSABILIDADES PARA EL TRATAMIENTO DE RIESGOS.

- EL PLAN DE TRATAMIENTO DE RIESGOS ES USADO Y ACTUALIZADO PROACTIVAMENTE COMO INFORMA LA HERRAMIENTA DE GESTIÓN DE LA SEGURIDAD.

EL AUDITOR DEBE CONFIRMAR QUE EL PROPÓSITO Y LA MANERA DE MEDICIÓN DE LA EFECTIVIDAD DE LOS CONTROLES SELECCIONADOS HAN SIDO CLARAMENTE DEFINIDOS.

EL AUDITOR DEBE CHEQUEAR SI LOS CONTROLES ACTUALMENTE REDUCEN EL RIESGO O IMPACTOS DE LOS INCIDENTES EN EL MÉTODO DE MEDICIÓN DE LA EFECTIVIDAD DE LOS CONTROLES.

AL AUDITAR LAS OPERACIONES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, EL AUDITOR DEBE EVALUAR CÓMO LA ORGANIZACIÓN ASEGURA LA EFECTIVIDAD DE LOS CONTROLES: ASI ES EL QUE AUDITOR DEBE EVALUAR LA EXTENSIÓN Y SUFICIENCIA DE LA MEDICIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

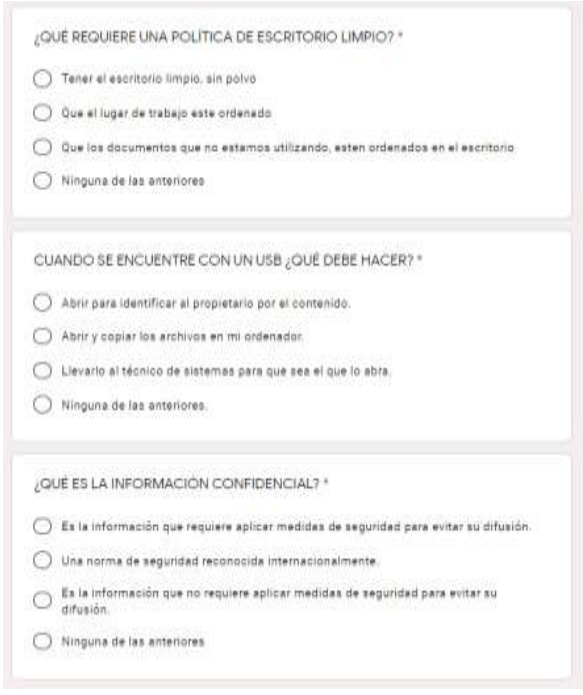
5. REVISIÓN Y MONITOREO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

EVIDENCIA DEL AUDITOR	GUÍA PRÁCTICA
• REPORTE DE EVENTOS DE SEGURIDAD E INCIDENTES DE SEGURIDAD. • DOCUMENTOS PARA REVISIÓN DE GERENCIA (ENTRADAS Y SALIDAS). • PROCEDIMIENTOS DE MEDICIÓN, INCLUYENDO LA EFECTIVIDAD DE LOS CONTROLES Y REGISTRO SOBRE LA MEDICIÓN Y EVALUACIÓN DE CONTROLES. • REGISTRO DE HABER USADO LA MEDICIÓN, INCLUYENDO LAS MEDIDAS PARA FORTALECER LOS CONTROLES, REGISTRAR LAS ACCIONES PREVENTIVAS Y EL PLAN DE TRATAMIENTO DE RIESGOS. • DOCUMENTOS QUE CONTIENEN INFORMACION ACERCA DE LOS ACTIVOS DE INFORMACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS, PLAN DE TRATAMIENTO DE RIESGOS Y DECLARACIÓN DE APLICABILIDAD. • PLAN ANUAL DE SEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN.	EL AUDITOR DEBE REVISAR LOS PROCESOS DE MONITOREO Y REVISIÓN DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, USANDO EVIDENCIA COMO LOS PLANES, REUNIONES DE REVISIÓN, REPORTES DE AUDITORÍA INTERNA DE GERENCIA, REPORTE DE BRECHAS O INCIDENTES, ETC. EL AUDITOR DEBE EVALUAR LA EXTENSIÓN DEL PROCESAMIENTO DE ERRORES, BRECHAS DE SEGURIDAD Y OTROS INCIDENTES DETECTADOS, REPORTADOS Y ABORDADOS. EL AUDITOR DEBE DETERMINAR COMO ES QUE LA ORGANIZACIÓN ES PROACTIVA Y EFECTIVA EN LA IMPLEMENTACIÓN Y REVISIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA ASEGURAR QUE LOS CONTROLES DE SEGURIDAD IDENTIFICADOS EN EL PLAN DE TRATAMIENTO DE RIESGO ESTA ACTUALMENTE IMPLEMENTADO Y EN OPERACIÓN. EL AUDITOR DEBE REVISAR LAS MEDICIONES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SU USO PARA EL CONTINUO MANEJO DE LAS MEJORAS EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. EL AUDITOR DEBE CUIDAR PARTICULARMENTE LOS PROCESOS DE AUDITORÍA, MONITOREO Y REVISIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ESTO SERÁ UN POCO DIFERENTE DEPENDIENDO DEL TIPO Y TAMAÑO DE LA ORGANIZACIÓN, PERO LAS ACTIVIDADES QUE NECESITAN SER DEMOSTRADAS POR LA ORGANIZACIÓN ESTAN CLARAMENTE EXPUESTAS EN LA ISO 27001.

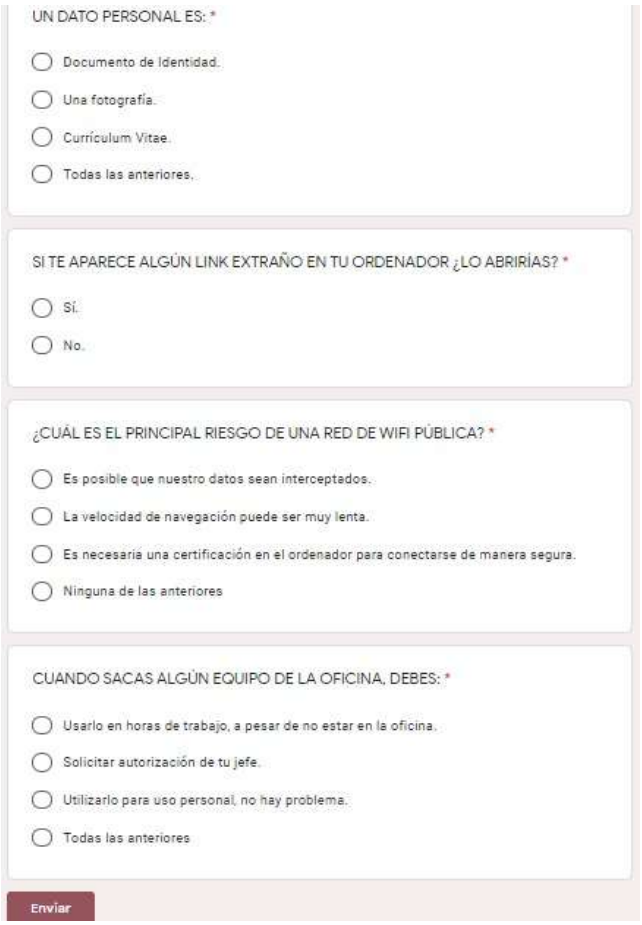
DEBE SER DE PARTICULAR INQUIETUD PARA EL AUDITOR EL HECHO QUE LA ORGANIZACIÓN HA CONSIDERADO CAMBIOS INTERNOS Y/O EXTERNOS EN SUS OPERACIONES Y SI ESOS CAMBIOS AFECTAN EN SU SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

PÁGINA 6

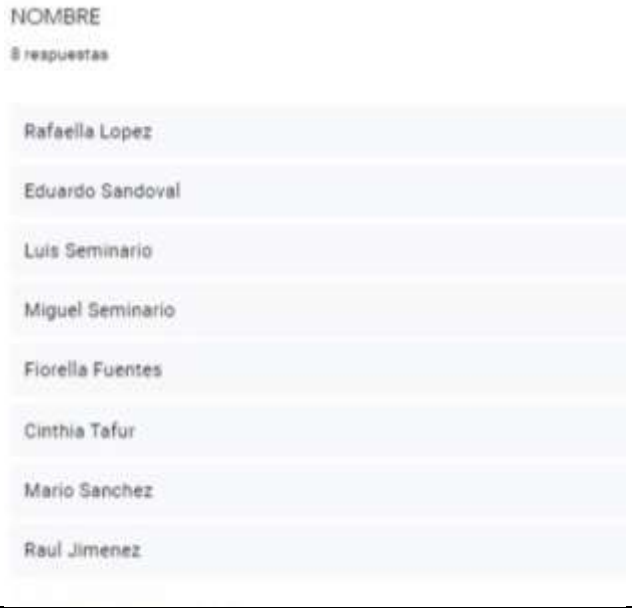
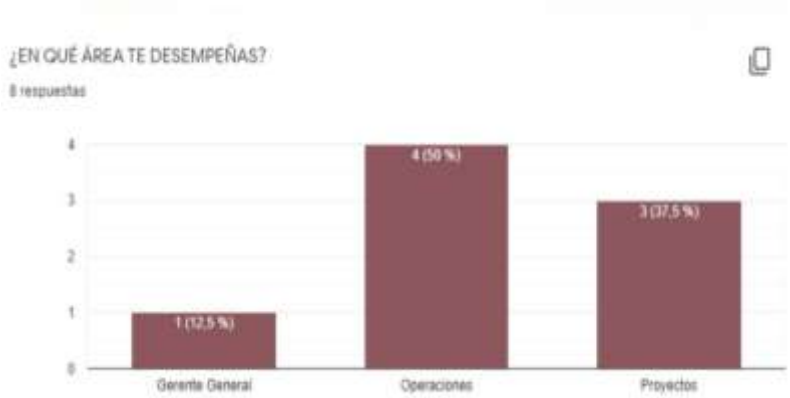
ANEXO n.° 13. Cuestionario Pre test de Seguridad de la Información

<table>
<tr><th colspan="3">Encuestas</th></tr>
<tr><td>Observación</td><td colspan="2">Encuesta envíada mediante un link de ingreso a cada uno de los 8 colaboradores, la encuesta fue realizada haciendo uso de google formularios</td></tr>
<tr><td>Fecha</td><td>20/02/20</td><td>Imagen</td></tr>
<tr><td rowspan="2">Descripción</td><td>Primera parte del cuestionario</td><td> 
</td></tr>
<tr><td>Segunda parte del cuestionario</td><td> 
</td></tr>
</table>

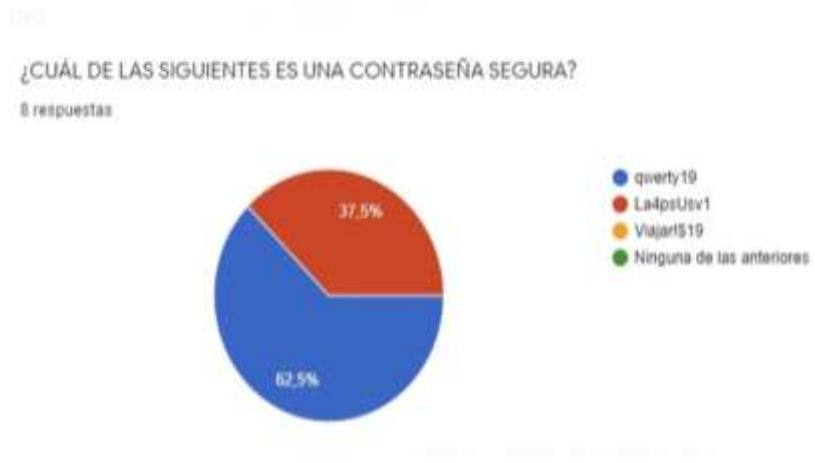
Tercera parte del cuestionario



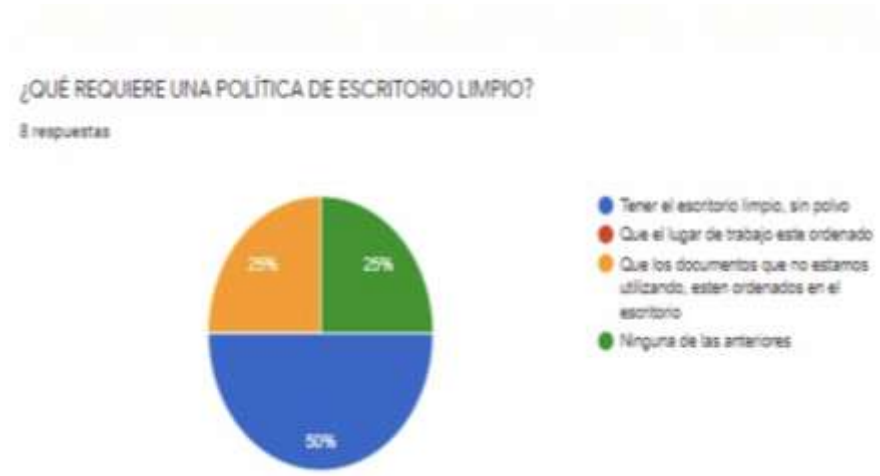
ANEXO n.° 14. Resultados pre test

Cuestionario Pre Test		
Observación	Resumen de los resultados de la prueba pre test para diagnosticar el estado del conocimiento en seguridad de la información de los 8 colaboradores de la entidad técnica L & M Seminario Group S.A.C.	
Fecha	**21/02/20**	**Imagen**
Descripción	Nombre de todos los participantes de la encuesta	
	Áreas en las que se desempeñan los colaboradores	

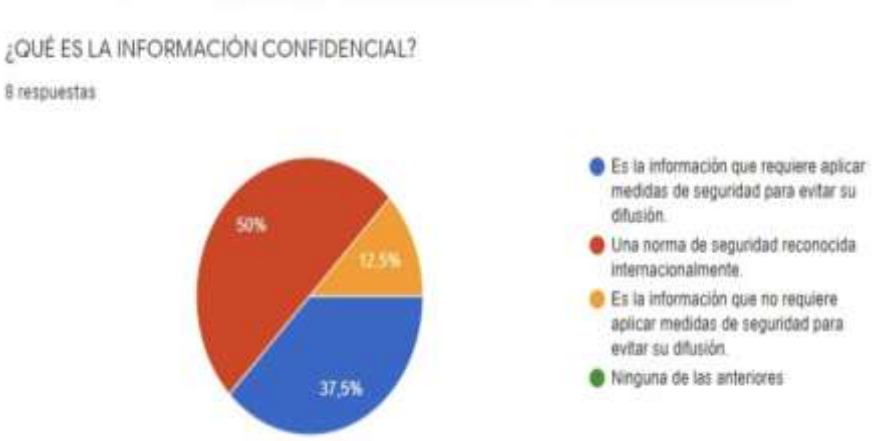
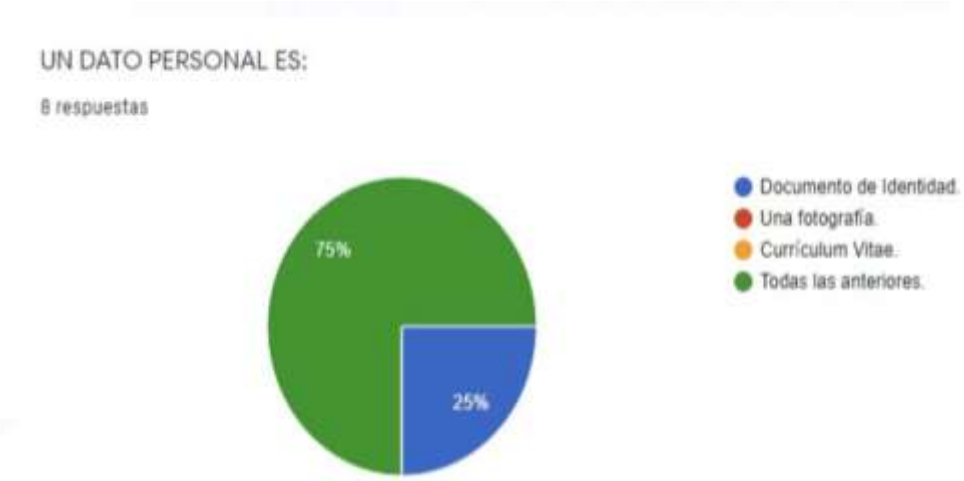
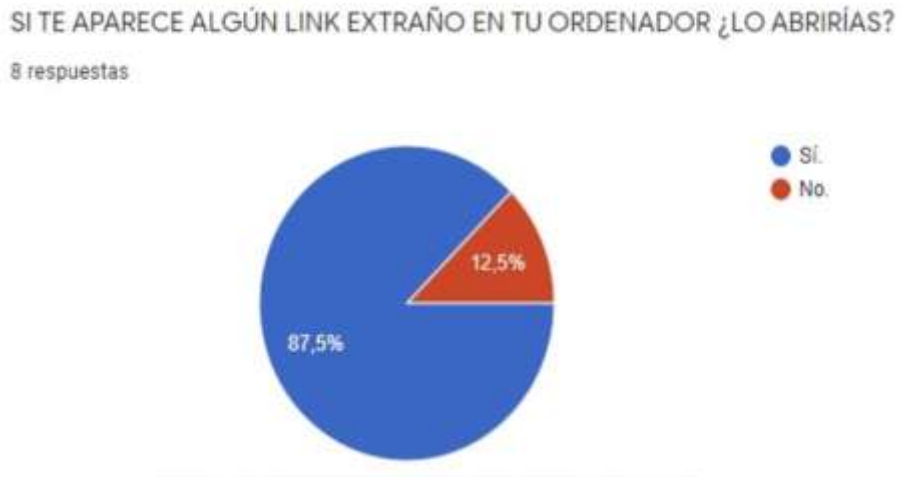
Pregunta 1: Cuál de las siguiente es una contraseña segura?

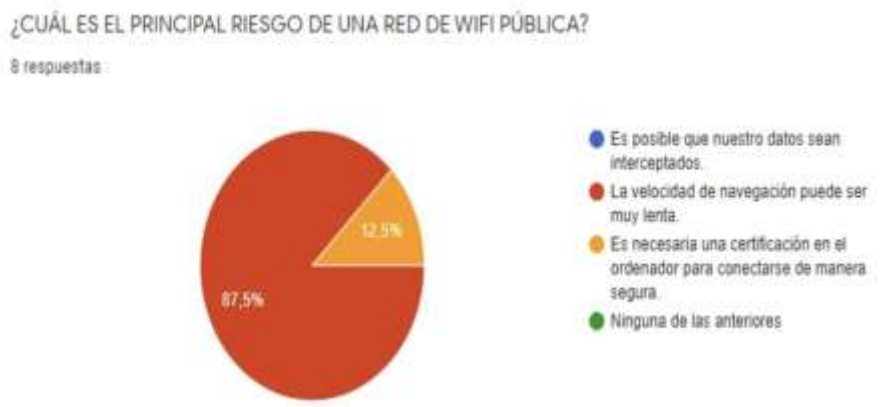
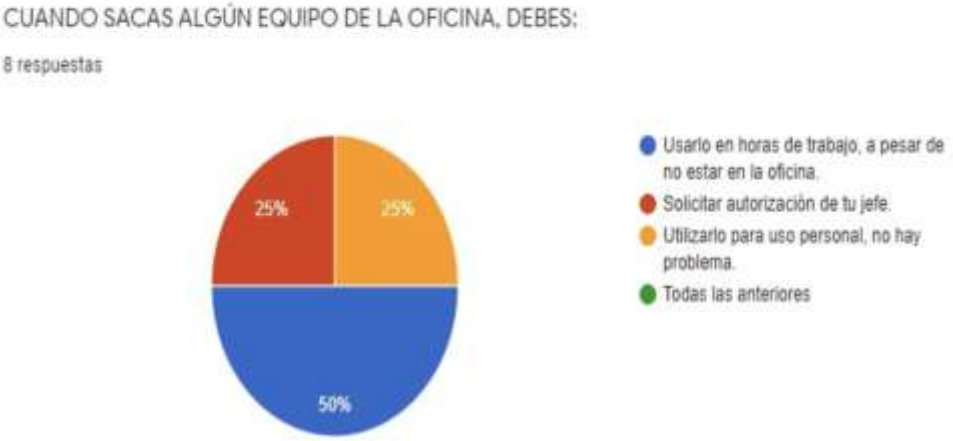


Pregunta 2: Qué requiere una política de escritorio limpio?



Pregunta 3: Qué requiere una política de escritorio limpio?

Pregunta 4: Qué es la información confidencial?	
Pregunta 5: Un dato personal es	
Pregunta 6: Si te aparece algún link extraño en tu ordenador, lo abriría?	

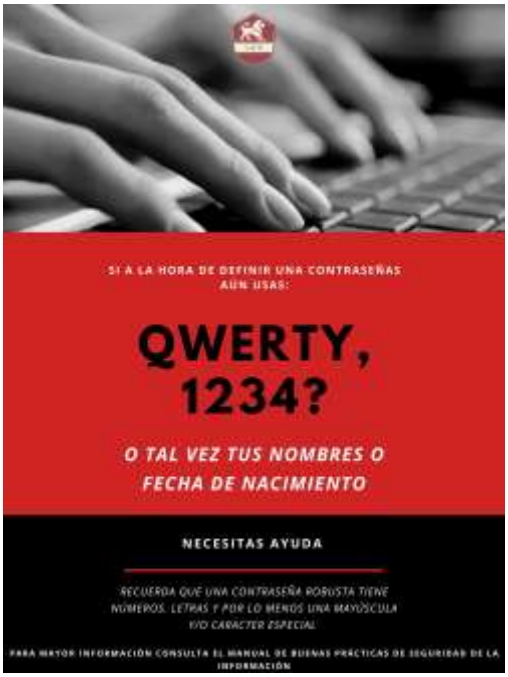
Pregunta 7: Cuál es el principal riesgo de una red de wifi pública?	
Pregunta 8: Cuándo sacas algún equipo de la oficina, debes:	

ANEXO n.° 15. Ficha del programa de capacitación

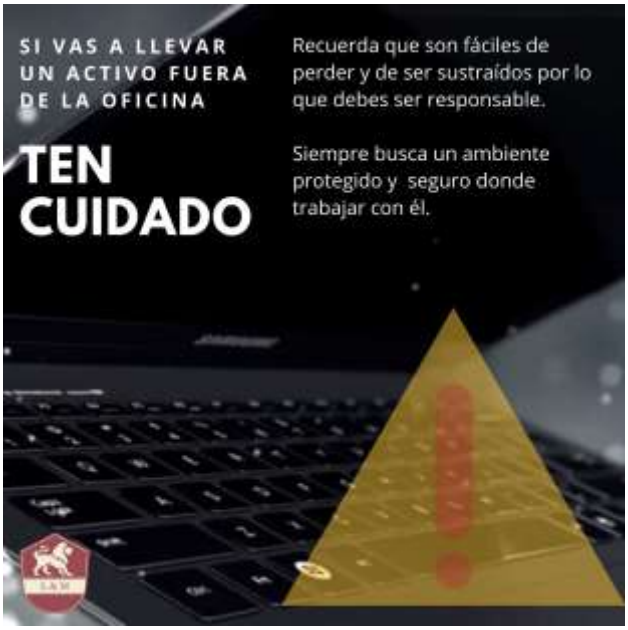
Ficha de capacitación				
Fecha		2	3	2020
Modelador	**Fernando Lopez Sanchez**			
Título	**Objetivo**	**Temas a cubrir**	**Recursos**	**Duración**
La Seguridad de la Información en nuestras funciones	Incrementar el conocimiento y generar concientización en seguridad de la información en los 8 colaborades de la entidad Técnica L & M Seminario Group S.A.C.	Conceptos básicos de la seguridad de la información. Escritorio y pantalla limpia. Remoción de medios. Contraseñas	Material impreso, material audiovisual (proyector) y útiles de escritorio	4 horas (30 minutos coffee break)

ANEXO n.° 16. Plan de Afiches del Programa de Concientización

PLAN DE AFICHES		
Instrucciones:	**Colocar Afiche en la pared de la oficina en la fecha estipulada a continuación**	
Fecha	**Retroalimentación de tema**	**Afiche**
3/03/2020 - 06/03/2020	Escritorio Limpio	
09/03/2020 - 12/03/2020	Medios Removibles	

13/03/2020 - 13/03/2020	Contraseñas	

ANEXO n.° 17. Plan de Boletines del Programa de Concientización

<table>
<tr><th colspan="3">PLAN DE BOLETINES INFORMATIVOS</th></tr>
<tr><td>Instrucciones:</td><td colspan="2">Colocar Através del correo electrónico, enviar este boletín en las fechas estipuladas</td></tr>
<tr><td>Fecha</td><td>Retroalimentación de tema</td><td>Boletín Informativo</td></tr>
<tr><td>06/03/2020</td><td>Escritorio Limpio</td><td> 
</td></tr>
<tr><td>12/03/20</td><td>Medios Removibles</td><td> 
</td></tr>
</table>

16/03/20 Contraseñas

ANEXO n.° 18. Implementación del antivirus

	ANÁLISIS PRELIMINAR					EVALUACIÓN DEL ANTIVIRUS							
N°	ACTIVO LAPTOPS	CARACTERÍSTICAS	VERSIÓN DE WINDOWS	FIREWALL	ANTIVIRUS	ANTIVIRUS	VERSION	TIPO	COSTO UNITARIO	TIEMPO PARA LA EVALUACIÓN	INICIO DE EVALUACION	FIN DE EVALUACIÓN	ANALISIS POSTERIOR - RESULTADOS
1	LAPTOP HP PROBOOK 440 G6	Intel Core i5 - 8265U RAM 8 GB	Windows 10 Pro - 1909	No Actualizado	No Instalado	NOD32	13.1.21.0	Antivirus - Internet Security	S/139.00	4 semanas	10/02/20	9/03/20	0 ARCHIVOS INFECTADOS
2	ALL IN ONE HP	Procesador AMD Athlon™ X2 3250e	Windows® 7 Home Premium original 64 bit	No Actualizado	No Instalado								
3	ALL IN ONE HP	Intel Pentium N3540	Windows 10 Pro -	Activo	Instalado - Sin Licencia								
4	ALL IN ONE HP	Procesador AMD Athlon™ X2 3250e	Windows® 7 Home Premium original 64 bit	No Actualizado	No Instalado								
5	ALL IN ONE HP	Intel Pentium N3540	Windows 10 Pro -	Activo	Instalado - Sin Licencia								

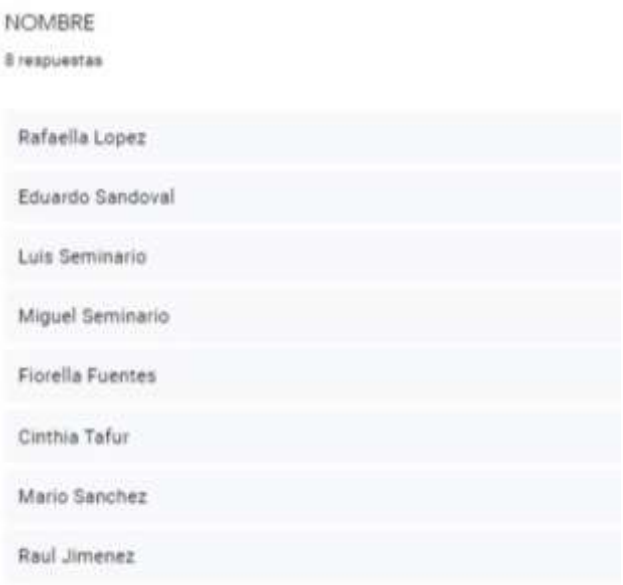
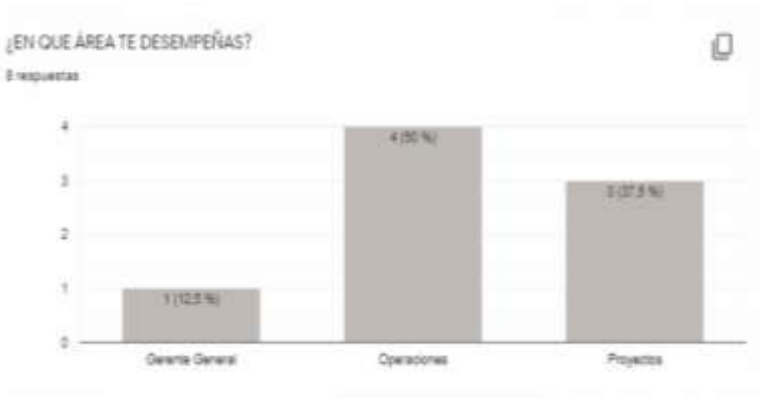
ANEXO n.° 19. Cuestionario Post Capacitación

Cuestionario Post Capacitación		
Observación	Encuesta envíada mediante un link de ingreso a cada uno de los 8 colaboradores, la encuesta fue realizada haciendo uso de google formularios	
Fecha	**17/03/20**	**Imagen**
Descripción	Primera parte del cuestionario	

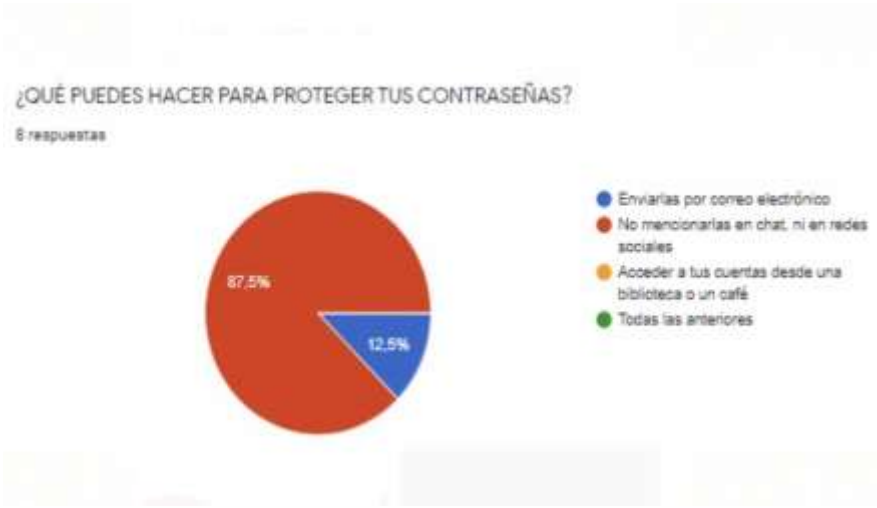
Segunda parte del cuestionario

Tercera parte del cuestionario

ANEXO n.° 20. Resultados Post Capacitación

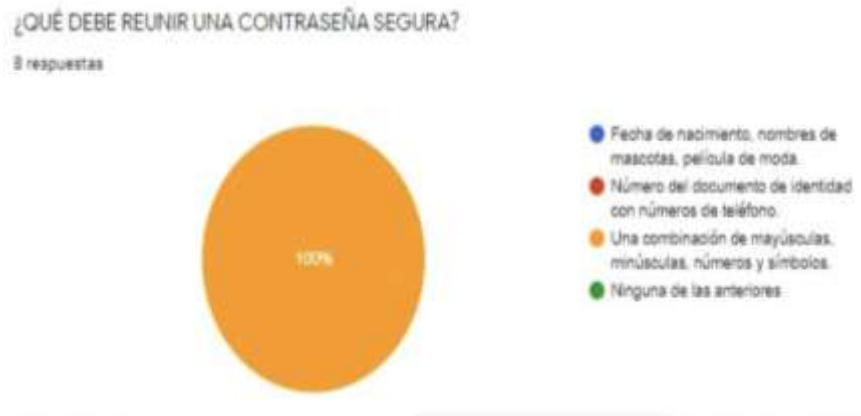
<table>
<tr><th colspan="3">Cuestionario Post Test</th></tr>
<tr><td>Observación</td><td colspan="2">Resumen de los resultados de la prueba post test para diagnosticar el estado del conocimiento en seguridad de la información de los 8 colaboradores de la entidad técnica L & M Seminario Group S.A.C.</td></tr>
<tr><td>Fecha</td><td>21/02/20</td><td>Imagen</td></tr>
<tr><td rowspan="2">Descripción</td><td>Nombre de todos los participantes de la encuesta</td><td> 
</td></tr>
<tr><td>Áreas en las que se desempeñan los colaboradores</td><td> 
</td></tr>
</table>

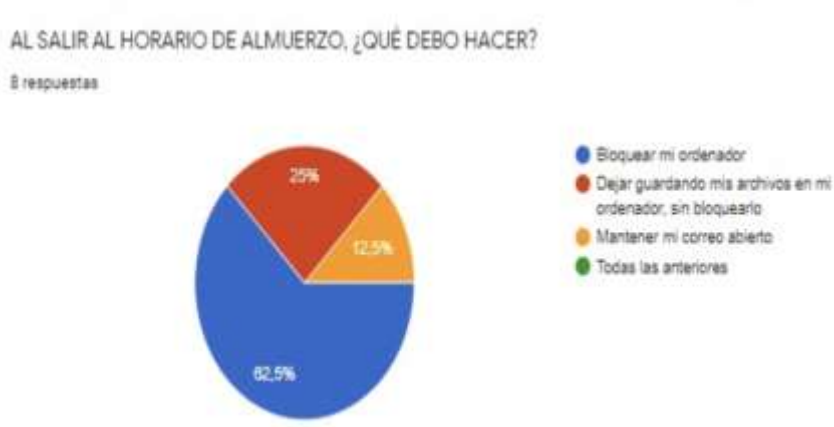
Pregunta 1: Qué puedes hacer para proteger tus contraseñas?

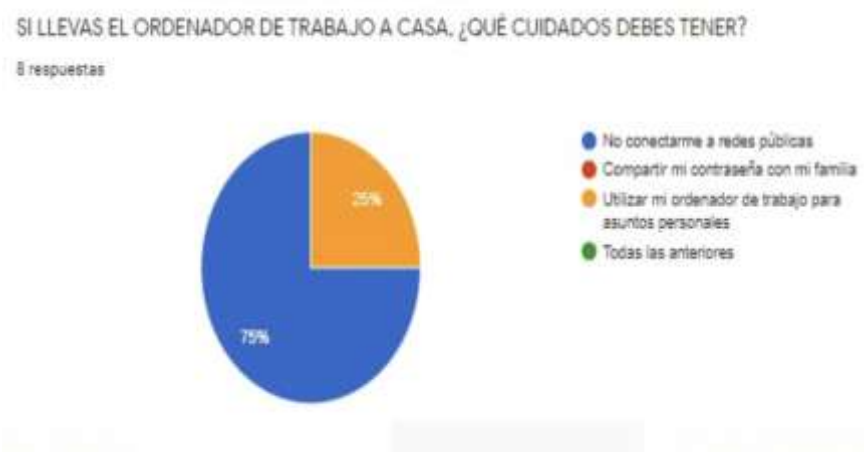


Pregunta 2: Además de crear una difíciles de adivinar, qué puedes hacer para proteger tu contraseñ?

Pregunta 3: Qué requiere una contraseña segura?



Pregunta 4: Es conveniente tener alimentos y/o bebidas en mi escritorio?	
Pregunta 5: Dónde se debe guardar la información sensible de la empresa?	
Pregunta 6: Al salir al horario de almuerzo, qué debo hacer?	

Pregunta 7: Qué debes hacer cuando retiras tu ordenar de la oficina ?	
Pregunta 8: Si llevas el ordenador de trabajo a casa, qué cuidados debes tener?	

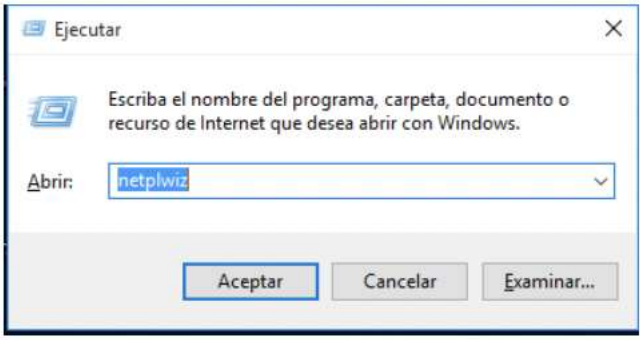
ANEXO n.° 21. Guía para crear usuarios

GUÍA DE CÓMO CREAR CUENTAS DE USUARIOS

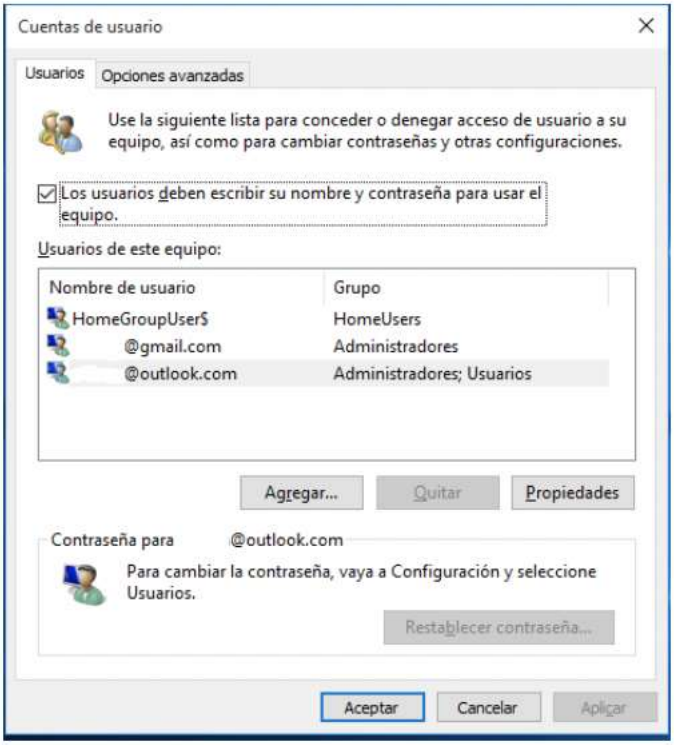
CREAR CUENTAS DE USUARIOS

1. Presiona la combinación de teclas Windows + R.

2. En la ventana que se despliega, escribe el comando netplwiz y haz clic en Aceptar o presiona la tecla Enter.



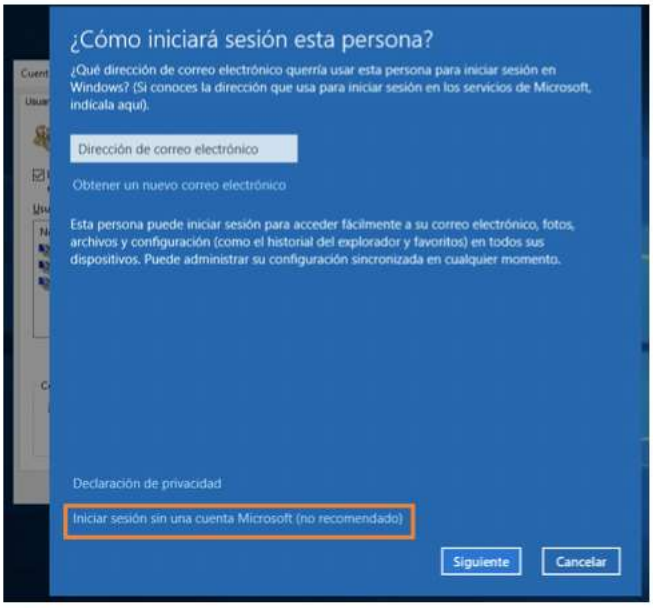
3. En la ventana Cuentas de usuario, haz clic en el botón Agregar para ingresar una nueva cuenta.

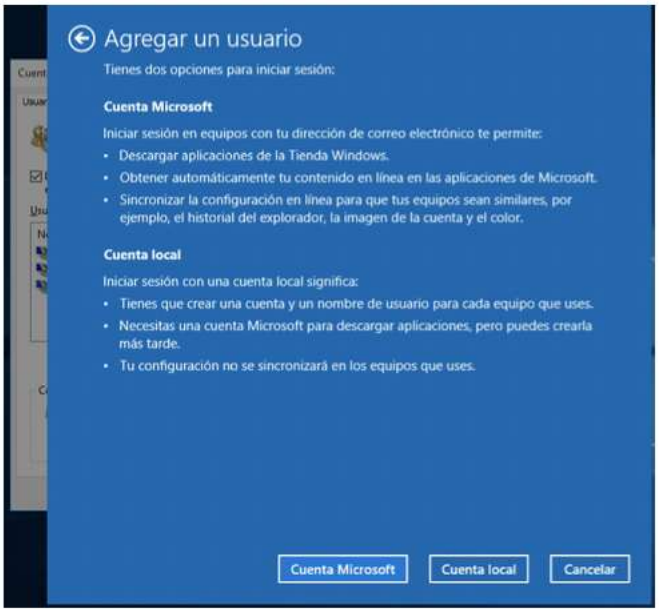


L & M SEMINARIO GROUP S.A.C. 1

GUÍA DE CÓMO CREAR CUENTAS DE USUARIOS

4. El sistema te dará la opción de crear una cuenta asociada a un correo o una cuenta local sin correo. Si eliges crear una con correo, ingresalo en el recuadro Dirección de correo electrónico y sigue las indicaciones del sistema. Por ejemplo crearemos una sin correo; recuerda que es una opción no recomendada. Hacemos clic en Siguiente y luego, en la ventana de la explicación de cada tipo de cuenta, hacemos clic en Cuenta local.

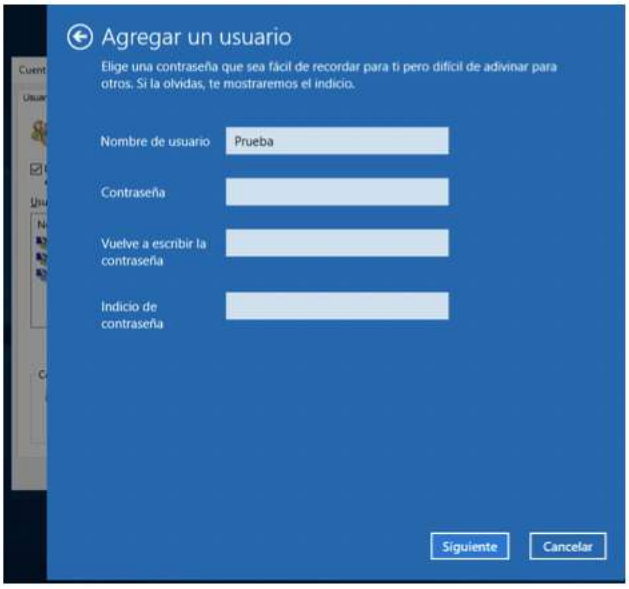




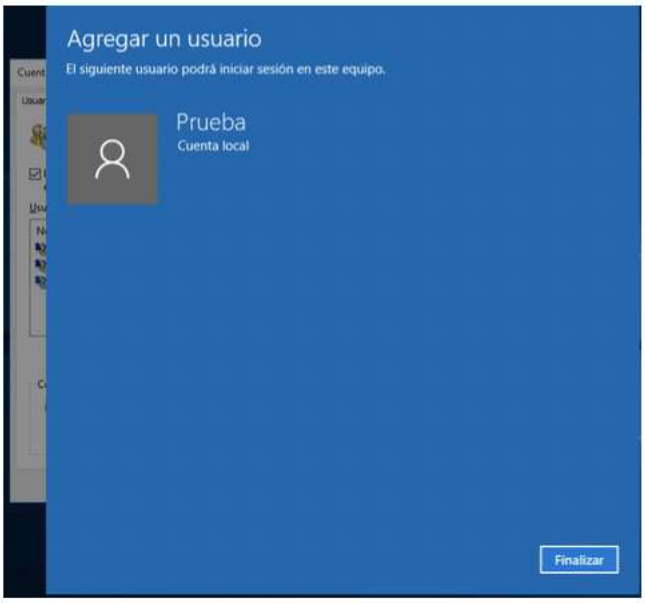
GUÍA DE CÓMO CREAR CUENTAS DE USUARIOS

5. En la casilla Nombre de usuario, escribes el nombre con el cual identificarás tu nueva cuenta y la contraseña, la cual es opcional pero recomendada. Si ingresas contraseña, te recomendamos, deja una pista que solo tú reconozcas en la casilla Indicio de contraseña.

Clic en Siguiente.

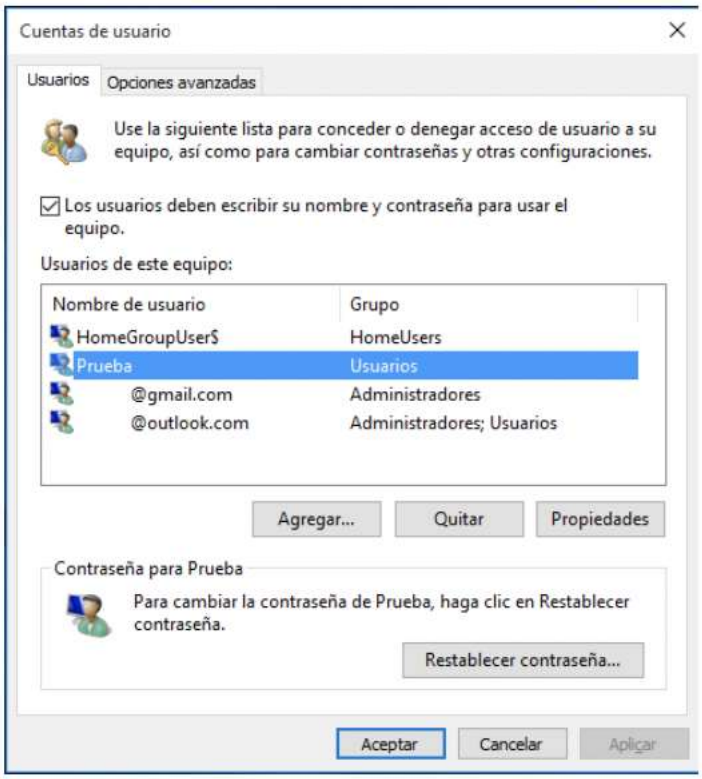


6. Verificación del proceso, clic en Finalizar.



GUÍA DE CÓMO CREAR CUENTAS DE USUARIOS

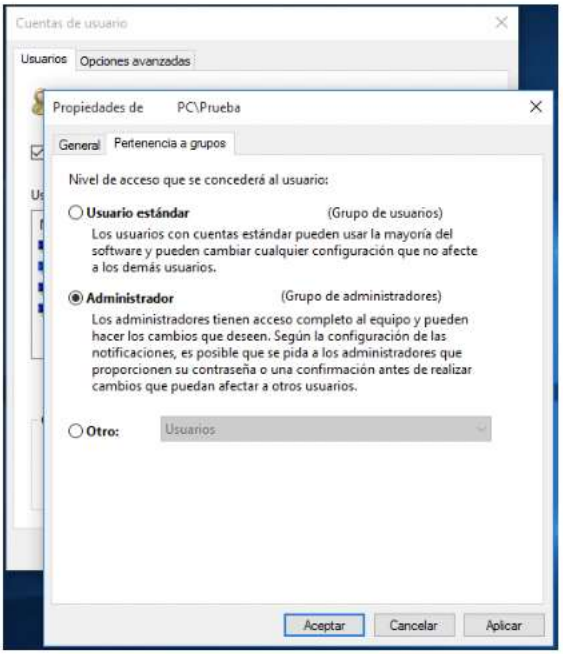
7. Vuelves a la ventana de Cuentas de usuario, seleccionas la nueva cuenta y haces clic en el botón Propiedades.



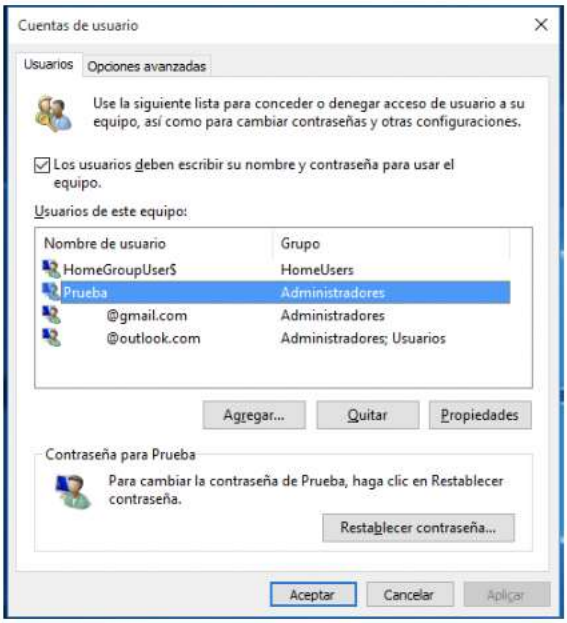
8. En la nueva ventana si quieres que la nueva cuenta tenga permisos de administrador, vas a la pestaña Pertenencia a grupos y le das permisos de administrador seleccionando la opción Administrador y luego clic en el botón Aplicar y clic en el botón Aceptar.

Nota: Las nuevas cuentas quedan por defecto con permisos de Usuario estándar.

GUÍA DE CÓMO CREAR CUENTAS DE USUARIOS



9. Finalmente, verificas que tu cuenta haya quedado correctamente configurada y haces clic en el botón Aceptar.



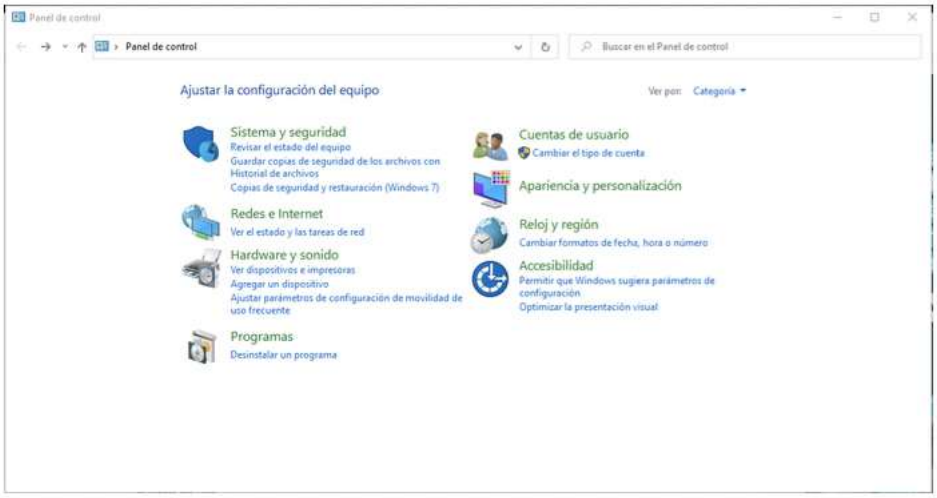
Y ¡listo!, ya habrás creado una nueva cuenta de usuario en Windows 10.

ANEXO n.° 22. Manual de procedimiento para la copia de seguridad

MANUAL PARA REALIZAR UNA COPIA DE SEGURIDAD

COPIA DE SEGURIDAD

- Accede al panel de control del sistema desde el menú de usuario de Windows 10 (botón derecho del ratón sobre el botón de inicio)



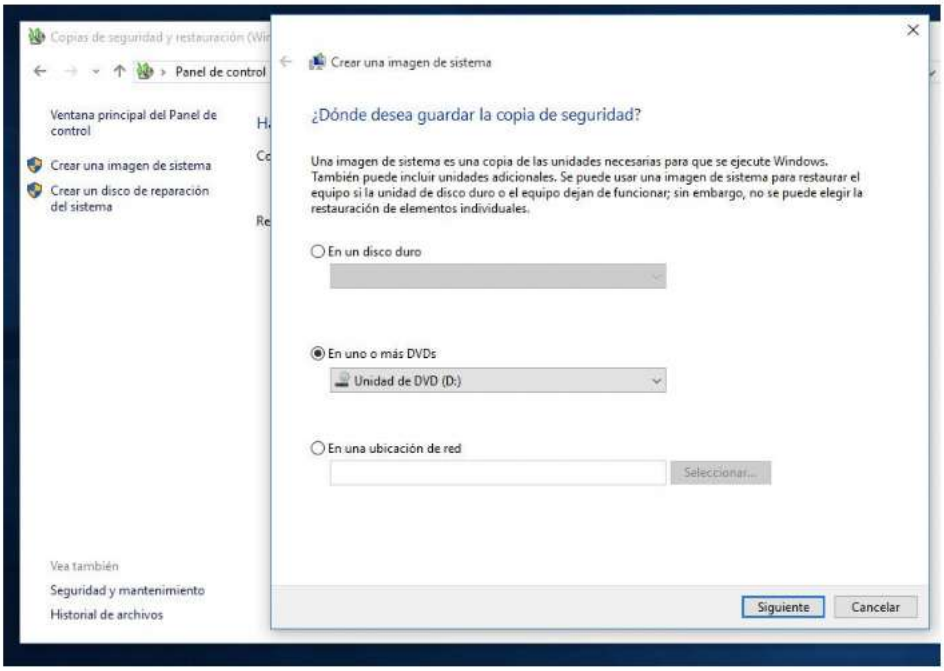
- Pulsa sobre Copias de seguridad y restauración (Windows 7)

- Pulsa sobre Crear una imagen del sistema

L & M SEMINARIO GROUP S.A.C. 1

MANUAL PARA REALIZAR UNA COPIA DE SEGURIDAD

- Elige donde se guardará la imagen, en un disco duro o pendrive, en discos ópticos DVD o en una unidad de red
- Confirma e inicia el proceso haciendo clic en Iniciar copia de seguridad



Es el método indicado para guardar una copia de seguridad de archivos para recuperarlos si se pierden o dañan.

- Accede al panel de control del sistema
- Pulsa sobre Historial del archivo
- Conecta una unidad externa como un disco duro o pendrive USB o elige una unidad de red
- Si tienes varios selecciona la unidad a utilizar por el historial de archivos
- Pulsa sobre el botón Activar
- La herramienta guardará los archivos de las Bibliotecas, Escritorio, Contacto y Favoritos
- Si no deseas guardar carpetas y bibliotecas específicas puedes agregarlas en el apartado de exclusiones

L & M SEMINARIO GROUP S.A.C. 2

MANUAL PARA REALIZAR UNA COPIA DE SEGURIDAD

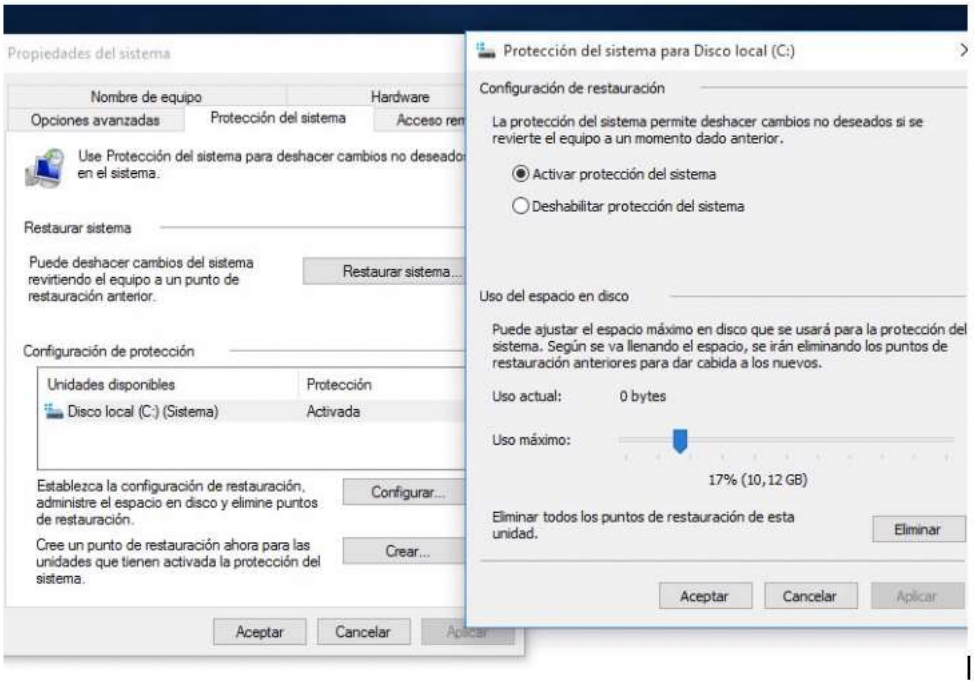
Una vez activa por primera vez, puedes acceder a la *Configuración Avanzada* para elegir la frecuencia con la que se realizará las copias y el tiempo que se mantendrán las versiones guardadas. En caso de problemas solo tienes que pulsar sobre la opción *Restaurar archivos personales* y elegir la versión de los archivos que quieres devolver a su ubicación original.

Complementando las opciones anteriores de copia de seguridad y restauración, Windows 10 también ofrece una herramienta de recuperación avanzada que deshace cambios realizados en el sistema revirtiendo el equipo a un punto de restauración anterior. Muy útil en caso de problemas con la instalación de un driver o aplicación que impida el funcionamiento normal del sistema operativo. Para activarlo:

- Accede al panel de control del sistema
- Pulsa sobre Recuperación
- Pulsa sobre Configurar Restaurar sistema
- Activa la protección del sistema y uso de espacio en disco haciendo clic en Configurar
- Crea un punto de restauración del sistema

L & M SEMINARIO GROUP S.A.C. 3

MANUAL PARA REALIZAR UNA COPIA DE SEGURIDAD



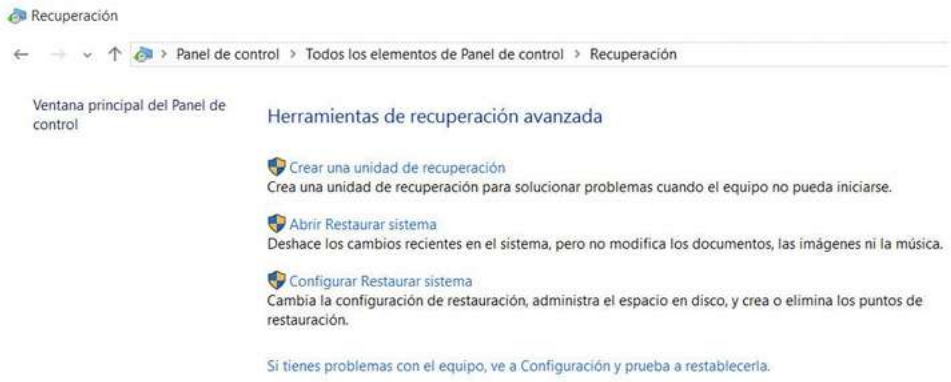
A partir de aquí se irán creando automáticamente puntos de restauración. Según se vaya llenando el espacio elegido para la protección del sistema se irán eliminando puntos de restauración anteriores. Para volver a un punto anterior la misma herramienta ofrece la función para restaurar el sistema y corregir los problemas. Restaurar el sistema no afecta a documentos, imágenes u otros datos personales.

La herramienta anterior también ofrece la posibilidad de crear una unidad de recuperación para usarla cuando el equipo no se pueda iniciar o en caso de problemas. De la siguiente forma:

- Accede al panel de control del sistema
- Pulsa sobre Recuperación
- Pulsa sobre Crear una unidad de recuperación
- La unidad externa a utilizar debe tener al menos 8 Gbytes de espacio libre. (Todos los datos serán eliminados de esta unidad)

L & M SEMINARIO GROUP S.A.C. 4

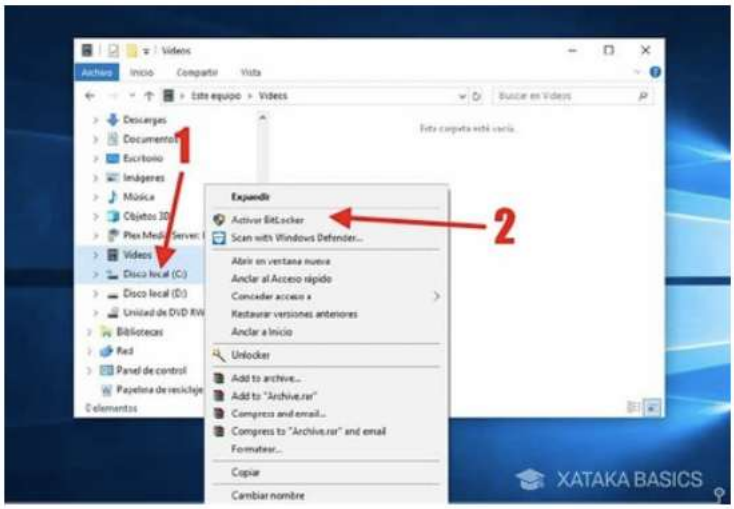
MANUAL PARA REALIZAR UNA COPIA DE SEGURIDAD



Una vez creada podremos utilizarla para acceder al equipo y solucionar problemas. Si utilizamos la opción de Realizar copia de seguridad de archivos del sistema también podremos usarla para reinstalar Windows en caso de necesitarse.

ANEXO n.° 23. Manual para encriptar un ordenador

MANUAL PARA ENCRIPTAR DISCO DURO

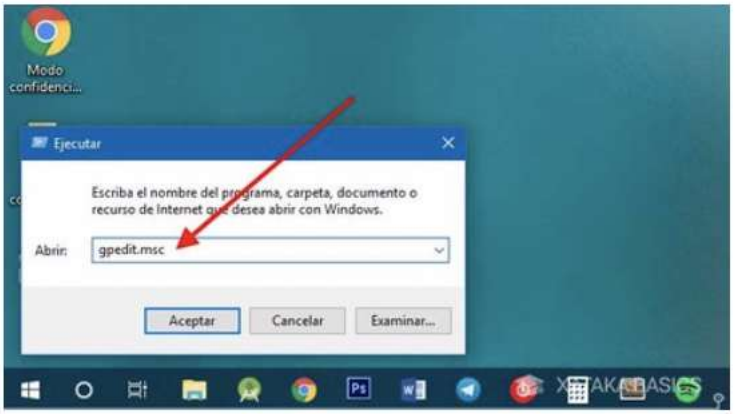


Si te aparece un mensaje como el anterior, eso quiere decir que tu PC no cuenta con un TPM compatible. TPM son las siglas de Trusted Platform Module: un chip especializado para guardar claves de cifrado para descifrar el hardware. Es recomendable, pero no estrictamente necesario para usar BitLocker. Lo único es que necesitarás un paso adicional. Si no te aparece el mensaje anterior, pasa directamente al punto tres de este tutorial.

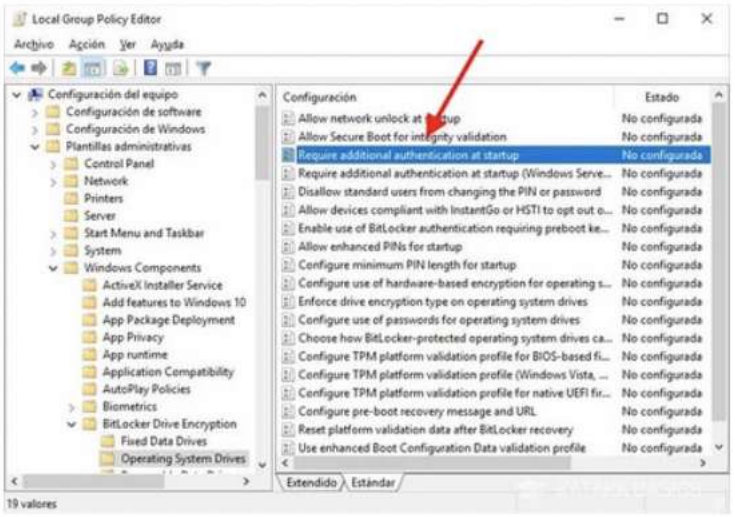
L & M SEMINARIO GROUP S.A.C. 1

MANUAL PARA ENCRIPTAR DISCO DURO

2. Usa BitLocker sin TPM (si no tienes)



Puedes usar BitLocker sin TPM, pero para que Windows te deje debes cambiar una configuración en el Editor de directivas de grupo local, el famoso gpedit. Para abrirlo, pulsa Win + R en el teclado, escribe gpedit.msc y luego pulsa Aceptar.



Ya en el editor de políticas de grupo local, deberás moverte por las carpetas para ir a la ruta

Configuración del equipo / Plantillas administrativas

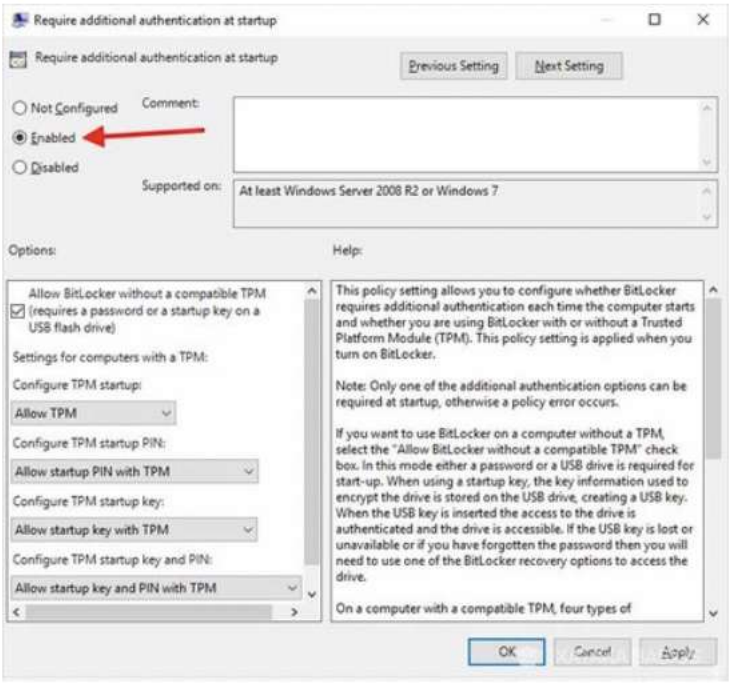
/ Windows Components / BitLocker Drive Encryption

/ Operating System Drives.

Debes hacer doble clic en cada carpeta para entrar a su interior. Después de seleccionar la última deberías encontrar Require Additional Authentication at

MANUAL PARA ENCRIPTAR DISCO DURO

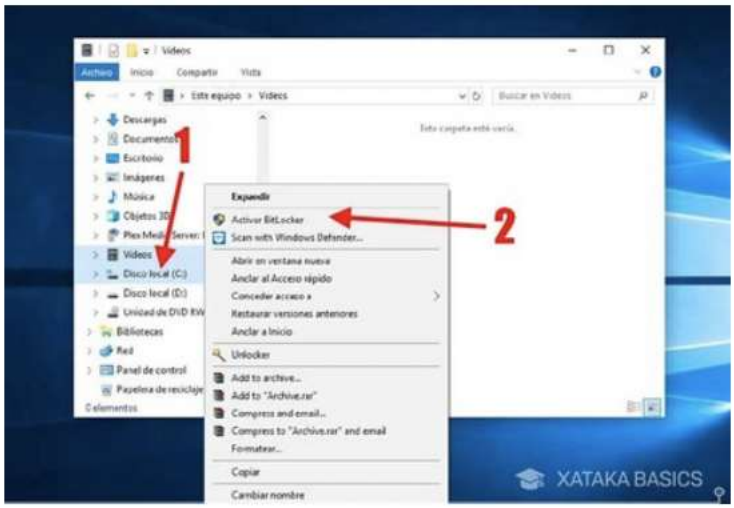
startup o Requerir autenticación adicional al iniciar, si te aparece en español. Haz doble clic para editar su valor.



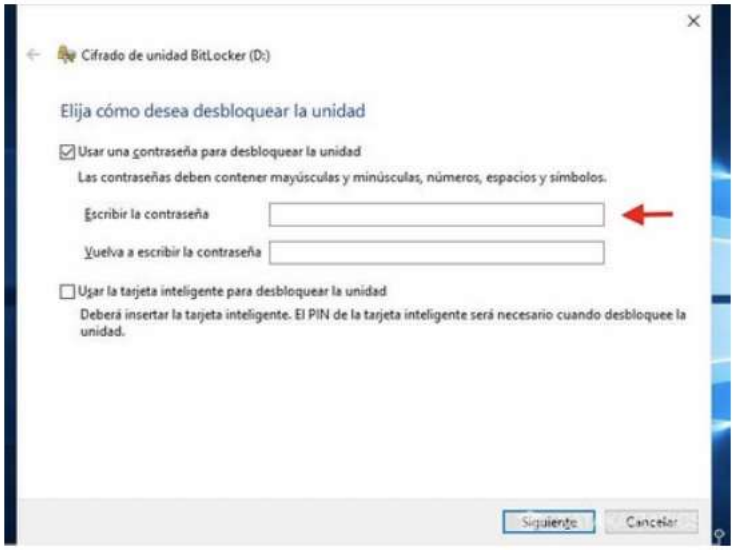
En la ventana emergente, marca la opción Enabled (o activado). El resto de opciones predeterminadas son las que necesitas para que funcione BitLocker sin TPM, así que no necesitas cambiar nada más. Pulsa OK. Ahora ya puedes usar BitLocker sin TPM.

MANUAL PARA ENCRIPTAR DISCO DURO

3. Cifra tu disco duro

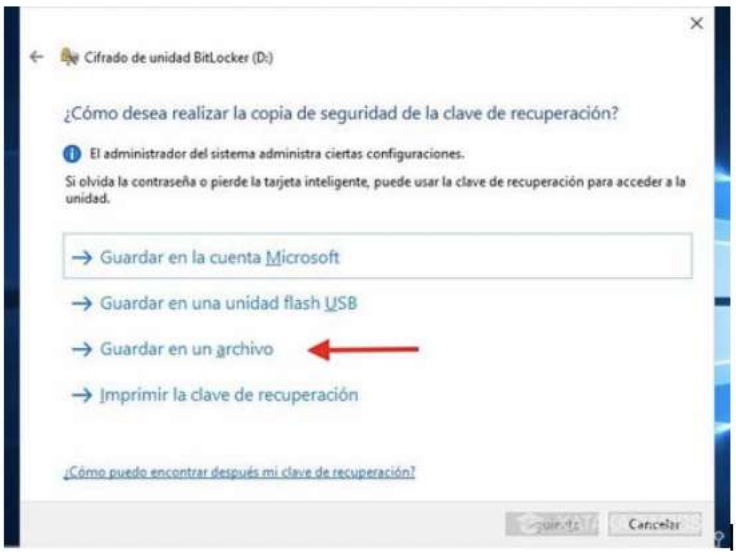


Si el anterior intento de cifrar tu disco duro te tiró para atrás por no tener TPM, ya no deberías tener ese problema. Ve de nuevo al explorador de archivos, haz clic con el botón derecho en la unidad que quieres cifrar (1) y después elige en el menú desplegable Activar BitLocker (2).

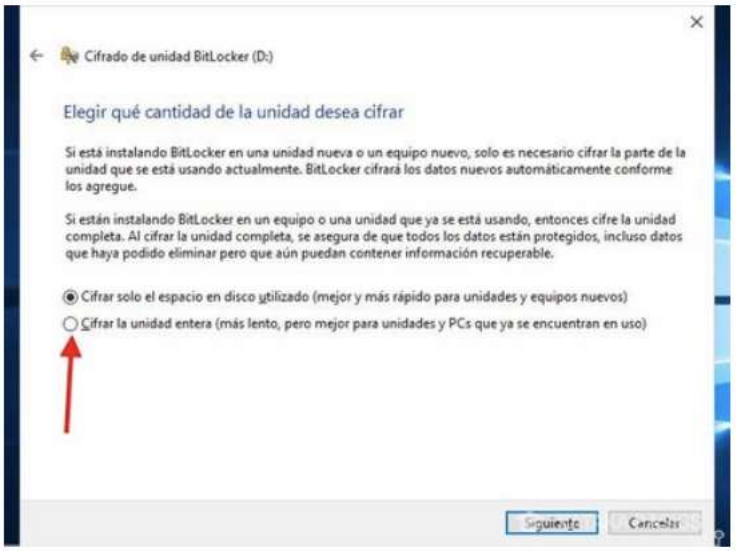


BitLocker hará de nuevo la comprobación de compatibilidad y si todo va bien verás una ventana como la anterior. Aquí debes elegir cómo quieres desbloquear la unidad: si será mediante una contraseña (que debes escribir dos veces) o mediante una tarjeta inteligente que necesitas insertar en el PC.

MANUAL PARA ENCRIPTAR DISCO DURO

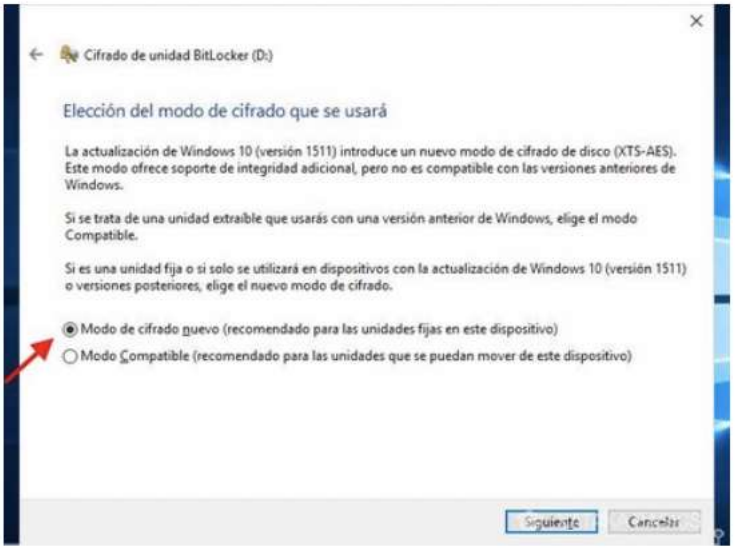


En el siguiente paso tienes todavía más opciones, en este caso para crear una copia de seguridad de la clave de recuperación. La puedes guardar en tu cuenta de Microsoft, en una unidad USB, en un archivo o imprimirla. Una de las opciones más polivalentes es la de guardar como archivo, pero elijas lo que elijas... pon la clave a buen recaudo.

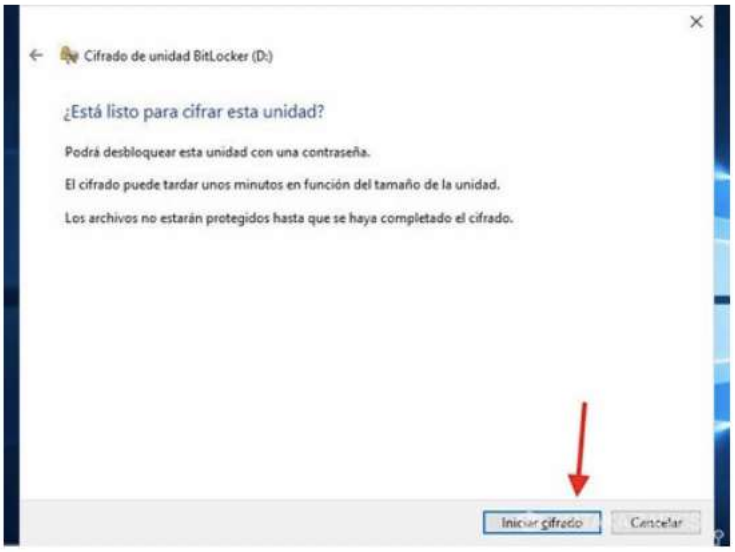


En el siguiente paso debes elegir entre si quieres cifrar solo el espacio utilizado o si quieres cifrar la unidad entera. La primera opción es más rápida, pero la segunda es más apropiada cuando estás cifrando un PC que llevas ya tiempo usando. Para mayor seguridad, elige cifrar la unidad entera.

MANUAL PARA ENCRIPTAR DISCO DURO



La última opción que deberás elegir antes de empezar a cifrar es si quieres usar el cifrado nuevo o el cifrado compatible. El cifrado nuevo no funcionará en versiones más antiguas de Windows, pero teniendo en cuenta que Windows 10 se actualiza "casi" por si mismo, es relativamente difícil encontrar versiones de Windows anteriores a cuando se cambió el cifrado.



Ya está todo listo. Pulsa iniciar cifrado para que comience a cifrarse la unidad. Nosotros hemos cifrado una unidad distinta a la de Windows, por lo que el cifrado empieza inmediatamente y en segundo plano, de modo que puedes seguir usando el PC mientras tanto. Si elegiste cifrar la unidad de Windows, necesitarás reiniciar antes de que comience el cifrado.

ANEXO n.° 24. Formato para las acciones de mejora

PLAN DE ACCIONES DE MEJORA									
ID	ACCIÓN POR TOMAR	TIPO		ESTADO ACTUAL	RESPONSABLES	RECURSOS	ACTIVIDADES	INICIO	FIN
		MEJORA	CORRECTIVA						

ANEXO n.° 25. Diagrama de proceso de mejora continua