FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE REQUISITOS DE LA ISO/IEC 27001:2013 PARA LA SEGURIDAD DE INFORMACIÓN EN UNA PYME CONSULTORA

PRESENTADA POR

KATHERIN CINTHIA DE LA SOTA SHICSHE

YVONNE JHOSSELYN MECHAN CRISTOBAL

ASESORES

SUSSY BAYONA ORÉ

LUIS ESTEBAN PALACIOS QUICHIZ

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2018

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES
FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE REQUISITOS DE LA ISO/IEC 27001:2013 PARA LA SEGURIDAD DE INFORMACIÓN EN UNA PYME CONSULTORA

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADA POR

DE LA SOTA SHICSHE, KATHERIN CINTHIA

MECHAN CRISTOBAL, YVONNE JHOSSELYN

LIMA, PERÚ

2018

Quiero dedicar esta tesis a mis padres, mi hermana, mi abuelo y mi mejor amigo, por darme su apoyo incondicional, amor y sobre todo por motivarme a seguir adelante con mis metas.

Quiero dedicar este gran logro a mi familia, en especial a mis padres, a mis hermanos y sobrinos por todo el sacrificio, amor, apoyo incondicional. También a mis amistades por brindarme su apoyo y por motivarme a seguir adelante.

AGRADECIMIENTO

Expresamos un sincero agradecimiento a nuestros asesores y a las personas involucradas por su apoyo y conocimientos, ya que hicieron posible la realización de esta tesis. Además, queremos agradecer a la Gerente de Administración de la consultora por su constante compromiso con este proyecto.

RESUMEN

El objetivo de este proyecto consistió en implementar controles y cumplir con los requisitos de la ISO/IEC 27001:2013 en la consultora VF CONSULTING S.A.C., con el fin de mejorar la seguridad de la información en el proceso core y en los procesos involucrados. En el desarrollo de la implementación se utilizó la metodología del Ciclo de Deming (PHVA), la cual se divide en cuatro fases: planear, hacer, verificar y actuar; para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). Como resultado, se consiguió mejorar la seguridad de la información, para lograrlo se identificó el estado de cumplimiento inicial y final de la ISO/IEC 27001:2013 en la empresa. Además, se realizó la evaluación de riesgos, la implementación de los controles, el cumplimiento de los requisitos y la concientización del personal. Todo esto nos sirvió para sentar las bases hacia una certificación futura en dicha norma. La investigación nos permitió concluir en la importancia de contar con un SGSI en cualquier empresa, ya que independientemente de su tamaño o sector, el sistema ayuda a proteger los activos de información, gestionando los riesgos que generan.

Palabras claves: Seguridad de la información, ISO/IEC 27001, SGSI, Gestión del riesgo, PHVA.

ABSTRACT

The objective of this project was to implement controls and comply with the requirements of ISO/IEC 27001:2013 in the consultancy VF CONSULTING S.A.C., to improve the security of information in the core process and in the processes involved. In the development of the implementation the methodology of the Deming Cycle (PDCA) was used, which is divided into four phases: plan, do, check and act; to establish, implement, maintain and improve the Information Security Management System (ISMS). As a result, it was possible to improve the security of the information, to achieve it, the state of initial and final compliance of ISO/IEC 27001:2013 in the company was identified. In addition, the risk assessment, the implementation of the controls, the compliance with the requirements and the awareness of the personnel were carried out. All this served to lay the groundwork for a future certification in that standard. The research allowed us to conclude on the importance of having an ISMS in any company, because regardless of its size or sector, the system helps protect information assets, managing the risks they generate.

Keywords: Information security, ISO/IEC 27001, ISMS, Risk management, PDCA.

INTRODUCCIÓN

"En la actualidad, las empresas tanto privadas como públicas priorizan la seguridad de la información, la cual es clasificada como uno de los bienes más importantes para la continuidad del negocio y genera un valor agregado hacia la competencia" (Monsalve, Aponte y Chaves, 2015, p. 67).

La empresa VF CONSULTING S.A.C. ofrece servicios de consultoría enfocados al sector de las telecomunicaciones, desarrollan proyectos sobre BCSC, canales digitales y mediación. Los proyectos son desarrollados tanto en las instalaciones de la empresa como en la empresa contratista.

Teniendo en cuenta la importancia de la información, es considerada a menudo como una herramienta esencial en una empresa para el funcionamiento de todos sus procesos. "Si el flujo de la información es continuo, los procesos se ejecutarán de manera óptima; pero si es restringido o afectado, la organización se puede deteriorar o morir, lo cual se convierte en un riesgo de seguridad de la información" (Cárdenas, Martínez y Becerra, 2016, p. 932).

Al analizar la situación inicial de VF CONSULTING S.A.C., se detectaron activos de información, los cuales necesitaban fortalecerse mediante la gestión de seguridad de la información; es decir, la información de la consultora se encontraba disponible para todo el personal, sin considerar la integridad, disponibilidad y confidencialidad. Asimismo, se identificó la carencia de concientización y capacitación al personal acerca de la seguridad de información.

Estas deficiencias ocasionaron que la información de la empresa sea utilizada y manipulada sin autorización previa.

Según Baca (2016) "la seguridad de la información en una organización requiere de la incorporación de ésta como elemento estratégico. Así, la organización al gestionar la seguridad de su información cumple con sus obligaciones, regulaciones y genera la confianza necesaria en sus clientes."

Bajo este contexto, se implementaron controles y se verificó el cumplimiento de los requisitos de la ISO/IEC 27001:2013 en la empresa, lo cual garantizará la mejora de la seguridad de información.

El presente trabajo está esquematizado en cinco capítulos. En el primer capítulo se desarrollan los antecedentes, bases teóricas y definición de términos.

En el segundo capítulo se describe la metodología utilizada para la implementación, el Ciclo de Deming (PDCA), el cual está compuesto por las siguientes fases: Plan, Do, Check y Act.

En el tercer capítulo se detalla cómo se estableció e implementó el SGSI, de acuerdo con la metodología mencionada en el segundo capítulo.

En el cuarto capítulo se muestran las pruebas y resultados de la implementación, es decir, se realiza una comparación entre la situación inicial y final de la empresa, resaltando los logros obtenidos y demostrando el cumplimiento efectivo de los objetivos planteados.

Para el desarrollo del quinto capítulo, sobre discusiones y aplicaciones, interpretamos los resultados del capítulo anterior y evaluamos las mejoras en la empresa.

Finalmente, exponemos las conclusiones obtenidas del análisis de los resultados de la implementación y precisamos algunas recomendaciones para las futuras tesis.

Desde el punto de vista de la situación del problema, las amenazas tecnológicas son parte de nuestra sociedad, pero son más latentes en las organizaciones, ya que se pueden presentar de diversas formas, desde un pequeño virus hasta los más recientes ataques de ransomware (software malicioso que restringe el acceso de nuestros sistemas de negocio y exige el pago de un rescate para eliminar dicha restricción), es por ello que se requiere de la implementación de medidas de seguridad. (Valencia y Orozco, 2017).

Si bien existe una mayor conciencia sobre lo importante que es la seguridad de la información, muchas de las organizaciones todavía se mantienen renuentes a la implementación de un SGSI. Es por ello que se debe tener en cuenta lo que sostiene Baca (2016) respecto a la seguridad de la información, que ésta no es un activo que se compra, sino que al contrario, debe ser gestionado por la empresa, apuntando a una meta concreta, estableciendo criterios de evaluación y sobre todo poder medirse.

Con transcurso del tiempo, la seguridad de información se vuelve un sistema dinámico en constante evolución, es por esa razón que las empresas deben ser evaluadas y monitoreadas en periodos establecidos con diferentes escenarios, como por ejemplo, tomar decisiones de los riesgos que se enfrentan y los recursos con los que cuentan.

Para reducir las amenazas que las empresas puedan apreciar, se debe generar un plan de acción, conocido como SGSI, y contiene datos referidos a los lineamientos, responsables y documentos necesarios para asegurar que el SGSI se aplique, se acepte y se genere una mejora continua (Arévalo y Orozco, 2015).

En el año 2014, alrededor de 6600 organizaciones en todo el mundo se encontraban en el proceso de implementación de un SGSI, a través de la Norma ISO/IEC 27001.

Como menciona Monsalve et al. (2014), “Implementar un sistema de gestión de seguridad de la información (SGSI) basado en la norma 27001 es un proceso complejo; comprende tareas como la identificación de activos y de amenazas, el análisis de riesgos y el razonamiento de seguridad” (p.68).

Es por esa razón que para las empresas es un gran desafío y que algunas de ellas evitan este tipo de implementación, pero tarde o temprano lo realizan, debido a que con el tiempo se dan cuenta que la información es un activo primordial y, como tal, debe ser asegurada.

La seguridad de información ha tomado gran importancia en el transcurso del tiempo, lo cual se corrobora en los números de certificados que han sido otorgados por la Organización Internacional para la Estandarización (ISO) en los últimos años.

En la encuesta que realizó la ISO Survey en el año 2016 a nivel mundial, se presentó un crecimiento de 21% en comparación del 2015. El número total de certificaciones obtenidas en el 2016 fue de 33,290 superando un 5,754 del número de certificaciones del 2015. Los países que resaltan con un mayor número de empresas certificadas son Japón y Reino Unido (Charlet, 2017). Y con respecto a Perú, según GTDI - Tecnologías de la Información y Consultoría, en el 2016 se emitieron un total de 32 certificaciones de la ISO/IEC 27001.

Entre las entidades públicas que han alcanzado la certificación entre la versión 2005 y 2013, tenemos al INDECOPI, ONP, Osinergmin, mientras que entre las empresas del sector privado se encuentran ATENTO PERÚ, Telefónica, Hermes y Americatel.

Según Fernández, director general de AENOR PERÚ, empresa de origen español que se encarga de capacitar, evaluar, certificar y auditar empresas que cumplan con las normativas internacionales de ISO/IEC, sostiene que el mercado peruano todavía es pequeño y no tan atractivo para la colocación de certificaciones internaciones de ISO/IEC en cuanto a calidad y sistema de seguridad de información (AENOR PERÚ, 2015).

El problema en sí, se define como la inadecuada gestión de seguridad de la información para proteger los activos de información en el proceso operativo y los procesos involucrados, en la empresa VF CONSULTING S.A.C.

Definido el problema, surge la pregunta general: ¿De qué manera podremos mejorar la gestión de seguridad de la información en el proceso core y los procesos involucrados?

Lo cual conlleva a la formulación de las preguntas específicas siguientes:

- ¿Cuál es el nivel de cumplimiento respecto a los requisitos y controles de la Norma ISO/IEC 27001:2013?
- ¿Cuál es el nivel de riesgo de los activos de la seguridad de información?
- ¿De qué manera concientizar al personal sobre la importancia de la seguridad de la información?

Como objetivo general, la presente investigación se orienta a mejorar la seguridad de la información mediante requisitos y controles basados en la Norma ISO/IEC 27001:2013.

Así mismo, como objetivos específicos se cumplen los siguientes logros previos:

- Identificar el nivel de cumplimiento de la norma ISO/IEC 27001:2013, realizando análisis de brechas tanto de los requisitos como de los controles.

- Calcular los riesgos de los activos de información, realizando la evaluación de riesgos.
- Capacitar y concientizar al personal involucrado en el proceso de prestación de servicios telcos y los procesos involucrados, en temas de seguridad de información.

Establecida la necesidad e importancia de la investigación los trabajos precedentes que respaldan la justificación, son los siguientes:

Según Suarez (2015), "la confidencialidad, integridad y disponibilidad de la información más sensible llegan a ser esenciales para mantener los niveles de competitividad, beneficio económico, conformidad legal e imagen empresarial hacia los clientes."

Los riesgos a los que están expuestos los activos de información, en todo tipo de empresas, pueden ocasionar grandes gastos y posicionamiento del mercado si no actúan de manera rápida. Con relación a lo mencionado, se propone la implementación de controles y el cumplimiento de requisitos de la ISO/IEC 27001:2013, la cual nos brindará una guía necesaria para identificar los activos de información; además de calcular el nivel de riesgo de los activos más relevantes.

La justificación principal es mejorar la seguridad de información en el proceso core y los procesos involucrados en la empresa VF CONSULTING S.A.C., con el fin de obtener beneficios: i) a nivel de imagen, es decir generar mayor valor y prestigio, mejorando la confianza de los clientes, ii) a nivel organizacional, es decir adaptar y alinear los controles a todas las áreas de la empresa, fortaleciendo la organización interna y los procesos de mejora continua; y iii) a nivel preventivo, a través del cumplimiento de las leyes y reglamentos pertinentes reduciendo así la posibilidad enfrentarse a multas y sanciones. Consiguiendo así una ventaja competitiva y diferenciándola de otras empresas del sector, tales como: HITSS, TEMSOFT, MDP CONSULTING, entre otras.

Además, al realizar la investigación se encontraron tesis de maestrías y pregrado que establecieron e implementaron la ISO/IEC 27001:2013 en grandes empresas; sin embargo, en el caso de las PYMES no se encontraron investigaciones, ya que existe la idea – errónea – de que es muy costoso y conlleva demasiado tiempo y esfuerzo realizarlo. Sin embargo, esto no debería ser así ya

que, al ser una PYME, se requiere de un establecimiento e implementación que sea ágil y útil, que se adapte a las necesidades y actividades de la empresa.

En ese sentido y dado que VF CONSULTING S.A.C. tiene la condición de pequeña empresa, en esta tesis aportaremos la experiencia obtenida al implementar un SGSI en una PYME, ya que no se encontró registro de investigaciones vinculadas a dicho tema.

La rapidez con la que las empresas actuales incluyen cada vez más el uso de la tecnología de información va de la mano con el incremento de los riesgos de que sus activos de información sean transferidos fácilmente. Por lo que debe asegurarse la información relevante para evitar este tipo de amenazas (Moody, Siponen y Pahnila, 2018).

Es pertinente señalar que el alcance del proyecto se vio limitado por los factores tiempo y recursos, tanto por el plazo que conlleva la realización de esta tesis como por los recursos necesarios para ello.

Bajo ese contexto es que nuestro alcance se vio limitado de la manera siguiente:

1. En cuanto a los procesos, en el capítulo III, se especificó que procesos están incluidos y cuales no lo están.
2. En el Plan de tratamiento de riesgos **(Anexo 18)**, se especificó qué controles están incluidos dentro del alcance y cuáles no. Así, los clasificamos en "Grupo Uno" y “Grupo Dos”, en el primero de ellos se especifica qué controles se implementaron en esta tesis, y en el segundo se detallan los que han sido planificados.

Al no haberse implementado todos los controles en esta tesis, no se pudieron realizar las fases: verificar y actuar; sin embargo, se realizó la documentación necesaria para su futura ejecución.

INDICE GENERAL

INDICE DE GRÁFICOS

FIGURAS **Página**

TABLAS

CAPÍTULO I:
MARCO TEÓRICO

En este capítulo se detallarán los antecedentes, bases teóricas y definición de términos, obtenidos de la investigación realizada, con la finalidad de contar con los conocimientos necesarios para la culminación satisfactoria de esta tesis.

1.1 ANTECEDENTES

Actualmente, para cualquier organización, implementar un SGSI es de suma importancia para la protección de sus activos de información, más aún en caso obtuviesen la certificación le sumaría un valor agregado al servicio que ofrecen a sus clientes ya que alcanzarían un grado de reconocimiento internacional, el cual les dará a sus clientes una mayor garantía sobre la seguridad de la información. A continuación, mencionamos algunas organizaciones que han tenido éxito al implementar la SGSI:

1.1.1 Entidades que implementaron la ISO/IEC 27001 a nivel nacional

1.1.1.1 Ministerio de Transporte y Comunicaciones

Como primer antecedente, tomamos como referencia a una entidad pública peruana, la cual después de realizar el análisis de brecha inicial, determinó que no cumplía con la mayoría de los requisitos que exigía la norma. Además, se estableció como el proceso más crítico el proceso tecnológico de emisión de licencias de conducir. Dada la carencia de una administración de seguridad, diseñaron un plan del SGSI, basado en la NTP/ISO: IEC 27001:2008, con el fin de proteger los activos de información en el proceso crítico ya mencionado. Para ello, hicieron uso de la metodología MAGERIT para la evaluación de riesgos y para el desarrollo del proyecto utilizaron la metodología del Ciclo de Deming (Plan - Do - Check - Act). Sin embargo, solo llegaron a cubrir las dos primeras fases,

organización (Plan) y planificación (Do). Como resultado, se mejoró el porcentaje de cumplimiento de la norma. Al culminar con las fases restantes, el uso del SGSI traerá como beneficios a futuro: una reducción de riesgos, ahorro de costos, la gestión de la seguridad de información y la certificación, contribuyendo a obtener un valor agregado en el mercado (Cruz, 2014).

1.1.1.2 Consultora de Software

Según el tipo de servicios que presta la empresa, el intercambio de información es inevitable. Esto implica un riesgo tanto para el cliente como para la consultora, es por ello que buscaron garantizar que el intercambio de información - tanto del emisor como el receptor - obtenga confiabilidad, disponibilidad e integridad. Para ello se desarrolló un SGSI, basada en la ISO/IEC 27001:2013. Esta investigación se divide en cuatro fases: establecer, implementar, mantener y mejorar un SGSI. Se concluyó que el considerar ciertos estándares, aunque no estén referenciados en el estándar 27001, pueden ayudar a elaborar de mejor manera los componentes que permitan cumplir éste; además se determinó que implementar ideas innovadoras para la metodología de gestión de riesgos o la verificación del cumplimiento, facilitan la implementación del SGSI. Se recomienda que el alcance del SGSI se asuma teniendo en consideración la disponibilidad de recursos en la empresa (Santos, 2016).

1.1.2 Entidades que implementaron la ISO/IEC 27001 a nivel internacional

1.1.2.1 Corporación Universitaria de Colombia

Se elaboró un plan de implementación de la ISO 27001:2013 con el objetivo de obtener las bases para un SGSI, para lograr una certificación a mediano plazo, para la Gerencia de Servicios Tecnológicos (GST) de la sede principal. En cuanto al enfoque y método a seguir, desarrollaron un plan de seguridad que implicó seguir cinco fases. Como paso inicial, fase uno, se realizó un análisis de brecha inicial para observar el estado actual; como fase dos se procedió a realizar el esquema documental; como fase tres, se realizó el análisis de riesgos; en la fase cuatro, se realizaron propuestas de proyectos; y en la fase cinco, se llevó a cabo la auditoria de cumplimiento. Como conclusión se tuvo que inicialmente se había proyectado trabajar únicamente con el personal de la Unidad de GST; sin embargo, en el

proceso se tuvo que involucrar también al personal de otras unidades, ya que el trabajo en grupo permitió generar recursos humanos, técnicos y de capital necesarios para transformar y alinear los procesos de la Unidad de GST (Chaparro, 2016).

Como principal recomendación a futuras investigaciones, sugieren que el apoyo y compromiso de la alta dirección es indispensable para el desarrollo de un proyecto de este tipo, es por ello que se ha tenido en consideración para el desarrollo de esta tesis y que incluso fue uno de nuestros primeros pasos. También destacan como necesario el apoyo y compromiso del personal de la empresa para adecuarse a los instructivos, procesos y registros que se requieran.

1.2 BASES TEORÍCAS

1.2.1 Seguridad de la Información

Antes de definir que es la seguridad de la información, se debe saber que no tiene el mismo significado que la seguridad informática.

Según Solarte *et al.* (2015), "la seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos" (p. 497).

Y con respecto a la seguridad informática, Solarte *et al.* (2015), "La seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos" (p. 497).

En conclusión, la seguridad de información abarca todas las medidas preventivas que se deben realizar para la proteger de los activos de información bajo sus tres criterios que son confidencialidad, disponibilidad e integridad y que puede ser presentada en diversos formatos. En cambio, la seguridad informática está más relacionada a proteger las infraestructuras de la T.I. que soporta al negocio.

A continuación, Burgos y Campos (2013), detallan las normas de mayor utilización a nivel mundial respecto a la seguridad de la información:

- ISO/IEC 17799: “Es un estándar para la administración de la seguridad de la información, que implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización” (p. 238).
- Objetivos de Control para la información y Tecnologías Relacionadas (COBIT): Es un estándar que se preocupa por temas de gobernabilidad, control, aseguramiento y auditorias de TIC.
- Biblioteca de Infraestructura de Tecnologías de la Información (ITIL): “es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial” (p. 239).
- Serie ISO/IEC 27000: es una serie de estándares que incluye definiciones de vocabulario (ISO/IEC 27000), requisitos para sistemas de gestión de seguridad de la información (ISO/IEC 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO/IEC 27002), una guía de implementación de SGSI, (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act), (ISO/IEC 27003), especificación de métricas para determinar la eficacia de SGSI (ISO/IEC 27004), una guía de técnicas de gestión de riesgo (ISO/IEC 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO/IEC 27006), una guía de auditoria de SGSI (ISO/IEC 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO/IEC 27011), una guía de continuidad de negocio en cuanto a TIC (ISO/IEC 27031), una guía de ciberseguridad (ISO/IEC 27032), una guía de seguridad en redes (ISO/IEC 27033), una guía de seguridad en aplicaciones (ISO/IEC 27034), y una guía de seguridad de la información en el sector sanitario (ISO/IEC 27799).

La gestión de seguridad contiene varios factores y elementos que se relacionan entre sí, en los países más desarrollados las PYMES suelten tener cierta dificultad de comprensión de la seguridad de información y medidas de control de seguridad, ya que dejan olvidado la gestión de riesgos o la implementación de políticas de seguridad. Esto es debido a que carecen de recursos y conocimientos para controlar la seguridad de la información y ofrecer una adecuada seguridad. (Sanchez, Villafranca, Fernandez y Piattini, 2014)

1.2.2 La familia ISO/IEC

ISO (Organización Internacional de Normalización) es el más grande desarrollador voluntario de Normas Internacionales que reúne a expertos para compartir conocimientos y desarrollar normas, ayudando a las organizaciones que sean eficientes y eficaces (Charlet, 2017).

Según la página oficial International Organization for Standardization, los beneficios de la ISO son las siguientes:

- Garantizan que los productos y servicios sean de manera segura, confiable y de buena calidad.
- Reducen el costo al minimizar desperdicios y errores, aumenta la productividad.
- Ayuda a las organizaciones a acceder a nuevos mercados.

En conclusión, la norma ISO es desarrollada por un grupo de personas expertas, dentro de un comité técnico, una vez que se ha establecido una necesidad de una norma, estos expertos se reúnen para discutir este proyecto. Luego de que el proyecto se ha desarrollado, se comparte con los miembros de la ISO y pide observaciones antes de ser aprobada. Si el proyecto llega a un consenso se convierte en estándar ISO, sino lo remite nuevamente al comité técnico para que se realicen más ediciones.

Según Sánchez (2013), los principios fundamentales aplicados para una elaboración de una Norma son los siguientes:

1. Responder a una necesidad del mercado.
2. Obtener una opinión internacional de expertos.

3. Desarrollarse por medio de un proceso de stakeholders.
4. Obtener conformidad de las personas involucradas.

Según Berríos y Rocha (2015), el concepto de IEC:

La Comisión Electrotécnica Internacional es la organización que lidera en el mundo para la publicación y preparación de normas internaciones que esté relacionado a electricidad, electrónica y tecnología. Fue fundada en el año 1906.

Las normas ISO/IEC se constituyen con una serie de estándares en que se agrupa por familias, aunque existen más de 1800 normas publicadas por ISO/IEC, resaltaremos las más importantes en cuanto su aplicación e impacto en los sectores (ISOTools, 2015).

Las normas más utilizadas por las empresas son las siguientes:

- ISO 9001: Es la Norma que frecuentemente las empresas implementan para demostrar la satisfacción del cliente y asegurar la calidad de los servicios y productos.
- ISO 14001: Es el segundo estándar más reconocido. Se encarga de verificar que las empresas cumplan la legislación ambiental establecida en cada zona geográfica.
- ISO/IEC 27001: Encargada de asegurar las buenas prácticas para la seguridad de información y así evitar riesgos, amenazas y mejorando procesos de información.

1.2.3 ISO/IEC 27001

La 27001 Academy (2018) publicó que la ISO/IEC 27001 es una norma que describe cómo administrar la seguridad de la información en las organizaciones. La revisión de los estándares ISO se realiza con una frecuencia de 4 a 5 años; la revisión última revisión de ésta fue en el año 2013 y con el nombre de ISO/IEC 27001:2013.

Esta norma es adaptable para cualquier tipo de empresa, con o sin fines de lucro, puede ser pública y privada, pequeña o grande, además, fue redactada por los especialistas internacionales desatacados en seguridad.

La ISO/IEC 27001 es la norma más conocida a nivel internacional para implementar un SGSI y, en efecto, a la fecha hay muchas empresas que han certificado su cumplimiento.

En el Reino Unido, la acreditación de organismos de certificación es manejada por el Servicio de Acreditación del Reino Unido (UKAS), que mantiene una lista de todas las organizaciones autorizadas para certificar la ISO 27001, es por eso que una certificación de esta organización se reconoce mundialmente (Calder, 2013).

1.2.3.1 Certificaciones en la ISO/IEC 27001 a nivel mundial

Según Rojo (2017), la Norma ISO/IEC 27001, presenta un aumento de número de certificados en los tres penúltimos años a nivel mundial. La presencia en los distintos países se queda con la misma cifra en los años 2015 y 2016 que no se ha reflejado ningún aumento **(Figura 1.1).**

FIGURA 1.1 PRESENCIA DE LA ISO/IEC 27001 EN EL MUNDO
FUENTE: SBQ CONSULTORES (2017)

Los datos fijan el ranking de la siguiente forma:

1. Japón con 8,945 certificados
2. Reino Unido con 3,367 certificados
3. India con 2,902 certificados
4. China con 2,618 certificados
5. Alemania con 1,388 certificados
6. Italia con 1,220 certificados
7. Estados Unidos con 1,115 certificados

8. República de China con 1,087 certificados
9. España con 752 certificados
10. Países bajos con 670 certificados

En todo el mundo se encuentran varias organizaciones que han implementado un SGSI y este se encuentra operando, pero muy pocas con la certificación como, por ejemplo: EQUIFAX Chile, Amazon Web Services (AWS), Microsoft Global Foundation Services (GFS), Google Apps, IFX Networks Colombia (Santos, 2016).

1.2.3.2 Certificaciones en la ISO/IEC 27001 en América Latina

Actualmente los países en América Latina con una mayor demanda en certificaciones de la ISO/IEC 27001 son México, Colombia y Brasil **(Figura 1.2)**, éstos se encuentran en constante crecimiento. Sin embargo, no tan lejos, en el sexto puesto encontramos a Perú, si bien no tiene una cifra de certificaciones tan elevada como los tres primeros puestos, ha tenido un gran avance en estos años. Además, se debe tener en cuenta que estas listas van variando e incrementándose con los años.

FIGURA 1.2 CERTIFICACIONES DE LA ISO/IEC 27001 EN AMÉRICA LATINA
FUENTE: ISO (2017)

1.2.3.3 Certificaciones en la ISO/IEC 27001 en el Perú

Anualmente la ISO/IEC realiza una encuesta de certificaciones sobre sus estándares del SGSI. Para GTDI (2017), en el Perú se reporta un total de 32 certificaciones de ISO/IEC 27001 hasta el año 2016 **(Figura 1.3).**

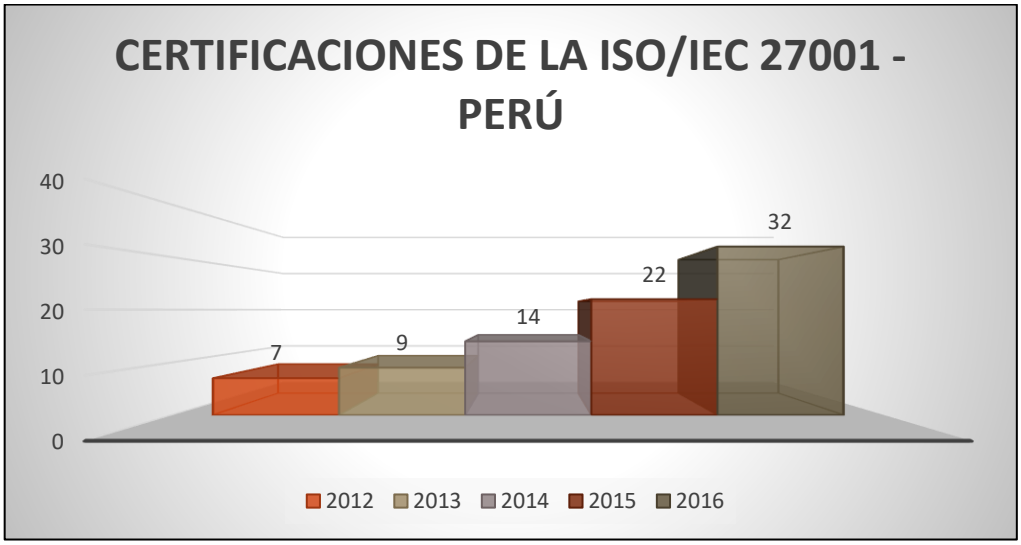


FIGURA 1.3 CERTIFICACIONES DE LA ISO/IEC 27001 – PERÚ
FUENTE: GTDI (2017)

A continuación, veremos en la **Tabla 1.1**, que según CDI (2017), solo tres entidades públicas, tales como: ONP, INDECOPI y Osinergmin han sido certificadas con la ISO/IEC 27001, mientras que el resto solo había sido reconocido, es decir, habían completado el proceso de implementación, pero no obtuvieron la certificación.

TABLA 1.1 EMPRESAS PÚBLICAS RECONOCIDAS Y CERTIFICADAS

RAZÓN SOCIAL/ EMPRESA	ISO/IEC	FECHA ÚLTIMA ACREDITACIÓN	ACREDITADORA
Oficina de Normalización Previsional (ONP)	27001:2005	Año 2012 (Certificó)	British Standards Institution
Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)	27001:2005	Año 2013 (Certificó)	AENOR
Oficina Nacional del Proceso Electorales (ONPE)	27001:2013	Año 2016 (Reconocimiento más no certificada)	AENOR Perú
Organismo Supervisor de la Inversión en Energía y Minera (Osinergmin)	27001:2005	Año 2014 (Certificó)	-

FUENTE: CDI (2017)

También veremos en la **Tabla 1.2,** que según CDI (2017) solo cuatro empresas privadas habían sido certificadas con la ISO/IEC 2700, en tanto los demás se hallaban en proceso de certificación (reconocimiento).

TABLA 1.2 EMPRESAS PRIVADAS RECONOCIDAS Y CERTIFICADAS

RAZÓN SOCIAL/ EMPRESA	ISO/IEC	FECHA ÚLTIMA ACREDITACIÓN	ACREDITADORA
Seguridad de la Información Continuidad del negocio Gobierno de TI (ISEC)	27001:2013	Año 2014 (Certificó)	BSI Group
ATENTO Perú	27001:2013	Año 2015 (Recertificación)	AENOR
Bolsa de Valores de Lima	27001:2005	Año 2015 (Reconocimiento más no certificada)	Empresa SGS
RENIEC	27001:2013	Año 2015 (Reconocimiento más no certificada)	-
Telefónica del Perú	27001:2005	Año 2015 (Certificó)	-
HERMES – Transportes Blindados	27001:2005	Año 2015 (Certificó)	Empresa SGS
AMERICATEL Perú	27001:2013	Año 2016 (Certificó)	AENOR

FUENTE: CDI (2017)

1.2.3.3 Familia de la Norma ISO/IEC 27000

Son un grupo de estándares que se encargan de hacer un marco de gestión de seguridad de la información para cualquier tipo de organización.

Según Meza (2016), las normas ISO/IEC publicadas en la **Tabla 1.3**.

TABLA 1.3 FAMILIA DE LA NORMA ISO/IEC 27000

NORMA	CONTENIDO
ISO 27000	Visión general de la serie. Se maneja un vocabulario estándar para el SGSI.
ISO 27001	Norma principal de la serie. Requisitos de la implementación de la SGSI. Esta es la única norma certificable.
ISO 27002	Guía de buenas prácticas.
ISO 27003	Directrices para la implementación del SGSI.
ISO 27004	Métricas para la gestión de seguridad de la información.
ISO 27005	Gestión de riegos de seguridad de la información.
ISO 27006	Requisitos para la acreditación de entidades de auditoría y certificación.
ISO 27007	Guía de auditoria de SGSI.
ISO 27799	Guía para implementar ISO 27002
ISO 27035	Detección y evolución de incidentes de seguridad.

FUENTE: MEZA ALVARADO (2016)

Calder (2013) especificó que la familia de normas ISO/IEC 27000 ofrece un conjunto de estándares, códigos de conducta y mejores prácticas para las organizaciones, y que además garantiza una buena gestión de servicios de TI.

Cuando se hace referencia a la ISO/IEC 27001, automáticamente se piensa en un SGSI y todo lo que dicho sistema conlleva; esto significa que para para efectos de obtener una certificación o pasar una auditoría, su SGSI debe cumplir con los requisitos que establecidos por la 27001.

1.2.3.4 Sistema de Gestión de Seguridad de la Información

En el 2017, Nieves sostuvo que "un SGSI es aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, almacenada electrónicamente, proyectada, enviada por correo, transmitida en conversaciones, entre otros)."

En conclusión, la SGSI es un proceso de mejora continua y gran flexibilidad a los cambios que pueden producir las organizaciones debido a sus procesos claves. Además, toda información debe ser protegida por lo siguiente: **confidencialidad**, la información solo debe ser accedida por el personal autorizado, **integridad** que la información no sea alterada ni modificada y **disponibilidad** asegurar que las personas tengan acceso de la información solo cuando sea necesario.

Según Berríos y Rocha (2015) mencionan que "SGSI en las empresas ayuda a establecer estas políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización" (p.25).

En definitiva, con la implementación del SGSI, se comprenden cuáles son los riesgos a los que se encuentra expuesta la información y debe gestionar el sistema, ésta debe ser documentada y conocida por todos, además de estar en constante revisión y mejora.

Actualmente las organizaciones poseen información privada, la cual es su mayor activo. La cantidad de amenazas es muy frecuente por lo tanto deben tomar

el camino necesario para proteger. Es por esa razón que la implementación de la SGSI es necesaria, ya que da un cambio radical a toda organización, dejando todo atrás la manera en que estaban operando y empezar a tomar medidas de seguridad. La SGSI ayuda en tener un mayor conocimiento de la organización y determinando estrategias para asegurar y mejorar sus activos (Abad, 2015).

Un SGSI proporciona una guía para la implementación de las mejores prácticas que se considera cada vez como una necesidad en términos de cumplimiento en las organizaciones, que buscan certificarse antes de participar en las transacciones comerciales importantes (Calder, 2013).

1.2.3.5 Beneficios del SGSI

Según Abad (2015), algunos de los beneficios que consiguen la implementación de un SGSI son los siguientes:

- La organización demostrará que ha tomado las medidas necesarias al momento de cumplir con las normativas legales que engloba la protección de datos y la seguridad de la información.
- La implementación de la SGSI ayuda a las organizaciones a tomar decisiones fundamentadas en datos y estadísticas, por lo que aumentará la credibilidad hacia sus colaboradores y terceros.
- Al implementar la SGSI se tendrá la posibilidad de integrar otras certificaciones de ISO como: ISO 9001, ISO 14001 y OHSAS 18001.

1.2.3.6 Introducción de la Norma ISO/IEC 27001:2013

La ISO/IEC 27001:2013, cuya versión española es ISO/IE 27001:2014, es la primera revisión de la ISO/IEC 27001:2005 (ISO 2005), cuya versión española es ISO/IEC 27001:2007. La nueva versión se caracteriza principalmente por ofrecer mayor flexibilidad de implementación. Además, ofrece una mayor homogeneidad en su estructura con respecto a otros estándares ISO, lo que permitirá, si es oportuno, obtener otras certificaciones relacionadas (calidad, medio ambiente, etc.) que tendrán múltiples documentos en común (Abad, 2015).

1.2.3.7 Estructura de la Norma ISO/IEC 27001:2013

Según Abad (2015), la ISO/IEC 27001:2013 está estructurada según las siguientes cláusulas con el Ciclo de Deming **(Figura 1.4)**.

FIGURA 1.4 ESTRUCTURA DE LA NORMA ISO/IEC 27001:2013
FUENTE: AENOR (2014)

A continuación, se detalla las cláusulas de la estructura de la Norma ISO/IEC 27001:2013 según Abad (2015):

- **Cláusula 0: Introducción**

En esta cláusula se explica la razón de esta norma, indicando que busca el establecimiento, implementación, mantenimiento y mejora continua de un SGSI. Además, que el SGSI deberá ajustarse a las necesidades de la organización y demostrar la capacidad que tienen ellas al cumplir con los requisitos establecidos.

- **Cláusula 1: Alcance**

Aquí nos indica que el estándar es adaptable y pueden ser aplicados para cualquier organización.

- **Cláusula 2: Normas para consulta**

Para cualquier consulta se puede revisar el estándar 27000, el cual se convierte en la única referencia normativa de consulta obligatoria.

- **Cláusula 3: Términos y definiciones**

Como se detalló anteriormente, para cualquier consulta sobre los términos se encuentran en la 27000.

- **Cláusula 4: Contexto de la Organización**

Aquí se debe centrar en identificar las partes interesadas de la organización, ofreciéndonos las pautas y puntos de vista que se debe plantear la organización para la correcta identificación.

- **Cláusula 5: Liderazgo**

En esta cláusula se definen al SGSI como un proceso estratégico para la organización y establece el comportamiento que deberá de tomar la alta dirección con respecto a la SGSI.

- **Cláusula 6: Planificación**

Esta es una cláusula clave en la creación y mantenimiento del SGSI. Se enfoca en detallar la gestión de riesgos, detección de oportunidades y definición de los objetivos de seguridad. Aquí también se detalla el uso del Anexo A para controlar los riesgos en base a la creación del documento llamado “Declaración de Aplicabilidad” o SOA.

- **Cláusula 7: Soporte**

En esta cláusula hace referencias a los medios que son necesarios en la organización para alcanzar el desarrollo exitoso de la SGSI; además, de resaltar la importancia de los recursos humanos, debido a sus capacidades para asegurar un buen desempeño.

- **Cláusula 8: Operación**

Es la encargada de explicar cómo asegurar un correcto funcionamiento de la SGSI una vez implementado dentro de la organización.

- **Cláusula 9: Evaluación de desempeño**

Aquí se deben comparar los resultados con los objetivos y metas a cumplir ya que es importante en la SGSI. Mediante esta cláusula se sabrá si los objetivos de la organización se están cumpliendo o no.

- **Cláusula 10: Mejora**

En esta cláusula se especifica métodos para tratar cuando se encuentren una pauta susceptible de mejora continua.

- **Anexo A: Objetivos de control y controles de referencia**

Incluye una lista de los 114 controles necesarios y sus respectivos objetivos, como se indicó en la cláusula 6.

1.2.3.8 ventajas y desventajas de la ISO 27001:2013

El blog especializado en (SGSI) en el año 2014 publicó las ventajas que ofrece la ISO 27001:2013:

- Todas las definiciones se pueden encontrar en el estándar ISO 27000
- Los riesgos en la seguridad de información tienen que ser resueltos.
- Los documentos requeridos se encuentran establecidos depende del tamaño de la organización y la complejidad.
- Se tienen en cuenta todas las acciones preventivas.
- Facilita la integración de todos los sistemas de gestión.

Y las desventajas:

- No existe una descripción detallada de cómo identificar los riesgos.
- Los requisitos son difíciles de interpretar.
- No se hace mención al modelo PHVA.

1.2.4 ISO/IEC 27002

La ISO/IEC 27002 es un conjunto de medidas a tomar en cuenta, según su necesidad, para la seguridad de información en las organizaciones.

Al respecto, Miranda (2013) mencionó “los objetivos de seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa” (p.8)

Es decir, que para conseguir cada uno de estos objetivos se propone una serie de medidas o controles que se encuentran en la ISO/IEC 27002.

La ISO 27002 es una herramienta esencial para las empresas ya sea grande o pequeña, ya que es una norma flexible. Posee 14 dominios, la cual contiene 35 objetivos de control y 114 controles de procedimientos que reducen el nivel de riesgos. **(Figura 1.5)** y para visualizar en desglose todos los dominios con sus respectivos controles **(Anexo 1).**

FIGURA 1.5 DOMINIOS DE CONTROL DE NORMA ISO/IEC 27002
FUENTE: INCIBE (2016)

1.2.5 Comparación de la ISO/IEC 27001:2005 vs 27001:2013

La implantación de ISO/IEC 27001:2013 no debería implicar demasiadas complicaciones en una organización que cuente con la versión del 2005 dado que la nueva norma busca simplificar metodologías para lograr una integración más natural en el negocio.

Las diferencias entre las ambas se aprecian tanto en la estructura como en los contenidos **(Figura 1.6)**. Las modificaciones más destacadas las encontramos en el Anexo A, donde el número de dominios ha pasado de 11 a 14 y los controles de 133 a 114.

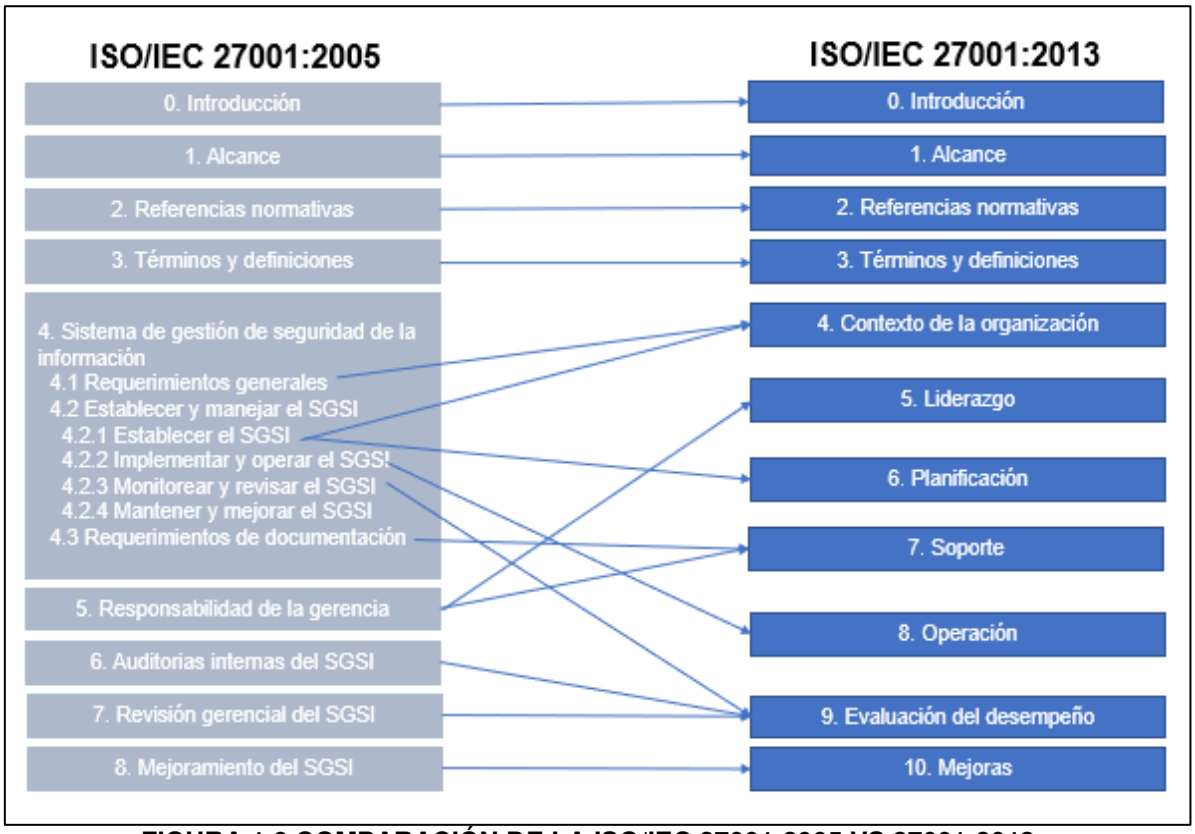


FIGURA 1.6 COMPARACIÓN DE LA ISO/IEC 27001:2005 VS 27001:2013
FUENTE: SGSI – BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (2014)

Se encontraron una relación comparativa entre las cláusulas de ambas versiones, a continuación, se detallará en forma escrita y mediante un cuadro comparativo. **(Anexo 2).**

A continuación, se detalla las cláusulas de comparación de la estructura de la ISO 27001:2005 con la 27001:2013 según Abad (2015):

- **Cláusula 0: Introducción**

En esta sección se encuentran grandes similitudes, sin embargo, se debe destacar que se ha eliminado la definición del proceso PDCA que se encontraba en la sección “Enfoque del proceso”. Como se ha mencionado, esta nueva edición requiere de un método que garantice la mejora continua, pero sin obligar a usar la

metodología del Ciclo de Deming (PDCA) en ningún momento, es decir, se puede usar cualquier metodología que cumpla con la mejora continua.

- **Cláusula 1: Objeto y campo de aplicación**

Similar descripción, mientras que antes bastaba con cumplir los requisitos especificados en las cláusulas 4, 5, 6, 7 y 8, ahora es obligatorio cumplir con los requisitos especificados en las cláusulas de la 4 a la 10.

- **Cláusula 2: Normas para consulta**

Antes se referenciaba al estándar 17799:2005, actualmente se obliga la consulta de la ISO/IEC 27000.

- **Cláusula 3: Términos y definiciones**

No encontramos ninguna de las definiciones de términos que encontrábamos en la versión anterior, todos ellos han sido incluidos en la sección tres del estándar 27000, que es a la que se hace referencia ahora.

- **Cláusula 4: Contexto de la Organización**

Esta es una de las cláusulas que mayor cambio ha experimentado debido a que en la versión del 2005, el ciclo PDCA se describía en ella por completo. Sin embargo, ahora, no se contempla.

Además, en la nueva versión aparece un nuevo concepto de las partes interesadas, es fundamental este concepto para poder definir el alcance de la SGSI.

- **Cláusula 5: Responsabilidades de la dirección**

En la nueva versión se introduce el concepto de “alta dirección” y se insiste en su compromiso de ser un ejemplo en la gestión del SGSI.

- **Cláusula 6: Auditorías internas del SGSI y Cláusula 7: Revisión del SGSI por la dirección**

Estas dos cláusulas, se reubican en la nueva norma dentro de las cláusulas 9.2 y 9.3 respectivamente.

- **Cláusula 8: Mejora del SGSI**

La mejora continua y acciones correctivas son en la nueva versión las cláusulas 10.2 y 10.1 respectivamente.

- **Anexos**

El Anexo A normativo ha sido reestructurado y el número de dominios ha pasado de 11 a 14 y los controles de 133 a 114. Los anexos B y C informativos de la versión del 2005 desaparecen en la versión del 2013.

1.2.6 Metodologías

1.2.6.1 Ciclo de Deming (PDCA O PHVA)

Esta metodología está compuesta por cuatro fases **(Figura 1.7),** las cuales son PDCA: "Plan", "Do", "Check" y "Act", o PHVA, Planificar, Hacer, Verificar y Actuar, en español. Este es un ciclo que se repite de forma continua.

A continuación, se detallan las fases: en la primera fase **Planear** se establecen las actividades que se van a mejorar y los objetivos a alcanzar. En la segunda etapa **Hacer,** se ejecuta lo establecido, es decir implementar lo propuesto. En la tercera etapa **Verificar,** se prueba lo implementado por un plazo de tiempo para verificar su funcionamiento óptimo. Si lo propuesto no cumple lo planteado inicialmente entonces se tiene que variar para ajustarlo a los objetivos establecidos. Por último, en la última etapa **Actuar**, al finalizar el plazo de prueba se estudia lo obtenido, es decir la situación final, y se compara con la situación inicial de las actividades (Jimeno, 2013).

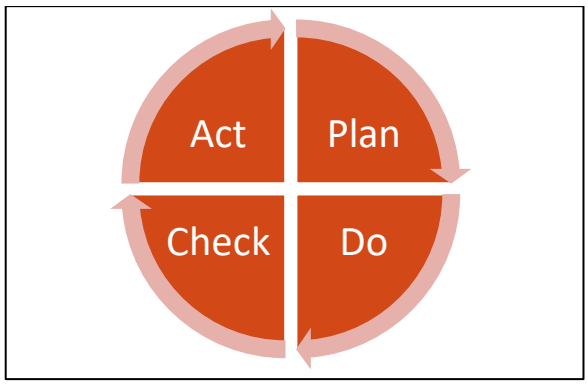


FIGURA 1.7 FASES DE LA METODOLOGÍA CICLO DE DEMING
FUENTE: JIMENO J. (2013)

1.2.6.2 Metodologías para la Implementación de un SGSI

Se construyó un proceso metodológico basado en cuatro normas: ISO/IEC 27001, 27002, 27003 y 27005; específicamente en la interrelación de estas normas, para las que se desarrollaron actividades requeridas para cumplir con lo requerido en el estándar 27001, la 27002 presenta controles de seguridad, la gestión de riesgos de la 27005, y lo sugeridos del estándar 27003. Esta metodología da respuesta a la interrogante del cómo llevar un proyecto con la importancia del contexto actual en las organizaciones y basándose en estándares internacionales. Es una metodología que cuenta con cinco fases secuenciales **(Figura 1.8)**. Además, fue creada específicamente para incrementar el éxito y reducir la inseguridad en los resultados en las futuras implementaciones de la ISO/IEC 27001:2013 en las organizaciones (Valencia y Orozco, 2017).

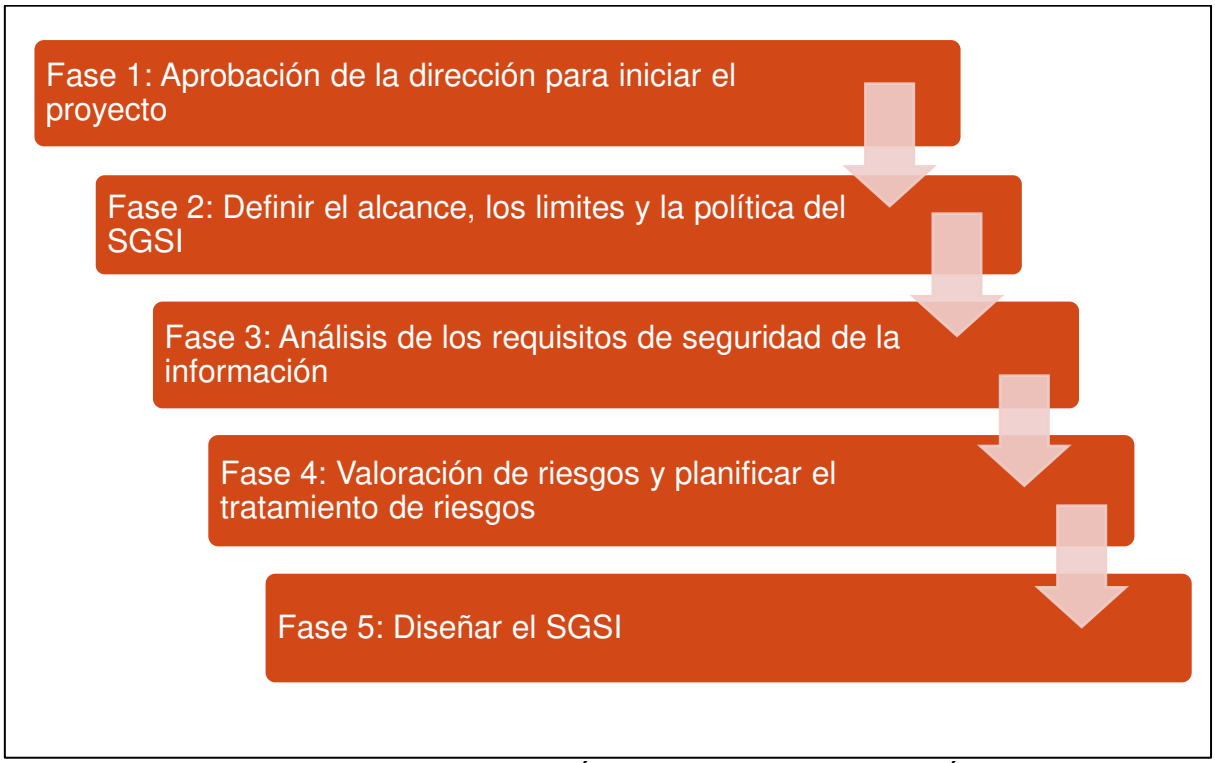


FIGURA 1.8 FASES DE LA METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL SGSI
FUENTE: VALENCIA Y OROZCO (2017)

1.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir.
- **Alta dirección:** Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema a una organización.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoria.
- **Competencia:** Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.
- **Confidencialidad:** Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- **Conformidad:** Cumplimiento de un requisito.
- **Contexto externo:** Entorno externo en el que la organización busca alcanzar sus objetivos.
- **Contexto interno:** Entorno interno en el que la organización busca alcanzar sus objetivos.
- **Control:** Medida que modifica un riesgo.
- **Control de acceso:** Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y seguridad.
- **Corrección:** Acción para eliminar una no conformidad detectada.
- **Disponibilidad:** Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.
- **Información documentada:** Información que una organización tiene que controlar y mantener, y el medio en el que está contenida.
- **Integridad:** Propiedad de exactitud y completitud.
- **Mejora continua:** Actividad recurrente para mejorar el desempeño.
- **Nivel de riesgo:** Magnitud de riesgo o combinación de riesgos, expresados en términos de la combinación de consecuencias.

- **No conformidad:** Incumplimiento de un requisito.
- **Objetivo de control:** Declaración que describe lo que se quiere lograr como resultado de la implementación de controles.
- **Parte interesada:** Persona u organización que puede afectar, estar afectada o percibir que está afectada por una decisión o actividad.
- **Política:** Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.
- **Probabilidad:** Posibilidad de que algún hecho se produzca.
- **Propietario del Riesgo:** Persona o entidad con la capacidad y autoridad para gestionar un riesgo.
- **Requisito:** Necesidad o expectativa que está establecida, generalmente implícita u obligatoria, "generalmente implícita".
- **Riesgo:** Efecto de la incertidumbre sobre la consecución de los objetivos.
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **Sistema de Gestión de Seguridad de Información:** Consiste en políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información.
- **Tratamiento del riesgo:** Proceso destinado a modificar el riesgo.
- **Vulnerabilidad:** Debilidad de un activo o de un control.

CAPÍTULO II:
METODOLOGÍA

En esta tesis se trabajó la investigación aplicada, la cual permite obtener información sobre la problemática actual, identificar las necesidades y aplicar conocimientos prácticos obtenidos en los cursos de pregrado. A continuación, se detallará los materiales y métodos utilizados para la investigación de la tesis.

2.1 MATERIALES

A continuación, los materiales que ayudaron en la investigación de la tesis.

2.1.1 Hardware

Para el desarrollo de la documentación de la tesis se usó el material de hardware mostrado en la **Tabla 2.1**

TABLA 2.1 MATERIAL DE HADWARE

Cantidad	Hardware	Características
2	Laptop Asus	Intel Core i7-5500U 2.40GHz, Memoria RAM 12GB, Disco duro 1TB SATA
1	Laptop Asus	Intel Core i5-5200U 2.20GHz, Memoria RAM 6GB, Disco duro 1TB SATA
1	Laptop Dell	Intel Core i7-6500U 2.50GHz, Memoria RAM 8GB, Disco duro 1TB SATA

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

2.1.2 Software

Para el desarrollo de la documentación de la tesis se usó el material de software mostrado en la **Tabla 2.2**

TABLA 2.2 MATERIAL DE SOFTWARE

Software	Descripción
Microsoft Word	Procesador de texto Microsoft Office
Microsoft Excel	Procesador de cálculos
Bizagi	Modelamiento de procesos
Servidor (nube)	Google Drive
Gantter	Gestión de proyectos
Adobe Reader	Visor de PDF

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

2.1.3 Recursos Humanos

Para el desarrollo de la documentación de la tesis se usaron los recursos expuestos en la **Tabla 2.3**

TABLA 2.3 MATERIAL DE RECURSOS HUMANOS

Cantidad	Perfil de recurso
1	Coordinadora de Calidad
1	Coordinadora de RR. HH.
1	Analista de seguridad de información
1	Jefe de proyectos

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

2.1.4 Costo de Proyecto

Para la implementación se requirió una inversión de **S/.12,733.60** como se puede ver en la **Tabla 2.4**

TABLA 2.4 COSTO TOTAL DEL PROYECTO

Descripción	Valor Nuevos Soles S/
Actividades	S/ 3,224.00
Recursos de hardware y software	S/ 6,735.00
Perfil de recurso	S/ 2,280.60
Costos indirectos	S/ 494.00
Total de la implementación de la SGSI	**S/ 12,733.60**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Para obtener el presupuesto total del proyecto, se realizaron cálculos sobre el costo de las actividades detalladas en la **Tabla 2.5**

TABLA 2.5 COSTO POR ACTIVIDADES

Actividades	Descripción	En soles	Cantidad	Total
Asesoría	Asesor en ISO/IEC 27001	S/ 1,860.00	1 persona	S/ 1,860.00
Auditor	Asesor para revisión	S/ 700.00	1 persona	S/ 700.00
Capacitación y concientización en seguridad de información	Coffee break	S/ 564.00	25 personas	S/ 564.00
	Impresiones y folletos	S/ 100.00	01 millar	S/ 100.00
SUBTOTAL				**S/ 3,224.00**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Además, se realizaron cálculos sobre los costos de los recursos de hardware y software, detallados en la **Tabla 2.6**, donde se observa la procedencia de los recursos, la cantidad, costo unitario y el costo total.

TABLA 2.6 COSTOS POR RECURSOS DE HARDWARE Y SOFTWARE

Hardware/Software	Procedencia	Cantidad	Costo Unitario	Total
Intel Core i7-5500U 2.40GHz, Memoria RAM 8GB, Disco duro 1TB SATA	Empresa	2	S/ 1,600	S/ 3,200.00
Intel Core i5-5200U 2.20GHz, Memoria RAM 6GB, Disco duro 1TB SATA	Autor	1	S/ 1,700	S/ 1,700.00
Intel Core i7-6500U 2.50GHz, Memoria RAM 8GB, Disco duro 1TB SATA	Empresa	1	S/ 1,450	S/ 1,450.00
Licencias de Office	Nexsys	2	S/ 29	S/ 58.00
	Office 365 (USMP institucional)	2	0	S/ 0.00
Bizagi	Software libre	4	0	S/ 0.00
Google Apps	Xertica (G Suite)	1	0	S/ 327.00
	Google Apps libres	2	0	S/ 0.00
Gantter	Software libre	1	0	S/ 0.00
Adobe Reader	Software libre	1	0	S/ 0.00
SUBTOTAL				**S/ 6,735.00**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

También se consideró el costo por perfil de recurso, detallado en la **Tabla 2.7**, donde se contabilizó la tarifa por jornada (cada jornada equivale a 9 horas), cantidad de días, cantidad de horas por día y el total de cada perfil.

TABLA 2.7 COSTOS POR PERFIL DE RECURSO

Perfil de recurso	Abreviatura	Tarifa x jornada	Tarifa x hora	Cantidad de días	Cantidad de horas x día	Total x Perfil S/
(1) Coordinadora de calidad	CC	S/ 38.71	S/ 4.30	15d	4h	S/ 258.00
(1) Coordinadora de RR.HH.	CRRHH	S/ 29.80	S/ 3.31	15d	4h	S/ 198.60
(1) Analista de seguridad de información	ASI	S/ 40.20	S/ 4.46	40d	5h	S/ 892.00
(1) Jefe de proyectos	JP	S/ 41.94	S/ 4.66	40d	5h	S/ 932.00
SUBTOTAL						**S/ 2,280.60**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En la implementación del proyecto se tomó en consideración los costos indirectos de los servicios tales como: el agua, luz, internet fijo y otros gastos que se pueden visualizar en la **Tabla 2.8.**

TABLA 2.8 COSTOS INDIRECTOS

Detalle	Costo	Cantidad	Total
Agua	S/ 20	3	S/ 60.00
Luz	S/ 30	3	S/ 90.00
Internet fijo	S/ 78	3	S/ 234.00
Otros gastos	S/ 110	1	S/ 110.00
SUBTOTAL			**S/ 494.00**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

2.1.5 Cronograma del Proyecto

	PROYECTO - IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE REQUISITOS	67 días	lun 12/03/18	lun 28/05/18		RECURSOS
	FASE 1 – PLANEAR	**39 días**	**lun 12/03/18**	**mié 25/04/18**		
3	**Realizar el análisis de brecha inicial**	**4 días**	**lun 12/03/18**	**jue 15/03/18**		
4	Realizar cuestionario de análisis de brecha	2 días	lun 12/03/18	mar 13/03/18		ASI
5	Responder cuestionario de análisis de brecha	2 días	mié 14/03/18	jue 15/03/18	4	JP, ASI, CC, CRRHH
6	Informe de análisis de brecha inicial	0 días	jue 15/03/18	jue 15/03/18	5	JP, ASI
7	**Compromiso con la alta dirección**	**3 días**	**vie 16/03/18**	**lun 19/03/18**		
8	Realizar una propuesta del proyecto	2 días	vie 16/03/18	sáb 17/03/18	6	JP
9	Realizar acta de compromiso de la alta dirección	1 día	vie 16/03/18	vie 16/03/18	6	ASI
10	Revisión de la alta dirección	1 día	lun 19/03/18	lun 19/03/18	8,9	ASI, JP
11	Acta de compromiso de la alta dirección	0 días	lun 19/03/18	lun 19/03/18	10	ASI
12	Propuesta comercial del proyecto	0 días	lun 19/03/18	lun 19/03/18	10	JP

	PROYECTO - IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE REQUISITOS	67 días	lun 12/03/18	lun 28/05/18		RECURSOS
13	**Comprender el contexto de la organización**	**2 días**	**mar 20/03/18**	**mié 21/03/18**		
14	Análisis del contexto de la organización	1 día	mar 20/03/18	mar 20/03/18	12	ASI, JP
15	Realizar informe de contexto de la organización	1 día	mié 21/03/18	mié 21/03/18	14	ASI, JP
16	Informe del contexto de la organización	0 días	mié 21/03/18	mié 21/03/18	15	ASI, JP
17	**Comprender necesidades y expectativas de las partes interesadas**	**2 días**	**jue 22/03/18**	**vie 23/03/18**		
18	Reunión para evaluar las necesidades y expectativas de las partes interesadas	1 día	jue 22/03/18	jue 22/03/18	16	ASI, CRRHH, CC, JP
19	Análisis de necesidades y expectativas de las partes interesadas	1 día	vie 23/03/18	vie 23/03/18	18	ASI, JP
20	Informe de necesidades y expectativas de las partes interesadas	0 días	vie 23/03/18	vie 23/03/18	19	ASI, JP
21	**Determinar el alcance del SGSI**	**2 días**	**sáb 24/03/18**	**lun 26/03/18**		
22	Evaluar el alcance del SGSI	1 día	sáb 24/03/18	sáb 24/03/18	16,20	ASI
23	Revisión de la Alta Dirección	1 día	lun 26/03/18	lun 26/03/18	22	ASI, JP
24	Declaración del alcance del SGSI	0 días	lun 26/03/18	lun 26/03/18	23	ASI, JP
25	**Determinar política de seguridad de la información**	**3 días**	**mar 27/03/18**	**jue 29/03/18**		
26	Desarrollo de la política de seguridad de la información	2 días	mar 27/03/18	mié 28/03/18	16,20,23	ASI, JP
27	Revisión de la Alta Dirección	1 día	jue 29/03/18	jue 29/03/18	26	ASI, JP
28	Política de seguridad de la información	0 días	jue 29/03/18	jue 29/03/18	27	ASI, JP
29	**Actualizar manual de organización y funciones (ficha de puesto)**	**3 días**	**vie 30/03/18**	**lun 02/04/18**		
30	Identificar roles y responsabilidades para la seguridad de la información	2 días	vie 30/03/18	sáb 31/03/18	28	ASI, JP
31	Elaborar ficha de puesto para roles de la seguridad de la información	1 día	lun 02/04/18	lun 02/04/18	30	ASI, JP
32	Ficha de puesto para los roles de seguridad de la información	0 días	lun 02/04/18	lun 02/04/18	31	ASI, JP
33	**Establecer procedimiento de control de documentación**	**3 días**	**mar 27/03/18**	**jue 29/03/18**		
34	Desarrollo de procedimiento de control de documentación	3 días	mar 27/03/18	jue 29/03/18	24	ASI, JP
35	Procedimiento de control de documentación	0 días	jue 29/03/18	jue 29/03/18	34	ASI, JP
36	**Establecer procedimiento de evaluación y tratamiento de riesgos**	**2 días**	**vie 30/03/18**	**sáb 31/03/18**		
37	Desarrollo de procedimiento de evaluación y tratamiento de riesgos	2 días	vie 30/03/18	sáb 31/03/18	35	ASI, JP
38	Procedimiento de evaluación y tratamiento de riesgos	0 días	sáb 31/03/18	sáb 31/03/18	37	ASI, JP
39	**Establecer procedimiento de gestión de incidentes**	**2 días**	**vie 30/03/18**	**sáb 31/03/18**		
40	Desarrollo de procedimiento de gestión de incidentes	2 días	vie 30/03/18	sáb 31/03/18	35	ASI, JP
41	Procedimiento de gestión de incidentes	0 días	sáb 31/03/18	sáb 31/03/18	40	ASI, JP
42	**Establecer procedimiento de auditoria interna**	**2 días**	**vie 30/03/18**	**sáb 31/03/18**		
43	Desarrollo del procedimiento de auditoria interna	2 días	vie 30/03/18	sáb 31/03/18	35	ASI, JP
44	Procedimiento de auditoria interna	0 días	sáb 31/03/18	sáb 31/03/18	43	ASI, JP
45	**Gestión de Riesgos**	**14 días**	**lun 02/04/18**	**mar 17/04/18**		
46	Realizar metodología de evaluación de riesgos	2 días	lun 02/04/18	mar 03/04/18	37	ASI, JP
47	Metodología de evaluación de riesgos	0 días	mar 03/04/18	mar 03/04/18	46	ASI, JP
48	Realizar el inventario de activos de información	6 días	mié 04/04/18	mar 10/04/18	47	ASI, CC, CRRHH, JP
49	Inventario de activos de información	0 días	mar 10/04/18	mar 10/04/18	48	ASI, JP
50	Determinar amenazas y vulnerabilidades de los activos de información	6 días	mié 11/04/18	mar 17/04/18	49	ASI, CC, CRRHH, JP
51	Evaluación de riesgos	0 días	mar 17/04/18	mar 17/04/18	50	ASI, JP
52	**Elaborar plan de tratamiento de Riesgos**	**5 días**	**mié 18/04/18**	**lun 23/04/18**		
53	Realizar plan de tratamiento de riesgos	4 días	mié 18/04/18	sáb 21/04/18	51	JP
54	Realizar informe de gestión de riesgos	1 día	lun 23/04/18	lun 23/04/18	53	JP
55	Plan de tratamiento de riesgos	0 días	sáb 21/04/18	sáb 21/04/18	53	JP
56	Informe de la gestión de riesgos	0 días	lun 23/04/18	lun 23/04/18	54	ASI, JP
57	**Elaborar declaración de aplicabilidad de controles**	**4 días**	**vie 16/03/18**	**mar 20/03/18**		
58	Elaborar declaración de aplicabilidad de controles	4 días	vie 16/03/18	mar 20/03/18	6	ASI, JP
59	Declaración de aplicabilidad de controles	0 días	mar 20/03/18	mar 20/03/18	58	ASI, JP
60	**Elaborar matriz de comunicación interna y externa**	**2 días**	**mié 18/04/18**	**jue 19/04/18**		
61	Realizar matriz de comunicación interna	2 días	mié 18/04/18	jue 19/04/18	51	ASI
62	Matriz de comunicación interna	0 días	jue 19/04/18	jue 19/04/18	61	ASI
63	**Elaborar plan de capacitación y concientización**	**3 días**	**lun 23/04/18**	**mié 25/04/18**		
64	Realizar plan de capacitación y concientización	3 días	lun 23/04/18	mié 25/04/18	55	ASI
65	Plan de capacitación y concientización	0 días	mié 25/04/18	mié 25/04/18	64	ASI
66	**FASE 2 – HACER**	**23 días**	**mié 02/05/18**	**lun 28/05/18**		
67	**Implementar plan de capacitación y concientización**	**11 días**	**mié 02/05/18**	**lun 14/05/18**		
68	Ejecución del plan de capacitación y concientización	10 días	mié 02/05/18	sáb 12/05/18	65FC+5 días	ASI, CC, CRRHH, JP
69	Realizar informe de ejecución de plan de capacitación y concientización	1 día	lun 14/05/18	lun 14/05/18	68	ASI
70	Informe de plan de capacitación y concientización	0 días	lun 14/05/18	lun 14/05/18	69	ASI
71	**Implementar plan de tratamiento de riesgos (Grupo uno)**	**13 días**	**lun 14/05/18**	**lun 28/05/18**		
72	Ejecución del plan de tratamiento de riesgos	12 días	lun 14/05/18	sáb 26/05/18	55,59,68	ASI, CC, CRRHH, JP
73	Realizar informe de ejecución de plan de tratamiento de riesgos	1 día	lun 28/05/18	lun 28/05/18	72	JP

PROYECTO - IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE REQUISITOS		67 días	lun 12/03/18	lun 28/05/18		RECURSOS
74	Informe de plan de tratamiento de riesgos	0 días	lun 28/05/18	lun 28/05/18	73	JP

FIGURA 2.1 CRONOGRAMA DEL PROYECTO
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

2.2 MÉTODOS

2.2.1 Selección del Método/ Metodología (Criterios)

En base a la investigación realizada sobre metodologías usadas para el desarrollo de proyectos similares al que contempla esta tesis, se encontraron dos tipos de metodologías: Ciclo de Deming y metodologías propias creadas para la implementación del SGSI. Dentro de las metodologías propias, encontramos la "Metodología para la Implementación de un SGSI".

Sobre lo mencionado, realizamos una comparación entre usar el Ciclo de Deming o usar una metodología propia **(Tabla 2.10)**, para ello tuvimos una escala de puntaje **(Tabla 2.9)**, teniendo en cuenta las conclusiones y recomendaciones de lo investigado.

TABLA 2.9 ESCALA DE PUNTAJE DE METODOLOGÍA

Descripción	Valor
Alto	5
Medio alto	4
Medio	3
Medio bajo	2
Bajo	1

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

TABLA 2.10 COMPARACIÓN DE METODOLOGÍAS

Criterios de selección	Metodologías	
	Ciclo Deming	Metodología para la Implementación de un SGSI
Adaptabilidad	4	2
Simplicidad	4	2
Flexibilidad	4	3
Mejora continua	5	3
Experiencia	5	2
TOTAL	**22**	**10**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Analizando los resultados de la valoración sobre las metodologías, se observa que el puntaje total del Ciclo de Deming es mayor **(22)** que el de la otra metodología, es decir, es la más indicada a usar para el desarrollo del proyecto. Se eligió esta metodología ya que es adaptable para cualquier otro proyecto; actualmente la consultora está planificando la implementación de las ISO 9001 y 14001, para las cuales se usará también el Ciclo de Deming. Contempla una mayor simplicidad por sus cuatro fases, ya estructuradas. Flexibilidad, se pueden adaptar a cualquier parte de la organización o proyecto que requiera una mejora continua. El Ciclo de Deming está orientado a la mejora continua ya que es una metodología cíclica. En cuanto a la experiencia, podemos encontrar muchos proyectos que han usado esta metodología en las cuales plantean recomendaciones para su uso.

2.2.2 Metodología seleccionada

Ciclo de mejora continua o Deming

Se empleará el uso de la metodología del Ciclo de Deming para lograr establecer, implementar, mantener y mejorar el SGSI. Actualmente, en la ISO/IEC 27001, no específica ni sugiere explícitamente el uso de esta metodología; sin embargo, ha sido sugerida en sus versiones anteriores, y la estructura de la norma es muy adaptable a esta metodología. Además, ayuda a cumplir con la mejora continua del SGSI.

El Ciclo de Deming según Justino (2015) “un proceso metodológico desarrollado por Shewhart y Deming basado en proyectos de mejora sobre procesos propios, externos e internos, muchas normas y estándares apoyan sus requisitos en este ciclo de mejora, y establecen que lo usen los sistemas de gestión.”

La metodología enfocada en la implementación de la ISO 27001:2013 se puede ver en la **Figura 2.2**

Planificar (Plan), establecer las labores a llevar a cabo para establecer el SGSI. Para ello, debemos realizar las siguientes actividades:

- Análisis de brecha inicial
- Compromiso de la Alta Dirección
- Comprender el contexto de la organización

- Comprender necesidades y expectativas de las partes interesadas
- Determinar el alcance del SGSI
- Determinar la política de seguridad de la información
- Determinar objetivos de seguridad de la información
- Crear procedimiento de gestión de riesgos
- Crear procedimiento de gestión de incidencia
- Crear procedimiento de auditoria interna
- Gestionar los riesgos
- Crear plan de tratamiento de riesgos
- Determinar la declaración de aplicabilidad
- Crear plan de capacitación y concientización

Hacer (Do), se ejecuta lo planificado anteriormente. Después de haberse puesto en marcha o estar implementado, se puede ir a la siguiente fase. Las actividades por realizar en esta fase son:

- Implementar plan de tratamiento de riesgos
- Implementar plan de capacitación y concientización

Verificar (Check), se evalúan los resultados conseguidos mediante una auditoria. Las actividades por realizar en esta fase son:

- Preparar la auditoría interna
- Ejecutar auditoría
- Revisar con la alta dirección los resultados obtenidos

Mejorar (Act), por último, aquí se aplica la mejora continua, aplicando las acciones correctivas e identificando oportunidades de mejora, y seguirá con el proceso cíclico. Las actividades por realizar en esta fase son:

- Crear plan de acciones correctivas y mejoras
- Implementar plan de acciones correctivas y mejoras
- Análisis de brecha final

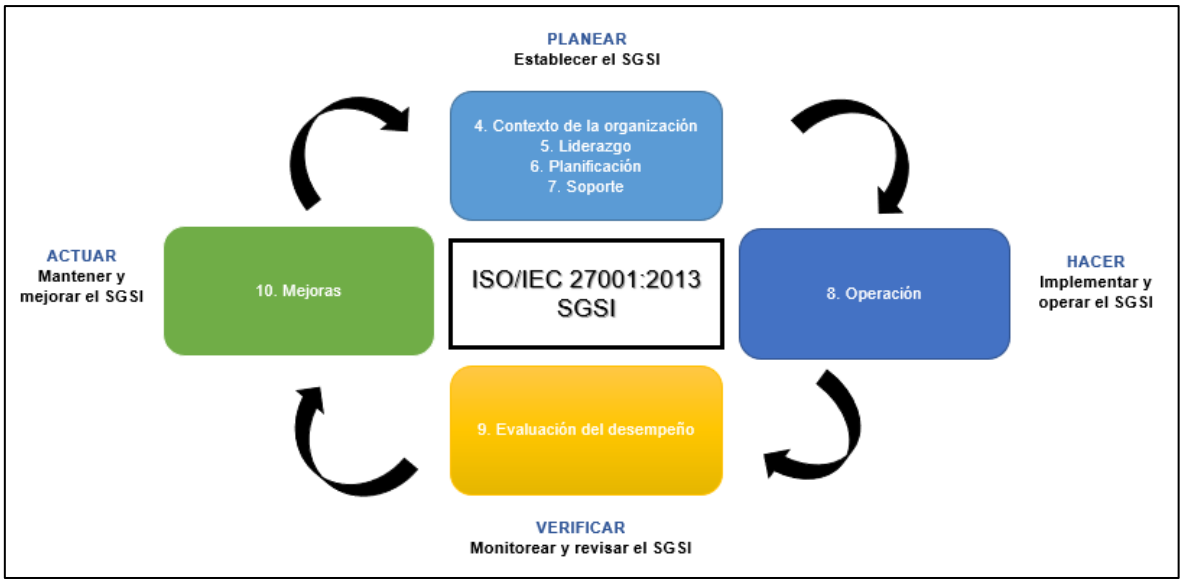


FIGURA 2.2 CICLO PDCA
FUENTE: GÓMEZ L. Y FERNÁNDEZ P. (2015)

Se ha establecido una lista de documentos pertenecientes a los requisitos de la ISO 27001:2013. En la **Tabla 2.11** se encuentran ordenadas por cada fase.

TABLA 2.11 LISTA DE DOCUMENTOS PDCA

PLAN/ PLANEAR
Informe de contexto de la organización
Informe de necesidades y expectativas de las partes interesadas
Declaración del alcance del SGSI
Política de Seguridad de la Información
Tablero de control de objetivos del SGSI
Procedimiento para el control de información documentada
Procedimiento para de gestión de riesgos y oportunidades
Declaración de aplicabilidad
Plan de Tratamiento de Riesgos y Oportunidades
Plan de Capacitación y Concientización
Matriz de Comunicación
DO / HACER
Informe de la implementación de riesgos
Informe de la Capacitación y Concientización
CHECK / VERIFICAR
Informe de auditoría externa
Revisión por la Dirección
ACT / ACTUAR
Procedimiento de No conformidades y Acciones correctivas
Plan de Acciones Correctivas
Informe de implementación de acciones correctivas

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

CAPÍTULO III:
DESARROLLO DEL PROYECTO

En este capítulo se explica la situación de la empresa, se detallan las dos primeras fases descritas en el capítulo anterior, las cuales están compuestas de las actividades y documentos realizados.

3.1 SITUACIÓN ACTUAL DE LA EMPRESA

A continuación, se explican los servicios que ofrece la empresa actualmente, su estructura organizacional y sus macroprocesos.

VF CONSULTING S.A.C. es una empresa de consultoría con conocimiento experto, enfocados al sector de las telecomunicaciones, en el cual desarrollan proyectos sobre BSCS (Business Support and Control System), canales digitales (Retail y CRM), mediación, entre otros. VF es socio estratégico de sus clientes debido al diseño, implementación y despliegue exitoso de soluciones especializadas.

La estructura organizacional se visualiza en la **Figura 3.1**

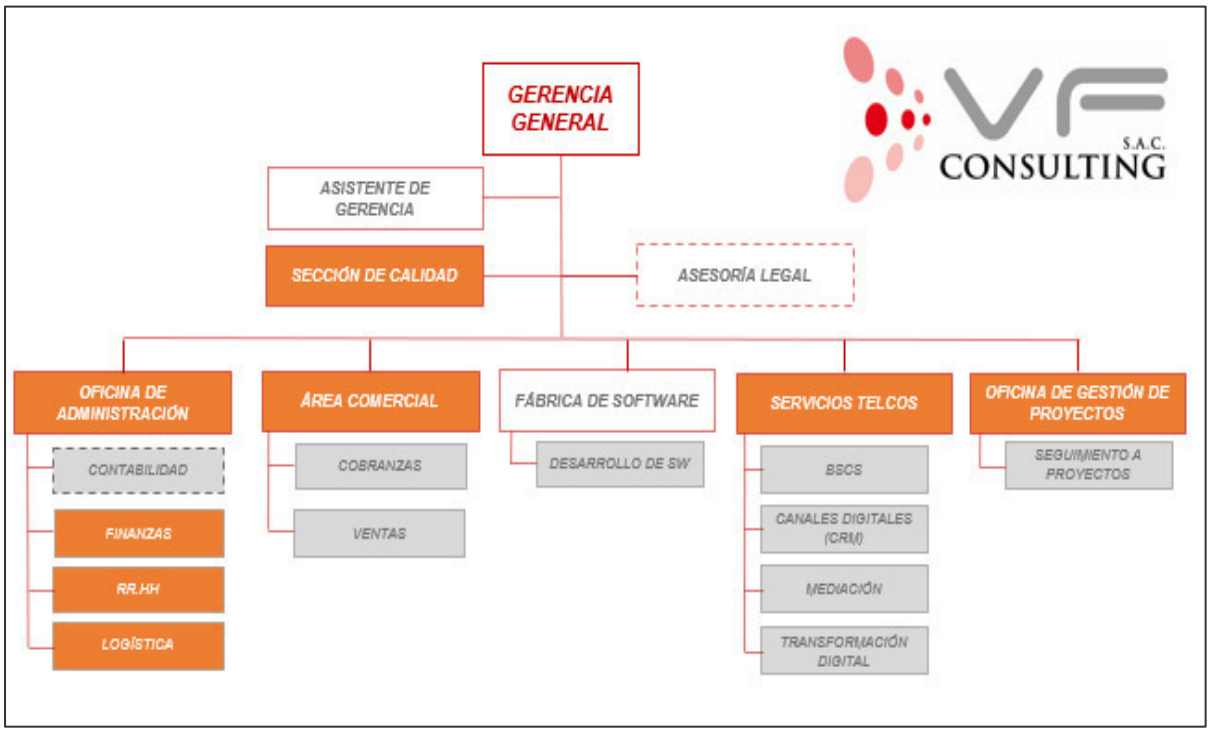


FIGURA 3.1 ORGANIGRAMA ORGANIZACIONAL
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Las áreas que estarán contempladas en la implementación de la ISO/IEC 27001:2013 son las que están resaltadas en naranja. El área principal es **"Servicios Telcos".**

Los macroprocesos de VF CONSULTING S.A.C. se muestran en la **Figura 3.2**, los procesos resaltados en un círculo rojo son los que están dentro de nuestro alcance. El proceso core es el de **"Prestación de Servicios Telcos"**.

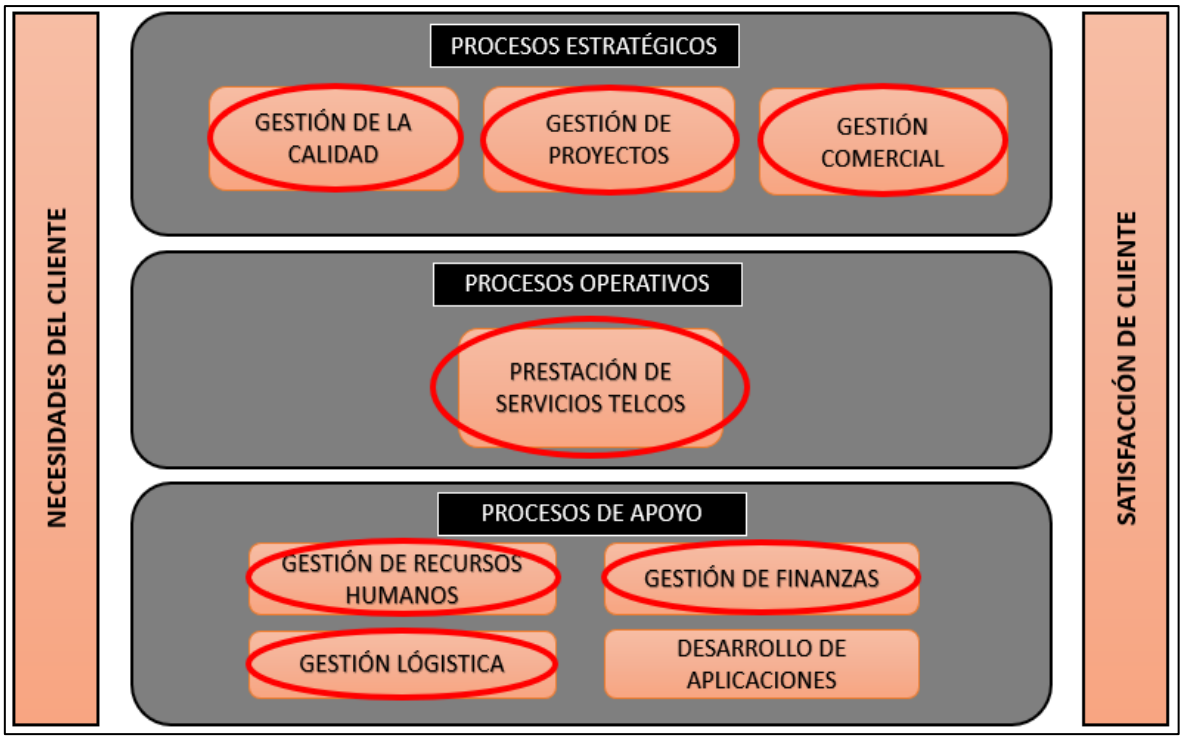


FIGURA 3.2 MACROPROCESOS DE LA EMPRESA
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Los procesos involucrados con el proceso core son los siguientes:

1) **Gestión de proyectos:** Es el proceso que se encarga de la ejecución de las propuestas aceptadas, asignando los recursos correspondientes con respecto a la complejidad y alcance del servicio. Además, realiza seguimientos y reportes de todos los proyectos desde que inicia hasta el fin del servicio. Este proceso se involucra con el proceso core debido a que primero debe hacerse toda la parte de gestión para luego sin inconvenientes proceder a realizar la prestación de servicio.

2) **Gestión comercial:** Es el proceso en el cual se venden propuestas de servicios Telcos a los clientes dependiendo de sus necesidades y requerimientos. Se inicia de dos maneras, la primera al recibir requerimientos de los clientes y la segunda cuando el subgerente comercial identifica una necesidad de negocio. Luego el subgerente comercial se encarga de formular y realizar las propuestas solicitando la estimación de tiempo, alcance y recursos para dicho servicio. Una vez realizado la

propuesta, esta es enviada al cliente para su conformidad, si el cliente acepta el servicio quiere decir que es una propuesta ganada lo cual procede al desarrollo y finaliza cuando comunica al cliente que genere la orden de compra correspondiente al porcentaje inicial que se detalló en las condiciones comerciales de la propuesta. Este proceso se involucra con el proceso core ya que para llegar a este se debe iniciar con la venta de los servicios, además para el desarrollo de la prestación de servicios se necesita primero conocer los requerimientos y necesidades de las empresas Telcos.

3) **Gestión de recursos humanos:** Es el proceso que se encarga de manejar todos los datos personales, planilla de sueldos, contratos, elaboración de EPS, gestión de AFP u ONP, vacaciones, es decir todos los beneficios que debe tener el empleado. Este proceso se involucra con el proceso core ya que maneja toda la información (datos de personal, sueldos, contratos, cv, etc.) que necesitan los gestores de proyectos y el área comercial como input para realizar propuestas técnicas y comerciales, gestionar permisos VPN de nuestros clientes, gestionar permisos de entrada y entre otros. Sin esta información no se podría realizar la gestión de manera ordenada, el desarrollo de los servicios prestados y la confidencialidad de los clientes.

4) **Gestión de contabilidad y finanzas:** Es el proceso que se encarga de la parte contable y financiera de la empresa. El proceso de contabilidad gestiona todos los gastos y pagos que genera la empresa mediante un registro de caja chica; sin embargo, todo lo que tenga que ver con la SUNAT, SUNAFIL y el ministerio de trabajo es encargado a la parte contable externa. Es por esta razón que no se involucra con el proceso core, ya que el proceso contable interno es de pequeña gestión. El proceso de finanzas abarca toda la parte de cobranzas, facturación y financiera de la empresa. Inicia cuando el asistente comercial envía la orden de compra de las propuestas de servicios aceptados al coordinador de finanzas, este registra cada orden de compra para que luego ser enviado al asistente administrativo, el cual genera la factura correspondiente y por último se procede a presentar en mesa de partes o por medio de correo electrónico a los clientes para que reciban la

factura y pueda ser cobrada en el respectivo tiempo, esto con ayuda de reportes financiero de todos los servicios que se han sido aceptado o están en proceso de aceptación, es decir propuestas ganadas, negociadas o canceladas. Es por esa razón que es un proceso involucrado al core ya que es una salida de este al momento de vender, negociar, desarrollar y terminar los servicios prestados.

5) **Gestión logística:** Este proceso se encarga en la asignación de máquinas o equipos hacia los empleados para su debido uso, también de llevar un control de todos los activos de software tanto como licencias, programas, instaladores, además de los activos de soporte de información, tales como: USB, disco externo, cable de seguridad, entre otros. Este proceso se involucra con el proceso core debido a que sin ninguna asignación de equipos no se podría empezar a desarrollar los servicios hacia los clientes como también si se presenta algún fallo, ya sea de hardware o software, se debe gestionar de manera rápida y dar una solución pronta para que no afecte en el desarrollo y así evitar atrasos en las entregas de servicios.

6) **Gestión de calidad:** Este proceso levanta información, evalúa y realiza los diagramas de flujos y procedimientos de cada proceso o subproceso de la empresa, es por ello que se involucra con el proceso core, ya que tiene una visión general de la empresa.

7) **Prestación de servicios Telcos:** En este proceso se brindan servicios a los servicios de telecomunicaciones, garantizando la satisfacción de las necesidades y expectativas de los clientes. Inicia desde que el gestor de proyecto da el “GO” a la ejecución hasta dar por terminado el servicio. Este es el proceso core ya que obtiene ingresos, ganancias y rentabilidad por la manera que fueron vendidas; sin embargo, los sistemas, ubicación utilizados en este proceso son de la empresa contratista, excepto el recurso humano y los equipos entregados.

8) **Desarrollo de aplicaciones:** En este proceso desarrollan sistemas de uso interno como aplicaciones web y móviles. No es un proceso involucrado ya que por ahora solo se ha desarrollado un sistema de asistencia, y este no influye en el proceso core. Se está planteando a futuro desarrollar este proceso para vender productos, sistemas web y móviles, como también en agilizar los procesos internos debido a que actualmente todo es manual, pero aún no se sabe cuándo se realizará.

Las fases desarrolladas en este proyecto fueron las dos primeras, planear y hacer, las cuales detallaremos a continuación:

3.2. FASE 1: PLANEAR (PLAN)

Esta es la primera fase, en la cual se buscó establecer el SGSI, para ello se realizó el análisis de brecha con el fin de conocer la situación inicial sobre los requisitos y controles de la ISO/IEC 27001:2013 en la organización; además de las actividades y documentos necesarios, los cuales se detallan en los siguientes puntos.

3.2.1 Análisis de Brecha

Se realizaron dos análisis de brechas, uno para conocer el estado inicial del cumplimiento de los requisitos y otro para el de los controles.

3.2.1.1 Análisis de Brecha inicial de requisitos

Para este análisis de brecha se tomaron los requisitos de la ISO/IEC 27001:2013 y fueron evaluados tomando en cuenta los niveles de cumplimiento que se visualizarán en la **Tabla 3.1**

TABLA 3.1 NIVELES DE CUMPLIMIENTO DE REQUISITOS

NIVELES DE CUMPLIMIENTO DE REQUISITOS		
DESCRIPCIÓN	**NIVEL DE CUMPLIMIENTO**	**DETALLE**
NO EXISTE	0	**No existe, 0% de ocurrencia** Sin evidencias del cumplimiento del requisito.
INICIO	1	**Inicio, aproximadamente 40% de ocurrencia.** La organización ha reconocido que los problemas existen y que necesitan ser tratados. Existen indicios del cumplimiento del requisito; sin embargo, no existe una evidencia de estos.
DESARROLLO	2	**En desarrollo, aproximadamente 70% de ocurrencia** Existe un gran avance en cuanto al cumplimiento del requisito y la evidencia de este; sin embargo, no se encuentra al 100%.
COMPLETO	3	**Se completó,100% de ocurrencia** Cumplimiento y evidencia del requisito al 100%.

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En el **"Informe de Análisis de Brecha Inicial de Requisitos" (Anexo 3)** se visualizan los resultados por cada requisito de la Norma ISO/IEC 27001:2013 **(Figura 3.3)**, obtenidos en la evaluación.

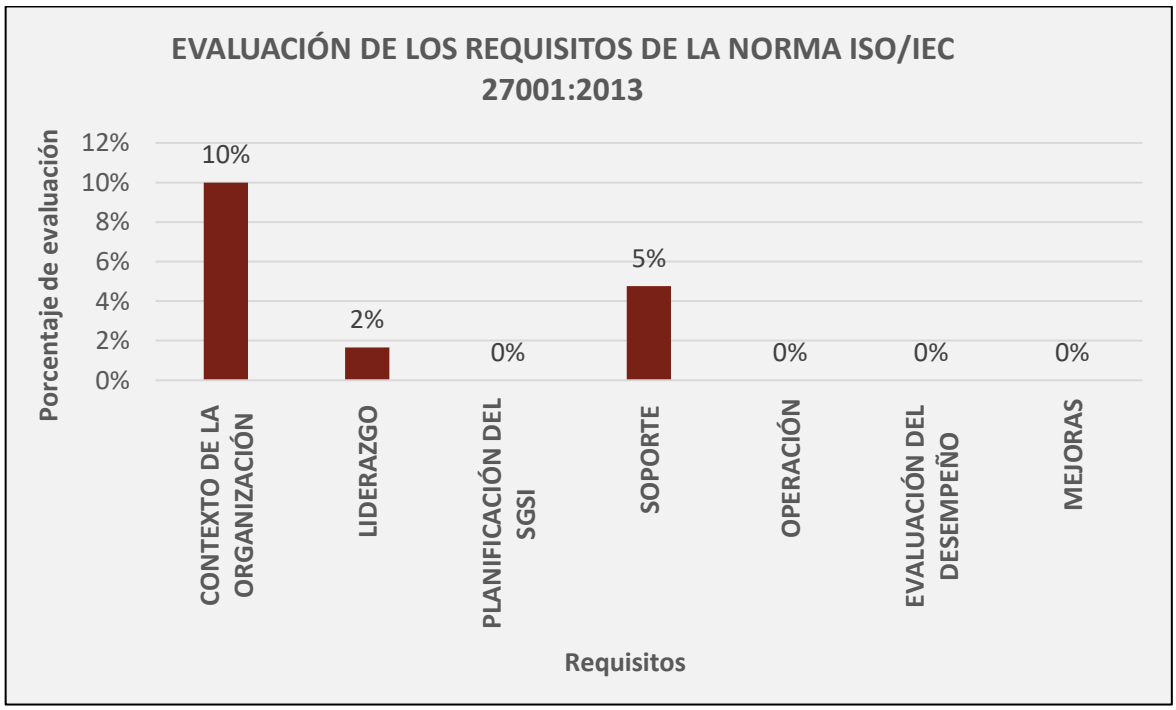


FIGURA 3.3 EVALUACIÓN DE LOS REQUISITOS DE LA NORMA ISO/IEC 27001:2013
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Después de realizar el análisis por cada requisito, se tuvo en promedio un nivel de cumplimento del **2% (Figura 3.4)**

FIGURA 3.4 NIVEL DE CUMPLIMIENTO DE REQUISITOS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.2.1.2 Análisis de Brecha inicial de controles

Se realizó el análisis de brecha de controles, ya que era importante tener una idea clara de qué controles no se encontraban implementados y cuales sí, además de conocer cuáles eran o no necesarios, por ello evaluamos la aplicabilidad de controles el detalle de esto se visualiza en la **Tabla 3.2**.

TABLA 3.2 APLICABILIDAD DE CONTROLES

¿ES NECESARIO?	DESCRIPCIÓN	DETALLE
Sí	**APLICA**	El control sí es necesario para la organización
No	**NO APLICA**	El control no es necesario para la organización.

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Para todos los controles que señalaron que sí eran necesarios, es decir aplicaban, fueron evaluados con los siguientes niveles de cumplimiento que se visualizan en la **Tabla 3.3**.

TABLA 3.3 NIVELES DE CUMPLIMIENTO DE CONTROLES

DESCRIPCIÓN	PUNTAJE	PUNTUACIÓN Porcentual	DETALLE
Completo	***4***	**100%**	El control está implementado, ha sido aprobado por la alta dirección y ha sido publicado (de ser necesario).
En proceso	***3***	**70%**	El desarrollo de control está en proceso de implementación.
Inicio	***2***	**40%**	Se ha identificado la necesidad del implementar un control. El control apenas está iniciando.
No existe	***1***	**0%**	El control está ausente, no existe.

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Al realizar la evaluación se obtuvieron estos resultados por cada control de la ISO/IEC 27002 **(Tabla 3.4)**, para visualizar de manera gráfica, **Figura 3.5.** En el **"Informe de Análisis de Brecha Inicial de Controles" (Anexo 4)**, se explica el resultado de cada control.

TABLA 3.4 PORCENTAJES DE CUMPLIMIENTO POR CONTROL

N°	DOMINIOS EVALUDOS SEGÚN ISO 27002	ANALISIS DE BRECHA INICIAL	
A.5	Políticas de seguridad de la información	**10%**	**Inicio**
A.6	Organización de la seguridad de la información	**0%**	**No existe**
A.7	Seguridad de los recursos humanos	**4%**	**Inicio**
A.8	Gestión de activos	**10%**	**Inicio**
A.9	Control de acceso	**11%**	**Inicio**
A.10	Criptografía	**-**	**No aplica**
A.11	Seguridad física y ambiental	**5%**	**Inicio**
A.12	Seguridad de las operaciones	**10%**	**Inicio**
A.13	Seguridad de las comunicaciones	**27%**	**Inicio**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	**-**	**No aplica**
A.15	Relación con los proveedores	**0%**	**No existe**
A.16	Gestión de Incidentes de seguridad de la información	**0%**	**No existe**
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	**13%**	**Inicio**
A.18	Cumplimiento	**20%**	**Inicio**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

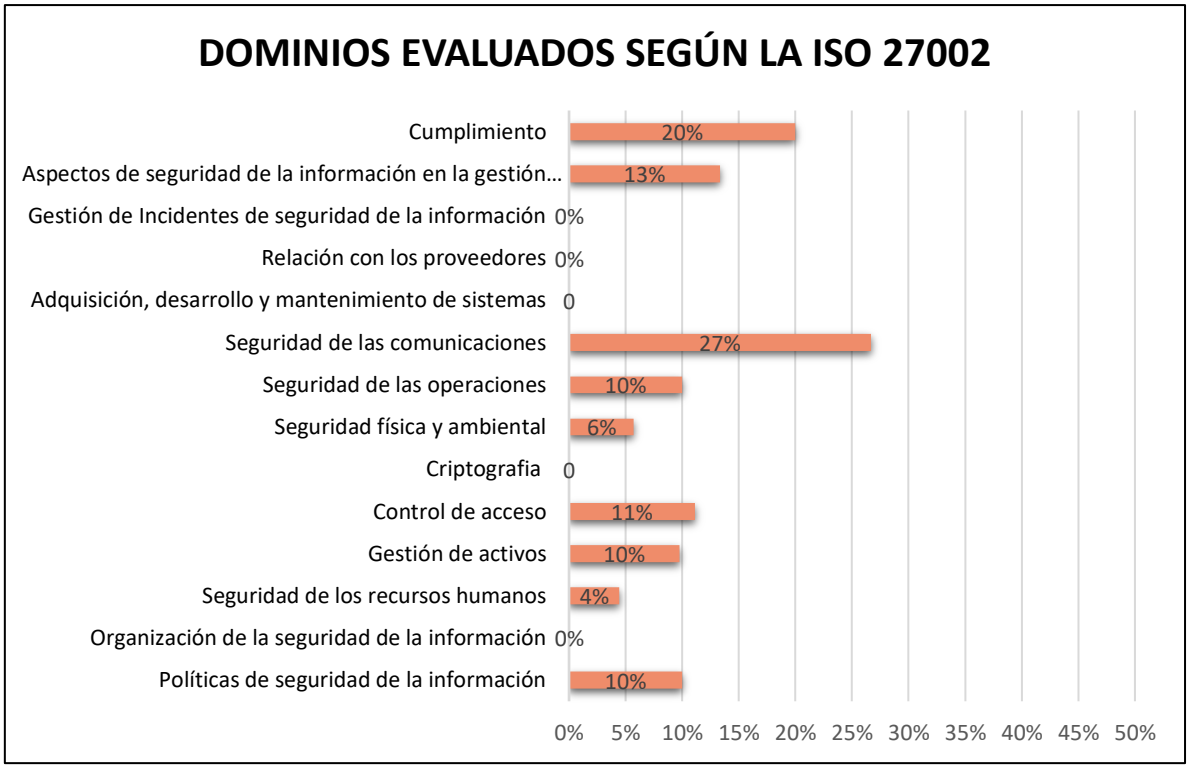


FIGURA 3.5 DOMINIOS EVALUADOS SEGÚN LA ISO 27002
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Luego de haber realizado el análisis por cada dominio de control, se tuvo en promedio un nivel de cumplimento del **9.19%** respecto a la seguridad de información de la empresa **(Figura 3.6)**.

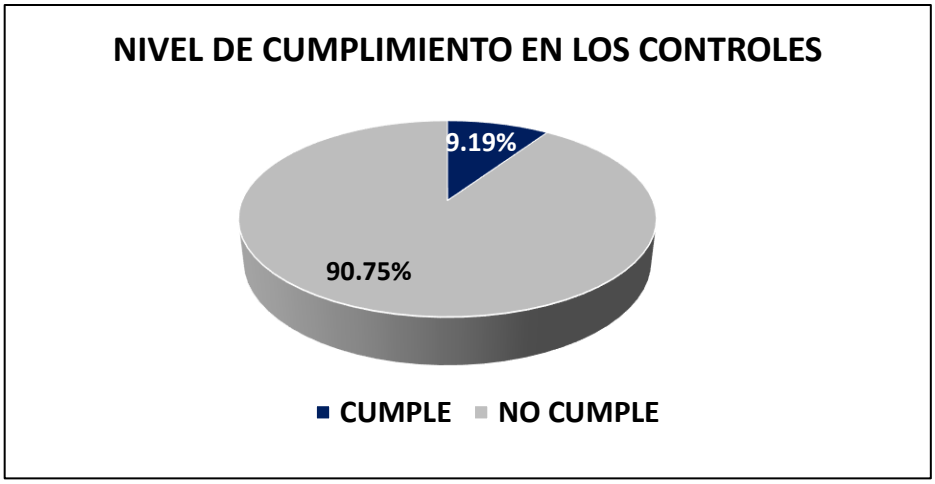


FIGURA 3.6 NIVEL DE CUMPLIMIENTO
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En la **Tabla 3.5** y **Figura 3.7**, se muestra el diagnóstico del nivel de cumplimiento de controles en la empresa.

TABLA 3.5 PORCENTAJES DE CUMPLIMIENTO DE CONTROLES

NIVELES DE MADUREZ	CUMPLIMIENTO
Completo	0%
En proceso	0%
Inicio	64.29%
No existe	21.43%
No aplica	14.29%

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

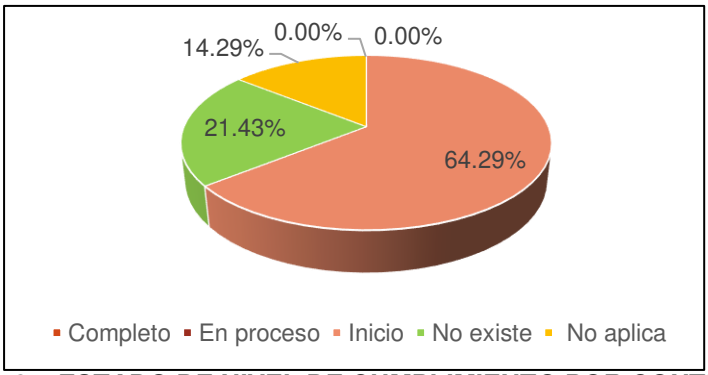


FIGURA 3.7 ESTADO DE NIVEL DE CUMPLIMIENTO POR CONTROLES
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Para obtener los resultados anteriores, se realizó una reunión con los responsables de cada área en la cual se desarrolló una **"Acta de Reunión" (Anexo 5)**. Se entiende que es una empresa que recién estaba iniciando su proceso de seguridad de información, debido a las exigencias y reglas que han empezado a surgir en el mercado.

A continuación, se mencionan los roles de los responsables que asistieron en la reunión para el desarrollo de los análisis de brechas:

- Coordinadora de Recursos Humanos y Logística
- Coordinadora de Calidad
- Jefe de proyecto/Coordinadora de Finanzas y Contabilidad
- Analista de Seguridad de Información (Externo)

En conclusión, los análisis de brecha nos han brindado información necesaria de la empresa para tener una idea de la situación actual de la empresa y así poder evaluar de forma preliminar el esfuerzo, tiempo, dinero y recursos requeridos para las dos primeras fases del SGSI.

3.2.2 Compromiso de la Alta Dirección

Se debe tener en cuenta que este es un paso fundamental para el SGSI, como ya se ha explicado anteriormente. Para ello en primera instancia se realizó la **"Propuesta Comercial" (Anexo 7)**, la cual se presentó al Gerente de Administración y Gerente General explicándoles la situación actual, basándonos en el análisis de brecha explicado en el punto anterior, y lo propuesto como mejora, incluyendo actividades, recursos, tiempo y alcance. Además, se realizó el **"Acta de Compromiso" (Anexo 6)**, la cual indica los puntos específicos a los que se comprometen para establecer, implementar, mejorar y mantener el SGSI. Luego de aprobar la propuesta, se procedió a explicar el acta de compromiso de alta dirección y a ser firmada por el Gerente General y el Gerente de Administración.

3.2.3 Contexto de la Organización

Con el objetivo de comprender el contexto de la organización, se analizaron la visión, misión y se determinaron los factores externos e internos de la organización, para esto se realizó un FODA **(Tabla 3.6).**

TABLA 3.6 FODA DE LA EMPRESA

FACTORES INTERNOS	
FORTALEZAS	**DEBILIDADES**
➢ Capacidad para incorporar, desarrollar y conservar consultores expertos. ➢ Experiencia en la implementación de sistemas de información para la industria de telecomunicaciones. ➢ Líderes comprometidos con el buen servicio que originan un 75% de clientes fidelizados. ➢ Gerentes con visión estratégica compartida. ➢ Equipo compacto y en crecimiento que aprovecha su flexibilidad, rapidez y pasión. ➢ Conocimiento especializado del core del sector de telecomunicaciones. ➢ Somos reconocidos como empresa que brinda servicio de calidad, reconocido como la empresa que tiene los mejores talentos dentro de ENTEL.	➢ Procesos internos manuales que generan eficiencia en la gestión comercial, implementación y soporte. ➢ Escasa optimización de tiempo y empleo de herramientas para actividades internas. ➢ Falta de alianzas estratégicas con proveedores locales, expertos en nichos (RRHH, digitalización, costos, finanzas) ➢ Ausencia de un plan estratégico formal. ➢ Poca gestión de conocimiento. ➢ Calidad del servicio y producto no certificada. ➢ Plan de aprendizaje y certificación poco formalizado. ➢ PMO en desarrollo. ➢ Poco acceso a herramientas de gestión de proyectos. ➢ Carencia de publicidad.

FACTORES EXTERNOS	
OPORTUNIDADES	**AMENAZAS**
➢ Posibilidad de alianzas estratégicas con empresas proveedores de servicios de clase mundial (Ericson). ➢ Crecimiento del mercado de telecomunicaciones en el Perú. ➢ Nuestro principal cliente está en crecimiento. ➢ Demanda de movilidad en los negocios vía aplicaciones de smartphones o similares. ➢ Continuidad de servicios en clientes actuales basado en la confianza. ➢ Incorporar proveedores adicionales a TMForum, Microsoft, Cloware, ZohoSoft, Softnet Perú y Nexsys. ➢ Enfocarse en oportunidades empresariales de implementación en nuevos clientes en Latinoamérica en ENTEL PERÚ, AMÉRICATEL PERÚ y WOM CHILE. ➢ Nuevas necesidades de información para las áreas comerciales de las Telcos.	➢ Mayor agresividad comercial de competidores (precio, promoción, portafolio producto). ➢ Cambio de reglas de juego desde el proveedor propietario. ➢ Líder del mercado ERICSON introduce competidores en crecimiento y con mayor número de influenciados en Perú. ➢ Entrada de empresas competidoras regionales.

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.2.4 Necesidades y expectativas de las partes interesadas

Después de comprender el contexto de la organización, el siguiente paso fue evaluar y determinar las necesidades y expectativas referentes a la seguridad de información de las partes interesadas **(Tabla 3.7)**; tales como: clientes, proveedores, personal de VF, etc.

TABLA 3.7 NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Parte Interesada		Interacción		Requerimiento	
		Contexto	Proceso con el que interacciona	Necesidad	Expectativa
Clientes	Entel WOM Americatel	Externo	Prestación de Servicios Telcos	• Cumplimiento de las cláusulas en el Acuerdo de Seguridad de la información	• Resguardar su información.

Parte Interesada		Interacción		Requerimiento	
		Contexto	Proceso con el que interacciona	Necesidad	Expectativa
Proveedores	Nexsys Xertica Amazon	Externo	Gestión logística	• Mantener Información sobre sus contratos de manera confidencial	• Recibir Información correcta y específica sobre lo que se requiere
Organismos Legales	Ministerio del Trabajo Ministerio de Justicia PCM	Externo	Gestión de Recursos Humanos	• Cumplir con la Ley de Protección de Datos Personales • Cumplir con la Ley de Delitos Informáticos	• Contar con organizaciones que estén alineadas al régimen laboral.
Recursos Humanos	Gerente de Administración Coordinadora de RR.HH.	Interno	Gestión de Recursos Humanos	• Cumplimiento de las especificaciones en el contrato y acuerdos con el personal	• Personal informado en la seguridad de la información y datos personales
Comercial	Gerente Comercial Gerente de Ventas	Interno	Gestión Comercial	• Prevenir fugas o pérdida de información sobre los clientes	• Información integra, constante y actualizada para toma de decisiones
Personal	Todo el personal de VF	Interno	Gestión de Recursos Humanos	• Contar con información disponible que permita agilizar su trabajo. • Mantener su información personal de forma confidencial.	• Recibir capacitaciones e incentivos por su cumplimiento con el SGSI.

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.2.5 Alcance del SGSI

Teniendo como base todos los puntos mencionados anteriormente, se procedió a determinar los límites del alcance del SGSI, mencionando los procesos que estarían incluidos y los que no. Además, se le comunicó al Gerente de Administración para su respectiva aprobación.

Se definió que el SGSI tendrá como alcance el proceso de “Prestación de Servicios Telcos” en las instalaciones de la sede Miraflores de la empresa VF CONSULTING S.A.C., incluyendo los procesos involucrados, según establece la norma como requisito.

Los procesos involucrados son los siguientes:

- Gestión Comercial
- Gestión de Proyectos
- Gestión de Recursos Humanos
- Gestión de Contabilidad y Finanzas
- Gestión Logística
- Gestión de Calidad

Los procesos que NO están incluidos en el alcance son:

- Desarrollo de Aplicaciones

3.2.6 Política de Seguridad de Información

Para determinar la política de seguridad de la información se tuvo en cuenta todo lo mencionado anteriormente. Este documento **“Política de Seguridad de Información” (Anexo 8)**, incluye compromisos y objetivos de seguridad de la información, de acuerdo con el sector de la organización. Además, fue aprobada por el Gerente General.

Adicional a ello, esta política fue comunicada mediante un correo, en la charla de seguridad de información, se colocó en la pared de la oficina de la empresa y está disponible en el repositorio de la empresa con acceso a todos los colaboradores de VF para que puedan consultarla cuando lo requieran.

3.2.7 Ficha de puesto

Para identificar los roles y responsabilidades en VF CONSULTING S.A.C., detallamos su estructura en el **“Organigrama Funcional” (Figura 3.8)**, el cual fue comunicado a la organización en la Charla de Seguridad de Información.

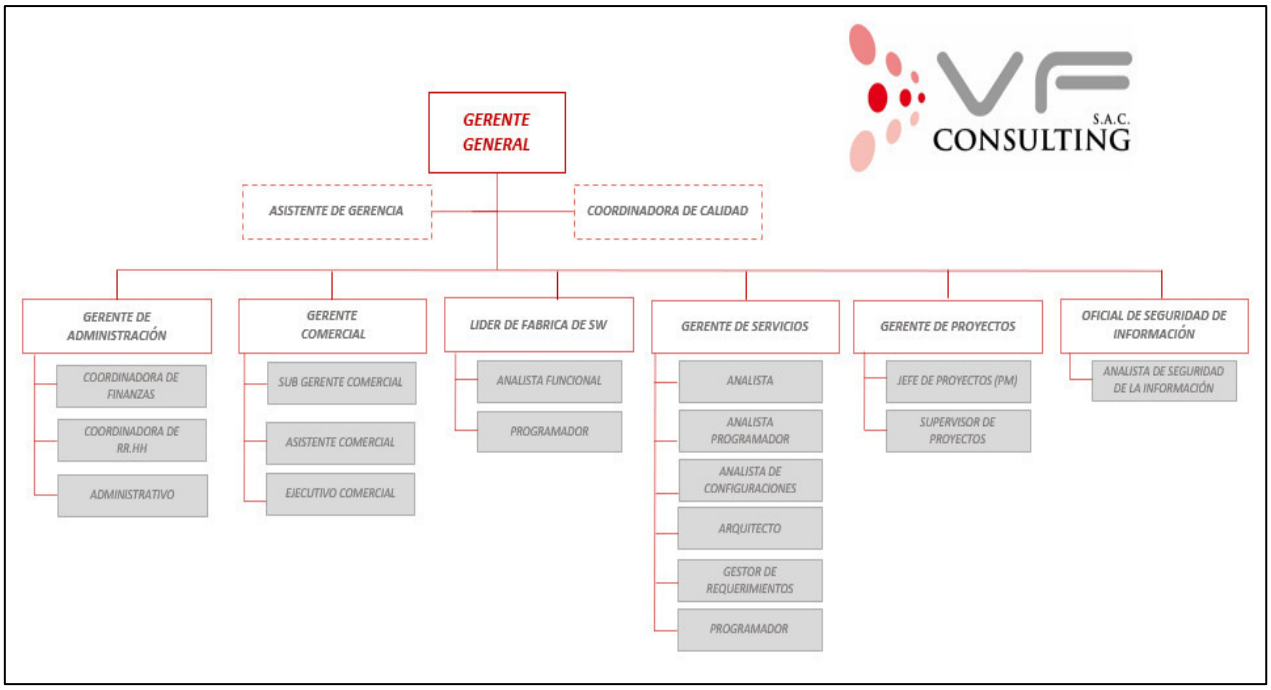


FIGURA 3.8 ORGANIGRAMA FUNCIONAL
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Se tiene definida la **"Ficha de Puesto" (Anexo 9)**, del Oficial de Seguridad de la información y Analista de Seguridad de la información, donde se detallan las funciones y responsabilidades, estos son comunicados por la Coordinadora de RR.HH. y subidos al repositorio de la empresa.

Previamente a la comunicación en general a la organización, se revisó la aprobación del Gerente de Administración.

3.2.8 Procedimiento de Control de Información Documentada

A lo largo de la implementación se requiere de información documentada como evidencia, debido a esto se creó el **"Procedimiento de Control de Información Documentada" (Anexo 10),** el cual especifica los pasos a seguir para controlar la información documentada que es creada o actualizada. Anteriormente, no tenían un procedimiento para esto, y debido a este nuevo procedimiento se está implementando también fuera del SGSI, es decir en toda la documentación de la empresa. En este caso se requirió la aprobación del procedimiento al Gerente de Administración.

3.2.9 Procedimiento de Gestión de Riesgos

Se realizó un **"Procedimiento de Gestión de Riesgos" (Anexo 11)**, para conocer los pasos obtener el inventario de activos, evaluación de riesgos, el plan de tratamiento y el informe de gestión de riesgos, los cuales detallaremos más adelante. Este procedimiento fue comunicado a los responsables de los procesos, en la capacitación de seguridad de información, tomados en el alcance y requirió la aprobación del Gerente de Administración.

3.2.10 Procedimiento de Gestión de Incidentes

El **"Procedimiento de Gestión de Incidentes" (Anexo 12),** fue creado para los colaboradores de VF, en este procedimiento indica qué hacer al identificar una incidencia, por esto se les informó y explicó el procedimiento en la charla de seguridad de información. Además, se les envió por correo la ruta del procedimiento subido al repositorio de la empresa. También requirió aprobación del Gerente de Administración.

3.2.11 Procedimiento de Auditoria Interna

Se ha establecido el **"Procedimiento de Auditoria Interna" (Anexo 13),** en el cual se indican los pasos a seguir para verificar que el SGSI se encuentre conforme con los requisitos de la normativa ISO/IEC 27001:2013. Este documento también requirió la aprobación del Gerente de Administración.

3.2.12 Gestión de Riesgos

3.2.12.1 Metodología de Gestión de Riesgos

La **"Metodología de Gestión de Riesgos" (Anexo 14),** ha desarrollado los pasos del cómo asegurar el control de los riesgos de seguridad de la información llevándolos a niveles aceptables.

3.2.12.2 Inventario de Activos de Información

Una vez que se tiene la metodología de riesgos, se procede a realizar el inventario de activos de información. Inicialmente, la empresa no contaba con ningún inventario, para eso se realizó una encuesta al personal de todas las áreas identificando los activos para luego registrarlos en la **"Lista de Activos de**

Información" (Anexo 15). Luego se valorizaron todos los activos **(Anexo 16)**, de los cuales nos quedamos con todos los de impacto ALTO y dos activos de impacto MEDIO **(Tabla 3.8).**

TABLA 3.8 ACTIVOS DE INFORMACIÓN DE GRAN IMPACTO

ÁMBITO	CATEGORÍA	ID	ACTIVO	CRITERIOS			TOTAL	IMPACTO
				C	I	D		
DATOS	[D] Datos	[D-001]	Datos del personal	7	7	8	7	A
		[D-002]	Control de salarios	10	9	9	9	A
		[D-013]	Registros de órdenes de compras y facturas	7	10	8	8	A
		[D-020]	Formato de gestión de oportunidades	9	7	7	8	A
		[D-021]	Propuesta técnica y económica	9	10	7	9	A
		[D-022]	Reporte de actas de aceptación	9	6	7	7	A
		[D-023]	Diseño técnico detallado	7	8	7	7	A
		[D-024]	Reporte de acceso de usuarios VPN	8	9	9	9	A
		[D-026]	Reporte de estatus de proyectos	6	8	8	7	A
		[D-028]	Control de procedimiento	4	9	6		M
		[D-031]	Control de políticas	3	8	10	7	A
SERVICIOS	[S] Servicios	[S-001]	Internet	4	7	9	7	M
		[S-002]	Correo electrónico	7	6	7	7	M
		[S-003]	Repositorio de versionamiento	8	10	9	9	A
SOFTWARE	[SW] Software	[SW-002]	Lista de instaladores de software	7	9	10	9	A
HARDWARE	[HW] Hardware	[HW-003]	Laptops de desarrollo	9	9	10	9	A
MEDIA	[M] Media	[M-002]	Documentación técnica	7	9	10	9	A
INSTALACIÓN	[I] Instalaciones	[I-001]	Oficina Miraflores	8	6	9	8	A

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Una vez valorizados los activos, se procedió a realizar un diagrama de flujo **(Figura 3.9),** para comprobar que los activos de información que resultaron impacto ALTO tienen más relación e importancia con el proceso "Prestación de servicios Telcos" y así poder evaluarlos correctamente

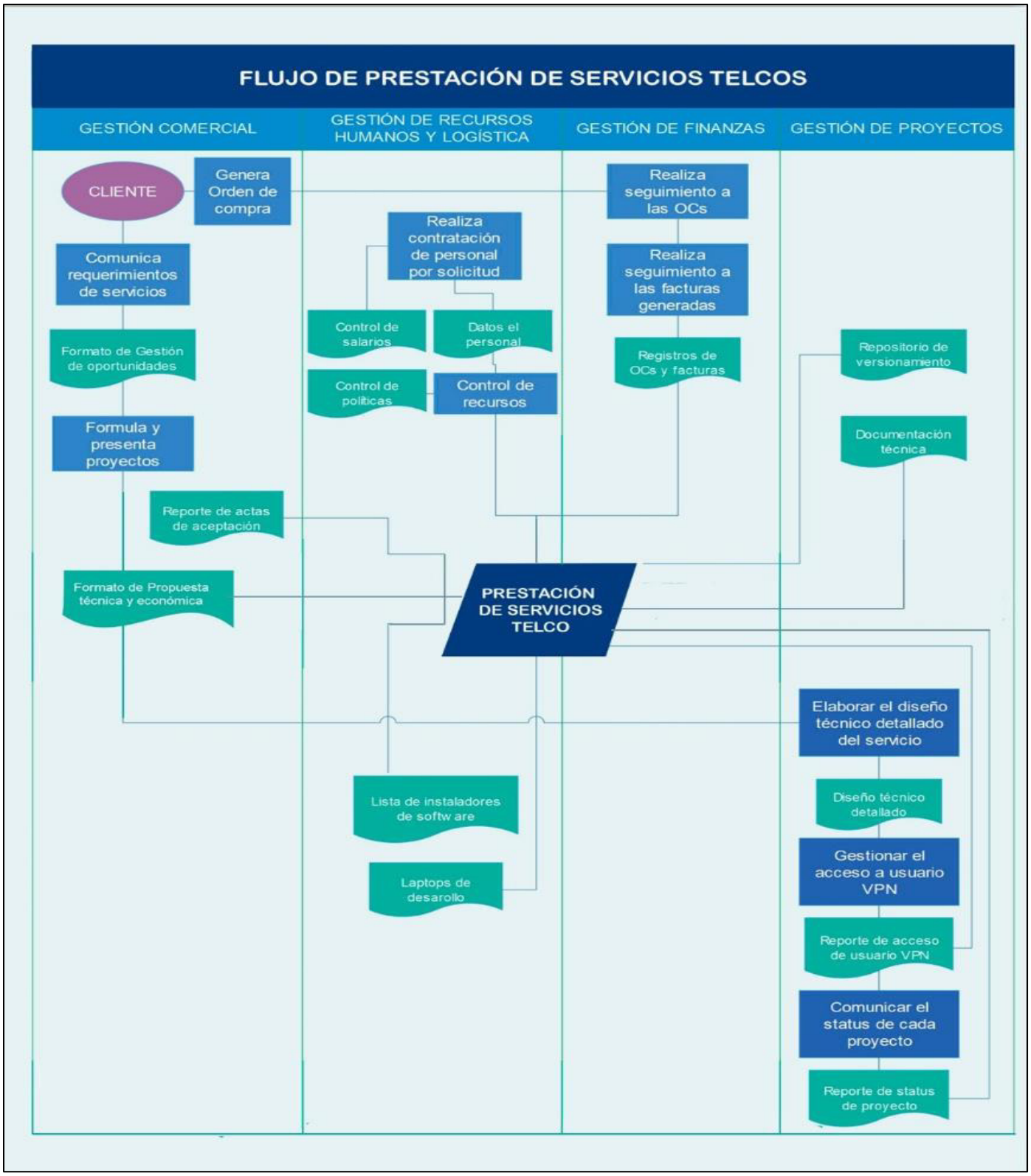


FIGURA 3.9 DIAGRAMA DE FLUJO DE PRESTACIÓN DE SERVICIOS TELCOS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.2.12.3 Evaluación de Riesgos

Luego de tener el Inventario de Activos de Información, se procede a la **"Evaluación de Riesgos" (Anexo 17)**, el cual evalúa el impacto de las amenazas y la probabilidad de ocurrencia, obteniendo el riesgo al multiplicar ambos, además de la zona de riesgos que indica cuáles de los activos son de extremo a bajo riesgo. Esto nos ayuda a ver que controles debemos aplicar y tener en consideración para asumir, evitar, reducir o transferir dicho riesgo.

Estos son los activos de mayor impacto de riesgos **(Tabla 3.9).**

TABLA 3.9 EVALUACIÓN DE RIESGOS

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN RECURSOS HUMANOS	Control de salarios	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT063	ALTO	3	PROBABLE	3	9	E
		ALT007	ALTO	3	IMPROBABLE	2	6	A
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	CASI SEGURO	4	12	E
		MOD001	MEDIO	2	IMPROBABLE	2	4	M
	Control de salarios	EXT016	ALTO	3	PROBABLE	3	9	E
		ALT011	MEDIO	2	PROBABLE	3	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	MEDIO	2	IMPROBABLE	2	4	M
	Correo electrónico	ALT002	MEDIO	2	PROBABLE	3	6	A
		ALT015	MEDIO	2	PROBABLE	3	6	A
		ALT016	ALTO	3	IMPROBABLE	2	6	A
		ALT020	ALTO	3	IMPROBABLE	2	6	A
		ALT021	MEDIO	2	PROBABLE	3	6	A
		ALT027	MEDIO	2	PROBABLE	3	6	A
	Datos del personal	ALT006	MEDIO	2	PROBABLE	3	6	A
		ALT011	MEDIO	2	PROBABLE	3	6	A
		ALT015	MEDIO	2	CASI SEGURO	4	6	A
		ALT029	MEDIO	2	PROBABLE	3	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	BAJO	1	PROBABLE	3	3	M
		MOD021	BAJO	1	PROBABLE	3	3	M
		BAJ001	MEDIO	2	RARO	1	2	B
	Control de políticas	ALT011	ALTO	3	IMPROBABLE	2	6	A
		ALT015	ALTO	3	IMPROBABLE	2	6	A
		ALT030	ALTO	3	IMPROBABLE	2	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD014	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	MEDIO	2	RARO	1	2	B

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN DE CALIDAD	Control de procedimiento	EXT001	ALTO	3	CASI SEGURO	4	12	E
		EXT047	ALTO	3	PROBABLE	3	9	E
		ALT011	MEDIO	2	PROBABLE	3	6	A
		ALT015	MEDIO	2	PROBABLE	3	6	A
		ALT031	MEDIO	2	PROBABLE	3	9	A
		BAJ001	BAJO	1	IMPROBABLE	2	2	B
	Persona	EXT002	ALTO	3	CASI SEGURO	4	12	E
		EXT015	ALTO	3	PROBABLE	3	9	E
	Toda la documentación información	ALT035	MEDIO	2	PROBABLE	3	6	A
	Oficina de Miraflores	MOD015	MEDIO	2	IMPROBABLE	2	4	M
GESTIÓN COMERCIAL	Formato de gestión de oportunidades	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT010	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT027	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	CASI SEGURO	4	12	E
		EXT052	ALTO	3	PROBABLE	3	9	E
		EXT058	ALTO	3	PROBABLE	3	9	E
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	PROBABLE	3	9	E
	Propuesta técnica y económica	EXT005	ALTO	3	PROBABLE	3	9	E
		EXT011	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT027	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT052	ALTO	3	CASI SEGURO	4	12	E
		EXT057	ALTO	3	PROBABLE	3	9	E
		EXT059	ALTO	3	PROBABLE	3	9	E
		ALT028	ALTO	3	IMPROBABLE	2	6	A
	Reporte de actas de aceptación	MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD003	MEDIO	2	IMPROBABLE	2	4	M
		MOD004	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	BAJO	1	CASI SEGURO	4	4	M
		MOD009	BAJO	1	CASI SEGURO	4	4	M
		MOD010	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	BAJO	1	IMPROBABLE	2	2	B
	Registro de gestión de oportunidades	ALT033	ALTO	3	IMPROBABLE	2	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN DE PROYECTOS	Diseño técnico detallado	EXT001	ALTO	3	CASI SEGURO	4	12	E
		EXT012	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		ALT002	MEDIO	2	PROBABLE	3	6	A
		ALT013	MEDIO	2	CASI SEGURO	4	8	A
		ALT024	MEDIO	2	PROBABLE	3	6	A
		ALT034	MEDIO	2	CASI SEGURO	4	8	A
		MOD005	MEDIO	2	IMPROBABLE	2	4	M
		MOD018	MEDIO	2	IMPROBABLE	2	4	M
	Reporte de acceso de usuarios VPN/Token	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT013	ALTO	3	CASI SEGURO	4	12	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT018	ALTO	3	PROBABLE	3	9	E
		EXT019	ALTO	3	CASI SEGURO	4	12	E
		EXT028	ALTO	3	CASI SEGURO	4	12	E
		EXT029	ALTO	3	PROBABLE	3	9	E
		EXT032	ALTO	3	CASI SEGURO	4	12	E
		EXT053	ALTO	3	CASI SEGURO	4	12	E
		EXT058	ALTO	3	CASI SEGURO	4	12	E
		ALT009	ALTO	3	IMPROBABLE	2	6	A
		ALT011	MEDIO	2	CASI SEGURO	4	8	A
		ALT025	ALTO	3	PROBABLE	3	9	E
	Persona	EXT002	ALTO	3	CASI SEGURO	4	12	E
		EXT015	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	CASI SEGURO	4	12	E
	Reporte de estatus de proyectos	EXT001	ALTO	3	PROBABLE	3	9	E
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD006	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	MEDIO	2	IMPROBABLE	2	4	M
		MOD012	BAJO	1	CASI SEGURO	4	4	M
		MOD019	BAJO	1	PROBABLE	3	3	M
GESTIÓN DE FINANZAS	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	PROBABLE	3	9	E
	Registros de órdenes de compras y facturas	ALT002	ALTO	3	MEDIO	2	6	A
		ALT008	ALTO	3	MEDIO	2	6	A
		ALT013	ALTO	3	MEDIO	2	6	A
		ALT014	ALTO	3	MEDIO	2	6	A
		ALT015	MEDIO	2	PROBABLE	3	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
PRESTACIÓN DE SERVICIOS TELCOS Y LOGÍTISCA	Lista de instaladores de software	EXT001	ALTO	3	PROBABLE	3	9	E
		ALT001	MEDIO	2	PROBABLE	3	6	A
		ALT012	MEDIO	2	CASI SEGURO	4	8	A
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	CASI SEGURO	4	12	E
	Laptops de desarrollo	EXT022	ALTO	3	CASI SEGURO	3	9	E
		EXT054	ALTO	3	PROBABLE	3	9	E
		ALT001	ALTO	2	IMPROBABLE	2	6	A
		ALT004	ALTO	2	IMPROBABLE	2	6	A
		ALT012	ALTO	2	IMPROBABLE	2	6	A
		ALT017	ALTO	2	IMPROBABLE	2	6	A
	Oficina de Miraflores	EXT003	ALTO	3	CASI SEGURO	4	12	E
		EXT004	ALTO	3	PROBABLE	3	9	E
PRESTACIÓN DE SERVICOS TELCOS	Repositorio de versionamiento	EXT001	ALTO	3	CASI SEGURO	4	12	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT031	ALTO	3	CASI SEGURO	4	12	E
		ALT010	ALTO	3	IMPROBABLE	2	6	A
		ALT026	MEDIO	2	CASI SEGURO	4	8	A
		MOD007	MEDIO	2	PROBABLE	2	4	M
		MOD013	MEDIO	2	PROBABLE	2	4	M
		MOD020	BAJO	1	PROBABLE	3	3	M
	Documentación técnica	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT014	ALTO	3	PROBABLE	3	9	E
		EXT027	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT052	ALTO	3	PROBABLE	3	9	E
		EXT060	ALTO	3	PROBABLE	3	9	E
		ALT011	MEDIO	2	CASI SEGURO	4	8	A
		ALT019	MEDIO	2	PROBABLE	3	6	A
		MOD008	ALTO	3	PROBABLE	3	9	M
		BAJ002	BAJO	3	IMPROBABLE	2	2	B
	Persona	EXT002	ALTO	3	CASI SEGURO	4	12	E
	Laptops de desarrollo	EXT006	ALTO	3	PROBABLE	3	9	E
		EXT007	ALTO	3	PROBABLE	3	9	E
		EXT008	ALTO	3	PROBABLE	3	9	E
		EXT009	ALTO	3	CASI SEGURO	4	12	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT030	ALTO	3	PROBABLE	3	9	E
		EXT046	ALTO	3	CASI SEGURO	4	12	E
		ALT001	ALTO	3	IMPROBABLE	2	6	A
		ALT005	MEDIO	2	CASI SEGURO	4	8	A
	Lista de instaladores	ALT011	ALTO	3	IMPROBABLE	2	6	A
TODOS LOS PROCESOS	Oficina Miraflores	EXT003	ALTO	3	PROBABLE	3	9	E
		EXT037	ALTO	3	PROBABLE	3	9	E
		EXT056	ALTO	3	PROBABLE	3	9	E
		ALT001	ALTO	3	IMPROBABLE	2	6	A
		ALT018	ALTO	3	IMPROBABLE	2	6	A
		MOD015	ALTO	3	RARO	1	3	M

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.2.11.4 Plan de Tratamiento de Riesgos

Una vez de haber definidos los criterios de aceptación de riesgos, se procede a realizar el **"Plan de Tratamiento de Riesgos" (Anexo 18),** es el paso en el que se tiene que moverse de la teoría a la práctica, mostrar resultados de todo lo planteado en ese plan. Para eso se define quién es el responsable de implementar cada control, cuándo y que plan de acción se tomará en cuenta para el cumplimiento. Además, este documento debe tener la aprobación de la alta dirección, ya que llevará mucho tiempo y esfuerzo dependiendo de la dificultad de aplicar dicho control y sin su compromiso no obtendrá los recursos necesarios.

3.2.13 Declaración de Aplicabilidad

En esta actividad de la **"Declaración de aplicabilidad" (Anexo 19)** se enumera los objetivos de control y controles listados en el **Anexo 1,** que están alineados con la norma **ISO/IEC 27002,** para saber cuáles controles son o no aplicables para la empresa y sobre todo evaluar las respectivas justificaciones de elección.

3.2.14 Matriz de Comunicación Interna y Externa

La comunicación interna y externa se detalla en la **Tabla 3.10**, describe qué comunicar, cuándo comunicar, a quién comunicar, quien debe comunicar y el medio por el cual la comunicación debe ser efectuada referente al SGSI.

TABLA 3.10 MATRIZ DE COMUNICACIÓN INTERNA Y EXTERNA

N°	¿Qué se debe comunicar?	¿Cuándo Comunicar?	¿Quién debe comunicar?	¿A quién comunicar?	Tipo	Registro	Proceso de Comunicación
1	Política de Seguridad de la información (Incluye objetivos de seguridad de la información)	Cuando se actualiza y aprueba la Política de Seguridad de la información	Oficial de Seguridad de la Información	Todo el personal de VF Proveedores.	Externa	Correo electrónico institucional Ruta de documentos	Comunicación de la Política de seguridad de la información, a través del correo electrónico institucional y en la ruta de documentos (Drive).

N°	¿Qué se debe comunicar?	¿Cuándo Comunicar?	¿Quién debe comunicar?	¿A quién comunicar?	Tipo	Registro	Proceso de Comunicación
2	Organización de la Seguridad de la información (Roles y Responsabilidades) MOF	Cuando se actualiza y aprueba los Roles y Responsabilidades del SGSI	Coordinadora de Calidad	Todo el personal de VF Oficial de Seguridad de la información	Interna	Correo electrónico institucional Ruta de documentos	Comunicación de la Organización de Seguridad de la Información, a través del correo electrónico institucional y en la ruta de documentos (Drive).
3	Manual del SGSI	Cuando se actualiza y aprueba el Manual del SGSI	Oficial de Seguridad de la información	Responsables de cada área Analista de Seguridad de la información	Interna	Correo electrónico institucional Ruta de documentos	Difusión del Manual del SGSI, a través del correo electrónico institucional y en la ruta de documentos.
4	Plan de capacitación y concientización en Seguridad de la información	Semestral	Oficial de Seguridad de la información	Todos los colaboradores del proceso de prestación de servicios Telcos y los procesos involucrados.	Interna	Correo electrónico institucional	Comunicación del plan de capacitación y concientización a través de un correo electrónico.
5	Informe del estado de la Implementación de los controles de Seguridad de la información.	Mensual	Oficial de Seguridad de la información	Responsables de cada área	Interna	Acta de reunión	Reporte del estado de implementación de controles, a través de una reunión.
6	Informe de la revisión del SGSI por la dirección	Bimestral	Oficial de Seguridad de la información	Alta dirección	Interna	Acta de reunión	Reporte del informe de revisión del SGSI a través de una reunión con la alta dirección.
7	Informe de la gestión de incidentes de seguridad de información	Bimestral	Oficial de Seguridad de la información	Alta dirección Todos los colaboradores	Interna	Correo electrónico institucional Ruta de documentos (Drive)	Comunicación del estado de incidentes de seguridad de la información, en las reuniones. Difusión del informe del estado de incidentes de seguridad de la información a través del correo electrónico institucional.

N°	¿Qué se debe comunicar?	¿Cuándo Comunicar?	¿Quién debe comunicar?	¿A quién comunicar?	Tipo	Registro	Proceso de Comunicación
8	Informe de resultados de las auditorías Internas del SGSI	De acuerdo con el Programa de Auditorías Internas	Oficial de Seguridad de la Información	Alta Dirección	Interna	Acta de reunión Correo electrónico	Comunicación de los resultados de las auditorías internas del SGSI, en una reunión. Difusión del informe de resultados de las auditorías internas del SGSI, a través del correo electrónico institucional.
9	Informe de las acciones correctivas y de mejora	Después de las auditorias	Oficial de Seguridad de la Información	Alta Dirección Responsable cada área	Interna	Acta de reunión Correo electrónico	Comunicar el reporte de acciones correctivas y de mejora en una reunión. Difusión del informe del estado de las solicitudes de acción correctivas y de mejora, a través del correo electrónico institucional.
10	Resultados de la auditoría de certificación del SGSI	De acuerdo con lo programado	Oficial de Seguridad de la Información	Alta Dirección	Interna	Acta de reunión Correo electrónico	Comunicación de los resultados de la auditoría de certificación del SGSI, en una reunión. Difusión del informe de resultados de la auditoría de certificación del SGSI, a través del correo electrónico institucional.

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.2.15 Plan de Concientización y Capacitación

La toma de conciencia del personal es una actividad de difusión importante y constante, para ello se realizaron actividades tales como: charla y campaña de seguridad de información. Además, se realizó una capacitación en seguridad de información, todas estas actividades se encuentran detalladas en el **"Plan de concientización y capacitación" (Anexo 20),** resultado se obtuvo que la mayoría del personal en VF CONSULTING S.A.C. es consciente de:

- La importancia de la seguridad de información para la organización.
- Su contribución a la efectividad del SGSI incluyendo los beneficios de un mejor desempeño de seguridad de la información.
- Procedimientos, formatos y registros establecidos para la implementación del SGSI.
- La política de seguridad de la información.

3.3 FASE 2: HACER (DO)

En esta fase se implementaron los planes establecidos en la primera fase, es decir el plan de tratamiento de riesgos y el de capacitación y concientización. Además, se realizó la documentación necesaria para dejar evidencias de ello.

3.3.1 Implementación del Plan de Tratamiento de Riesgos

Para la implementación del Plan de tratamiento de riesgos se aplicaron las siguientes medidas de seguridad. Solo los controles pertenecientes al "Grupo 1" se llegaron a implementar mientras que el "Grupo 2" no, debido a que involucra un mayor presupuesto para realizarse; sin embargo, se elaboró un **"Plan de implementación de medidas de seguridad" (Anexo 24)** como guía para el futuro desarrollo del "Grupo 2". Además, en el **Anexo 25** se encuentran los documentos que se han actualizado y aprobado por las áreas encargadas.

En la **Tabla 3.11** se muestra el plan de acción tomado para cada control de seguridad de la información identificado como necesario:

TABLA 3.11 MÉDIDAS DE SEGURIDAD PARA LA APLICABILIDAD DE LOS CONTROLES

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Memorándum (llamada de atención)	Documento en la cual se comunicará al personal la actualización obligatoria de su información, así mismo este documento servirá como una llamada de atención a aquel personal que infringe este control.	6.1.1 7.2.3 9.1.2	- Control de salarios - Control de procedimiento - Formato de gestión de oportunidades - Diseño técnico detallado - Reporte de acceso de usuarios VPN/ Token - Reporte de estatus de proyectos - Lista de instaladores de software - Repositorio de versionamiento - Documentación técnica - Persona	1
Aviso de actualización de datos por vía correo	Enviar un correo masivo indicando o haciendo recordar que deben actualizar los datos o subir a la carpeta drive compartida de su área correspondiente. A demás recordarles que deben hacer copias de respaldos a los equipos.	6.1.1 7.2.2 7.3.1 9.2.5 12.3.1	- Control de salarios - Control de procedimiento - Propuesta técnica y económica - Formato de gestión de oportunidades - Diseño técnico detallado - Reporte de acceso de usuarios VPN/ Token - Reporte de estatus de proyectos - Lista de instaladores de software - Repositorio de versionamiento - Documentación técnica - Laptops de desarrollo	1
Organigrama de puestos	Identificar cuáles son los responsables de cada área para segregar tareas para evitar el uso incorrecto de los activos.	6.1.2	- Persona	1
Ficha de puestos	Buscar a personas con conocimiento en seguridad de la información en caso de que no segregar la tarea de registrar, actualizar y evitar el mal uso de activos.	6.1.2	- Persona	1
Proveedores de instalación de medidas de seguridad para oficinas.	Contar con una empresa externa que se encargue en la protección de incendios y además de asesoramiento al personal para que pueda desenvolverse adecuadamente ante un aviso de incendio.	6.1.3	- Oficina de Miraflores	2

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)	Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros.	6.1.3 11.1.4 17.1.2 17.1.3	- Oficina de Miraflores - Laptops de desarrollo	2
Procedimiento de propuestas	Agregar en términos y condiciones de las propuestas que la información brindada en las propuestas como el alcance, tiempo y costo sea confidencial y no divulgada con usuarios no autorizados tanto para la consultora y el cliente.	6.1.5 6.2.1	- Propuesta técnica y económica	1
El acuerdo de confidencialidad de la seguridad de la información	Cláusula que señale el uso correcto de la información expuesta en el correo institucional de los colaboradores para evitar fugas de información, accesos no autorizados. Cláusula que señale el uso correcto de la información de brindados al personal al inicio y durante su contratación, incluye la política de seguridad de la información de la empresa y los métodos de trabajo apropiados. Cláusula que señale el uso correcto de los usuarios de VPN y que sanciones aquel personal que infringe este acuerdo. Cláusula que señale el uso correcto de la información de datos del personal para evitar fugas de talentos. Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos.	6.1.5 6.2.1 7.1.1 7.1.2 7.2.1 7.2.3 9.2.2 9.2.4 9.3.1 13.2.2 13.2.4	- Propuesta técnica y económica - Formato de gestión de oportunidades - Propuesta técnica y económica - Diseño técnico detallado - Reporte de acceso de usuarios VPN/ Token - Documentación técnica - Persona - Laptops de desarrollo - Registro de órdenes de compras - Correo electrónico - Datos del personal - Control de salarios - Repositorio de versionamiento - Reportes de actas de aceptación - Reporte de estatus de proyectos	1

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Política de seguridad de correo electrónico	Política para el uso correcto del correo electrónico, recalcando que la información es confidencial y no se debe usar para fines propios.	6.1.5 6.2.1 9.1.1 9.2.1 13.2.3	- Propuesta técnica y económica - Datos del personal - Control de políticas - Control de procedimientos - Registros de órdenes de compras y facturas - Lista de instaladores de software - Correo electrónico	1
Política de teletrabajo y penalidades	Política para los colaboradores que trabajan en remoto o cuando se llevan las laptops para realizar actividades desde a fuera de la oficina.	6.2.2 8.1.4 11.2.5 11.2.6	- Laptops de desarrollo	1
Formato de entrega de equipos	Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo.	6.2.2 11.2.4 11.2.7	- Laptops de desarrollo	1
Contratar una empresa aseguradora (Póliza de equipos)	Contar con una empresa aseguradora que permita proteger los equipos electrónicos (computadoras, laptops, etc.) contra robos, vandalismo o daños internos.	6.2.2 8.3.1 17.1.2 17.1.3	- Laptops de desarrollo - Oficina de Miraflores	2
Lista de contacto de autoridades	Lista en la cual se encuentran las autoridades pertinentes a contactar de presentarse un incidente mayor.	6.1.3	- Oficina de Miraflores	2
Lista de contacto con grupos de interés en seguridad de la información	Lista en la cual se encuentran los grupos de interés pertinentes a contactar de presentarse alguna inquietud respecto a la seguridad de la información en la empresa.	6.1.4	- Persona	2
Política de uso, manejo de información confidencial y pérdida de información VF	Definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación.	7.1.2	- Formato de gestión de oportunidades - Propuesta técnica y económica - Diseño técnico detallado - Reporte de acceso de usuarios VPN/ Token - Documentación técnica	1
Política de proveedores	Política basada en establecer condiciones necesarias en caso de acceso a la información de la empresa por los proveedores.	7.2.1 15.1.1 15.1.2 15.1.3	- Persona - Laptops de desarrollo	1

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Plan de capacitación y concientización	Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros.	7.2.2 8.1.3 9.1.1 11.2.8 11.2.9	- Persona - Control de salarios - Formato de gestión de oportunidades - Propuesta técnica y económica - Diseño técnico detallado - Reporte de acceso de usuario VPN/Token - Laptops de desarrollo - Repositorio - Documentación técnica - Control de procedimiento - Registro de órdenes de compras y facturas - Lista de instaladores de softwares - Datos del personal - Reporte de estatus de proyectos	1
Política de seguridad de la información	Política en que todo colaborador debe saber los objetivos planteados que se deben cumplir de acuerdo a la confidencialidad, integridad y disponibilidad de la seguridad de la información.	7.2.2	- Control de salarios - Formato de gestión de oportunidades - Propuesta técnica y económica - Diseño técnico detallado - Reporte de acceso de usuario VPN/Token - Laptops de desarrollo - Repositorio - Lista de instaladores de software	1
Árbol de carpeta para el acceso a usuarios	Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	7.2.2 9.1.1 9.2.1 9.2.5	- Control de salarios - Formato de gestión de oportunidades - Propuesta técnica y económica - Diseño técnico detallado - Reporte de acceso de usuario VPN/Token - Laptops de desarrollo - Repositorio de versionamiento - Documentación técnica - Lista de instaladores de software - Registro de órdenes de compras y facturas - Reporte de actas de aceptación - Reporte de estatus de proyectos	1

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Tipos de sanciones de acuerdo a la seguridad de la información	Contar con tipos de sanciones en reglamento interno que infringe la seguridad de la información de la empresa y así tomar decisiones correctas al momento de aplicarlas.	7.2.3 18.2.1	- Persona	1
Comunicado de terminación y cambio de empleo	Comunicar a todo el personal tanto a gerentes y colaboradores la terminación de un contrato de un personal para que estén informados y actualizados.	7.3.1	- Reporte de acceso de usuario VPN/Token	1
Inventariado de activos	Inventariar los activos más relevantes en su ciclo de vida y documentar su importancia, además debe ser preciso y en constante actualización. A demás, todo activo debe tener su propio propietario que aseguren que los activos estén bien clasificados, que se deben revisar en un determinado tiempo y tener en cuenta las políticas aplicable de control acceso.	8.1.1 8.1.2 12.6.1	- Reporte de acceso de usuario VPN/Token - Laptops de desarrollo	1
Clasificación y valorización de activos de información	Se debe valorizar los activos de acuerdo a los tres criterios: confidencialidad, integridad y disponibilidad, además la clasificación y valorización se deben actualizar cuando cambie su valor a lo largo de su ciclo de vida.	8.2.1 12.6.1	- Todos los activos mencionados	1
Etiquetado de información	Se debe etiquetar los activos dependiendo de su alto impacto hacia la empresa, una vez identificado, se debe realizar procedimientos de desarrollo e implementar de acuerdo al impacto.	8.2.2 8.2.3	- Todos los activos mencionados	1
Agregar el procedimiento de entrega de activos en el proceso de desvinculación del personal	En el proceso de desvinculación del personal se debe agregar el procedimiento en donde el personal debe retornar todos los activos de la consultora ya sea por contrato o acuerdo.	8.1.4	- Laptops de desarrollo	1

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Procedimiento de destrucción o eliminación de documentos	Contar con procedimientos que permitan eliminar de forma segura de los documentos que contienen información que ya no sean necesarios para así evitar fugas de información de usuarios no autorizados.	8.3.2	- Formato de gestión de oportunidades - Propuesta técnica y económica - Documentación técnica - Datos del personal - Control de salarios - Reporte de actas de aceptación - Reporte de estatus de proyectos	1
Política de control de acceso	Contar con una política en donde indique cuales son los responsables que deben tener acceso a las carpetas del drive y que información pueden acceder.	9.1.1 9.2.3	- Control de salarios - Formato de gestión de oportunidades - Propuesta técnica y económica - Diseño técnico - Reporte de acceso de usuario VPN/Token - Documentación técnica - Laptops de desarrollo - Reporte de actas de aceptación - Reporte de estatus de proyectos - Repositorio de versionamiento	1
Política de seguridad de pantallas, escritorios limpios y contraseñas seguras	Cláusula en donde especifique la seguridad de los activos de información con las contraseñas de autenticidad para verificar la identidad de los usuarios.	9.2.4 9.3.1 11.2.1 11.2.4 11.2.8 11.2.9	- Laptops de desarrollo	1
Agregar el procedimiento de desvinculación de acceso a usuario en el proceso de desvinculación del personal	Tras la finalización del empleo, los derechos de acceso del personal a la información y activos asociados deberían eliminarse o suspender para evitar fugas de información.	9.2.6	- Todos los activos mencionados	1
Soporte técnico externo para el mantenimiento preventivo y correctivo de los equipos.	Contar con una empresa externa que permita realizar periódicamente mantenimiento, diagnóstico y reparación a los equipos informáticos (laptops, impresoras, monitores, cargadores, entre otros)	6.1.3 11.2.1 12.1.1 15.1.1 15.1.2 15.1.3	- Laptops de desarrollo	2
Directrices para comer beber y fumar en las instalaciones de la oficina.	Contar con directrices donde indique lo que se debe o no se debe hacer en las instalaciones de la oficina y no afectar a los activos.	11.2.1	- Laptops de desarrollo	1

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Control de softwares instalados	Tener un control de los softwares autorizados para evitar daños en los equipos y fugas de información	12.2.1 12.6.2	- Laptops de desarrollo	2
Creación de perfil de usuarios	Crear perfiles de usuarios al momento de asignar un equipo, solo algunos usuarios tendrán acceso al usuario "administrador" y otros solo "usuario" para restringir la instalación de softwares no autorizados	12.6.2	- Laptops de desarrollo	2
Actualizaciones de los drivers o instaladores	Cronograma de actualizaciones de drivers o instaladores de los programas que son necesarios para el desarrollo de los proyectos.	6.1.3	- Laptops de desarrollo	1
Agregar investigaciones de antecedentes el proceso de contratación del personal	En el proceso de contratación debe ir un procedimiento en donde indique investigaciones de antecedentes penales de los futuros colaboradores debido a que se asignará información clasificada y confidencial.	7.1.1	- Datos del personal	1
Contratar una empresa externa de mensajería	Contar con una empresa que se encargue de mensajería segura y confiable para los documentos que se necesiten ser trasladados.	8.3.3	- Registros de órdenes de compras y facturas - Reporte de actas de aceptación	2
Proveedor externo en instalaciones de suministros	Contar con un proveedor que se encargue de las instalaciones de suministro (energía, electricidad, calefacción, ventiladores o aire acondicionado, entre otros) que aseguren que estén en correcto funcionamiento y así evitar problemas en el área laboral.	11.2.2	- Oficina de Miraflores	2
Manuales, procedimientos y configuraciones	Contar con manuales de usuarios para los softwares utilizados, además procedimientos y configuraciones de los servicios pasados ya sea por los sistemas de nuestros clientes.	12.1.1	- Documentación técnica	2

MÉDIDAS DE SEGURIDAD	DESCRIPCIÓN	CONTROL	ACTIVOS	GRUPO
Carpeta pública para el personal donde visualicen las políticas internas	Contar con una carpeta pública en donde se encuentren todas las políticas de la empresa para su conocimiento de todo el personal.	9.2.5	- Control de políticas	1
Establecer controles de seguridad cuando se trasladen en la siguiente oficina	Contar con controles de seguridad como tarjetas de autenticación de control de acceso con número único por cada personal, acceso de ingreso a las áreas correspondientes, cámaras de vigilancias.	11.1.2 11.1.3	- Oficina de Miraflores	2
Procedimiento de gestión de incidentes	Este procedimiento tiene como objetivo la gestión adecuada de los incidentes reportados, es decir, identificarlos, evaluarlos, ejecutar acciones para corregirlos y mantener un informe de estos para futuras revisiones.	16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.6 16.1.7	- Todos los activos mencionados	1
Plan de continuidad de la seguridad de la información	Tiene como objetivo preservar la seguridad de información en la empresa ante situaciones adversas.	17.1.1	- Laptops de desarrollo	1
Cláusula de requisitos contractuales y legislación aplicable	Se requiere ingresar una cláusula en la propuesta técnica y económica, revisada por la asesora legal, la cual asegure el cumplimiento de los requisitos contractuales y legislación vigente.	18.1.1 18.1.3	- Control de salarios - Formato de gestión de oportunidades - Reporte de acceso de usuario VPN/Token - Propuesta técnica y económica - Documentación técnica	1
Procedimiento de control de información documentada	Tiene como objetivo describir las actividades para establecer, documentar, controlar y mantener los documentos (procedimientos, formatos, registros, etc), de acuerdo con los requisitos establecidos por la organización.	18.1.3	- Datos del personal - Control de salarios - Control de procedimiento - Registros de órdenes de compras y facturas - Diseño técnico detallado	1
Revisión de la seguridad de información	Establecer la revisión de la seguridad de información periódica para identificar oportunidades de mejora.	18.2.2	- Toda la documentación referente a la seguridad de información	2

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.3.2 Implementación del Plan de Capacitación y Concientización

En la implementación del Plan de capacitación y concientización se desarrollaron los siguientes temas:

3.3.2.1 Charla de Seguridad de información

En la charla de seguridad de información se concientizó al personal sobre la importancia de la seguridad de información. Antes de empezar la charla se envió el enlace de la evaluación y se pasó una **"Lista de Asistencia" (Anexo 21)**, la cual se había calculado para aproximadamente 25 personas, es decir el total del personal en VF CONSULTING S.A.C.; sin embargo, por motivos de cruce de horarios en cursos o reuniones de trabajo no llegaron a asistir a la charla. En la **Tabla 3.12** mostramos la cantidad de asistentes y no asistentes en la charla.

TABLA 3.12 ASISTENCIA EN LA CHARLA DE SEGURIDAD DE INFORMACIÓN

Categoría	Cantidad de asistentes
Asistentes	16
No asistentes	9
TOTAL DEL PERSONAL	**25**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Además, se contabilizó la cantidad de asistencia por área de la empresa en la **Tabla 3.13:**

TABLA 3.13 ASISTENCIA POR ÁREAS A LA CHARLA DE SEGURIDAD DE INFORMACIÓN

Áreas de la empresa	Cantidad de asistentes
Prestación de servicios Telcos	11
Área logística y RR.HH.	1
Área comercial	1
Área de calidad	1
Oficina de proyectos	1
Área de finanzas	1
TOTAL DE ASISTENTES	**16**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Después de tomar la asistencia y evaluación, se realizó la charla de seguridad y al finalizar se envió la misma evaluación otra vez, para tener un indicador inicial y final del conocimiento que tenían sobre seguridad de la información.

Las preguntas en ambas evaluaciones fueron las mismas y referentes a lo que se explicó en la charla. Como primer resultado se puede ver en la **Tabla 3.14**, la cantidad de personas que obtuvo cierto puntaje antes de la charla, siendo el mínimo puntaje cero y el máximo cuatro.

TABLA 3.14 PUNTAJE POR ÁREA ANTES DE LA CHARLA

ÁREAS	PUNTAJES				
	0	1	2	3	4
Prestación de servicios Telcos	2 personas	6 personas	1 persona	2 personas	-
Oficina de proyectos	-	1 persona	-	-	-
Área comercial	-	-	-	-	1 persona
Área de calidad	-	-	-	-	1 persona
Área logística y RR.HH.	-	-	-	-	1 persona

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En la siguiente evaluación se obtuvo un mejor resultado en los puntajes, debido a que para algunos en la charla se aclararon algunas dudas y para otros se les brindó el conocimiento básico de la seguridad de información, para ver el detalle de los resultados por área ver la **Tabla 3.15.**

TABLA 3.15 PUNTAJE POR ÁREA DESPUÉS DE LA CHARLA

ÁREAS	PUNTAJES				
	0	1	2	3	4
Prestación de servicios Telcos	-	-	-	2 personas	9 personas
Oficina de proyectos	-	-	-	-	1 persona
Área comercial	-	-	-	-	1 persona
Área de calidad	-	-	-	-	1 persona
Área logística y RR.HH.	-	-	-	-	1 persona

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Al finalizar la evaluación final, se realizó un feedback con el personal sobre la evaluación realizada y algunos conceptos. Como parte de esta charla se procedió a entregar constancias digitales de la participación en la charla.

3.3.2.2 Capacitación en Seguridad de Información

La capacitación en seguridad de la información se realizó el mismo día se la charla, sin embargo, está se realizó al culminar la charla. Para esta capacitación se requirió a un responsable designado por cada área involucrada en el SGSI. La capacitación se basó en dar a conocer la importancia del SGSI y un resumen de lo realizado hasta el momento, lo cual incluye los procedimientos, formatos y registros.

En este caso, asistieron los responsables en su totalidad, lo cual se detalla en la **Tabla 3.16.**

TABLA 3.16 ASISTENCIA POR ÁREA EN LA CAPACITACIÓN

Áreas de la empresa	Cantidad de asistentes
Prestación de servicios Telcos	1
Área logística y RR.HH.	1
Área comercial	1
Área de calidad	1
Oficina de proyectos	1
TOTAL DE ASISTENTES	**5**

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En el caso de las responsables del área de calidad y RR.HH. ya conocían una gran parte de los temas expuestos, ya que fueron parte del proyecto, sin embargo, era necesario explicarles algunos puntos que no llegaron a ver por ello se requirió su asistencia.

Al concluir la explicación se realizó una evaluación sobre los temas vistos en la capacitación y se entregó un certificado de capacitación en seguridad de información a todos los responsables, ya que todos aprobaron esta evaluación ver detalle en la **Tabla 3.17**:

TABLA 3.17 PUNTAJE DE LA EVALUACIÓN EN CAPACITACIÓN

RESPONSABLE POR ÁREA	PUNTAJES										
	0	1	2	3	4	5	6	7	8	9	10
Prestación de servicios Telcos	-	-	-	-	-	-	-	-	X	-	-
Oficina de proyectos	-	-	-	-	-	-	-	-	-	X	-
Área comercial	-	-	-	-	-	-	-	-	-	-	X
Área de calidad	-	-	-	-	-	-	-	-	-	-	X
Área logística y RR.HH.	-	-	-	-	-	-	-	-	-	-	X

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

3.3.2.3 Campaña de Seguridad de Información

La campaña de seguridad de información se ejecutó antes de realizar la charla y capacitación, es decir se enviaron correos con información, se pegaron posters o afiches para ir induciendo al personal a investigar y tener cierto conocimiento previo. Se dividió en tres fases: diseño de la campaña, promoción de la campaña y ejecución de la campaña.

Se buscó hacer diseños juveniles y referentes a temáticas actuales, se recibió una buena recepción de la campaña de seguridad ya que se empezaron a usar los posters como salvapantallas, e incluso el personal fue dando ideas para futuras campañas de seguridad de información.

Además, como evidencia de estos, se encuentra el **Anexo 23**, en el cual se encuentra el salvapantalla y afiche más usado en la consultora.

CAPÍTULO IV:
PRUEBAS Y RESULTADOS

En este capítulo, se presentan los resultados obtenidos en las pruebas, las cuales consisten en la comparación entre la situación inicial y actual con la solución implementada de controles y cumplimiento de requisitos, así como evaluar el logro de los objetivos planteados.

4.1 PRUEBAS

Las pruebas se realizan en base al objetivo general y específicos planteados en el proyecto, lo que permitirá analizar y medir dichos objetivos.

A continuación, se detalla la medición de los objetivos planteados del proyecto:

- **Identificar el nivel de cumplimiento de la Norma ISO 27001:2013, realizando análisis de brechas tanto de los requisitos como de los controles.**

Para la comprobación de este objetivo, se realizó una reunión con algunos responsables de áreas, se desarrolló un acta de reunión **(Anexo 5)**, en esta reunión se realizaron una serie de preguntas con respecto a los requisitos y controles de la Norma ISO/IEC 27001:2013. Producto de esta reunión obtuvimos los Informes de análisis de brecha de requisitos y controles tanto el antes y el después de la implementación. **(Anexo 3 y 4)**

- **Calcular los riesgos de los activos de información realizando la evaluación de riesgos.**

Para la comprobación de este objetivo se realizó una encuesta a todo el personal con respecto a los activos de información y así poder identificar cuáles de los activos tienen un mayor riesgo.

En la consultora, el total de personas es de 25 aproximadamente y en la encuesta realizada, 22 personas contestaron; es decir un 88% respondieron dicha encuesta. **(Figura 4.1)**.

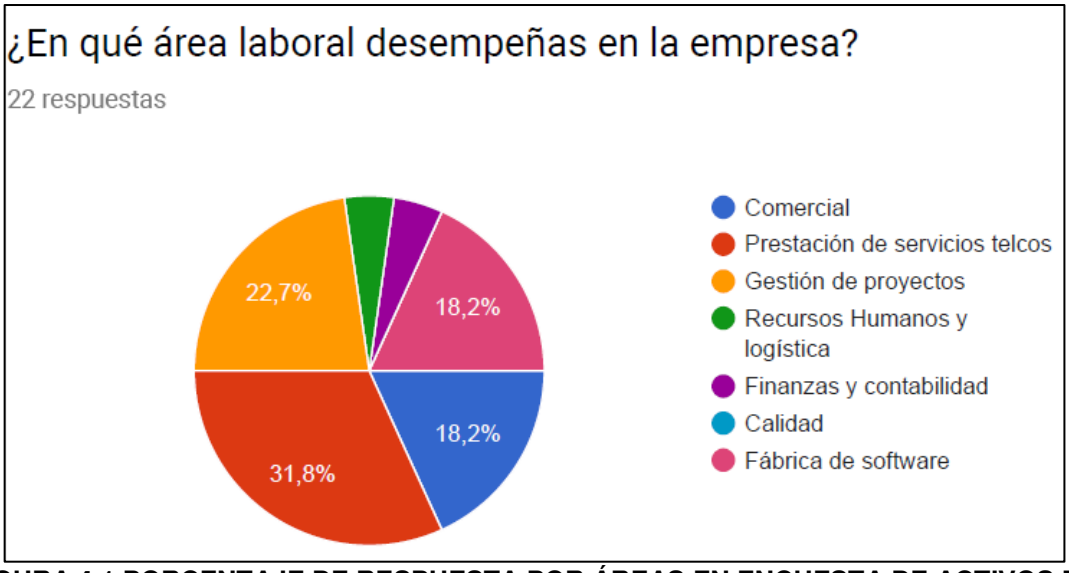


FIGURA 4.1 PORCENTAJE DE RESPUESTA POR ÁREAS EN ENCUESTA DE ACTIVOS DE INFORMACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Además, indicaron que los activos de mayor impacto y que no se están tomando en cuenta son los siguientes:

- Activos de software (instaladores, licencias)
- Activos de datos (planilla, contratos, procedimientos, políticas, propuestas, gestión de oportunidades, órdenes, facturas)
- Activos de servicios (internet, correo electrónico, repositorio)
- Activos de media (manuales, documentos administrativos)
- Activos de equipamiento auxiliar (caja de seguridad, archivadores)
- Activos de hardware (laptops, equipos)
- Activos intangibles (Confianza en los clientes, reputación, imagen de la organización, reputación comercial)

- El activo más importante la persona.
- Activo de instalación (edificio, oficina)

Luego respondieron que si al perder sus activos afectarían en su desarrollo laboral y ocasionaría las siguientes incidencias: **(Figura 4.2)**

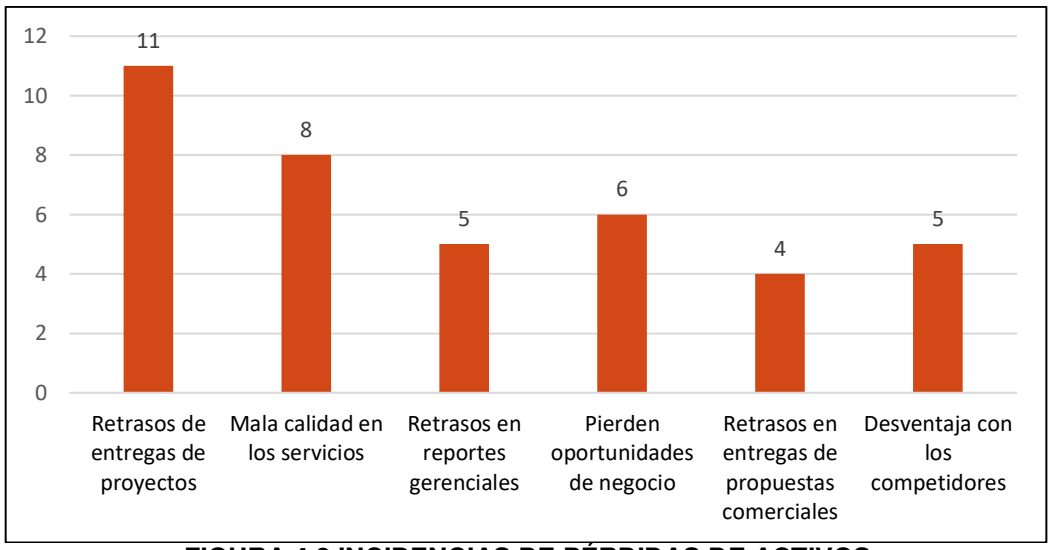


FIGURA 4.2 INCIDENCIAS DE PÉRDIDAS DE ACTIVOS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Con respecto a uno de los pilares de la seguridad de la información, la "disponibilidad", se preguntó si tenían acceso a sus activos definidos en sus áreas laborales, para lo cual respondieron un 54.5% que sí y el 45.5% que no, **(Figura 4.3)**, debido a que no se tenía un inventario de activos por áreas y desconocimiento de origen de información, no sabían por dónde acceder.

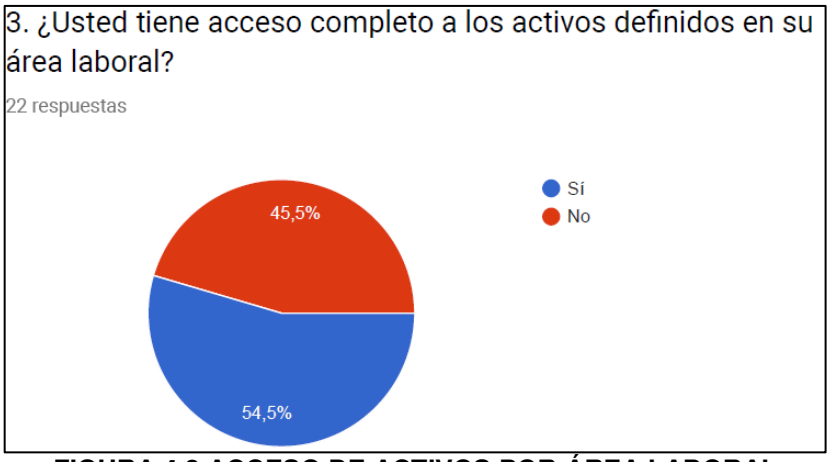


FIGURA 4.3 ACCESO DE ACTIVOS POR ÁREA LABORAL
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Con respecto a uno de los pilares de la seguridad de información, la “Integridad”, se preguntó, ¿qué pasaría si un activo de alta importancia se altera sin su conocimiento?, lo cual se obtuvo lo siguiente:

- Afecta a los entregables de proyectos.
- Reportes desactualizados de mal uso.
- Provocación de cuello de botella en las actividades.
- Posibles pérdidas financieras.
- Afecta al cumplimiento con los requisitos de los clientes.
- Impacta tiempo y dinero.

Y, por último, con respecto al pilar de la seguridad de la información, “la confiabilidad”, se preguntó, si un activo se divulgará, ¿qué impacto consideras que tendría en la empresa?, lo cual respondieron lo siguiente:

- Alto impacto si es sobre planilla, contratos y pagos a terceros.
- Perjudica a la empresa con respecto a la confiabilidad.
- Dañaría la imagen y orden de la empresa.
- Pérdidas de oportunidades de nuevas propuestas.
- Menores ingresos.

Esta encuesta fue una entrada para evaluar los riesgos de los activos de alto impacto (ver en resultados).

- **Capacitar y concientizar al personal involucrado en el proceso de prestación de servicios Telcos y los procesos involucrados, en temas de seguridad de información**

Para la comprobación de la charla y capacitación se realizó una Lista de asistencia para el personal, **(Anexo 21 y 22)**. Además, para evaluar sus conocimientos y concientización en seguridad de la información se realizaron evaluaciones del antes y después de la charla, además de una evaluación para después de la capacitación, sobre las evaluaciones de la charla se compararon los resultados, en cuanto a la evaluación de capacitación fue para evaluar su nivel de comprensión en cuanto al SGSI.

- **Mejorar la seguridad de la información mediante requisitos y controles basados en la norma ISO/IEC 27001:2013**

Para la comprobación del objetivo general se implementaron medidas de seguridad de información, además se realizó una encuesta sobre la seguridad de la información, para analizar la seguridad de información bajo la perspectiva de todo el personal de VF, se envió esta encuesta vía correo.

Basándonos en el total del personal que es de 25 aproximadamente y que en la encuesta realizada 20 personas contestaron; se puede decir que el 80% del personal respondió. Como parte de la encuesta se preguntó cuál era el área al que pertenecía para poder tener una idea del porcentaje de respuestas por área **(Figura 4.4)**.

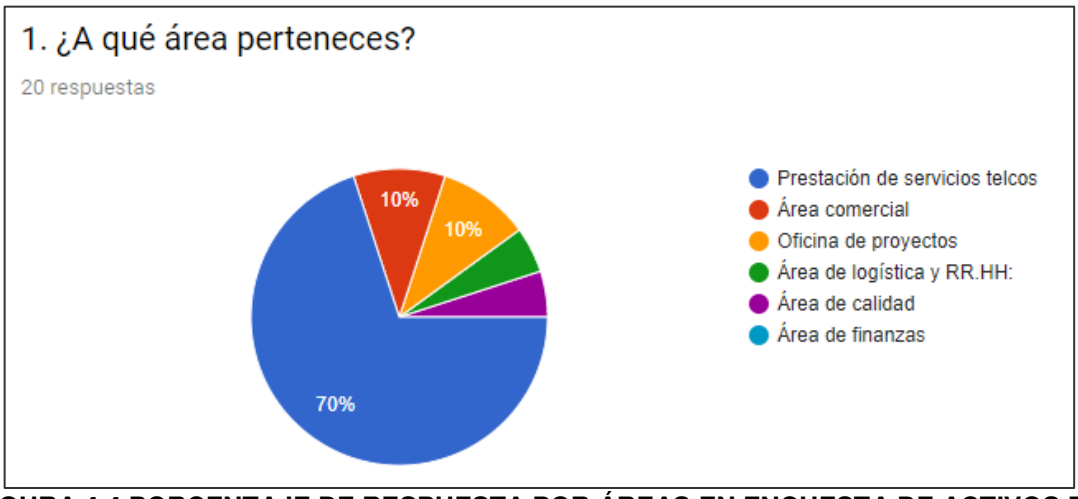


FIGURA 4.4 PORCENTAJE DE RESPUESTA POR ÁREAS EN ENCUESTA DE ACTIVOS DE INFORMACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Además, todos los que respondieron indicaron que consideran que la seguridad de la información es importante para la empresa **(Figura 4.5)**.

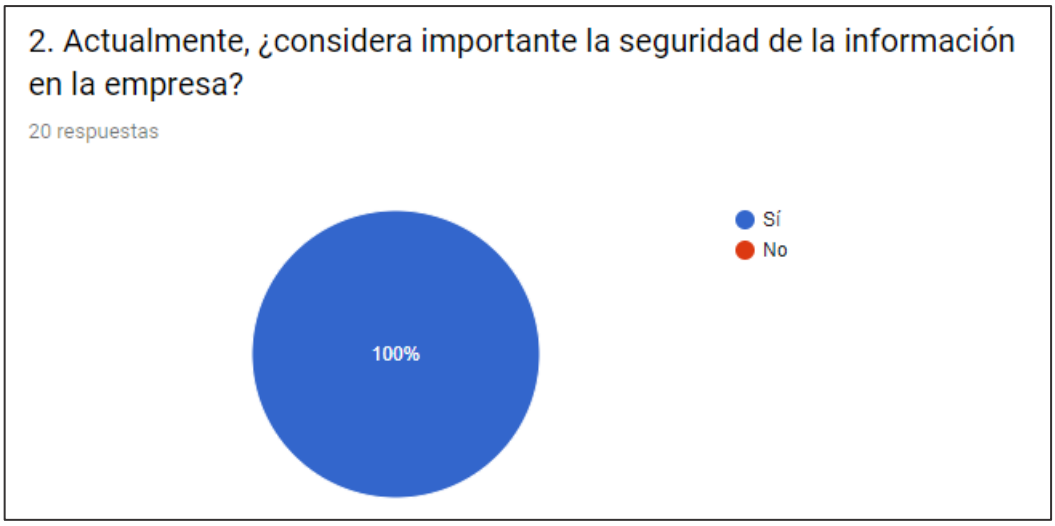


FIGURA 4.5 PORCENTAJE DE RESPUESTA POR ÁREAS EN ENCUESTA DE ACTIVOS DE INFORMACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Luego, se preguntó si se consideraban beneficiosos los controles de información implementados, las respuestas fueron afirmativas y los motivos fueron:

- Se obtuvo un mejor control de la seguridad en los equipos y del personal en cuanto a la información que manejan.
- Son importantes para resguardar la información.
- Ayudará con la evaluación de la homologación.
- La información es vital para la empresa.
- Ayuda a respaldar cualquier filtración de información.

Después respondieron si la empresa debería seguir invirtiendo en la seguridad de información, la respuesta de todos fue afirmativa y los motivos más relevantes fueron los siguientes:

- Trajo una mejora a pesar del corto tiempo de implementación.
- Nos muestra hacia los clientes como una empresa más formal y seria.
- Es necesario para seguir creciendo como empresa.

Con respecto a las medidas de seguridad que fueron más beneficiosas bajo su perspectiva respondieron de la siguiente forma, ver la **Figura 4.6**:

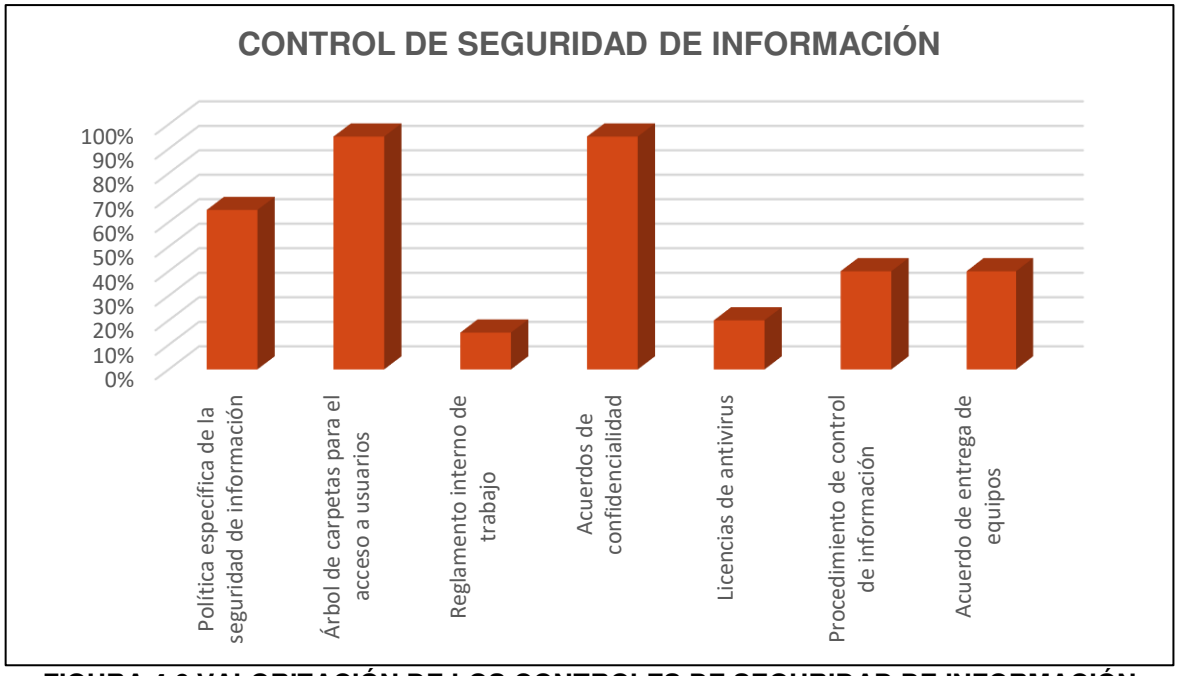


FIGURA 4.6 VALORIZACIÓN DE LOS CONTROLES DE SEGURIDAD DE INFORMACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

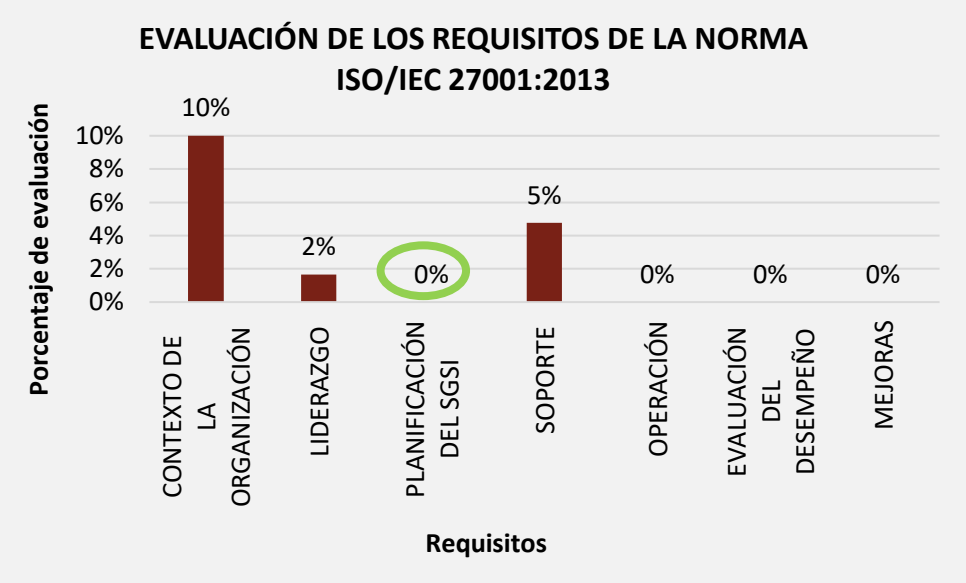
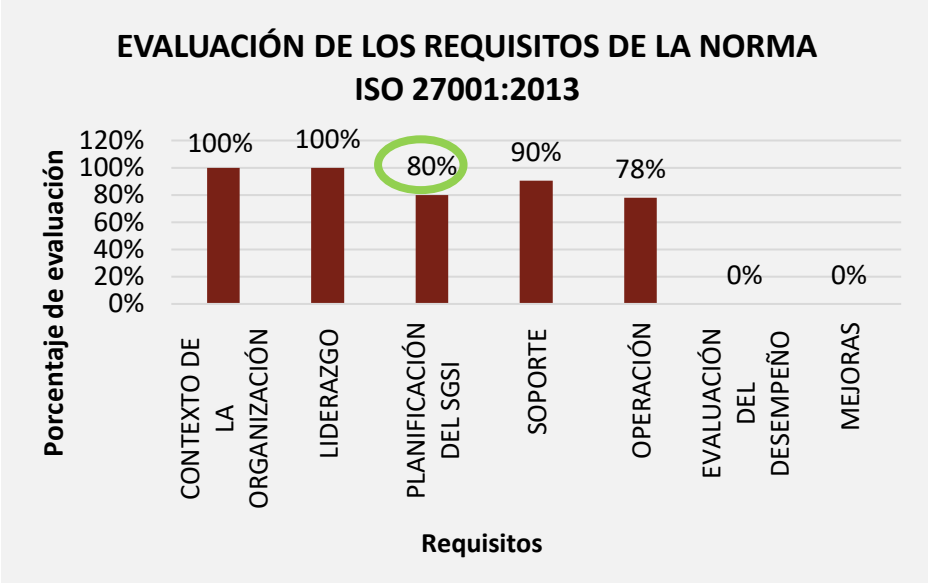
4.2 RESULTADOS

Los resultados se obtuvieron en base a las pruebas. A continuación, se detallan los resultados de los objetivos planteados del proyecto:

- **Identificar el nivel de cumplimiento de la Norma ISO 27001:2013, realizando análisis de brechas tanto de los requisitos como de los controles.**

  Como resultado de las pruebas realizadas se obtuvo los siguientes porcentajes de cada requisito **(Tabla 4.1)**, se puede observar la variación es alta, como por ejemplo en el requisito de "Planificación del SGSI" antes era un 0% y ahora es un 80%, así como aumentó, hay dos requisitos que se mantuvieron y es son de "Evaluación del desempeño" y "Mejoras" debido a que nuestro alcance no contemplada las Fase 3 y 4 de VERIFICAR, que contenía la auditoria y ACTUAR, hacer las mejoras para levantar no conformidades.

TABLA 4.1 COMPARACIÓN DE LOS RESULTADOS DE LA EVALUACIÓN DE REQUISITOS

REQUISITOS DE LA NORMA ISO/IEC 27001:2013	
ANTES	**DESPUÉS**
	

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Obteniendo un promedio total de los requisitos, el nivel de cumplimiento anterior era **2%** y ahora el nivel de cumplimiento es de **64%**. **(Figura 4.7)**

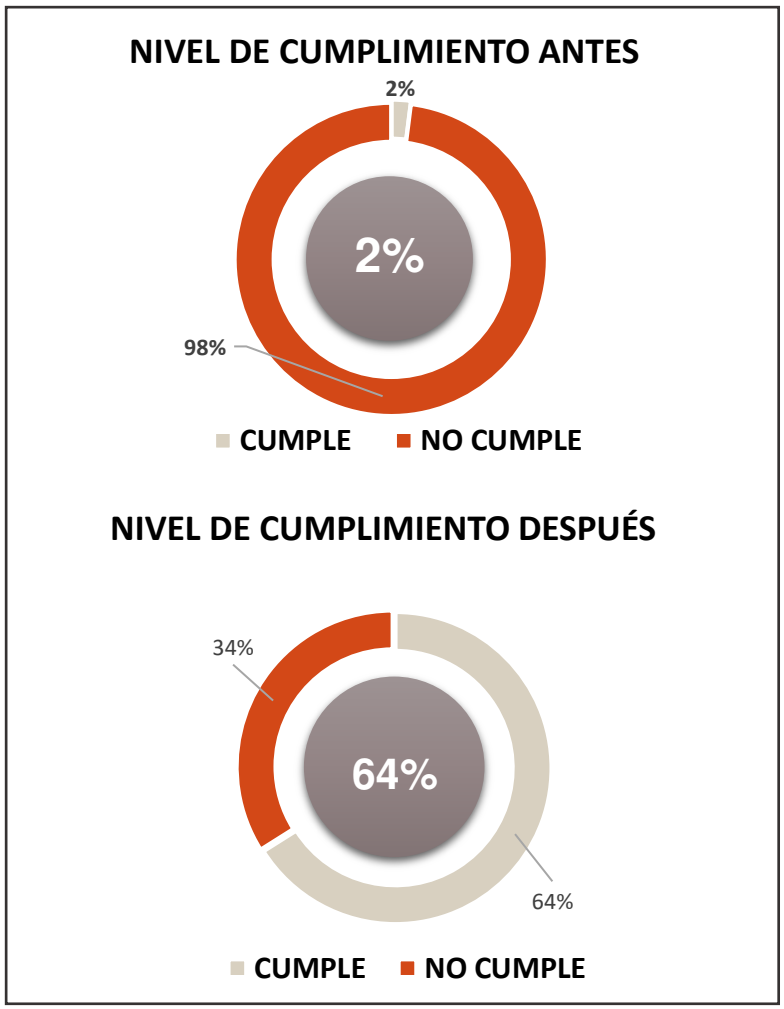
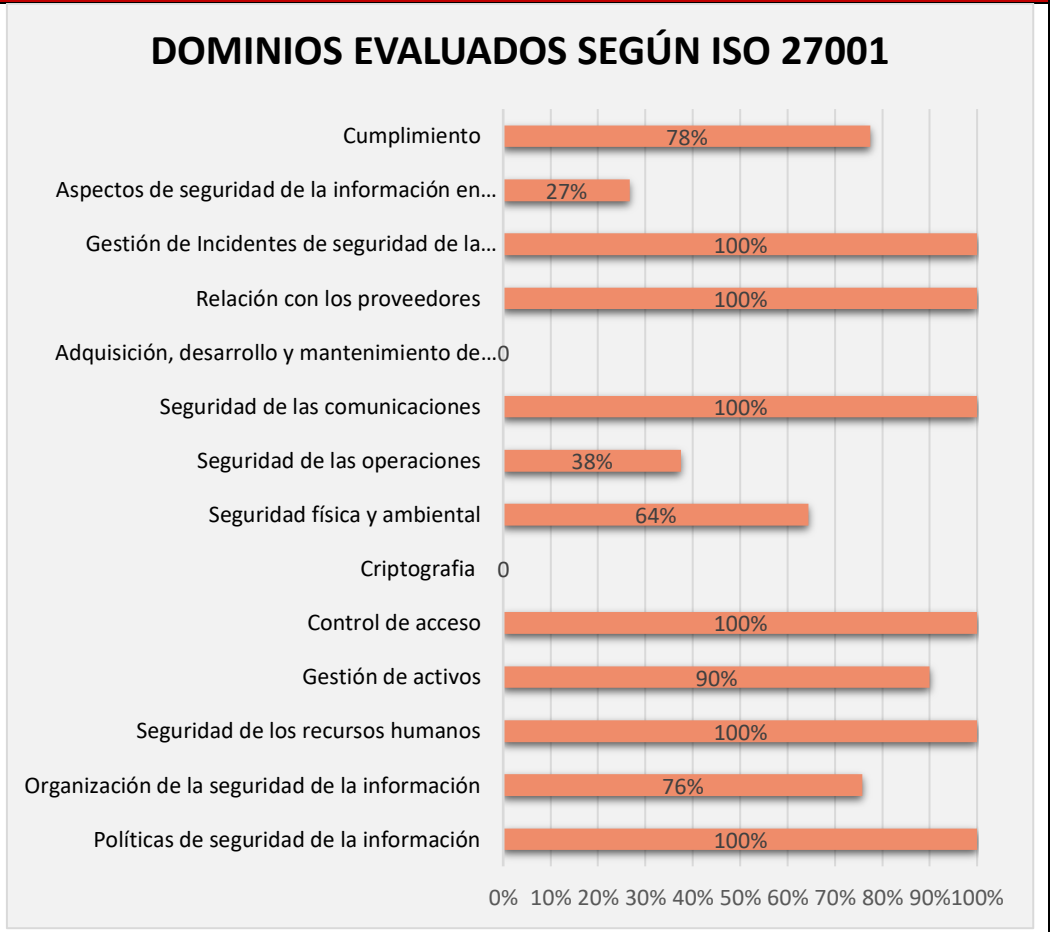


FIGURA 4.7 NIVEL DE CUMPLIMIENTO DE LOS REQUISITOS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Con respecto a los controles de la Norma ISO/IEC 27002, se obtuvo como resultados los siguientes porcentajes **(Tabla 4.2)**, se puede observar la variación es bastante, de los 14 dominios se cumplieron 6 y son: “Política de seguridad de la Información”, “Seguridad de los recursos humanos”, “Control de acceso”, “Seguridad de las comunicaciones”, “Relación con los proveedores” y “Gestión de incidentes de la seguridad de la información” que se aplicaron al 100%, mientras que 6 dominios están en proceso de aplicación y 2 dominios que no aplican.

TABLA 4.2 COMPARACIÓN DE PORCENTAJE DE CUMPLIMIENTO DE LOS DOMINIOS

CONTROLES DE LOS DOMINIOS DE LA ISO/IEC 27001:2013	
ANTES	**DESPUÉS**
	

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Obteniendo un porcentaje promedio de controles, el nivel de aplicabilidad anterior era de **9.19%** y ahora el nivel de aplicabilidad es de **80.99%**. **(Figura 4.8)**

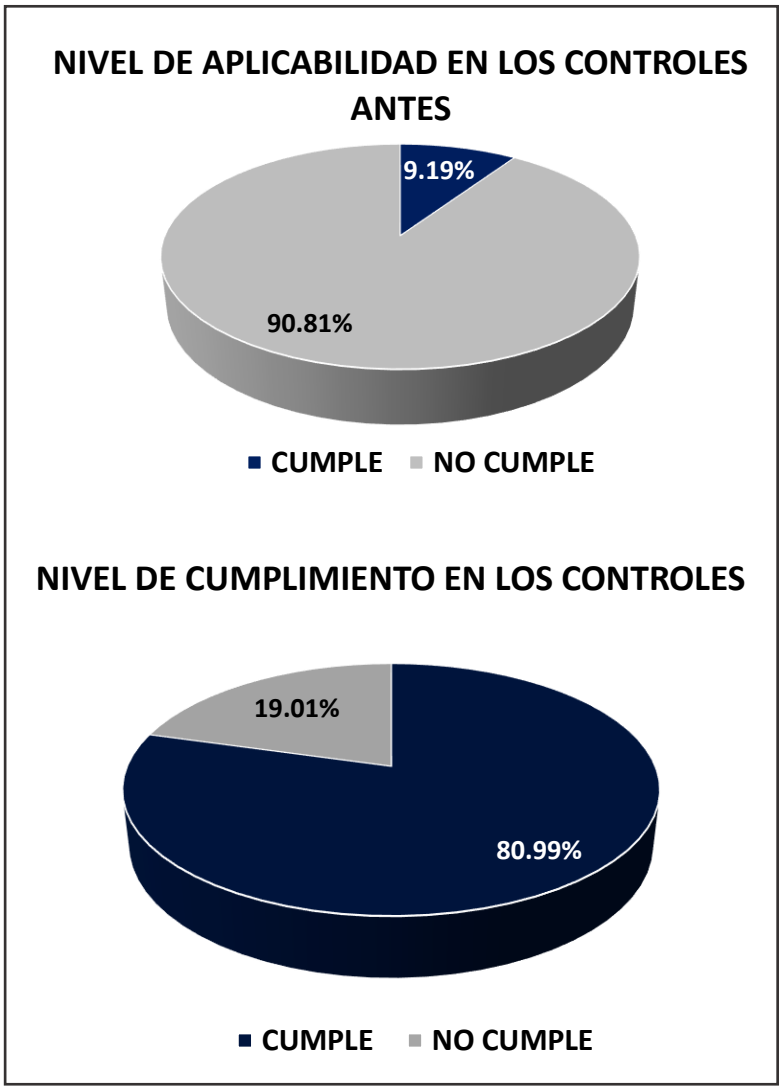


FIGURA 4.8 NIVEL DE APLICABILIDAD DE LOS CONTROLES DE LA NORMA ISO/IEC 27001:2013
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En resumen, como se mencionó anteriormente, la Norma ISO 27002 es un conjunto de medidas para la seguridad de la información que cuenta con 14 dominios, 35 objetivos y 114 controles. De las cuales se ha tomado en consideración los controles que son necesarios para tratar los riesgos de la consultora; es decir, solo los controles que se hayan incluido en la declaración de aplicabilidad debido a que hay controles que no aplican para la organización. Por lo tanto, nuestro 100% a implementar es un total de 12 dominios y 72 controles.

Lo que se ha implementado al 100% solo son 6 dominios, equivalente a 30 controles con un porcentaje de 41.67% y de los 6 dominios restantes, se ha llegado a implementar equis porcentaje (x%), equivalente a 25 controles siendo un porcentaje de 34.72%. De los dominios restante no se llegó cubrir al 100% debido a que no se llegó a implementar 17 controles, lo cual cuentan con un plan de acción del grupo 2 **(Anexo 24),** y se recomienda a la empresa que se implemente para proceder con la fase 3 y así poder auditarnos para la futura certificación.

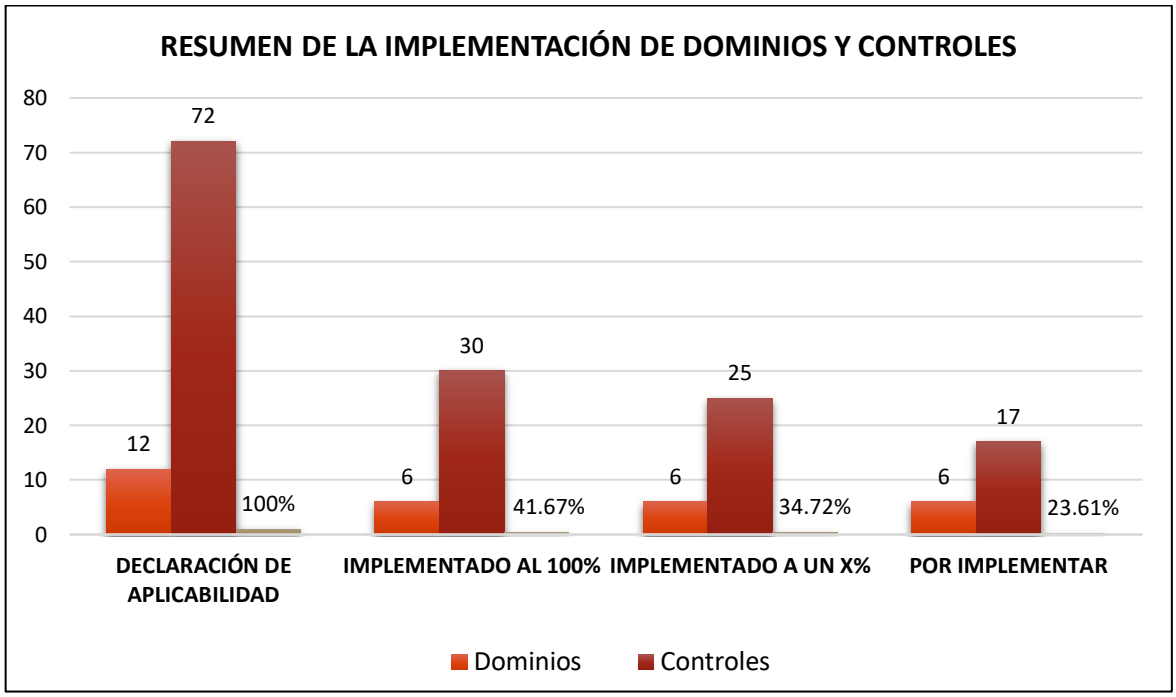


FIGURA 4.9 RESUMEN DE LA IMPLEMENTACIÓN DE CONTROLES
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

- **Calcular los riesgos de los activos de información realizando la evaluación de riesgos.**

Como resultado de la encuesta (PORQUE TU INFORMACIÓN VALE ORO), se realizó el inventario de activos y se identificó los activos de información por cada área **(Figura 4.10)**.

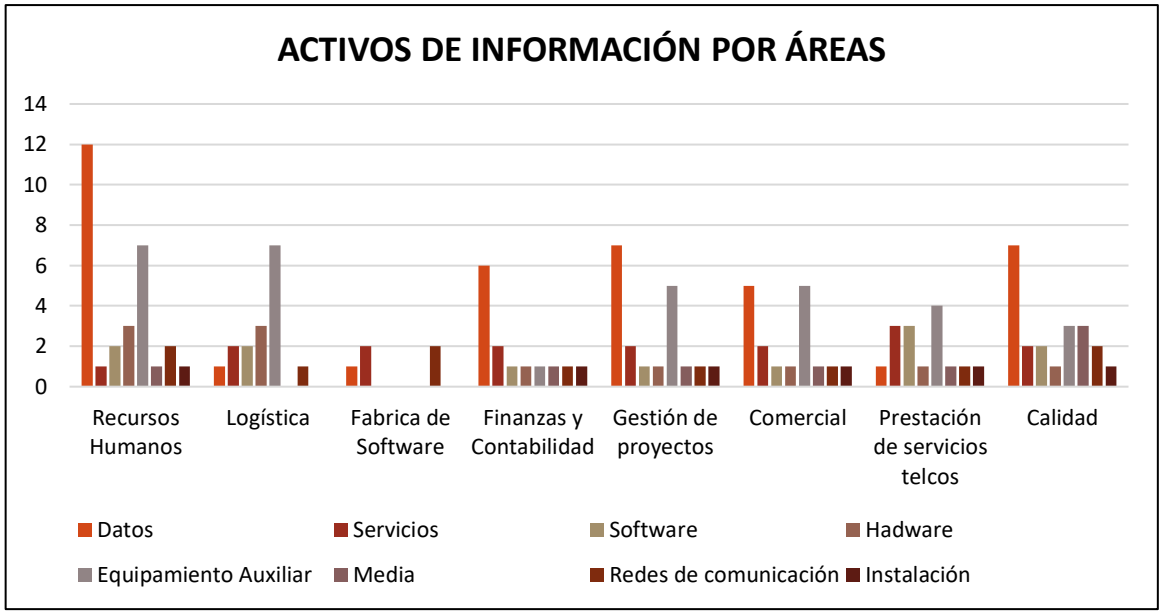


FIGURA 4.10 ACTIVOS DE INFORMACIÓN POR ÁREAS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Mediante la encuesta se pudo identificar cuáles activos de información tienen de alto impacto de importancia, se valorizaron de acuerdo a los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) y se obtuvo lo siguiente: **(Tabla 4.3)**

TABLA 4.3 VALORIZACIÓN DE ACTIVOS DE INFORMACIÓN

Ámbito	Categoría	ID	Activo	Criterios			Total	IMPACTO
				C	I	D		
DATOS	[D] Datos	[D-001]	Datos del personal	7	7	8	7	A
		[D-002]	Control de salarios	10	9	9	9	A
		[D-013]	Registros de órdenes de compras y facturas	7	10	8	8	A
		[D-020]	Formato de gestión de oportunidades	9	7	7	8	A
		[D-021]	Propuesta técnica y económica	9	10	7	9	A
		[D-022]	Reporte de actas de aceptación	9	6	7	7	A
		[D-023]	Diseño técnico detallado	7	8	7	7	A
		[D-024]	Reporte de acceso de usuarios VNP	8	9	9	9	A
		[D-026]	Reporte de estatus de proyectos	6	8	8	7	A
		[D-029]	Control de procedimiento	4	9	6	6	M
		[D-031]	Control de políticas	3	8	10	7	A

Ámbito	Categoría	ID	Activo	Criterios			Total	IMPACTO
				C	I	D		
SERVICIOS	[S] Servicios	[S-001]	Internet	4	7	9	7	M
		[S-002]	Correo electrónico	7	6	7	7	M
		[S-003]	Repositorio de versionamiento	8	10	9	9	A
SOFTWARE	[SW] Software	[SW-002]	Lista de instaladores de software	7	9	10	9	A
HARDWARE	[HW] Hardware	[HW-003]	Laptops de desarrollo	9	9	10	9	A
MEDIA	[M] Media	[M-002]	Documentación técnica	7	9	10	9	A
INSTALACIÓN	[I] Instalaciones	[I-001]	Oficina Miraflores	8	6	9	8	A

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Los activos que se encuentran en la **Tabla 4.3** son de alto impacto y están relacionado al proceso core, solo tres activos son medio debido a que no son de gran impacto para la empresa, pero también están relacionado al core; es decir, que estos activos se tomarán en consideración en la evaluación de riesgos.

Luego de valorizar los activos, se procedió a evaluar y se obtuvo un porcentaje de **49%** de mayor riesgo extrema **(Figura 4.11),** que tienen gran impacto de amenaza y la probabilidad es casi seguro o probable que pueda suceder y esto afecte a la empresa. Para ver el detalle en general de la evaluación de riesgo, se encuentra en el **Anexo 17.**

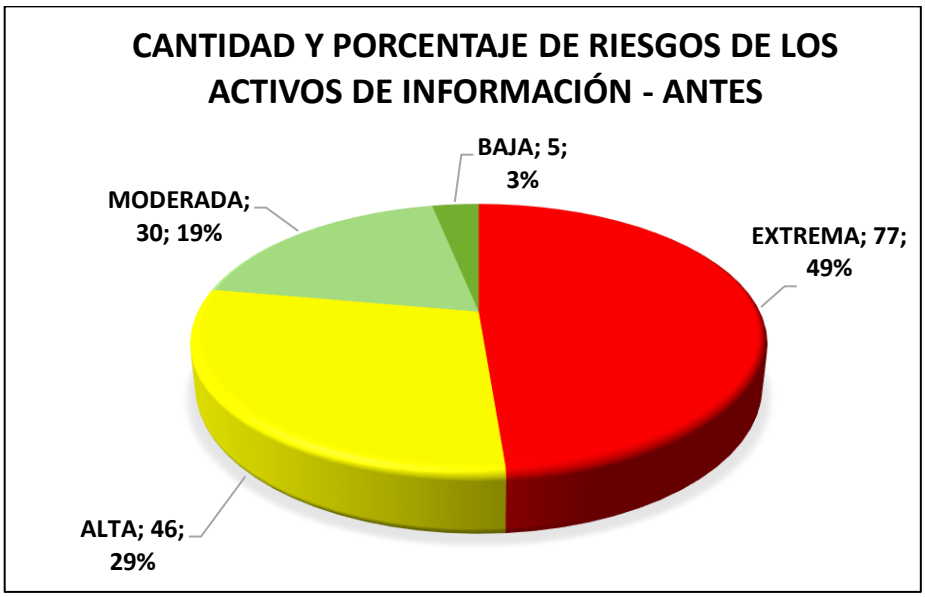


FIGURA 4.11 CANTIDAD Y PORCENTAJE DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN-ANTES
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Luego de la evaluación, se tiene que realizar el plan de tratamiento de riesgos y de ahí decidir qué hacer con los riesgos obtenidos, como en el anterior se obtuvo un porcentaje de riesgo extremo, nos dirigimos a esos riesgos en proceder a implementar el plan de acción; es decir, los controles que sean necesario para reducir la mayoría de esos riesgos. Como se visualiza en la **Figura 4.12**, el porcentaje de los riesgos extremos ha bajado del 49% al 11%, mientras que los riesgos moderados, los que se puede asumir o convivir con el riesgo, aumentaron del 19% al 49%.

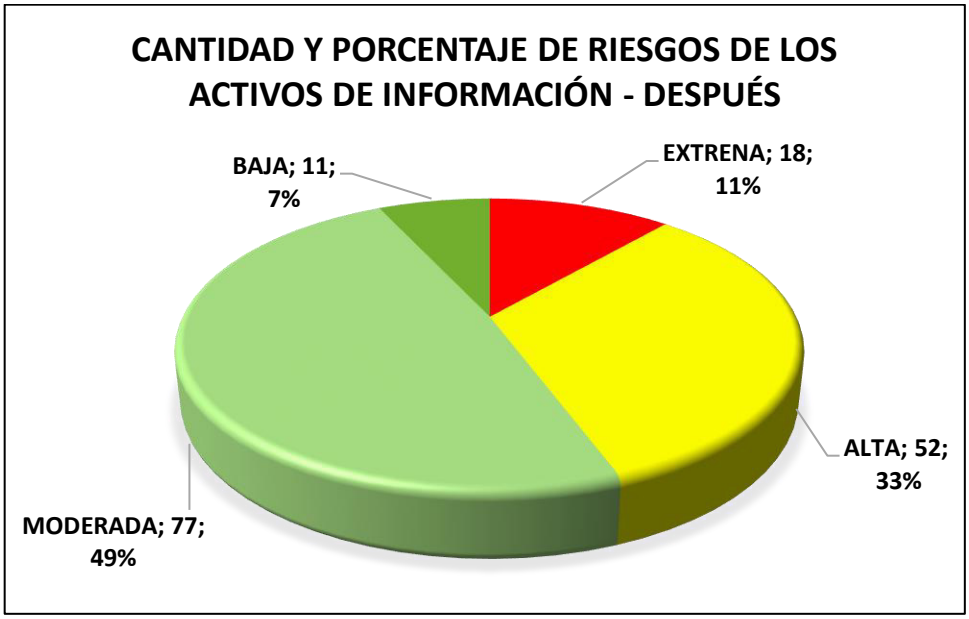


FIGURA 4.12 CANTIDAD Y PORCENTAJE DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN – DESPUÉS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

- **Capacitar y concientizar al personal involucrado en el proceso de prestación de servicios Telcos y los procesos involucrados, en temas de seguridad de información.**

Basado en la Lista de Asistencia para la charla **(Anexo 21)** se calculó el porcentaje de personal que asistió a la charla, el cual se muestra en la **Figura 4.13** Dado esto, se puede ver que asistió más de la mitad del personal de VF.

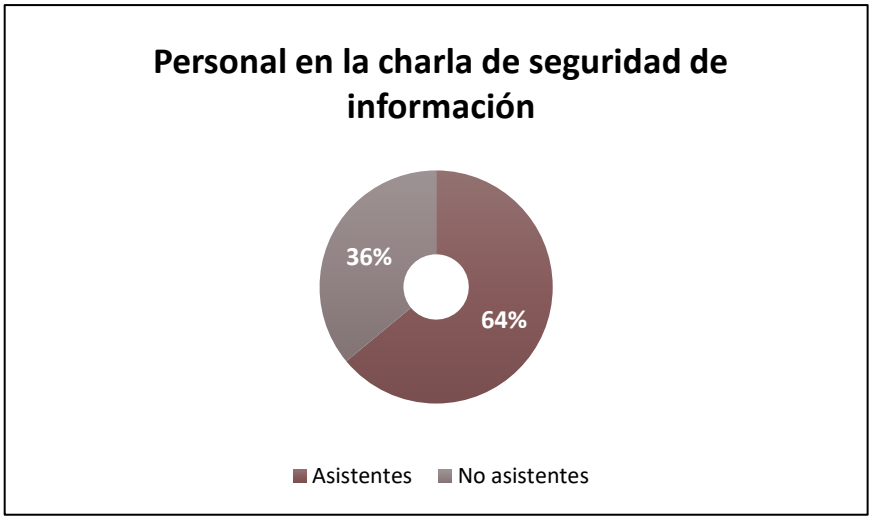


FIGURA 4.13 PORCENTAJE DE ASISTENTES A LA CHARLA
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Sobre la **Figura 4.14** podemos ver que el área que obtuvo un mayor porcentaje de asistencia es el de "Prestación de servicios Telcos", sobre las demás áreas asistió un responsable por área.

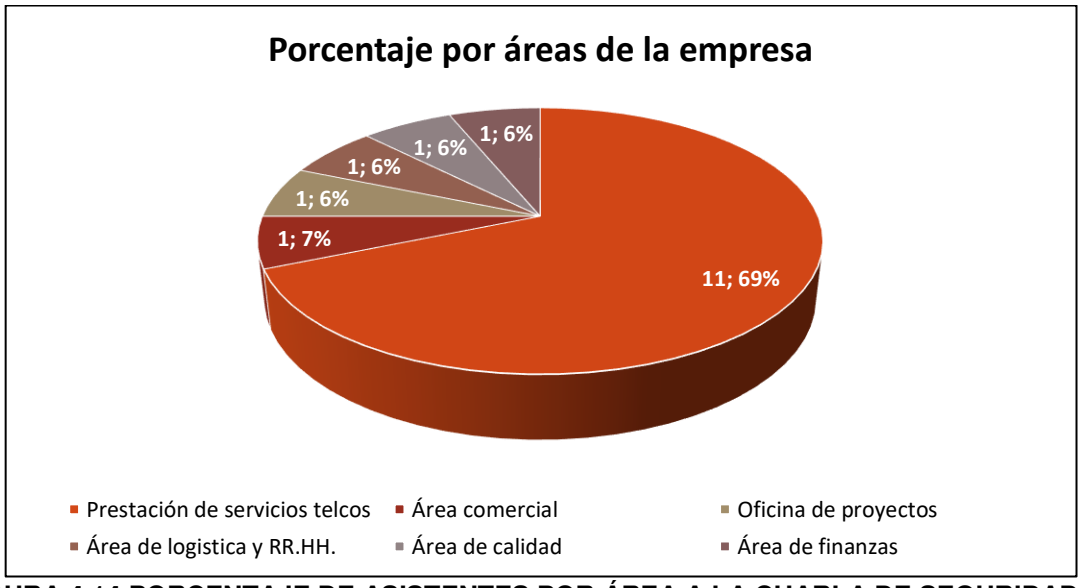


FIGURA 4.14 PORCENTAJE DE ASISTENTES POR ÁREA A LA CHARLA DE SEGURIDAD DE INFORMACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Además, como resultado de las evaluaciones realizadas en la charla se obtuvieron los puntajes por área, del antes y después, en la **Figura 4.15** se comparan ambos resultados.

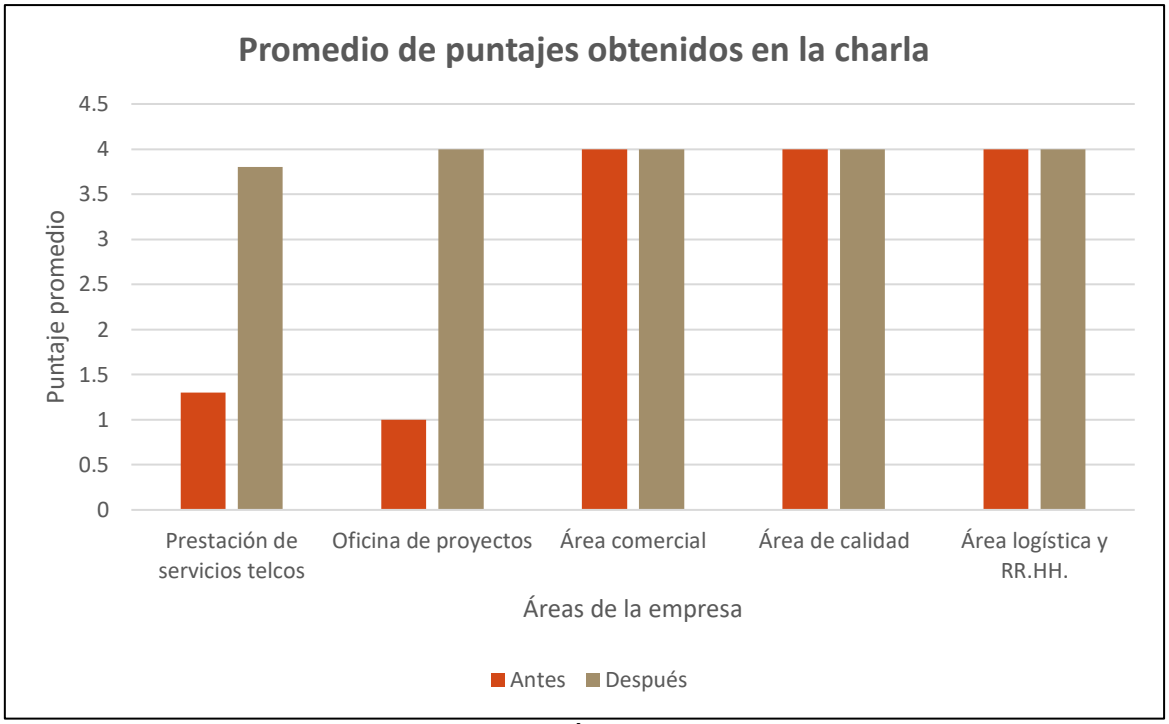


FIGURA 4.15 COMPARACIÓN DE PUNTAJES OBTENIDOS
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

En cuanto a la capacitación se puede observar en la **Figura 4.16** que asistió el 100% del personal requerido, es decir todos los responsables de cada área.

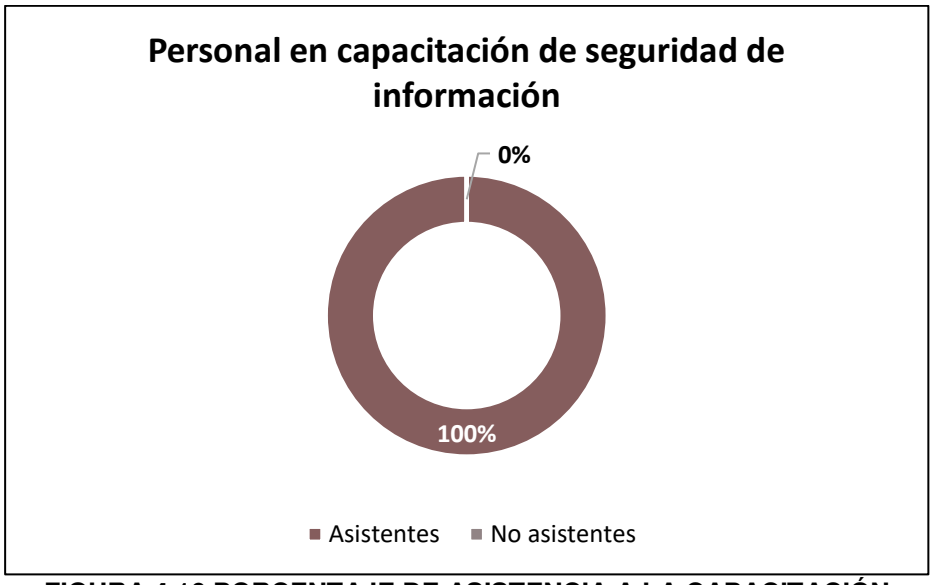


FIGURA 4.16 PORCENTAJE DE ASISTENCIA A LA CAPACITACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

Sobre la evaluación de la capacitación en la **Figura 4.17** se puede visualizar que aprobó el 100% del personal.

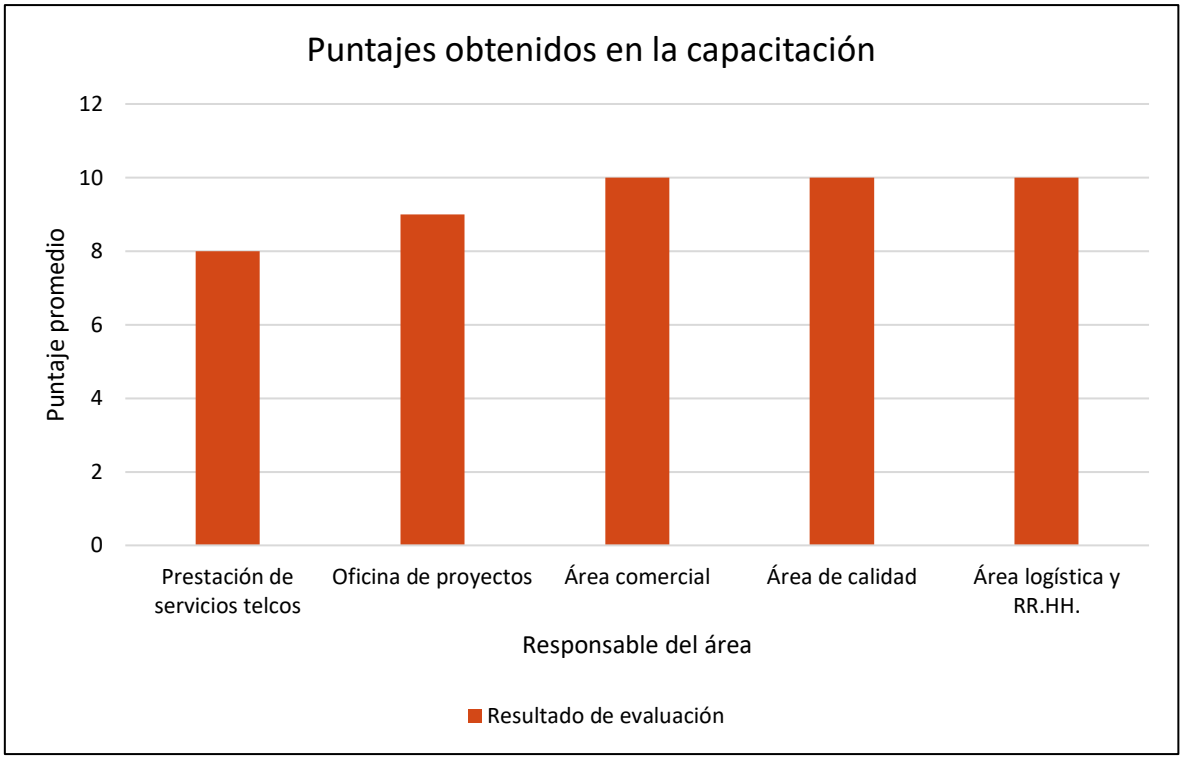


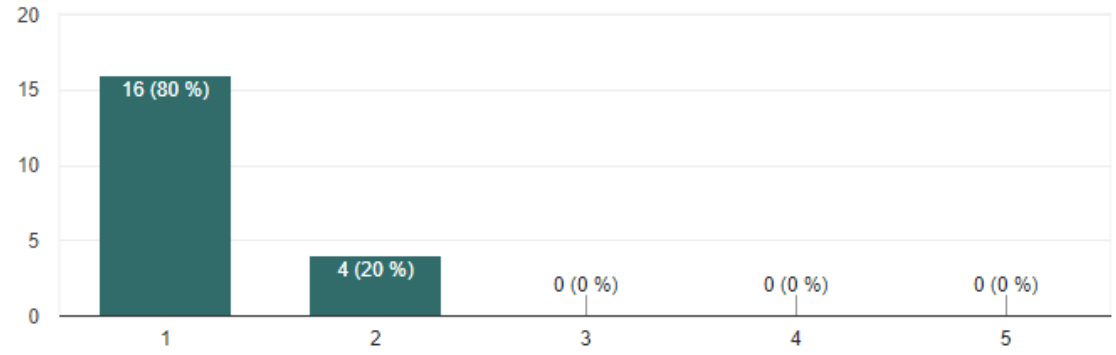
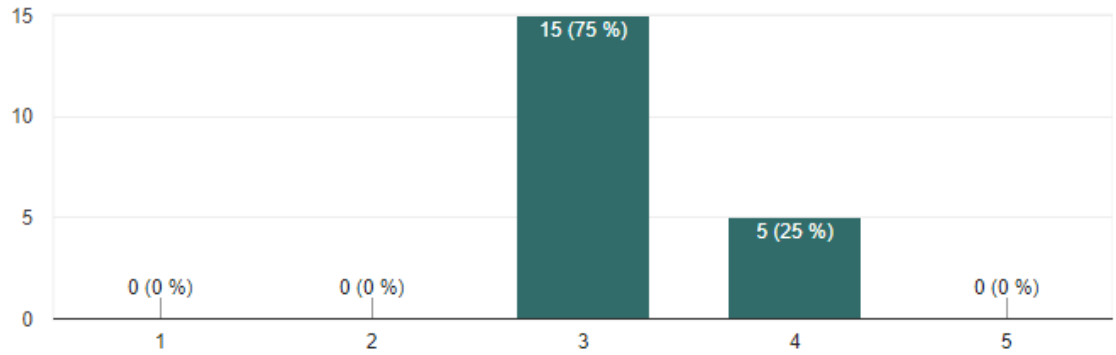
FIGURA 4.17 RESULTADOS DE LA EVALUACIÓN EN LA CAPACITACIÓN
FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

- **Mejorar la seguridad de la información mediante requisitos y controles basados en la norma ISO/IEC 27001:2013**

Como resultado de la encuesta "Perspectiva de la seguridad de información" se obtuvo una gran participación del personal. Además, se observó una mayor conciencia sobre la seguridad de información y sobre todo de la importancia de los controles de seguridad implementados.

En base a lo mencionado, se pidió una valorización del personal sobre la seguridad de información, para ello se pidió evaluar cómo se veía hace tres meses y como se percibe actualmente **(Tabla 4.4)**. La puntuación era del 5 a 1, siendo 5 el puntaje más alto y 1 el más bajo. Dado ello, se observa una considerable mejora en la perspectiva de la seguridad en el personal de VF CONSULTING S.A.C.

TABLA 4.4 LA SEGURIDAD DE INFORMACIÓN EN VF CONSULTING S.A.C

LA SEGURIDAD DE INFORMACIÓN EN VF CONSULTING S.A.C.
Si tendría que valorizar la seguridad de información hace tres meses en VF CONSULTING, ¿en qué escala cree que se encontraría?

Si tendría que valorizar la seguridad de información actual en VF CONSULTING, ¿en qué escala cree que se encontraría?


FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

CAPÍTULO V:
DISCUSIÓN Y APLICACIONES

En este capítulo se discuten los resultados obtenidos en el capítulo anterior y se menciona la aplicación de este proyecto a futuro en la consultora, así como su aplicación en otras organizaciones, de otros sectores y/o tamaños.

5.1 DISCUSIÓN

TABLA 5.1 DISCUSIÓN DE RESULTADOS POR OBJETIVOS

Objetivo General	Antes	Después	Resultado	Aplicado
• Mejorar la seguridad de la información mediante el cumplimiento de requisitos y controles basados en la Norma ISO/IEC 27001:2013.	• Personal sin motivación ni apoyo a la seguridad de la información. • Descontrol de la seguridad de la información • No contaban con medidas de seguridad de la información.	• Personal incentivado en apoyar y aprender sobre la seguridad de la información. • Mejor manejo en la seguridad de la información.	• Personal satisfecho. • Medidas de seguridad de la información (controles, políticas, acuerdos, entre otros) implementados con respecto a los requisitos y controles de la ISO/IEC 27001:2013.	SI

Objetivos Específicos	Antes	Después	Resultado	Aplicado
• Identificar el nivel de cumplimiento de la Norma ISO/IEC 27001:2013, realizando análisis de brechas tanto de los requisitos como de los controles.	• Porcentaje bajo del análisis de brecha inicial de requisitos • Porcentaje bajo del análisis de brecha inicial de controles.	• Porcentaje medio/alto del análisis de brecha final de requisitos • Porcentaje medio/alto del análisis de brecha final de controles.	• Informe del nivel de cumplimiento de requisitos y controles de la ISO/IEC 27001:2013 de la situación anterior y actual.	SI
• Calcular los riesgos de los activos de información, realizando la evaluación de riesgos.	• No contaban con un registro de inventario de activos. • No realizaban una evaluación del riesgo de los activos • No tenían una gestión de incidentes.	• Elaboración del inventario de activos. • Registro de evaluación de riesgos de los activos.	• Activos de información identificados por su impacto y área. • Evaluación de riesgos de los activos por áreas.	SI
• Capacitar y concientizar al personal involucrado en el proceso de prestación de servicios telcos y los procesos involucrados, en temas de seguridad de información.	• No realizaban capacitaciones o charlas con respecto a la seguridad de la información. • El personal no tomaba conciencia o no tenía conocimientos acerca de la seguridad de la información.	• Planificación e implementación de la charla de seguridad de información • Planificación e implementación de la capacitación en seguridad de información • Planificación e implementación de la campaña de seguridad de información.	• Mayor conciencia sobre la importancia de la seguridad de información. • Mayor conocimiento acerca del SGSI.	SI

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

5.2 APLICACIONES

La implementación de controles y cumplimiento de requisitos se puede extender en VF CONSULTING S.A.C., actualmente el alcance del SGSI no abarca al proceso de Desarrollo de aplicaciones; sin embargo, si este proceso llega a desarrollar productos que generen ingresos o automaticen algunos procedimientos, debería tenerse en cuenta para así tener un SGSI integrado.

Respecto a la implementación de controles y cumplimiento de requisitos basado en la ISO/IEC 27001, se puede realizar en cualquier sector y sin importar el tamaño de la organización; ya que es un estándar internacional, necesario y es adaptable. A pesar de esto, se cree que en una PYME es muy complicado su implementación lo cual no es verdad, simplemente se debe tener en cuenta que el compromiso de la Alta Dirección es fundamental como el inicio del proyecto.

CONCLUSIONES

1. La implementación de los controles de seguridad cumplió con los requisitos mínimos aceptables, relacionados a la Norma 27001, en consecuencia, se mejoró significativamente la seguridad de la información en la consultora quedando pendiente una segunda implementación de acuerdo con un plan de acción para cumplir con la totalidad exigible por la Norma 27001.
2. En cuanto al nivel de cumplimiento de los controles que requiere y exige la Norma 27001, podemos manifestar que de los 14 dominios se cumplieron 6, quedando pendientes 8, los cuales serán implementados en una segunda fase teniendo un plan de acción.
3. Al realizar el análisis de riesgos de los activos de información se pudo concluir que se ha identificado un nivel aceptable de riesgo ya que con la implementación de los mínimos controles requeridos se ha reducido el nivel de exposición en el que podrían estar los activos de información, en una segunda implementación se abarcaría más la reducción del nivel del riesgo en exposición de los activos, por consiguiente, tenemos un riesgo aceptable.
4. En relación con la capacitación y concientización al personal involucrado en el proceso de prestación de servicios telcos y los procesos involucrados, se ha conseguido a un nivel aceptable el involucramiento y conocimiento de los controles mínimos requeridos en la consultora, en consecuencia, periódicamente se estará difundiendo por los diferentes medios el fortalecimiento de la concientización ya que es un proceso constante.

RECOMENDACIONES

1. Se recomienda a la Alta Dirección continuar en una segunda fase con la implementación de los controles requeridos restantes para así reducir los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información de la organización.
2. Se recomienda continuar en un breve plazo con el plan de acción para completar la implementación de los controles faltantes, para ello la alta dirección debería disponer de los recursos necesarios para conseguir el objetivo tan apreciado.
3. Se recomienda a la Alta Dirección que cada área de la organización defina su análisis de riesgos de sus activos involucrados en cada uno de sus procesos y después monitorizar permanentemente todos los riesgos de la organización mediante una matriz de riesgos.
4. Se recomienda a la Alta Dirección generar programas de concientización semestralmente a todas las áreas de la organización para acrecentar la efectividad de la conciencia de la seguridad de información en relación a la seguridad y el personal.

ANEXOS

ANEXO 1

CONTROLES DE LA ISO/IEC 27001:2013

ANEXO 1 CONTROLES DE LA ISO/IEC 27001:2013

A.5 Políticas de Seguridad de la Información
- **5.1** Directrices de gestión de la Seguridad de la Información
  - **A.5.1.1** Políticas para la Seguridad de la Información
  - **A.5.1.2** Revisión de las Políticas para la Seguridad de la Información

A.6 Organización de la Seguridad de la Información
- **6.1** Organización Interna
  - **A.6.1.1** Roles y responsabilidades en seguridad de la información
  - **A.6.1.2** Segregación de tareas
  - **A.6.1.3** Contacto con las autoridades
  - **A.6.1.4** Contacto con grupos de interés especial
  - **A.6.1.5** Seguridad de la información en la gestión de proyectos
- **6.2** Los dispositivos móviles y el teletrabajo
  - **A.6.2.1** Política de dispositivos móviles
  - **A.6.2.2** Teletrabajo

A.7 Seguridad relativa a los recursos humanos
- **7.1** Antes del empleo
  - **A.7.1.1** Investigación de antecedentes
  - **A.7.1.2** Términos y condiciones del empleo
- **7.2** Durante el empleo
  - **A.7.2.1** Responsabilidades de gestión
  - **A.7.2.2** Concienciación, educación y capacitación en seguridad de la información
  - **A.7.2.3** Proceso disciplinario
- **7.3** Finalización del empleo o cambio en el puesto de trabajo
  - **A.7.3.1** Responsabilidades ante la finalización o cambio

A.8 Gestión de Activos
- **8.1** Responsabilidad sobre los activos
  - **A.8.1.1** Inventario de activos
  - **A.8.1.2** Propiedad de los activos
  - **A.8.1.3** Uso aceptable de los activos
  - **A.8.1.4** Devolución de activos
- **8.2** Clasificación de la Información
  - **A.8.2.1** Clasificación de la información
  - **A.8.2.2** Etiquetado de la información
  - **A.8.2.3** Manipulado de la información
- **8.3** Manipulación de los soportes
  - **A.8.3.1** Gestión de soportes extraíbles
  - **A.8.3.2** Eliminación de soportes
  - **A.8.3.3** Soportes físicos en tránsito

A.9 Control de Acceso
- **9.1** Requisitos del negocio para el control de acceso
  - **A.9.1.1** Política de control de acceso
  - **A.9.1.2** Acceso a las redes y a los servicios de red
- **9.2** Gestión de acceso de usuario
  - **A.9.2.1** Registro y baja de usuarios
  - **A.9.2.2** Provisión de acceso de usuario
  - **A.9.2.3** Gestión de privilegios de acceso
  - **A.9.2.4** Gestión de la información de secreta de autenticación de los usuarios
  - **A.9.2.5** Revisión de los derechos de acceso de usuario
  - **A.9.2.6** Retirada o reasignación de los derechos de acceso
- **9.3** Responsabilidades del usuario
  - **A.9.3.1** Uso de la información secreta de autenticación
- **9.4** Control de acceso a sistemas y aplicaciones
  - **A.9.4.1** Restricción del acceso a la información
  - **A.9.4.2** Procedimientos seguros de inicio de sesión
  - **A.9.4.3** Sistema de gestión de contraseñas
  - **A.9.4.4** Uso de utilidades con privilegiados del sistema

A.9.4.5 Control de acceso al código fuente de los programas

A.10 Criptografía

10.1 Controles Criptográficos

A.10.1.1 Política de uso de los controles criptográficos

A.10.1.2 Gestión de claves

A.11 Seguridad Física y del entorno

A.11.1 Áreas seguras

A.11.1.1 Perímetro de seguridad física

A.11.1.2 Controles de físicos de entrada

A.11.1.3 Seguridad de oficinas, despachos y recursos

A.11.1.4 Protección contra las amenazas externas y ambientales

A.11.1.5 El trabajo en áreas seguras

A.11.1.6 Áreas de carga y descarga

A.11.2 Seguridad de los equipos

A.11.**2.1** Emplazamiento y protección de equipos

A.11.2.2 Instalaciones de suministro

A.11.2.3 Seguridad del cableado

A.11.2.4 Mantenimiento de los equipos

A.11.2.5 Retirada de materiales propiedad de la empresa

A.11.2.6 Seguridad de los equipos fuera de las instalaciones.

A.11.2.7 Reutilización o eliminación segura de equipos

A.11.2.8 Equipo de usuario desatendido

A.11.2.9 Política de puesto de trabajo despejado pantalla limpia

A.12 Seguridad de las Operaciones

A.12.1 Procedimientos y responsabilidades operacionales

A.12.1.1 Documentación de procedimientos de operación.

A.12.1.2 Gestión de cambios

A.12.1.3 Gestión de capacidades

A.12.1.4 Separación de los recursos de desarrollo, prueba y operación

A.12.2 Protección contra el software malicioso (malware)

A.12.2.1 Controles contra el código malicioso

A.12.3 Copias de seguridad

A.12.3.1 Copias de seguridad de la información

A.12.4 Registros y supervisión

A.12.4.1 Registro de Eventos

A.12.4.2 Protección de la información de registro

A.12.4.3 Registros de administración y operación

A.12.4.4 Sincronización del Reloj

A.12.5 Control del software en explotación

A.12.5.1 Instalación de software en explotación

A.12.6 Gestión de la vulnerabilidad técnica

A.12.6.1 Gestión de las vulnerabilidades técnicas

A.12.6.2 Restricciones en la instalación de software

A.12.7 Consideraciones sobre la auditoría de sistemas de información

A.12.7.1 Controles de auditoría de sistemas de información

A.13 Seguridad de las Comunicaciones

A.13.1 Gestión de la seguridad de redes

A.13.1.1 Controles de red

A.13.1.2 Seguridad de los servicios de red

A.13.1.3 Segregación en redes

A.13.2 Intercambio de información

A.13.2.1 Políticas y procedimientos de intercambio de información

A.13.2.2 Acuerdos de intercambio de información

A.13.2.3 Mensajería electrónico

A.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 sistemas de información

A.14.1.1 Análisis de requisitos y especificaciones de Seguridad de la información

A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas
A.14.1.3 Protección de las transacciones de servicios de aplicaciones
A.14.2 Seguridad en el desarrollo y en los procesos de soporte
A.14.2.1 Política de desarrollo seguro
A.14.2.2 Procedimiento de control de cambios en sistema
A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A.14.2.4 Restricciones a los cambios en los paquetes de software
A.14.2.5 Principios de ingeniería de sistemas de seguros
A.14.2.6 Entorno de desarrollo seguro
A.14.2.7 Externalización del desarrollo de software
A.14.2.8 Pruebas funcionales de seguridad del sistema
A.14.2.9 Pruebas aceptación de sistema
A.14.3 Datos de prueba
A.14.3.1 Protección de los datos de prueba

A.15 Relación con Proveedores
15.1 Seguridad en las relaciones con los proveedores
A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores
A.15.1.2 Requisitos de seguridad en contratos con terceros
A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones
15.2 Gestión de la provisión de servicios del proveedor
A.15.2.1 Control y revisión de la provisión de servicios del proveedor
A.15.2.2 Gestión cambios en la provisión del servicio del proveedor

A.16 Gestión de Incidentes de Seguridad de la Información
A.16.1 Gestión de incidentes de seguridad de la información y mejoras
A.16.1.1 Responsabilidades y procedimientos
A.16.1.2 Notificación de los eventos de seguridad de la información
A.16.1.3 Notificación de puntos débiles de seguridad
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
A.16.1.5 Respuesta a incidentes de seguridad de la información
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
A.16.1.7 Recopilación de evidencias

A.17 Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio
A.17.1 Continuidad de la seguridad de la Información
A.17.1.1 Planificación de la continuidad de la seguridad de la información
A.17.1.2 Implementar la continuidad de la seguridad de la información
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.17.2 Redundancias
A.17.2.1 Disponibilidad de los recursos de tratamiento de la información

A.18 Cumplimiento
A.18.1 Cumplimiento de los requisitos legales y contractuales
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
A.18.1.2 Derechos de propiedad intelectual (DPI)
A.18.1.3 Protección de los registros de la organización
A.18.1.4 Protección y privacidad de la información de carácter personal
A.18.1.5 Regulación de los controles criptográficos

18.2 Revisiones de seguridad de información
A.18.2.1 Revisión independiente de la seguridad de la información
A.18.2.2 Cumplimiento con las políticas y normas de seguridad
A.18.2.3 Comprobación del cumplimiento técnico

ANEXO 2

COMPARACIÓN DE LA ISO 27001:2005 VS. 27001:2013

ANEXO 2 COMPARACIÓN DE LA ISO 27001:2005 VS. 27001:2013

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
4.1	La organización debe determinar las cuestiones externas e internas…	8.3, 8.3(a), 8.3 (e)
4.2(a)	Las partes interesadas que son relevantes para el sistema…	5.2.1(c), 7.3(c)(4),7.3(c)(5)
4.2(b)	los requisitos de estas partes interesadas…	5.2.1(c), 7.3(c)(4), 7.3(c)(5)
4.3	La organización debe determinar los límites y …	4.2.1(a)
4.3(a)	las cuestiones externas e internas referidas en el…	4.2.3(f)
4.3(b)	los requisitos referidos en el…	4.2.3(f)
4.3(c)	las interfaces y dependencias entre actividades	Requerimiento nuevo
4.3(c)	El alcance debe estar disponible como…	4.3.1(b)
4.4	La organización debe establecer, implementar, mantener…	4.1, 5.2.1(a)
5.1(a)	asegurando que se establecen las políticas y los objetivos…	4.2.1(b)(3)
5.1(b)	asegurando la integración de los requisitos…	Requerimiento nuevo
5.1(c)	asegurando que los recursos necesarios…	5.1(e)
5.1(d)	comunicando la importancia de una…	5.1(d)
5.1(e)	asegurando que el sistema de gestión de seguridad…	5.1(b), 5.1(g),5.1(h)
5.1(f)	dirigiendo y apoyando a las personas…	5.1(b), 5.1(g),5.1(h)
5.1(g)	promoviendo la mejora continua…	5.1(d)
5.1(h)	apoyando otros roles pertinentes d	5.1
5.2	alta dirección debe establecer una política…	4.2.1(b)(5),5.1(a)
5.2(a)	sea adecuada al propósito…	4.2.1(5),2.1(b)
5.2(b)	incluya objetivos de la seguridad de la información…	4.2.1(5),1(b)(1)
5.2(c)	incluya el compromiso de cumplir con los requisitos…	4.2.1(5),4.3.3
5.2(d)	incluya el compromiso de mejora continua…	5.1(d)
5.2(e)	estar disponible como información	4.3.1(5),3.1(a)
5.2(f)	comunicarse dentro de la organización…	5.1(d)
5.2(g)	estar disponible para las partes interesadas…	4.3.2(5),3.2(f)
5.3	alta dirección debe asegurarse de que…	5.1(c)
5.3(a)	asegurarse de que el sistema de gestión de la…	4.3.3
5.3(b)	informar a la alta dirección sobre el comportamiento…	4.3.3
6.1.1	Al planificar el sistema de gestión de seguridad…	4.2.1(d), 8.3(a)
6.1.1(a)	asegurar que el sistema de gestión de seguridad…	Requerimiento nuevo
6.1.1(b)	prevenir o reducir efectos indeseados;	Requerimiento nuevo

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
6.1.1(c)	lograr la mejora continua;	Requerimiento nuevo
6.1.1(d)	las acciones para tratar estos riesgos y…	4.2.1(e)(4), 8.3(b),8.3(c)
6.1.1(e)(1)	integrar e implementar las acciones en los…	4.3.1(f), 8.3(c)
6.1.1(e)(2)	evaluar la eficacia de estas acciones;	7.2(f)
6.1.2	organización debe definir y aplicar un proceso…	4.2.1(c), 4.2.1(c)(1)
6.1.2(a)	establezca y mantenga criterios sobre riesgos…	Requerimiento nuevo
6.1.2(a)(1)	los criterios de aceptación de riesgo;	4.2.1(b)(4), 4.2.1(c)(2),5.1(f)
6.1.2(a)(2)	los criterios para llevar acabo las apreciaciones…	4.2.3(d)
6.1.2(b)	asegure que las sucesivas apreciaciones de los riesgos…	4.2.1(c)(2)
6.1.2(c)	identifique los riesgos de seguridad de la información	4.2.1(d)
6.1.2(c)(1)	llevando a cabo el proceso de apreciación de…	4.2.1(d)(1),4.2.1(d)(2), 4.2.1(d)(3),4.2.1(d)(4)
6.1.2(c)(2)	identificando a los dueños de los riesgos;	4.2.1(d)(1)
6.1.2(d)	analice los riesgos de seguridad……	4.2.1 (e)
6.1.2(d)(1)	valorando las posibles consecuencias que resultarían…	4.2.1(e)(1)
6.1.2(d)(2)	valorando de forma realista la probabilidad…	4.2.1(e)(2)
6.1.2(d)(3)	determinando los niveles de riesgo;	4.2.1(e)(3)
6.1.2(e)	evalúe los riesgos de seguridad de la información:	4.2.1(e)(4)
6.1.2(e)(1)	comparando los resultados del análisis de riesgos…	4.2.1(e)(4)
6.1.2(e)(2)	priorizando el tratamiento de los riesgos…	4.2.1(e)(4)
6.1.2(e)(2)	La organización debe conservación debe conservar información documentada…	4.3.1(d),4.3.1(e)
6.1.3	organización debe definir y efectuar un proceso…	4.2.1(c)(1)
6.1.3(a)	seleccionar las opciones adecuadas de tratamiento de riesgos…	4.2.1(f),4.2.1(f)(1), 4.2.1(f)(2),4.2.1(f)(3), 4.2.1(f)(4)
6.1.3(b)	determinar todos los controles que sean necesarios…	4.2.1(g)
6.1.3(c)	comparar los controles determinados en el punto…	4.2.1(j)(1),4.2.1(j)(3)
6.1.3(d)	elaborar una “Declaración de aplicabilidad"…	4.2.1(j),4.2.1(j)(1), 4.2.1(j)(2),4.2.1(j)(3), 4.3.1(i)
6.1.3(e)	formular un plan de tratamiento de riesgos…	4.2.2(a)
6.1.3(f)	obtener la aprobación del plan de tratamiento de…	4.2.1(h)

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
6.1.3(f)	La organización debe conservar información documentada…	4.3.1(f)
6.2	La organización debe establecer los objetivos…	5.1(b)
6.2(a)	ser coherentes con la política de seguridad…	5.1(d)
6.2(b)	ser mediables (si es posible);	Requerimiento nuevo
6.2(c)	tener en cuenta los requisitos de seguridad…	Requerimiento nuevo
6.2(c)	y los resultados de la apreciación y del tratamiento…	Requerimiento nuevo
6.2(d)	ser comunicados; y…	5.1(d)
6.2(e)	ser actualizados, según sea apropiado.	4.2.3(b)
6.2(e)	La organización debe conservar información documentada…	4.3.1(a)
6.2(f)	lo que se va a hacer;	Requerimiento nuevo
6.2(g)	que recursos se requerirán;	Requerimiento nuevo
6.2(h)	quién será el responsable;	Requerimiento nuevo
6.2(i)	cuando se finalizará;	Requerimiento nuevo
6.2(k)	cómo se evaluarán los resultados.	Requerimiento nuevo
7.1	La organización debe determinar y proporcionar…	4.2.2(g),5.2.1
7.2(a)	determinar la competencia necesaria de las personas…	5.2.2,5.2.2(a)
7.2(b)	asegurarse de que estas personas sean competentes…	5.2.2
7.2(c)	cuando sea aplicable, poner en marcha acciones…	5.2.2(b),5.2.2(c)
7.2(d)	conservar la información documentada…	5.2.2(d)
7.3(a)	la política de la seguridad de la…	Requerimiento nuevo
7.3(b)	su contribución a la eficacia del sistema de…	4.2.2(e),5.2.2(d)
7.3(c)	las implicaciones de no cumplir con los requisitos del…	4.2.2(e),5.2.2(d)
7.4	La organización debe determinar la necesidad de…	4.2.4(c),5.1(d)
7.4(a)	el contenido de la comunicación;	Requerimiento nuevo
7.4(b)	cuando comunicar;	Requerimiento nuevo
7.4(c)	a quién comunicar;	Requerimiento nuevo
7.4(d)	quién debe comunicar;	Requerimiento nuevo
7.4(e)	los procesos por los que debe efectuarse la…	Requerimiento nuevo
7.5.1(a)	la información documentada requerida por esta…	4.3.1(a),4.3.1(b),4.3.1(h),4.3.1(i)
7.5.1(b)	la información documentada que la organización…	Requerimiento nuevo
7.5.2(a)	la identificación y la descripción…	4.3.2(j)
7.5.2(b)	el formato (por ejemplo, idioma, versión del software) …	4.3.1(i)
7.5.2(c)	la revisión y la aprobación con respecto	4.3.2(a),4.3.2(b)

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
7.5.3	La información documentada requerida por el sistema…	4.3.2
7.5.3(a)	esté disponible y preparada para su uso…	4.3.2(d)
7.5.3(b)	esté protegida adecuadamente…	4.3.3
7.5.3(c)	distribución, acceso, recuperación y uso;	4.3.2(f),4.3.2(h),4.3.2(i),
7.5.3(d)	almacenamiento y preservación, incluida la…	4.3.2(e),4.3.3
7.5.3(e)	control de los cambios (por ejemplo, control de la versión);	4.3.2(c)
7.5.3(f)	retención y disposición	4.3.2(f)
7.5.3(f)	La información documentada de origen externo…	4.3.2(g)
8.1	La organización debe planificar, implementar…	Requerimiento nuevo
8.1	La organización debe implementar también planes…	4.2.2(f)
8.1	En la medida necesaria la organización debe mantener…	4.3.3
8.1	La organización debe controlar los cambios planificados…	A.10.1.2,A.12.5.1, A.12.5.2,A.12.5.3
8.1	revisar las consecuencias de los cambios no previstos…	4.2.2(h), 8.3(b), 8.3(c)
8.1	La organización debe garantizar que los procesos…	A.10.2.1, A.10.2.2,A.10.2.3,A.12.5.5
8.2	La organización debe efectuar apreciaciones…	4.2.3(d)
8.2	La organización debe conservar información documentada…	4.3.1(e)
8.3	La organización debe implementar el plan de tratamiento…	4.2.2(b), 4.2.2(c)
8.3	La organización debe conservar información documentada…	4.3.3
9.1	La organización debe evaluar el desempeño…	4.2.3(a)(3), 4.2.3(b),4.2.3(c), 4.2.3(f), 6(d)
9.1(a)	a que es necesario hacer seguimiento…	4.2.2(d)
9.1(b)	los métodos de seguimiento, medición...	4.2.2(d)
9.1(c)	cuando se deben llevar a cabo el seguimiento…	Requerimiento nuevo
9.1(d)	quien debe hacer el seguimiento…	Requerimiento nuevo
9.1(e)	cuando se deben analizar y evaluar los resultados…	4.2.3(b)
9.1(f)	quien debe analizar y evaluar esos resultados	Requerimiento nuevo
9.1(f)	La organización debe conservar información documentada…	4.3.1(g)

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
9.2	La organización debe llevar a cabo auditorías internas…	4.2.3(e), 6
9.2(a)(1)	los requisitos propios de la organización…	6(b)
9.2(a)(2)	los requisitos de esta norma internacional.	6(a)
9.2(b)	está implementado y mantenido de manera eficaz.	6(c)
9.2©	planificar, establecer, implementar y mantener uno o…	6(d)
9.2(d)	para cada auditoría, definir sus criterios…	6(d)
9.2(e)	seleccionar los auditores y llevar a cabo auditorías para…	6(d)
9.2(f)	asegurarse de que se informa a la dirección…	6(d)
9.2(g)	conservar información documentada…	4.3.1(h), 4.3.3
9.3	La alta dirección debe revisar el sistema de gestión…	5.2.1(e), 7.1
9.3(a)	el estado de las acciones desde anteriores revisiones…	7.2(g)
9.3(b)	los cambios en las cuestiones externas e internas…	4.2.3(d)(1), 4.2.3(d)(2),4.2.3(d)(3), 4.2.3(d)(4),4.2.3(d)(5), 4.2.3(d)(6),7.2(c), 7.2(e), 7.2(h)
9.3(c)	la información sobre el comportamiento de la…	7.2(f)
9.3(c)(1)	no conformidades y acciones correctivas,	7.2(d)
9.3(c)(2)	seguimiento y resultado de las mediciones,	7.2(f)
9.3(c)(3)	resultados de auditoría, y	7.2(a)
9.3(c)(4)	cumplimiento de los objetivos de seguridad de la información.	Requerimiento nuevo
9.3(d)	los comentarios provenientes de las partes…	7.2(b)
9.3(e)	los resultados de la apreciación del riesgo y el estado…	7.2(e), 7.2(f)
9.3(f)	las oportunidades de mejora continua.	7.2(i)
9.3(f)	Los elementos de salida de la revisión por la dirección…	4.2.3(f), 7.1, 7.3(a)
9.3(f)	y cualquier necesidad de cambio en el sistema…	4.2.3(d)(1), 4.2.3(d)(2),4.2.3(d)(3), 4.2.3(d)(5),4.2.3(d)(6), 4.2.3(g), 7.1, 7.3(b), 7.3(c), 7.3(c)(1), 7.3(c)(2),7.3(c)(3), 7.3(c)(4),7.3(c)(5), 7.3(c) (6),7.3(d), 7.3(e)

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
9.3(f)	La organización debe conservar información documentada	4.3.1(h), 7.1
10.1(a)	reaccionar ante la no conformidad…	Requerimiento nuevo
10.1(a)(1)	llevar a cabo acciones para controlarla y…	Requerimiento nuevo
10.1(a)(2)	hacer frente a las consecuencias,	Requerimiento nuevo
10.1(b)	evaluar la necesidad de acciones para eliminar…	8.2(c), 8.3(b)
10.1(b)(1)	la revisión de la no conformidad,	8.2(a)
10.1(b)(2)	la determinación de las causas de la no conformidad, y	8.2(b)
10.1(b)(3)	la determinación de si existen no conformidades…	8.3(a)
10.1(c)	implementar cualquier acción necesaria;	4.2.4(b), 8.2, 8.2(d)
10.1(d)	revisar la eficacia de las acciones correctivas…	8.2, 8.2(f)
10.1(e)	si es necesario, hacer cambios al sistema de gestión…	Requerimiento nuevo
10.1(e)	Las acciones correctivas deben ser adecuadas…	8.3
10.1(f)	la naturaleza de las no conformidades…	Requerimiento nuevo
10.1(g)	los resultados de cualquier acción correctivas.	8.2(e)
10.2	La organización debe mejorar de manera continua…	4.2.4(a), 4.2.4(b), 4.2.4(d), 5.2.1(f), 8.1

Fuente: BSI group. (2013).

ANEXO 3

INFORME DE ANÁLISIS DE BRECHA INICIAL DE REQUISITOS

ANEXO 3 INFORME DE ANÁLISIS DE BRECHA INICIAL DE REQUISITOS

1. Apéndices

Los apéndices detallan los requisitos evaluados durante el análisis de brecha inicial, los resultados y los gráficos de cumplimiento.

Apéndice 1 – Resultados.

Apéndice 2 – Gráficos de cumplimiento.

2. Valoración del Nivel de Cumplimiento de Requisitos

NIVELES DE CUMPLIMIENTO DE REQUISITOS		
DESCRIPCIÓN	**NIVEL DE CUMPLIMIENTO**	**DETALLE**
NO EXISTE	0	**No existe, 0% de ocurrencia** Sin evidencias del cumplimiento del requisito.
INICIO	1	**Inicio, aproximadamente 40% de ocurrencia.** La organización ha reconocido que los problemas existen y que necesitan ser tratados. Existen indicios del cumplimiento del requisito; sin embargo, no existe una evidencia de estos.
DESARROLLO	2	**En desarrollo, aproximadamente 70% de ocurrencia** Existe un gran avance en cuanto al cumplimiento del requisito y la evidencia de este; sin embargo, no se encuentra al 100%.
COMPLETO	3	**Se completó,100% de ocurrencia** Cumplimiento y evidencia del requisito al 100%.

A1. Apéndice 1 – Resultados

PREGUNTA		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
4. ENTORNO/CONTEXTO DE LA ORGANIZACIÓN							
4.1.	¿La organización analiza de manera periódica su entorno, en los aspectos que le puedan influir?	Alta dirección	Debido al escaso personal (en la sección administrativa) no se realiza una revisión periódica de los procesos de la empresa.	0			

PREGUNTA		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
4.2.	¿Se han analizado y definido cuáles son las "partes interesadas" de la organización?	Alta dirección	Se tiene identificadas las partes interesadas, pero estas no cumplen con sus funciones adecuadamente.		1		
4.2.	¿La organización identifica, analiza y actualiza información sobre las necesidades y expectativas de sus clientes, proveedores, empleados y otras partes interesadas relevantes al SGSI?	Alta dirección / Coordinadora de Calidad	Se identifica las necesidades de los clientes, proveedores y empleados, pero no se ha establecido una política de SGSI. Por ejemplo; no hay un control documentado de esta información.		1		
4.1.	¿La organización cuenta con una dirección estratégica, derivada de la información clave interna y externa?	Alta dirección	No cuentan.	0			
4.3.	¿La organización ha establecido el alcance del SGSI?	Alta dirección	Se tiene un documento generalizado en el cual no se detalle el alcance como indica el SGSI.		1		
4.4	¿La Organización establece, implementa, mantiene y mejora continuamente el SGSI?	Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
4. ENTORNO/CONTEXTO DE LA ORGANIZACIÓN - NIVEL DE APLICACIÓN →					**10%**		
5. LIDERAZGO							
5.1	¿La dirección revisa el cumplimiento de los objetivos de seguridad de la información para el desarrollo de la dirección estratégica en función de las necesidades detectadas?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
5.1	¿El equipo directivo asegura la integración de los requisitos del SGSI en los procesos de la organización?	Alta dirección	No, debido a la reciente organización para la implementación de la SGSI.	0			
5.1	¿El equipo directivo asegura que los recursos necesarios para el SGSI estén disponibles?	Alta dirección	No, debido a la escasez personal que cuenta la organización.	0			

PREGUNTA		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
5.1	¿El equipo directivo comunica la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del SGSI?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
5.1	¿El equipo directivo ha definido, actualiza y comunica la Política de Seguridad de la Información y asegura que ésta es accesible?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
5.1	¿El equipo Directivo asegura que el sistema de SGSI logre sus resultados previstos?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
5.1	¿El Equipo Directivo dirige y apoya a las personas para que contribuyan con la efectividad del SGSI?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
5.1	¿El equipo directivo promueve la mejora continua y apoya a otros roles relevantes para demostrar su liderazgo?	Alta dirección	No promueve una mejora continua, ahora está aplicando un coaching para toda la organización	0			
5.2	¿El equipo directivo ha establecido una política de seguridad de la información?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
5.3.	¿Se han definido y actualizado los roles, responsabilidades y autoridades relevantes a la seguridad de la información?	Alta dirección / Coordinadora de recursos humanos / Coordinadora de Calidad	Si, recientemente se ha realizado al acta de comité de seguridad de información, pero aún no han aplicado los roles que le correspondiente.		1		
5. LIDERAZGO - NIVEL DE APLICACIÓN →					**2%**		
6. PLANIFICACIÓN							
6.1.1.	¿El sistema de gestión de seguridad implantado incluye el análisis de riesgos por la actividad de la organización?	Coordinadora de Calidad	No se tiene, ya que no hay un análisis de riesgos y oportunidades	0			
6.1.2.	¿La organización define y aplica un proceso de valoración de riesgo de seguridad de la información?	Coordinadora de Calidad	No existe una matriz de riesgos	0			

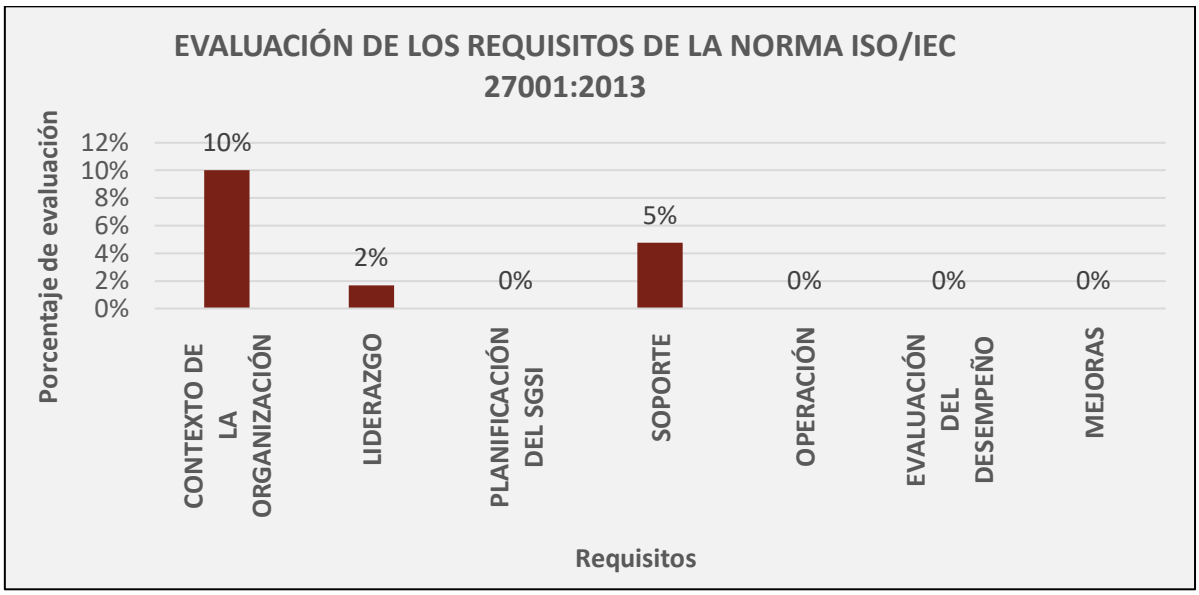
PREGUNTA		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
6.1.3	¿Existe un plan de tratamiento de riesgos por la actividad de la organización?	Coordinadora de Calidad	No existe una matriz de riesgos	0			
6.2	¿Se han definido y documentado los objetivos de Seguridad de la Información?	Alta dirección / Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
6.2	¿Se ha definido un plan de mejora enfocado al cumplimiento de objetivos?	Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
6. PLANIFICACIÓN - NIVEL DE APLICACIÓN →				**0%**			
7. SOPORTE							
7.1	¿La organización ha determinado y proporciona los recursos necesarios para gestionar el SGSI?	Alta dirección / Coordinadora de Calidad	Si se ha determinado los recursos que forman parte de la SGSI, pero aún no firman dicho acto.		1		
7.2.	¿Se realiza una evaluación y seguimiento del desempeño de las personas?	Líder de recursos humanos / Coordinadora de Calidad	No existe una evaluación de desempeño acerca de la seguridad de la información	0			
7.3.	¿El personal es consciente de la política de Seguridad de la Información, los objetivos, los beneficios del SGSI y la mejora?	Coordinadora de Calidad	No, ya que no existe una política de seguridad de información.	0			
7.4.	¿Se han definido cuáles son las comunicaciones internas y externas relevantes para el sistema de gestión de Seguridad de la Información?	Coordinadora de Calidad	No se han definido el canal de comunicación para el SGSI	0			
7.5.1.	¿Se ha documentado la información necesaria del SGSI para asegurar su efectividad?	Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
7.5.2.	¿Se asegura la identificación, descripción, formato y revisión de los documentos creados o actualizados?	Coordinadora de Calidad	Si hay un formato, si hay una revisión más no una identificación por parte de la alta dirección		1		

PREGUNTA		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
7.5.3.	¿Se controla que la información requerida para la gestión de seguridad esté protegida y disponible?	Coordinadora de Calidad	No se controla, en estos momentos toda información es visible	0			
7. SOPORTE - NIVEL DE APLICACIÓN →				**5%**			
8. OPERACIÓN							
8.1.	¿Existe una planificación, ejecución y control de los procesos del SGSI?	Alta dirección / Coordinadora de Calidad	No, porque los procesos no están formalizados por la alta gerencia.	0			
8.2.	¿Se realizan evaluaciones de riesgos de seguridad de la información en intervalos planificados o cuando se presentan cambios significativos?	Coordinadora de Calidad	No, solo se evalúa cuando hay alguna incidencia en la seguridad de información	0			
8.3.	¿La organización cuenta con un plan de tratamiento de riesgos?	Coordinadora de Calidad	No se cuenta con un plan de tratamiento de riesgos porque no se tiene identificado los riesgos aún	0			
8. OPERACIÓN - NIVEL DE APLICACIÓN →					**0%**		
9. EVALUACIÓN DEL DESEMPEÑO							
9.1	¿La organización hace seguimiento, medición, análisis y evaluación del SGSI?	Alta dirección / Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
9.2	¿La organización realiza auditorías internas a intervalos planificados	Alta dirección / Coordinadora de Calidad	No, porque recién se están levantando los procesos.	0			
9.2	¿La organización planifica, establece, implementa y mantiene un programa de auditorías?	Alta dirección / Coordinadora de Calidad	No cuenta con un plan de auditoria	0			
9.3	¿La dirección revisa el SGSI para asegurar su eficacia?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
9.3	¿La dirección toma decisiones y acciones en base a los resultados de la revisión del SGSI?	Alta dirección	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
9. EVALUACIÓN DEL DESEMPEÑO - NIVEL DE APLICACIÓN →					**0%**		

PREGUNTA		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
10. MEJORAS							
10.1.	¿La organización controla y corrige las NC?	Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
10.1.	¿La organización analiza las NC y adopta medidas para eliminar las causas (acciones correctivas)?	Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
10.2.	¿La organización mejora continuamente la conveniencia, adecuación y efectividad del SGSI?	Coordinadora de Calidad	No, debido que recién se está haciendo la implementación de manera adecuada.	0			
10. MEJORA - NIVEL DE APLICACIÓN →					**0%**		
SGC- ISO 27001:2013 - REQUISITOS - NIVEL DE APLICACIÓN →					**2%**		

A2. Apéndice 2 – Gráficos de Cumplimiento

Porcentajes de Cumplimiento Actual Detallado



ANEXO *4*

INFORME DE ANÁLISIS DE BRECHA INICIAL DE CONTROLES

ANEXO 4 INFORME DE ANÁLISIS DE BRECHA INICIAL DE CONTROLES

1. Apéndices

Los apéndices detallan los controles evaluados durante el análisis de brecha inicial, los resultados y los gráficos de cumplimiento.

Apéndice 1 – Resultados.

Apéndice 2 – Gráficos de cumplimiento.

2. Valoración del Nivel de Cumplimiento de Controles

Tabla de Aplicabilidad de Controles

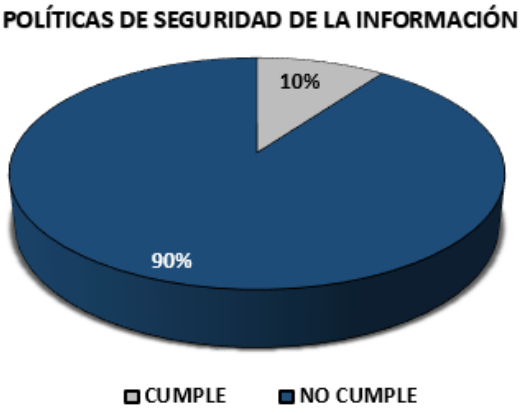
¿ES NECESARIO?	DESCRIPCIÓN	DETALLE
Sí	**APLICA**	El control sí es necesario para la organización
No	**NO APLICA**	El control no es necesario para la organización.

Nivel de Cumplimiento de Controles

DESCRIPCIÓN	PUNTAJE	PUNTUACIÓN	DETALLE
		Porcentual	
Completo	4	**100%**	El control está implementado, ha sido aprobado por la alta dirección y ha sido publicado (de ser necesario).
En proceso	3	**70%**	El desarrollo de control está en proceso de implementación.
Inicio	2	**40%**	Se ha identificado la necesidad del implementar un control. El control apenas está iniciando.
No existe	1	**0%**	El control está ausente, no existe.

A1. Apéndice 1 – Resultados

TÍTULO DE CONTROL		PREGUNTAS	¿ES NECESARIO?	RANGO				COMENTARIOS
				1	2	3	4	
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN								
A.5.1. DIRECCIÓN DE LA GERENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN								
A.5.1.1	**Políticas de seguridad de la información**	¿Existe un documento denominado Política de Seguridad de la información y que esté aprobado por la alta dirección?	SI	○	◉	○	○	Debido a que no hay un área de tecnología de información, creían que no era necesario alguna política de seguridad.
		¿Considera que los empleados conocen las políticas de seguridad de su organización?	SI	◉	○	○	○	Solo el personal administrativo maneja esa información
A.5.1.2	**Revisión de las políticas de seguridad de la información**	¿Su organización planifica intervalos de tiempo para la revisión de las políticas de seguridad de información?	SI	◉	○	○	○	Debido a que la política de seguridad no está bien establecida.
		Cuando se realizaron las revisiones de las políticas de seguridad de la información, ¿se evalúa la efectividad, adecuación y conveniencia de las políticas?	SI	◉	○	○	○	Debido a que solo se enfocaron en el control de acceso de usuario y no todo en general.



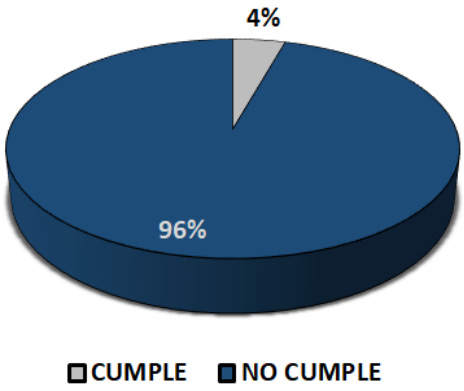
A.6 ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION								
A.6.1. ORGANIZACIÓN INTERNA								
A.6.1.1	**Roles y responsabilidades para la seguridad de la información**	¿Tienen definidos los roles que existen en la organización referentes a la seguridad de la información?	SI	◉	○	○	○	Se tiene establecido los roles en un organigrama, más no todas las funciones del comité de seguridad.
		¿Se han asignado responsabilidades a los roles de la organización referentes a la seguridad de la información?	SI	◉	○	○	○	Debido de que aún no se asignado esas responsabilidades
A.6.1.2	**Segregación de funciones**	¿La organización segregó algunas funciones a los roles en los activos de información?	SI	◉	○	○	○	Debido a que aún las funciones están en revisión
A.6.1.3	**Contacto con autoridades**	¿Existe un documento que indique cuales son las autoridades por contactar al momento que exista un incidente en la seguridad de la información?	SI	◉	○	○	○	No existe ese documento

A.6.1.4	**Contacto con grupos especiales de interés**	¿La organización tiene algún contacto con un grupo de interés que le asesoren con problemas de seguridad de información?	SI	◉	○	○	○	Se han buscado asesores, pero no han llegado a un acuerdo.
A.6.1.5	**Seguridad de la información en la gestión de proyectos**	¿La seguridad de la información se está integrando dentro del método de la gestión de proyectos de la organización?	SI	◉	○	○	○	Cuentan con un método más no están vinculando la seguridad de la información.
A.6.2 DISPOSITIVOS MOVILES Y TELETRABAJO								
A.6.2.1	**Política de dispositivos móviles**	¿Se usan medidas de seguridad contra los riesgos en los dispositivos móviles que pertenezcan a la organización?	SI	◉	○	○	○	No existe un control de seguridad para las apps de la organización.
A.6.2.2	**Teletrabajo**	¿Se usan medidas de seguridad con respecto a la información que se envía, recibe o almacena en el teletrabajo?	SI	◉	○	○	○	No existe medidas de seguridad respecto a la información compartida.

A.7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS								
A.7.1. ANTES DEL EMPLEO								
A.7.1.1	**Investigación de antecedentes**	¿Los encargados en la selección del personal verifican los antecedentes de los candidatos a empleados y contratistas para prevenir algún mal uso de la información de la organización (Ej. Referencias, DNI, comprobación del CV, etc.)?	SI	○	◉	○	○	Hace unas semanas se ha iniciado la validación de la información colocada en sus CV'S.
A.7.1.2	**Términos y condiciones del empleo**	¿Dentro del contrato se estipulan las responsabilidades del colaborador y la organización con respecto a la seguridad de la información?	SI	◉	○	○	○	Debido a que no está correctamente detallado en las cláusulas del contrato.
A.7.2. DURANTE EL EMPLEO								
A.7.2.1	**Responsabilidades de gestión**	¿La gerencia exige a los colaboradores y contratistas aplicar de seguridad de información de acuerdo con sus políticas y procedimientos establecidos?	SI	◉	○	○	○	No existe un documento o acuerdo que defina la aplicación de información.
A.7.2.2	**Conciencia, educación y capacitación sobre la seguridad de la información**	¿Los colaboradores han tenido alguna capacitación sobre la conciencia de la seguridad de la información?	SI	◉	○	○	○	No hay capacitaciones respecto a la seguridad de información

		¿Se comunican a los colaboradores las actualizaciones sobre políticas o procedimientos de seguridad de la información, según sea relevante para la función del trabajo que cumpla?	SI	◉	○	○	○	Debido que no se encuentra formalizada la política de seguridad de información.
A.7.2.3	**Proceso disciplinario**	¿La organización tiene algún proceso disciplinario formal para los colaboradores que hacen el mal uso de la información?	SI	◉	○	○	○	No tiene un proceso disciplinario
		¿Se ha comunicado este proceso disciplinario a los colaboradores?	SI	◉	○	○	○	Porque no tiene un proceso disciplinario
A.7.3. FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO								
A.7.3.1	**Responsabilidad antes la finalización o cambio**	¿Se definen y comunican las responsabilidades y obligaciones sobre la seguridad de la información que siguen vigentes después del cambio o finalización del empleo?	SI	◉	○	○	○	No se tiene definido ni comunicado las responsabilidades

SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS



A.8. GESTIÓN DE ACTIVOS

A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

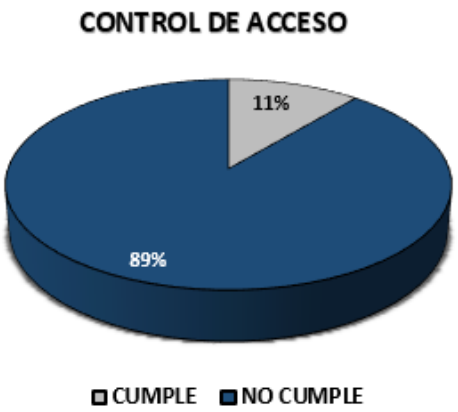
A.8.1.1	**Inventario de activos**	¿Se tienen identificados y documentados los activos de la información relevantes?	SI	◉	○	○	○	No se tiene identificado y documentado los activos.
A.8.1.2	**Propiedad de los activos**	¿Se tiene algún registro con los propietarios que manejan los activos de la información en la organización?	SI	○	◉	○	○	No se tiene.
A.8.1.3	**Uso aceptable de los activos**	¿Se han establecido, documentado e implantado reglas para asegurar el buen uso de los activos de información?	SI	◉	○	○	○	No, todavía.
A.8.1.4	**Devolución de activos**	¿Cuentan con algún documento en donde se especifique los activos de la información y activos que se usaron durante el trabajo?	SI	◉	○	○	○	No, todavía.

		¿Tienen algún documento formal (proceso de desvinculación) que asegure la devolución del activo físico o electrónico que sea de propiedad de la organización?	SI	○	◉	○	○	Hace una semana se ha iniciado con el proceso de desvinculación del personal que implica devolución de activos.
A.8.2. CLASIFICACIÓN DE LA INFORMACIÓN								
A.8.2.1	**Clasificación de la Información**	¿La empresa tiene clasificada su información según su importancia de revelación?	SI	◉	○	○	○	No existe
A.8.2.2	**Etiquetado de Información**	¿Usan un manual de procedimientos para etiquetar la información?	SI	◉	○	○	○	No tienen.
A.8.2.3	**Manipulado de la información**	¿Existe algún manual para manejar la información?	SI	◉	○	○	○	No tienen.
A.8.3. MANIPULACIÓN DE LOS SOPORTES								
A.8.3.1	**Gestión de medios removibles**	¿Se tiene documentado un procedimiento para la gestión de medios removibles?	SI	◉	○	○	○	No tienen.
A.8.3.2	**Disposición de medios**	¿Tienen algún procedimiento formal en donde destruyen o eliminan la información de los medios electrónicos de la organización?	SI	◉	○	○	○	No tienen.
A.8.3.3	**Transferencia de medios físicos**	¿Existe alguna medida de seguridad para el uso de equipos físicos fuera o dentro de la empresa?	SI	○	◉	○	○	Se tiene un formato de entregas de materiales de trabajo.

A.9. CONTROL DE ACCESO								
A.9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO								
A.9.1.1	**Política de control de acceso**	¿Existen políticas en la organización de control de accesos con respecto a las necesidades de seguridad y negocio de la organización?	SI	○	◉	○	○	Se tiene solo para el control de acceso que se tienen con los clientes.
A.9.1.2	**Acceso a redes y servicios de red**	¿Controlan los servicios de red en los usuarios en la organización?	SI	◉	○	○	○	No tienen.
A.9.2. GESTIÓN DE ACCESO DE USUARIO								
A.9.2.1	**Registro y baja de usuarios**	¿Existe algún proceso formal que permita el registro y la baja de usuarios para permitir la asignación de accesos?	SI	◉	○	○	○	No se tiene un proceso formal, solo es actuado.
A.9.2.2	**Aprovisionamiento de acceso a usuario**	¿Se utiliza algún sistema que permita el ingreso y eliminación de los usuarios?	SI	○	◉	○	○	Se tiene en el mismo Google en la parte de administrador.
A.9.2.3	**Gestión de privilegios de acceso**	¿Se tiene algún control del uso de accesos privilegiados?	SI	◉	○	○	○	No tienen

A.9.2.4	**Gestión de la información secreta de autentificación de los usuarios**	¿Se tienen políticas para la creación de las contraseñas?	SI	◉	○	○	○	No tienen
A.9.2.5	**Revisión de derechos de acceso de usuarios**	¿El monitoreo de los accesos de los usuarios son realizados en la organización?	SI	○	◉	○	○	Se tiene un control de monitoreo respecto a los clientes más no interno de la organización.
A.9.2.6	**Retirada o reasignación de los derechos de acceso**	¿Existe algún contrato o acuerdo que permita la exclusión al acceso de información a todos los empleados?	SI	◉	○	○	○	No tienen
A.9.3. RESPONSABILIDADES DE LOS USUARIOS								
A.9.3.1	**Uso de información secreta de autentificación secreta**	¿La organización presenta algún acuerdo que permita que el uso de la información sea secreta?	SI	◉	○	○	○	Solo se tiene un acuerdo por parte de nuestros clientes más no interno de la organización.
A.9.4. CONTROL DE ACCESO A SISTEMA Y APLICACIÓN								
A.9.4.1	**Restricción de acceso a la información**	¿La organización restringe el acceso a la información relevante?	NO	◉	○	○	○	No aplica
A.9.4.2	**Procedimientos de ingreso seguro**	¿Existe algún procedimiento de ingreso seguro en la organización para el acceso a los sistemas de forma segura?	NO	◉	○	○	○	No aplica
A.9.4.3	**Sistema de gestión de contraseñas**	¿Cuentan con un sistema de gestión en donde puedan establecer las contraseñas de manera segura y robustas?	NO	◉	○	○	○	No aplica

A.9.4.4	**Uso de programas utilitarios privilegiados**	¿Se restringe o controla rigurosamente el uso de utilidades que puedan invalidar los controles del sistema?	NO	◉	○	○	○	No aplica
A.9.4.5	**Control de acceso al código fuente de los programas**	¿Existe código fuente del cual no se permita poder manipular dentro de la organización, o sea que sea restringido?	NO	◉	○	○	○	No aplica



A.10. CRIPTOGRAFÍA								
A.10.1 CONTROLES CRIPTOGRÁFICOS								
A.10.1.1	**Política de uso de los controles criptográficos**	¿La organización cuenta con una política sobre el uso de controles criptográficos para la protección de la información?	NO	◉	○	○	○	No aplica
A.10.1.2	**Gestión de claves**	¿Se cuenta con especialistas para determinar el nivel apropiado de protección?	NO	◉	○	○	○	No aplica

A.11. SEGURIDAD FISICA Y AMBIENTAL								
A.11.1. ÁREAS SEGURAS								
A.11.1.1	**Perímetro de Seguridad Física**	¿Aseguran los perímetros de seguridad en las áreas de información sensible, será suficiente para controlar el riesgo de pérdida y/robo de información?	NO	◉	○	○	○	No aplica
A.11.1.2	**Controles de Ingreso Físico**	¿Detectan el acceso no autorizado, es decir aplicar algún medio de autenticación únicamente a personal autorizado?	SI	◉	○	○	○	No tienen
A.11.1.3	**Asegurar oficinas, áreas e instalaciones**	¿Previenen filtraciones en las oficinas, despachos y recursos, es decir se evita el acceso al público en general para prevenir cualquier pérdida y/robo de información?	SI	◉	○	○	○	No tienen
A.11.1.4	**Protección contra amenazas externas y ambientales**	¿Establecen las políticas contra las amenazas externas y ambientales?	SI	◉	○	○	○	No tienen.
A.11.1.5	**Trabajo en áreas Seguras**	¿Es seguro el área de trabajo de la organización?	NO	◉	○	○	○	No aplica
A.11.1.6	**Áreas de despacho y carga**	¿La organización cuenta con áreas de carga y descarga?	NO	◉	○	○	○	No aplica
A.11.2. SEGURIDAD DE EQUIPOS								

A.11.2.1	**Emplazamiento y protección de los equipos**	¿Considera importante el emplazamiento y la protección de equipos?	NO	◉	○	○	○	No aplica
A.11.2.2	**Servicio de suministro**	¿Se inspeccionan las instalaciones de suministros para su bien funcionamiento de la organización?	SI	◉	○	○	○	No se inspeccionan
A.11.2.3	**Seguridad del cableado**	¿Tienen disponibilidad de los servicios de cableado eléctrico y telecomunicaciones de forma segura en la organización?	SI	◉	○	○	○	Si pero para los equipos.
A.11.2.4	**Mantenimiento de equipos**	¿Realizan periódicamente mantenimientos de equipos?	SI	○	◉	○	○	Se inició en mandar a mantenimiento los equipos.
A.11.2.5	**Remoción de equipos**	¿Se realiza una buena logística en la seguridad de los equipos fuera de la organización?	SI	◉	○	○	○	No se realizan
A.11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**	¿Cuentan con un plan de seguridad con los activos que se encuentran fueras de las instalaciones?	SI	◉	○	○	○	No tienen
A.11.2.7	**Disposición o reutilización segura de equipos**	¿Cuenta con una reutilización o eliminación segura de equipos?	SI	◉	○	○	○	No tienen
A.11.2.8	**Equipos de usuario desatendidos**	¿Hay medidas de seguridad cuando el equipo es desatendido?	SI	○	◉	○	○	Se inició en que deben bloquear los equipos cuando no estén en uso

A.11.2.9	**Política de escritorio limpio y pantalla limpia**	¿Se cumplen políticas de puesto de trabajo despejado y pantalla limpia?	SI	◉	○	○	○	No cumplen

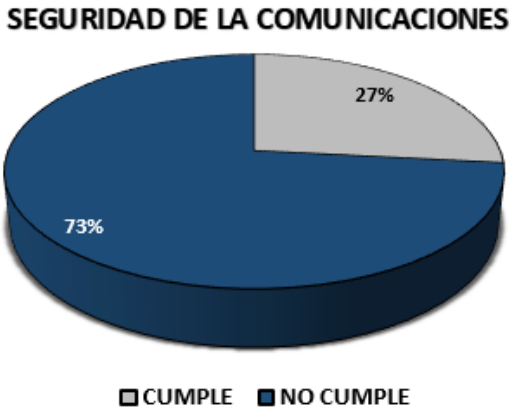
A.12 SEGURIDAD DE LAS OPERACIONES								
A.12.1.1	**Procedimientos operativos documentados**	¿Se tienen documentado los procedimientos de operación?	SI	◉	○	○	○	Solo se tiene aún el flujo y está en proceso.
		¿Estos procedimientos se tienen a disposición de los usuarios que los necesiten?	SI	◉	○	○	○	No lo tienen
A.12.1.2	**Gestión del cambio**	¿Se tiene alguna herramienta para controlar los cambios de los sistemas de procesamiento de información?	SI	◉	○	○	○	No lo tienen.
A.12.1.3	**Gestión de la capacidad**	¿Monitorea el uso de recursos de la organización?	NO	◉	○	○	○	Todo es manualmente.
A.12.1.4	**Separación de los entornos de desarrollo, pruebas y operaciones**	¿La organización tiene entornos de desarrollo, pruebas y operación?	NO	◉	○	○	○	No aplica porque no se está desarrollando software.

A.12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS								
A.12.2.1	**Controles contra códigos maliciosos**	¿Se tiene un software para protegerse de las amenazas cibernéticas?	SI	○	◉	○	○	Se limita el uso de licencias de antivirus solo al personal de alto uso de información.
A.12.3. RESPALDO								
A.12.3.1	**Respaldo de la información**	¿Se realiza de forma automática o manual el back up de la información?	SI	◉	○	○	○	Se realizan el back up de información cuando se realiza la desvinculación del personal.
A.12.4. REGISTROS Y MONITOREO								
A.12.4.1	**Registro de eventos**	¿Se revisa periódicamente los registros relacionados con eventos de actividad del usuario?	NO	◉	○	○	○	No aplica
A.12.4.2	**Protección de información de registros**	¿Cuentan con un servidor de respaldo de la información de toda la organización?	NO	◉	○	○	○	No aplica
A.12.4.3	**Registros del administrador y del operador**	¿Se cuenta con un sistema de actividad de intrusos?	NO	◉	○	○	○	No aplica
A.12.4.4	**Sincronización de reloj**	¿Se tiene un servidor establecido para la sincronización de relojes en los sistemas de la organización?	NO	◉	○	○	○	No aplica
A.12.1. CONTROL DEL SOFTWARE OPERACIONAL								
A.12.5.1	**Instalación de software en sistemas operacionales**	¿Tienen procedimiento que se deben implementar para controlar la instalación de software en sistemas operacionales?	NO	◉	○	○	○	No aplica.

A.12.6. GESTION DE VULNERABILIDAD TECNICA								
A.12.6.1	**Gestión de vulnerabilidades técnicas**	¿Se cuenta con un registro, control y monitoreo de vulnerabilidadde los activos de información?	SI	◉	○	○	○	No se tiene.
A.12.6.2	**Restricción en la instalación de software**	¿Se cuenta con procedimiento de control y monitoreo de uso de software instalado?	SI	◉	○	○	○	No cuentan.
A.12.7. CONSIDERACIONES PARA LA AUDITORIA DE LOS SISTEMA DE INFORMACION								
A.12.7.1	**Controles de auditoria de sistemas de información**	¿Se tiene un registro de auditoría de sistemas de información?	NO	◉	○	○	○	No aplica

A.13. SEGURIDAD DE LA COMUNICACIONES								
A.13.1. GESTION DE SEGURIDAD DE LA RED								
A.13.1.1	**Controles de la red**	¿Las redes de la organización son gestionadas y controladas?	NO	◉	○	○	○	No aplica.
A.13.1.2	**Seguridad de servicios de red**	¿Los servicios de red se gestionan internamente o es tercerizado?	NO	◉	○	○	○	No aplica.

A.13.1.3	**Segregación en redes**	¿Tienen segregada la red? ¿Cómo está planificado la segregación de red?	NO	◉	○	○	○	No aplica.
A.13.2. TRANSFERENCIA DE INFORMACIÓN								
A.13.2.1	**Políticas y procedimientos de transferencia de la información**	¿Se tiene establecido las políticas o procedimientos para el intercambio de información?	NO	◉	○	○	○	No aplica.
A.13.2.2	**Acuerdo sobre transferencia de información**	¿Se tienen acuerdos de intercambio de información de la organización con entidades externas? ¿Con todas las identidades se maneja el mismo procedimiento?	SI	◉	○	○	○	No tienen
A.13.2.3	**Mensajes electrónicos**	¿Se tiene un sistema para la protección de mensajes electrónicos sospechosos?	SI	○	◉	○	○	Se tiene el antivirus Avast, pero no lo gestionan adecuadamente.
A.13.2.4	**Acuerdos de confidencialidad o no divulgación**	¿Usan algún documento de requisitos para los acuerdos de confidencialidad?	SI	○	◉	○	○	Las políticas hacen mención a las leyes gubernamentales relacionadas a las telecomunicaciones.



A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN								
A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN								
A.14.1.1	**Análisis de requisitos y especificaciones de seguridad de la información**	¿Existen un análisis de los requisitos de seguridad de la información para nuevos sistemas o mejoras a los existentes?	NO	◉	○	○	○	No aplica.
A.14.1.2	**Asegurar los de servicios de aplicaciones en redes públicas**	Ante un eventual ataque a las redes, ¿poseen algún tipo de seguridad para protegerlas ante fraudes o robo de información?	NO	◉	○	○	○	No aplica.
A.14.1.3	**Protección de transacciones en servicios de aplicaciones**	Si al momento de transferir información se perdieran datos, ¿Se tiene algún plan de aseguramiento para que los datos no se pierdan?	NO	◉	○	○	○	No aplica.
A.14.2. SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE								
A.14.2.1	**Política de desarrollo seguro**	¿Cuentan con políticas la organización para el desarrollo de software / sistemas?	NO	◉	○	○	○	No aplica.
A.14.2.2	**Procedimientos de control de cambios del sistema**	¿Toman en cuenta las políticas que tiene la organización al realizar ambos a lo largo de ciclo de vida del desarrollo del software / sistemas?	NO	◉	○	○	○	No aplica.

A.14.2.3	**Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo**	¿Se realiza la revisión técnica de aplicaciones críticas para el negocio?	NO	◉	○	○	○	No aplica.
A.14.2.4	**Restricciones sobre cambios a los paquetes de software**	¿Cuentan con control de acceso al modificar el código fuente de los paquetes de software?	NO	◉	○	○	○	No aplica.
A.14.2.5	**Principios de ingeniería de sistemas seguros**	¿Establecen procedimientos de ingeniería de sistemas de información?	NO	◉	○	○	○	No aplica.
A.14.2.6	**Entorno de desarrollo seguro**	¿Se realiza la protección del ambiente de desarrollo para la integración de sistemas?	NO	◉	○	○	○	No aplica.
A.14.2.7	**Externalización del desarrollo de software**	¿Se realiza monitoreo a los sistemas contratados externamente?	NO	◉	○	○	○	No aplica.
A.14.2.8	**Pruebas funcionales de la seguridad de sistemas**	¿Se realizan las pruebas necesarias de la seguridad del sistema durante el desarrollo?	NO	◉	○	○	○	No aplica.
A.14.2.9	**Pruebas de aceptación del Sistemas**	¿Realizan algún tipo de plan de pruebas de aceptación para los sistemas?	NO	◉	○	○	○	No aplica.
A.14.3. DATOS DE PRUEBA								
A.14.3.1	**Protección de datos de prueba**	¿Se protege los datos de prueba?	NO	◉	○	○	○	No aplica.

A.15. RELACION CON LOS PROVEEDORES								
A.15.1. SEGURIDAD EN LAS RELACIONES CON PROVEEDORES								
A.15.1.1	**Política de seguridad de la información en las relaciones con los proveedores**	¿Se realizan políticas de seguridad de la información por parte del proveedor hacia los activos que la organización posee?	SI	◉	○	○	○	No se realiza
A.15.1.2	**Requisitos de seguridad en contratos con terceros**	¿Establece los requisitos de seguridad de la información con los proveedores acerca de la infraestructura de TI?	SI	◉	○	○	○	No se establecen
A.15.1.3	**Cadena de suministro de tecnología de la información y de las comunicaciones**	¿Los acuerdos con los proveedores incluyen requisitos para abordar los riesgos de la seguridad de la información?	SI	◉	○	○	○	No se tiene acuerdos con respecto a la seguridad de la información
A.15.2. GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR								
A.15.2.1	**Control y revisión de la provisión de servicios del proveedor**	¿Se monitorea y/o audita la entrega de servicios por parte de los proveedores?	NO	○	◉	○	○	No aplica
A.15.2.2	**Gestión de cambios en la provisión del servicio del proveedor**	¿Cuentan con un control ante la gestión de los cambios de provisión por parte de los proveedores?	NO	◉	○	○	○	No aplica

A.16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN								
A.16.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS								
A.16.1.1	**Responsabilidades y procedimientos**	¿Cuentan con una gestión de responsabilidades y procedimientos para los incidentes de seguridad de la información?	SI	◉	○	○	○	No cuentan
A.16.1.2	**Notificación de los eventos de seguridad de la información**	¿Se realizan reportes sobre los eventos de seguridad de la información?	SI	◉	○	○	○	No realizan
A.16.1.3	**Notificación de puntos débiles de la seguridad**	¿Se realizan reportes sobre las debilidades de seguridad de la información?	SI	◉	○	○	○	No realizan
A.16.1.4	**Evaluación y decisión sobre los eventos de seguridad de la información**	¿Realiza evaluaciones sobre incidentes de seguridad de la información?	SI	◉	○	○	○	No realizan
A.16.1.5	**Respuesta a incidentes de seguridad de la información**	¿Se responden a los incidentes de seguridad de la información de la organización?	SI	◉	○	○	○	No se responden
A.16.1.6	**Aprendizaje de los incidentes de seguridad de la información**	¿Resuelve los incidentes con los conocimientos adquiridos?	SI	◉	○	○	○	No se resuelven

A.16.1.7	**Recolección de evidencias**	¿Realiza con frecuencia la recolección de evidencia y recolección de información?	SI	◉	○	○	○	No se recoleccionan

A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE CONTINUIDAD DEL NEGOCIO								
A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN								
A.17.1.1	**Planificación de continuidad de seguridad de la información**	¿Cuentan con un plan en el cual determina los requisitos de seguridad de la información?	SI	○	◉	○	○	SÍ, está dentro de las políticas de seguridad de información.
A.17.1.2	**Implementación de continuidad de seguridad de la información**	¿La organización cuenta con documentación, la cual busca implementar procesos, procedimientos y controles para asegurar la continuidad de la seguridad de la información?	SI	◉	○	○	○	No cuentan
A.17.1.3	**Verificación, revisión y evaluación de continuidad de seguridad de la información**	¿Se realiza una verificación, revisión y evaluación de los controles de continuidad de seguridad de la información?	SI	◉	○	○	○	No se realizan

A.17.2. REDUNDANCIAS								
A.17.2.1	**Instalación de procesamiento de la información**	¿Existe un plan para asegurar la disponibilidad de la información?	NO	◉	○	○	○	No aplica

A.18. CUMPLIMIENTO								
A.18.1. CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES								
A.18.1.1	**Identificación de requisitos contractuales y de legislación aplicables**	¿Cuentan con requerimientos estatutarios, regulatorios y contractuales?	SI	◉	○	○	○	No se cuentan
A.18.1.2	**Derechos de propiedad intelectual DPI**	¿Al implementar los procedimientos cuenta con el cumplimiento de los requisitos legislativos, normativos y contractuales?	NO	◉	○	○	○	No aplica
		¿La organización tiene procedimientos para asegurar la protección de la propiedad intelectual?	NO	◉	○	○	○	No aplica
		¿Se adquiere software de fuentes conocidas y de buena reputación?	NO	○	◉	○	○	No aplica

A.18.1.3	**Protección de registros**	¿Tienen un plan en donde protegen los registros de la organización contra pérdidas, falsificación y publicaciones no autorizadas?	SI	◉	○	○	○	No tienen
A.18.1.4	**Privacidad y protección de datos personales**	¿Existe un control para asegurar la protección de la data y privacidad de información personal?	SI	◉	○	○	○	No existe
A.18.1.5	**Regulación de controles criptográficos**	¿La organización utiliza un control de cifrado de la información para verificar el cumplimiento con los acuerdos, legislación y normativas que se emplean?	NO	◉	○	○	○	No aplica
A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES								
A.18.2.1	**Revisión independiente de la seguridad de la información**	¿Existen una revisión independiente de la seguridad de la información?	SI	◉	○	○	○	No realizan revisiones
A.18.2.2	**Cumplimiento de políticas y normas de seguridad**	¿Se ha identificado las causas de incumplimiento de las políticas y normas de seguridad en la organización?	SI	○	◉	○	○	Se dio inicio debido que no se encuentran correctamente establecidas.
A.18.2.3	**Revisión del cumplimiento técnico**	¿Se han realizado pruebas de penetración y vulnerabilidad?	NO	◉	○	○	○	No aplica

A2. Apéndice 2 – Gráfico de Cumplimiento

Cuadro Porcentaje de Cumplimiento por Dominios

N°	DOMINIOS EVALUDOS SEGÚN ISO 27002	ANALISIS DE BRECHA INICIAL	
A.5	Políticas de seguridad de la información	**10%**	**Inicio**
A.6	Organización de la seguridad de la información	**0%**	**No existe**
A.7	Seguridad de los recursos humanos	**4%**	**Inicio**
A.8	Gestión de activos	**10%**	**Inicio**
A.9	Control de acceso	**11%**	**Inicio**
A.10	Criptografía	**0**	**No aplica**
A.11	Seguridad física y ambiental	**5%**	**Inicio**
A.12	Seguridad de las operaciones	**10%**	**Inicio**
A.13	Seguridad de las comunicaciones	**27%**	**Inicio**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	**0**	**No aplica**
A.15	Relación con los proveedores	**0%**	**No existe**
A.16	Gestión de Incidentes de seguridad de la información	**0%**	**No existe**
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	**13%**	**Inicio**
A.18	Cumplimiento	**20%**	**Inicio**

Histograma de Cumplimiento por Dominios

Gráfico Pastel del Cumplimiento General de los Controles

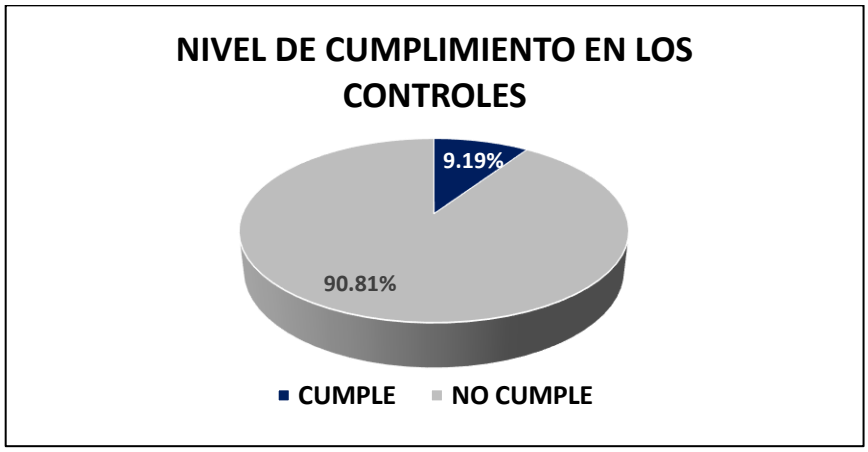
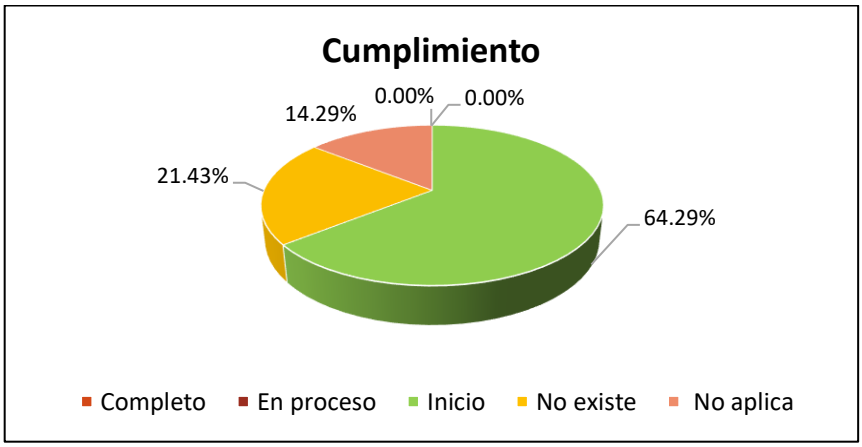


Gráfico Pastel de Nivel de Aplicación y Cumplimiento



ANEXO 5 ACTA DE REUNIÓN

Tema:	DESARROLLO DE LOS ANÁLISIS DE BRECHA DE CONTROLES Y REQUISITOS.		
Lugar:	CALLE GENERAL VARELA 356, MIRAFLORES.		
Fecha:	14/03/18		
Hora de Inicio:	06:00 p.m.	**Hora de fin:**	08:00 P.M.
CARGO		**FIRMA**	
COORDINADORA DE CALIDAD			
COORDINADORA DE RR. HH / LOGISTICA			
ANALISTA DE SEGURIDAD DE INF.			
JEFE DE PROYECTO DEL SGSI			

TEMAS TRATADOS

* ANÁLISIS DE BRECHA INICIAL DE REQUISITOS
- Se ha respondido el cuestionario de análisis de brecha.
- Se identificaron bajos niveles de cumplimiento, en general tiene un 2% de cumplimiento.
- Se requiere elevar el porcentaje del cumplimiento.
- El contexto de la organización y soporte tienen el porcentaje más alto, pero aún así es insuficiente.

* ANÁLISIS DE BRECHA INICIAL DE CONTROLES
- Se ha respondido al cuestionario de análisis de brecha.
- Aquí también se identificó un porcentaje bajo en cumplimiento de controles, en general es de un 9.25%.
- Se identificaron que controles son aplicables (necesarios) y cuales no lo son. Todo esto, de forma general y sujeto a cambios.
- Se requiere implementar los controles de activos que sean prioritarios y paulatinamente todos los necesarios.

ANEXO 6 ACTA DE COMPROMISO DE LA ALTA DIRECCIÓN

ACTA DE COMPROMISO DE LA ALTA DIRECCIÓN PARA LA IMPLEMENTACIÓN DE LA NORMA ISO 27001:2013 – SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI)

En mi calidad de Gerente general, junto al Gerente de Administración, manifiesto nuestro compromiso y respaldo a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), en cumplimiento de la ISO 27001:2013 en VF CONSULTING S.A.C.

Para dicho fin nos comprometemos a:

- Asignar los recursos necesarios para la implementación del SGSI.
- Realizar reuniones periódicas para verificar que la política seguridad y los objetivos de la seguridad de información estén alineados con la dirección estratégica de la organización.
- Realizar reuniones para identificar oportunidades de mejora en el SGSI
- Verificar que los requisitos del SGSI están integrados en los procesos pertinentes de la organización mediante reuniones.
- Comunicar la importancia de la Gestión de la información mediante correos y reuniones.
- Garantizar que el SGSI va a lograr alcanzar los resultados previstos mediante un seguimiento continuo.
- Apoyar a otros roles relevantes de gestión para demostrar su liderazgo aplicado a sus áreas de responsabilidad mediante capacitaciones.
- Motivar al personal para que contribuyan con la efectividad de la implementación del SGSI.

Firman en señal de conformidad, en la ciudad de Lima, a los 19 días del mes de MARZO del 2018.

GERENTE GENERAL

GERENTE DE ADMINISTRACIÓN

ANEXO *7*

PROPUESTA COMERCIAL DEL PROYECTO

ANEXO 7 PROPUESTA COMERCIAL DEL PROYECTO

1. OBJETIVO DE LA PROPUESTA

El objetivo de la propuesta es de implementar un Sistema de Gestión de la Seguridad de Información en VF CONSULTING S.A.C., bajo la norma ISO/IEC 27001:2013.

2. VALIDEZ DE LA PROPUESTA

La presente propuesta tiene una validez de 10 días calendario desde que se fue presentado al cliente.

3. ALCANCE DEL PROYECTO

Se ha definido que el Sistema de Gestión de Seguridad de la Información (SGSI) tiene como alcance el proceso de "Prestación de servicios" en las instalaciones de la sede Miraflores de la empresa VF CONSULTING S.A.C incluyendo los procesos de interacción y soporte según establece la ISO/IEC 27001:2013 como requisito.

4. ALCANCE NO CONTEMPLADO

En este proyecto no se contemplará los siguientes procesos:

- Desarrollo de aplicaciones
- Gestión contable (Pertenece a el área administrativa)

Debido de que estos procesos no interactúan con el proceso core de la empresa.

5. PROPUESTA DE SOLUCIÓN

La solución que se propone para la implementación de SGSI es usar la metodología del Ciclo de Deming o mejora continua PDCA (planear, hacer, verificar y actuar) de la norma ISO 27001.

Se dividirá por fases y cada una de ellas tendrá actividades que contemplen los documentos requisitos de la SGSI.

Los beneficios que aporta al implementar el Sistema de Gestión de la Seguridad de Información en una empresa son los siguientes:

- Permiten ofrecer servicios y productos más seguros y confiables a los clientes.
- Reducción de riesgo de pérdida o robo de información.
- Los riesgos y controles son continuamente revisados.
- Confianza de clientes y socios estratégicos.
- Posibilidad de integrarse con otros sistemas de gestión como la ISO/IEC 9001, ISO/IEC 14001, entre otros.
- Confianza y reglas claras para los colaboradores de la organización
- Reducción de costo y mejora de procesos y servicios.
- Genera un valor agregado a la organización y con ello mejora la imagen organizacional.

6. EQUIPO DE TRABAJO

La siguiente tabla muestra la organización propuesta para este proyecto. Los recursos asignados para la implementación del SGSI, son los siguientes:

Equipo de trabajo	Cantidad	Dedicación
Coordinadora de Calidad	1	50%
Coordinadora de RR. HH.	1	50%
Analista de Seguridad de Información	1	100%
Jefe de proyecto	1	100%

Tabla 1. Equipo de trabajo
Fuente: Elaboración de los autores

7. TIEMPO ESTIMADO DEL PROYECTO

El tiempo estimado es de 170 días de trabajo en total.

	PROYECTO - IMPLEMENTACIÓN DE LA ISO/IEC 27001	170 días	lun 12/03/18	mar 25/09/18		RECURSOS
	FASE 1 – PLANEAR	**39 días**	**lun 12/03/18**	**mié 25/04/18**		
3	**Realizar el análisis de brecha inicial**	**4 días**	**lun 12/03/18**	**jue 15/03/18**		
4	Realizar cuestionario de análisis de brecha	2 días	lun 12/03/18	mar 13/03/18		ASI
5	Responder cuestionario de análisis de brecha	2 días	mié 14/03/18	jue 15/03/18	4	JP, ASI, CC, CRRHH
6	Informe de análisis de brecha inicial	0 días	jue 15/03/18	jue 15/03/18	5	JP, ASI
7	**Compromiso con la alta dirección**	**3 días**	**vie 16/03/18**	**lun 19/03/18**		
8	Realizar una propuesta del proyecto	2 días	vie 16/03/18	sáb 17/03/18	6	JP
9	Realizar acta de compromiso de la alta dirección	1 día	vie 16/03/18	vie 16/03/18	6	ASI
10	Revisión de la alta dirección	1 día	lun 19/03/18	lun 19/03/18	8,9	ASI, JP
11	Acta de compromiso de la alta dirección	0 días	lun 19/03/18	lun 19/03/18	10	ASI
12	Propuesta comercial del proyecto	0 días	lun 19/03/18	lun 19/03/18	10	JP
13	**Comprender el contexto de la organización**	**2 días**	**mar 20/03/18**	**mié 21/03/18**		
14	Análisis del contexto de la organización	1 día	mar 20/03/18	mar 20/03/18	12	ASI, JP

	PROYECTO - IMPLEMENTACIÓN DE LA ISO/IEC 27001	170 días	lun 12/03/18	mar 25/09/18		RECURSOS
15	Realizar informe de contexto de la organización	1 día	mié 21/03/18	mié 21/03/18	14	ASI, JP
16	Informe del contexto de la organización	0 días	mié 21/03/18	mié 21/03/18	15	ASI, JP
17	**Comprender necesidades y expectativas**	**2 días**	**jue 22/03/18**	**vie 23/03/18**		
18	Reunión para evaluar las necesidades y expectativas	1 día	jue 22/03/18	jue 22/03/18	16	ASI, CRRHH, CC, JP
19	Análisis de necesidades y expectativas	1 día	vie 23/03/18	vie 23/03/18	18	ASI, JP
20	Informe de necesidades y expectativas de las partes interesadas	0 días	vie 23/03/18	vie 23/03/18	19	ASI, JP
21	**Determinar el alcance del SGSI**	**2 días**	**sáb 24/03/18**	**lun 26/03/18**		
22	Evaluar el alcance del SGSI	1 día	sáb 24/03/18	sáb 24/03/18	16,20	ASI
23	Revisión de la Alta Dirección	1 día	lun 26/03/18	lun 26/03/18	22	ASI, JP
24	Declaración del alcance del SGSI	0 días	lun 26/03/18	lun 26/03/18	23	ASI, JP
25	**Determinar política de seguridad de la información**	**3 días**	**mar 27/03/18**	**jue 29/03/18**		
26	Desarrollo de la política de seguridad de la información	2 días	mar 27/03/18	mié 28/03/18	16,20,23	ASI, JP
27	Revisión de la Alta Dirección	1 día	jue 29/03/18	jue 29/03/18	26	ASI, JP
28	Política de seguridad de la información	0 días	jue 29/03/18	jue 29/03/18	27	ASI, JP
29	**Actualizar manual de organización y funciones (ficha de puesto)**	**3 días**	**vie 30/03/18**	**lun 02/04/18**		
30	Identificar roles y responsabilidades para la seguridad de la información	2 días	vie 30/03/18	sáb 31/03/18	28	ASI, JP
31	Elaborar ficha de puesto para roles de la seguridad de la información	1 día	lun 02/04/18	lun 02/04/18	30	ASI, JP
32	Ficha de puesto para los roles de seguridad de la información	0 días	lun 02/04/18	lun 02/04/18	31	ASI, JP
33	**Establecer procedimiento de control de documentación**	**3 días**	**mar 27/03/18**	**jue 29/03/18**		
34	Desarrollo de procedimiento de control de documentación	3 días	mar 27/03/18	jue 29/03/18	24	ASI, JP
35	Procedimiento de control de documentación	0 días	jue 29/03/18	jue 29/03/18	34	ASI, JP
36	**Establecer procedimiento de evaluación y tratamiento de riesgos**	**2 días**	**vie 30/03/18**	**sáb 31/03/18**		
37	Desarrollo de procedimiento de evaluación y tratamiento de riesgos	2 días	vie 30/03/18	sáb 31/03/18	35	ASI, JP
38	Procedimiento de evaluación y tratamiento de riesgos	0 días	sáb 31/03/18	sáb 31/03/18	37	ASI, JP
39	**Establecer procedimiento de gestión de incidentes**	**2 días**	**vie 30/03/18**	**sáb 31/03/18**		
40	Desarrollo de procedimiento de gestión de incidentes	2 días	vie 30/03/18	sáb 31/03/18	35	ASI, JP
41	Procedimiento de gestión de incidentes	0 días	sáb 31/03/18	sáb 31/03/18	40	ASI, JP
42	**Establecer procedimiento de auditoria interna**	**2 días**	**vie 30/03/18**	**sáb 31/03/18**		
43	Desarrollo del procedimiento de auditoria interna	2 días	vie 30/03/18	sáb 31/03/18	35	ASI, JP
44	Procedimiento de auditoria interna	0 días	sáb 31/03/18	sáb 31/03/18	43	ASI, JP
45	**Gestión de Riesgos**	**14 días**	**lun 02/04/18**	**mar 17/04/18**		
46	Realizar metodología de evaluación de riesgos	2 días	lun 02/04/18	mar 03/04/18	37	ASI, JP
47	Metodología de evaluación de riesgos	0 días	mar 03/04/18	mar 03/04/18	46	ASI, JP
48	Realizar el inventario de activos de información	6 días	mié 04/04/18	mar 10/04/18	47	ASI, CC, CRRHH, JP
49	Inventario de activos de información	0 días	mar 10/04/18	mar 10/04/18	48	ASI, JP
50	Determinar amenazas y vulnerabilidades de los activos de información	6 días	mié 11/04/18	mar 17/04/18	49	ASI, CC, CRRHH, JP
51	Evaluación de riesgos	0 días	mar 17/04/18	mar 17/04/18	50	ASI, JP
52	**Elaborar plan de tratamiento de Riesgos**	**5 días**	**mié 18/04/18**	**lun 23/04/18**		
53	Realizar plan de tratamiento de riesgos	4 días	mié 18/04/18	sáb 21/04/18	51	JP
54	Realizar informe de gestión de riesgos	1 día	lun 23/04/18	lun 23/04/18	53	JP
55	Plan de tratamiento de riesgos	0 días	sáb 21/04/18	sáb 21/04/18	53	JP
56	Informe de la gestión de riesgos	0 días	lun 23/04/18	lun 23/04/18	54	ASI, JP
57	**Elaborar declaración de aplicabilidad de controles**	**4 días**	**vie 16/03/18**	**mar 20/03/18**		
58	Elaborar declaración de aplicabilidad de controles	4 días	vie 16/03/18	mar 20/03/18	6	ASI, JP
59	Declaración de aplicabilidad de controles	0 días	mar 20/03/18	mar 20/03/18	58	ASI, JP
60	**Elaborar matriz de comunicación interna y externa**	**2 días**	**mié 18/04/18**	**jue 19/04/18**		
61	Realizar matriz de comunicación interna	2 días	mié 18/04/18	jue 19/04/18	51	ASI
62	Matriz de comunicación interna	0 días	jue 19/04/18	jue 19/04/18	61	ASI
63	**Elaborar plan de capacitación y concientización**	**3 días**	**lun 23/04/18**	**mié 25/04/18**		
64	Realizar plan de capacitación y concientización	3 días	lun 23/04/18	mié 25/04/18	55	ASI
65	Plan de capacitación y concientización	0 días	mié 25/04/18	mié 25/04/18	64	ASI
66	**FASE 2 – HACER**	**82 días**	**mié 02/05/18**	**sáb 04/08/18**		
67	**Implementar plan de capacitación y concientización**	**11 días**	**mié 02/05/18**	**lun 14/05/18**		
68	Ejecución del plan de capacitación y concientización	10 días	mié 02/05/18	sáb 12/05/18	65FC+5 días	ASI, CC, CRRHH, JP
69	Realizar informe de ejecución del plan	1 día	lun 14/05/18	lun 14/05/18	68	ASI
70	Informe de plan de capacitación y concientización	0 días	lun 14/05/18	lun 14/05/18	69	ASI
71	**Implementar plan de tratamiento de riesgos**	**84 días**	**lun 14/05/18**	**sáb 04/08/18**		
72	**Ejecución del plan de tratamiento de riesgos**	**82 días**	**lun 14/05/18**	**jue 02/08/18**		
73	Grupo uno de controles	12 días	lun 14/05/18	sáb 26/05/18	55,59,68	ASI, CC, CRRHH, JP
74	Grupo dos de controles	50 días	mié 06/06/18	jue 02/08/18	73FC+20 días	ASI, CC, CRRHH, JP
75	Realizar informe de ejecución de plan de tratamiento de riesgos	2 días	vie 03/08/18	sáb 04/08/18	74	JP
76	Informe de plan de tratamiento de riesgos	0 días	sáb 04/08/18	sáb 04/08/18	75	JP
77	**FASE 3 – VERIFICAR**	**12 días**	**lun 06/08/18**	**sáb 18/08/18**		

	PROYECTO - IMPLEMENTACIÓN DE LA ISO/IEC 27001	170 días	lun 12/03/18	mar 25/09/18		RECURSOS
78	**Auditoría externa**	**12 días**	**lun 06/08/18**	**sáb 18/08/18**		
79	Preparar auditoria externa	4 días	lun 06/08/18	jue 09/08/18	76,70	JP, ASI
80	Ejecutar auditoria externa	7 días	vie 10/08/18	vie 17/08/18	79	JP, ASI
81	Informe de resultados de la auditoria externa	0 días	vie 17/08/18	vie 17/08/18	80	JP, ASI
82	Revisión por la Alta Dirección	1 día	sáb 18/08/18	sáb 18/08/18	81	JP, ASI
83	Acta de revisión por la Alta Dirección	0 días	sáb 18/08/18	sáb 18/08/18	82	JP, ASI, CC
84	**FASE 4 – ACTUAR**	**32 días**	**lun 20/08/18**	**mar 25/09/18**		
85	**Elaborar plan de acciones correctivas y mejoras**	**14 días**	**lun 20/08/18**	**mar 04/09/18**		
86	Identificar las acciones por cada observación	4 días	lun 20/08/18	jue 23/08/18	82	ASI, CC
87	Realizar el plan de acciones correctivas y mejoras	10 días	vie 24/08/18	mar 04/09/18	86	JP, ASI, CC
88	Plan de acciones correctivas y mejoras	0 días	mar 04/09/18	mar 04/09/18	87	JP, ASI, CC
89	**Implementar plan de acciones correctivas y mejoras**	**15 días**	**mié 05/09/18**	**vie 21/09/18**		
90	Aplicar el plan de acciones correctivas, levantamiento de observaciones y oportunidades de mejora	15 días	mié 05/09/18	vie 21/09/18	88	JP, ASI
91	**Realizar el análisis de brecha final**	**3 días**	**sáb 22/09/18**	**mar 25/09/18**		
92	Responder cuestionario de análisis de brecha	3 días	sáb 22/09/18	mar 25/09/18	90	JP, ASI, CC, CRRHH
93	Informe de análisis de brecha final	0 días	mar 25/09/18	mar 25/09/18	92	JP, ASI, CC, CRRHH

Fig. 2. Cronograma de proyecto
Fuente: Elaboración de los autores

8. PRESUPUESTO

Como presupuesto para la implementación de este proyecto, se necesita una inversión de **S/ 12,733.60** como se puede ver en la **Tabla 2:**

Tabla 2. Costo total del proyecto

Descripción	Valor Nuevos Soles S/
Actividades	S/ 3,224.00
Recursos	S/ 6,735.00
Perfil de recurso	S/ 2,280.60
Costos indirectos	S/ 494.00
Total de la implementación del SGSI	**S/ 12,733.60**

Fuente: Elaboración de los autores

Para obtener el presupuesto total del proyecto, se realizaron cálculos de los costos de las actividades detallada en la **Tabla 3:**

Tabla 3. Costo por Actividades

Actividades	Descripción	En soles	Cantidad	Total
Asesoría	Asesor en ISO 27001	S/ 1,860	1p	S/ 1,860.00
Auditor externo	Asesor para revisión	S/ 2,500	1p	S/ 700.00
Capacitación y Charla informativa	Coffe break	S/ 564.00	30	S/ 564.00
	Impresiones y folletos	S/ 100.00	01 millar	S/ 100.00
SUBTOTAL				**S/ 3,224.00**

Fuente: Elaboración de los autores (2018)

Además, se realizó los cálculos de los costos de los recursos de hardware y software detallados en la **Tabla 4,** donde se observa la procedencia de los recursos, la cantidad, costo unitario y el costo total.

Tabla 4. Costos por recursos de Hardware y software

Hardware/Software	Procedencia	Cantidad	Costo Unitario	Total
Intel Core i7-5500U 2.40GHz, Memoria RAM 8GB, Disco duro 1TB SATA	Empresa	2	S/ 1,600	S/ 3,200.00
Intel Core i5-5200U 2.20GHz, Memoria RAM 6GB, Disco duro 1TB SATA	Los autores	1	S/ 1,700	S/ 1,700.00
Intel Core i7-6500U 2.50GHz, Memoria RAM 8GB, Disco duro 1TB SATA	Empresa	1	S/ 1,450	S/ 1,450.00
Licencias de Office	Nexsys	2	S/ 29.00	S/ 58.00
	Office 365	2	0	S/ 0.00
Bizagi	Software libre	4	0	S/ 0.00
Servidor (Google Drive)	Xertica (G Suite)	1	0	S/ 327.00
	Google Drive	2	0	S/ 0.00
Gantter	Software libre	1	0	S/ 0.00
Adobe Reader	Software libre	1	0	S/ 0.00
SUBTOTAL				**S/ 6,735.00**

Fuente: Elaboración de los autores

También se consideró el costo por perfil de recurso, detallado en la **Tabla 5**, donde se contabilizó la tarifa por jornada, el porcentaje de ocupación y el total de jornadas de cada uno.

Tabla 5. Costos por Perfil de recurso

Perfil de recurso	Tarifa x jornada	Tarifa x hora	Cantidad de días	Cantidad de horas x día	Total x Perfil S/
(1) Analista de calidad	S/ 38.71	S/ 4.30	15d	4h	S/ 258.00
(1) Coordinadora de RR.HH.	S/ 29.80	S/ 3.31	15d	4h	S/ 198.60
(1) Analista de seguridad de información	S/ 40.20	S/ 4.46	40d	5h	S/ 892.00
(1) Jefe de proyectos	S/ 41.94	S/ 4.66	40d	5h	S/ 932.00
SUBTOTAL					**S/ 2,280.60**

Fuente: Elaboración de los autores

Para el desarrollo del proyecto se tomaron en cuenta los costos indirectos de los servicios como el agua, luz, internet fijo y otros gastos que se pueden visualizar en la **Tabla 6.**

Tabla 6. Costos Indirectos

Detalle	Costo	Cantidad	Total
Agua	S/ 20	3	S/ 60.00
Luz	S/ 30	3	S/ 90.00
Internet fijo	S/ 78	3	S/ 234.00
Otros gastos	S/ 110	1	S/ 110.00
SUBTOTAL			**S/ 494.00**

Fuente: Elaboración de los autores

ANEXO 8 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

En **VF Consulting S.A.C.** nos dedicamos a la prestación de servicios en la industria de telecomunicaciones, consideramos que la información es un activo de vital importancia, por esto su confidencialidad, disponibilidad e integridad es primordial para realizar nuestras actividades organizacionales.

Demostramos nuestro compromiso con nuestros clientes y stakeholders implementando, manteniendo y mejorando continuamente un sistema de gestión de seguridad de la información; cumpliendo a cabalidad cada uno de sus requisitos con el fin de alcanzar un nivel de clase mundial, siempre en cumplimiento de las leyes y regulaciones que nos sean aplicables.

Esta política incluye los siguientes objetivos de seguridad de la información:

- Reducir los incidentes de seguridad de la información reportados a niveles aceptables.
- Fortalecer la confianza de nuestros clientes y colaboradores mediante medidas de seguridad apropiadas.
- Garantizar la continuidad de nuestros servicios reduciendo los periodos de indisponibilidad reportados.

Nos comprometemos en alcanzar el éxito de nuestra política y el logro de nuestros objetivos, comprendiendo que la participación y el compromiso de nuestros colaboradores son de alta relevancia por lo que se delegan y disponen los recursos necesarios para la difusión y comprensión de esta política como parte fundamental en nuestros servicios.

En **VF Consulting S.A.C.** todos somos parte del éxito.

VICTOR FELIPE GANOZA
Gerente General

Calle General Varela No 356 of. 601 Miraflores. Lima - Perú. Teléfono: (+51-1) 2219970
customer_support@vfcons.com www.vfcons.com

ANEXO *9*

FICHA DE PUESTO

ANEXO 9 FICHAS DE PUESTO

OFICIAL DE SEGURIDAD DE INFORMACIÓN

1. GENERALES

Procesos:	Proceso de Gestión de Proyectos, Gestión Comercial, Gestión de Recursos Humanos, Gestión de Finanzas y Contabilidad y Gestión de Logística.
Reporta a:	Gerente General
Supervisa a:	Analista de Seguridad de la Información

2. ORGANIGRAMA

3. OBJETIVO

Mejorar la seguridad de información en la organización, a través de la planificación, coordinación e implementación de las políticas, controles de seguridad de información y difusión de la cultura de seguridad de información entre todos los miembros de la organización. Además de promover iniciativas y proyectos referentes a la seguridad, y ser responsable de la gestión del riesgo.

4. FUNCIONES

• Conocer y aplicar la metodología de análisis de riesgo para evaluar la seguridad de información en los activos de seguridad en la organización. • Establecer o actualizar la política de seguridad de información de la organización, además de fomentar su difusión. • Seleccionar los controles adecuados para la implementación o actualización referentes a la seguridad de información. • Crear o actualizar los procedimientos relacionados a la seguridad de información dentro de la organización. • Promover y gestionar las auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad de la información dentro de la organización.

5. REQUISITOS DEL PUESTO:

Requisitos:	• Título o bachiller en Ingeniera de Sistemas o carrera técnicas afines. • Curso de Auditor Líder ISO/IEC 27001:2013, mínimo de 40 horas. • Capacitación en cursos de protección de datos, mínimo de 10 horas. • Dominio en idioma inglés.
Conocimientos y competencias:	• Coordina y dirige los esfuerzos del servicio contratado. • Coordina y realiza las acciones que permitan que se cumpla la normativa de seguridad. • Dominio completo de Microsoft Office. • Liderazgo y toma de decisiones. • Manejo de personal • Experiencia dirigiendo equipo de trabajo • Habilidades blandas • Proactivo

Experiencia:	Mínimo de 1 año como Analista de Sistemas realizando actividades de seguridad de información y 2 años en el puesto de Oficial de Seguridad de la Información o encargado de la implementación y cumplimiento de la ISO/IEC 27001.

ANALISTA DE SEGURIDAD DE INFORMACIÓN

1. GENERALES

Procesos:	Proceso de Gestión de Proyectos, Proceso Comercial, Proceso de Recursos Humanos, Proceso de Finanzas y contabilidad, Proceso de Logística.
Reporta a:	Oficial de Seguridad de Información
Supervisa a:	-

2. ORGANIGRAMA

3. OBJETIVO

Apoyar en la seguridad de información de la organización, supervisando que los controles de seguridad se cumplan, apoyando con la difusión de la cultura de seguridad de información entre todos los miembros de la organización y ayudando con la gestión de riesgos.

4. FUNCIONES

• Actualizar la lista de activos, mediante encuestas o reuniones con los responsables de los procesos. • Conocer y aplicar la metodología de gestión de riesgos. • Apoyar con la difusión de la política y procedimientos de seguridad de información en la organización. • Apoyar con la implementación o actualización de los controles adecuados que deberán aplicarse para la mejora de la seguridad de información. • Identificar los incidentes de seguridad de información dentro de la organización. • Apoyar en las auditorias enfocadas en la seguridad de información, para evaluar las prácticas de seguridad de la información dentro de la organización.

5. REQUISITOS DEL PUESTO:

Requisitos:	• Título o bachiller en Ingeniera de Sistemas o carrera técnicas afines. • Dominio en idioma inglés.
Conocimientos y competencias:	• Coordina y dirige los esfuerzos del servicio contratado. • Coordina y realiza las acciones que permitan que se cumpla la normativa de seguridad. • Dominio completo de Microsoft Office. • Experiencia dirigiendo equipo de trabajo. • Habilidades blandas. • Proactivo.
Experiencia:	Mínimo de 1 año como Analista de Sistemas realizando actividades de seguridad de información y 1 año en el puesto de Analista de Seguridad de la Información o Asistente en la implementación y cumplimiento de la ISO/IEC 27001.

ANEXO 10

PROCEDIMIENTO DE CONTROL DE DOCUMENTACIÓN

ANEXO 10 PROCEDIMIENTO DE CONTROL DE DOCUMENTACIÓN

1. OBJETIVO, ALCANCE Y RESPONSABLES

El objetivo del presente documento es describir las actividades para establecer, documentar, controlar y mantener los documentos del SGSI, en base a los requisitos de la norma ISO/IEC 27001 y de acuerdo con los requisitos establecidos por la organización.

El alcance es para todos los documentos del SGSI en la organización. La responsabilidad empieza desde la alta gerencia y se extiende a todas las áreas administrativas y operativas para su cumplimiento de acuerdo con el alcance, asegurando la implementación del procedimiento.

2. DEFINICIONES Y ACRÓNIMOS

Copia controlada: Copia impresa de los documentos vigentes del SGSI, identificados con un sello de copia controlada.

Copia no controlada: Copia de los documentos del SGSI con fines didácticos o de revisión, que de estar impresos no requieren de ninguna identificación por no ser oficial.

SGSI: Sistema de gestión de seguridad de la información.

3. DOCUMENTOS Y REGISTROS

- Lista Maestra de documentos internos
- Lista Maestra de documentos obsoletos
- Lista de Distribución de documentos

4. PROCEDIMIENTO

N.º	Actividad	Descripción	Realiza	Registro
1	Comunicar necesidad de creación o cambio en documentos	Reporta la necesidad de elaborar o modificar un documento mediante un correo al responsable del proceso, quien comunicará dicha solicitud a la Coordinadora de Calidad.	Integrante de la organización	Correo electrónico

N.º	Actividad	Descripción	Realiza	Registro
2	Analizar la solicitud	Analiza solicitud de elaboración o modificación y, en caso crea conveniente se deba realizar, se aprueba y solicita al responsable del proceso que designe a una persona que conozca del tema, el cual pasará a ser responsable del documento, para realizar los cambios necesarios.	Coordinadora de Calidad	Correo electrónico
3	Elaborar o modificar documento	En caso se requiera elaborar un documento, el responsable del documento será quien desarrolle el mismo, considerando la estructura en el **Anexo 1 Estructura Documentaria.**	Responsable del documento	-
4	Revisar el documento	Revisa que los documentos estén correctamente elaborados.	Coordinadora de Calidad	-
5	Aprobar el documento	Previa verificación con la Coordinadora de Calidad sobre el contenido del documento brinda su aprobación.	Gerente de Administración	-
6	Registrar en Lista Maestra	Una vez aprobado el documento, los incluye en el registro “Lista Maestra de documentos internos”, de ser necesario, archiva el documento físico original en el file “Documentos Vigentes”. Además, si es un documento modificado, el desactualizado pasa a la “Lista Maestra de documentos obsoletos”.	Coordinadora de Calidad	Lista Maestra de documentos internos Lista Maestra de documentos obsoletos.

N.º	Actividad	Descripción	Realiza	Registro
7	Difundir el documento	La distribución se puede realizar por 2 medios: 1. Medio Digital Se escanea y guarda el documento aprobado en la nube y en la carpeta compartida. Se informa mediante correo a las personas involucradas indicando la ubicación del documento, el cual se encuentra subido en el repositorio (Drive). 2. Medio Físico Se distribuye físicamente los documentos aprobados a través de copias controladas de la siguiente manera: • Emite una copia del documento vigente. • Sella como “Copia controlada” en la primera página de la copia del documento vigente y consigna el número de copia que se le asigna al documento. Los documentos que no cuenten con dicho sello, son considerados como documentos no controlados. • Consignar en la “Lista de Distribución de documentos”, el nombre del documento vigente a distribuir y los nombres de las personas a quienes se les	Coordinadora de Calidad	Lista de Distribución de documentos

N.º	Actividad	Descripción	Realiza	Registro
		entregará la copia del documento. • Entrega la copia controlada del documento al personal, solicitando su firma en la "Lista de Distribución de documentos". • En caso exista un documento con versión desactualizada (obsoleto), solicita al personal las copias del documento obsoleto y procede a eliminarlo. Verifica que no existan documentos obsoletos (electrónico o físico) en poder del personal.		

5. Anexo

Anexo 1. Estructura Documentaria

LOGO	NOMBRE DEL DOCUMENTO	**Fecha:** Fecha de aprobación
	Código: Colocar Código	**Página**: X de X

Estructura para procedimientos:

1. HISTORIAL DE CAMBIOS
2. OBJETIVO, ALCANCE Y RESPONSABLES
3. DEFINICIONES
4. DOCUMENTOS Y REGISTROS
5. PROCEDIMIENTO
6. ANEXOS (Si aplica)

Estructura para otros documentos:

Mantendrá la estructura que mejor se acomode a la información que se desea describir.

Anexo 2. Codificación de la Información documentada

VF - XX - YZ - VV

VF: Siglas de VF Consulting

XX: Código del proceso

Y: Código del tipo de documento

Z: Correlativo del documento: 01, 02...etc.

VV: versión

Y	Tipo de documento	XX	Proceso	VV
FP	Ficha de Puesto	GC	Gestión de Calidad	
M	Manual	GP	Gestión de Proyectos	
P	Procedimiento	GC	Gestión Comercial	
F	Formato	GSI	Gestión de Seguridad de la información	
I	Instructivo	GST	Gestión de Prestación de Servicios	1.0,1.1,1.2
D	Documento	GRH	Gestión de Recursos Humanos	
A	Acta	GLOG	Gestión Logística	
		GCF	Gestión de Contabilidad y Finanzas	
		DA	Desarrollo de Aplicaciones	

ANEXO 11

PROCEDIMIENTO DE GESTIÓN DE RIESGOS

ANEXO 11 PROCEDIMIENTO DE GESTIÓN DE RIESGOS

1. OBJETIVO, ALCANCE Y RESPONSABLES

El objetivo del presente documento es definir las actividades para gestionar los riesgos evaluados en VF CONSULTING S.A.C y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplica de acuerdo con el alcance del SGSI establecido; es decir, a los activos de información del proceso core y los procesos involucrados. La responsabilidad de este documento es de todo el personal de VF CONSULTING S.A.C que participa en la gestión de riesgos.

2. DEFINICIONES

Activo de información: Elemento que contiene o manipula información, a través del cual la entidad obtiene beneficios para el logro de sus objetivos estratégicos.

Amenaza: Causa potencial de un incidente no deseado que puede ocasionar daños al sistema u entidad.

Control: Herramienta para mitigar un riesgo.

Inventario de activos: Es un registro conformado por los activos de información que tienen valor para la entidad y que están dentro del alcance del SGSI

SGSI: Sistema de gestión de seguridad de la información.

3. DOCUMENTOS Y REGISTROS

- Inventario de Activos
- Evaluación de Riesgos
- Plan de Tratamiento de riesgos
- Informe de Plan de tratamiento de riesgos

4. PROCEDIMIENTO

N.º	Actividad	Descripción	Realiza	Registro
1	Realizar lista de activos	Elabora o actualiza la lista de activos de información utilizando el “Inventario de Activos” y considerando “Metodología de Gestión de Riesgos”	Equipo de seguridad de la información	Inventario de Activos
2	Determinar amenazas	Identifica todas las amenazas relacionadas con cada activo. Cada activo puede estar relacionado a varias amenazas e incluso pueden ser las mismas.	Equipo de seguridad de la información	Evaluación de Riesgos
3	Evaluar el riesgo	Elabora o actualiza la evaluación de riesgos, utilizando el formato “Evaluación de Riesgos” considerando los criterios establecidos en la “Metodología de Gestión de riesgos”	Equipo de seguridad de la información	Evaluación de Riesgos
4	Aplicar los criterios de aceptación aprobados	Determina los criterios de aceptación de los riesgos en base a la “Metodología de Gestión de riesgos” y define controles que permitan reducir la probabilidad e impacto de los riesgos.	Oficial de Seguridad de información	Evaluación de Riesgos
5	Asignar propietarios de los riesgos	Determina el dueño de cada uno de los riesgos y el responsable del control. Esta persona puede o no ser la misma que el propietario del activo.	Oficial de Seguridad de información	Evaluación de Riesgos
6	Elaborar Plan de Tratamiento de riesgos	Elabora el “Plan de Tratamiento de riesgos” considerando el plazo estimado, responsables y acción por cada amenaza a tratar.	Equipo de Seguridad de la información	Plan de Tratamiento de riesgos
7	Realizar Informe de Gestión de riesgos	Realiza informe en el cual se resumen los activos de mayor impacto, sus amenazas y el plan de tratamiento para estos.	Oficial de Seguridad de información	Informe de Gestión de riesgos
8	Implementar Plan de Tratamiento de riesgos	Procede a implementar los controles y acciones establecidos en el “Plan de Tratamiento de riesgos”	Equipo de Seguridad de la información	-
9	Evaluar el riesgo residual	Realizar el cálculo del riesgo residual, considerando la evaluación de controles existentes**.**	Analista de Seguridad de información	Evaluación de Riesgos
10	Realizar Informe de Plan de Tratamiento de riesgos	Realiza informe sobre los controles implementados y establecidos en el “Plan de Tratamiento de riesgos”.	Oficial de Seguridad de información	Informe de Plan de Tratamiento de riesgos

ANEXO 12

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

ANEXO 12 PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de este procedimiento es tener una gestión adecuada de los incidentes reportados, es decir, identificarlos, evaluarlos, ejecutar acciones para corregirlos y mantener un informe de estos para futuras revisiones.

Este procedimiento aplica para todo el personal relacionado a los procesos identificados en el alcance del SGSI.

2. DEFINICIONES

Incidente: Cualquier caso adverso con relación a la seguridad de la información que afecte la integridad, confidencialidad o disponibilidad de la información de la entidad.

SGSI: Sistema de gestión de seguridad de la información.

3. DOCUMENTOS Y REGISTROS

- Monitoreo de Gestión de incidentes

4. PROCEDIMIENTO

N.º	Actividad	Descripción	Realiza	Registro
1	Identificar una incidencia	Durante las diferentes actividades organizacionales pueden presentar o identificar una incidencia.	Integrante de la organización	-
2	Comunicar incidencia	Se comunica el incidente a través de correo electrónico al correo: seguridad.informacion@vfcons.com Al informar el incidente se deberá tener en cuenta enviar la siguiente información: - Identificar el incidente - Responsable del incidente - Evidencias (de ser posible) Explicar qué pasó, qué lo produjo y cómo sucedió.	Integrante de la organización	Correo electrónico

N.º	Actividad	Descripción	Realiza	Registro
3	Registrar incidencia	Analizar el alcance, tipo de incidencia y nivel de criticidad **(Anexo 1 Y 2).** En caso no se encuentre claramente definido o no se evidencia lo ocurrido, se solicita vía correo electrónico, la corrección a la persona que lo comunicó. En caso la incidencia se encuentre bien documentada, se traspasa la incidencia al formato "Monitoreo de Gestión de incidentes"	Analista de Seguridad de información	Correo electrónico y Monitoreo de Gestión de incidentes
4	Ejecutar las acciones identificadas	Se ejecutan y documentan las acciones identificadas para la atención del incidente de seguridad.	Oficial de Seguridad de información	-
6	Comunicar respuesta ante incidente	Se debe comunicar la respuesta a los involucrados sobre lo realizado respecto al incidente.	Analista de Seguridad de información	Correo electrónico
7	Análisis de causa y cierre del incidente	Realiza un análisis de las causas del incidente. Registra el cierre del incidente en el formato "Monitoreo de Gestión de incidentes".	Oficial de Seguridad de información	Monitoreo de Gestión de incidentes
8	Realizar informe y revisión de los incidentes	Cada tres meses se realiza un informe sobre los incidentes identificados y se revisa este informe con la finalidad de evaluar la mejora o no de estos.	Oficial de Seguridad de información	Informe de Gestión de incidentes

5. ANEXOS

Anexo 1. Tipo de incidente

Tipo	Descripción	Ejemplos
Informático	Todos aquellos incidentes que afecten a las tecnologías de información	• Fallas de sistemas de información • Código malicioso • Accesos no autorizados a los sistemas de información
No informático	Todos aquellos incidentes no contemplados en el punto anterior	• Violaciones a la confidencialidad, integridad y disponibilidad (documentos, formatos, etc.) • Filtración de información reservada • Acceso físico no autorizado • Incidentes provocados por la naturaleza

Anexo 2. Nivel de criticidad

Parámetro	Descripción	Variables
Impacto	Importancia del incidente dependiendo de los procesos afectados y usuarios	• Bajo: No interrumpe el proceso core, solo a los involucrados con este proceso, y afecta de uno a dos colaboradores. • Medio: Interrumpe momentáneamente los procesos involucrados con el proceso core y afecta de tres a cinco colaboradores • Alto: Interrumpe el proceso core y procesos involucrados, y afecta a más de cinco colaboradores.
Urgencia	Tiempo máximo de demora que puede aceptar el proceso para la resolución del incidente	• Baja: 12 horas. • Media: 10 horas. • Alta: 4 horas.

ANEXO 13

PROCEDIMIENTO DE AUDITORIA INTERNA

ANEXO 13 PROCEDIMIENTO DE AUDITORIA INTERNA

1. OBJETIVO, ALCANCE Y USUARIOS

Establecer las actividades para la realización de las auditorías internas, con la finalidad de evaluar si el SGSI cumple con los requisitos de la ISO/IEC 27001:2013 y si está implementado de manera eficaz.

Se aplica a todo el alcance del SGSI. Los usuarios de este documento son el equipo de seguridad de información, la alta dirección y los responsables de cada área.

2. DEFINICIONES

Auditor: Persona con la competencia para llevar a cabo una auditoria.

Auditor Líder: Auditor que lidera un equipo auditor.

Auditoria Interna: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoria.

Equipo auditor: Numero de auditores necesarios en función del alcance y finalidad de la auditoría.

No conformidad: Incumplimiento con los requisitos especificados.

Hallazgo: Resultado de la evaluación de la evidencia objetiva de la auditoria recopilada frente a los criterios de auditoría.

Observaciones: Todo hallazgo que puede derivar una no conformidad.

Oportunidad de mejora: Hallazgo o idea que no afecta el sistema y que sugiere o se propone con el fin mejorar el proceso.

3. DOCUMENTOS Y REGISTROS

- Programa de Auditoría Interna
- Plan de Auditoría Interna
- Informe de Auditoría Interna
- Monitoreo de No Conformidades y Acciones Correctivas
- Acta de Reunión

4. PROCEDIMIENTO

N.º	Actividad	Descripción	Realiza	Registro
1	Planificar la auditoría	Planifica las auditorías a realizarse en el año mediante la propuesta "Programa de Auditoría Interna", en donde se definirán los procesos a auditar y los meses correspondientes para realizar una auditoría. Las auditorías internas o externas se realizarán como mínimo una vez al año, donde el Gerente General aprobará el "Programa de Auditoría Interna".	Oficial de Seguridad de la Información	Programa de Auditoría Interna
2	Seleccionar Auditor	Selecciona, organiza y designa al personal que participará en la auditoría, el cual puede estar conformado por personal interno o externo que tenga calificación apropiada para realizar auditorías y que no tengan compromiso directo con la actividad a auditar. Los requisitos para la calificación de auditores se detallan en el **Anexo 1. Requisitos para calificación de auditores**	Oficial de Seguridad de la Información	-
3	Preparar auditoría	Como parte de la preparación de la auditoría, informa a los responsables de los procesos el detalle de la ejecución de la auditoría a través del "Plan de Auditoría Interna" con mínimo cinco días útiles de anticipación.	Auditor	Plan de Auditoría Interna
4	Ejecutar auditoría	El desarrollo de la auditoría contempla las siguientes etapas: • Reunión inicial: Antes de iniciar la auditoria, el Auditor Líder explica a los auditados el objetivo de la auditoria y las actividades que se realizarán. • Ejecución de la auditoría: Los Auditores proceden a recoger evidencias del proceso auditado a través de entrevistas, observaciones de las actividades y revisiones de registros, con la finalidad de verificar la implementación del sistema y su eficacia. Se debe auditar teniendo en cuenta el alcance del SGSI de acuerdo	Auditor	-

N.º	Actividad	Descripción	Realiza	Registro
		a lo especificado en el Plan de Auditoria Interna. • Reunión de cierre: Se realiza al finalizar la auditoria, se procede a explicar cómo se ha desarrollado la misma y se realiza una breve descripción de las no conformidades y hallazgos detectados, así como las conclusiones de la auditoria.		
5	Elaborar informe	Los auditores internos en conjunto con el Auditor Líder preparan el "Informe de Auditoria Interna" en el que resume los datos principales del evento.	Auditor	Informe de Auditoría Interna
6	Comunicar informe	Dicho informe se comunica a la alta dirección mediante una reunión, y luego de ello pasa a ser distribuido a los responsables de los procesos involucrados.	Oficial de Seguridad de la Información	Acta de Reunión
7	Generar no conformidades, y oportunidades de mejora	Las no conformidades detectadas en la auditoría interna son agrupadas de acuerdo con la naturaleza de la no conformidad. Registra el detalle de estas en el formato "Monitoreo de No Conformidades y Acciones Correctivas" así mismo, las observaciones y oportunidades de mejora detectadas en la auditoría interna deben ser registradas como acciones para afrontar riesgos.	Oficial de Seguridad de la información	Monitoreo de No Conformidades y Acciones Correctivas

5. ANEXOS

Anexo 1: Requisitos para la calificación de auditores

Auditor Interno	Auditor Externo
Requisitos: • Participación como observador en una auditoria interna. • Curso de auditor interno aprobado	Requisitos: • Curso de auditor interno aprobado • Experiencia mínima en 1 auditoría en una empresa externa.

Auditor Líder Interno	Auditor Líder Externo
Requisitos: • Curso de auditor interno aprobado • Experiencia: Participación en 1 auditoría interna. • Antigüedad en la empresa no menor a 1 año.	Requisitos: • Curso de auditor interno aprobado • Experiencia: Mínimo 2 auditorías en empresas externas

ANEXO 14

METODOLOGÍA DE GESTIÓN DE RIESGOS

ANEXO 14 METODOLOGÍA DE GESTIÓN DE RIESGOS

1. OBJETIVO, ALCANCE Y USUARIOS

Establecer el marco metodológico para la ejecución del proceso de gestión de riesgos del Sistema de Gestión de Seguridad de la Información (SGSI).

La evaluación y tratamiento de riesgos se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un gran impacto sobre la seguridad de la información.

Los usuarios de este documento son todos los encargados como empleados de VF CONSULTING S.A.C. que participan en la evaluación y tratamiento de riesgos.

2. DEFINICIONES Y ACRÓNIMOS

No aplica.

3. DOCUMENTOS Y REGISTROS

No aplica.

4. METODOLOGÍA DE GESTIÓN DE RIESGOS

Esta metodología abarca los siguientes puntos:

a. Inventario de Activos

El análisis de riesgos se deberá iniciar con la elaboración del inventario de activos de información de los procesos considerados dentro del alcance del SGSI. Los activos de información identificados serán valorizados en base al impacto sobre la perdida de confidencialidad, integridad y disponibilidad.

Para cada proceso del alcance, se deberá preparar la lista de sus activos de información **(Anexo Inventario de Activos de Información),** en el cual se deberán categorizar por tipos de activos. La categorización que se realizó para el inventario de activos se encuentra en la **Tabla 1.**

Tabla 1. Categorización de activos

GRUPO	ABREVIATURA	DESCRIPCIÓN
Instalaciones	**[I]**	Las instalaciones que acogen equipos informáticos y de comunicaciones.
Hardware	**[HW]**	Los equipos informáticos (hardware) que permiten hospedar datos, aplicaciones y servicios.
Software	**[SW]**	Las aplicaciones informáticas (software) que permiten manejar los datos.
Datos	**[D]**	Datos que materializan la información.
Redes de Comunicación	**[COM]**	Instalaciones dedicadas como servicios de comunicaciones que permiten intercambiar datos.
Servicios	**[S]**	Servicios auxiliares que se necesiten para desarrollo de procesos y/o servicios
Equipamiento auxiliar	**[AUX]**	El equipamiento auxiliar que complementa el material informático.
Media	**[M]**	Documentación, procedimientos, manuales de usuarios.

Fuente: Pulgarín R. (2014)

b. Valorización de activos

Luego de hacer le inventarios de activos, debemos saber que el valor del activo se estima mediante el cálculo del promedio del valor del impacto de la pérdida de Confidencialidad, Integridad y Disponibilidad, como se visualiza en la siguiente fórmula:

$$Valor\ del\ activo = \frac{(Confiencialidad + Integridad + Disponibilidad)}{3}$$

Para estimar el valor del impacto de la pérdida de cada una de las tres aristas de valoración del activo, se emplea la siguiente escala. **(Ver Tabla 2)**

Tabla 2. Valorización de criterios de seguridad

Rango	Valor	Confidencialidad	Integridad	Disponibilidad
7-10	**ALTO**	La información asociada al activo es solo accedida por el Gerente o jefes responsables, pues su divulgación afectaría **gravemente** a la empresa.	El activo no puede tolerar pérdida o alteración de sus componentes **5%** pues la alteración de su integridad afectaría **gravemente** a la empresa.	Se requiere que el activo no esté disponible al menos una hora, pues su carencia afectaría **gravemente** a la empresa
4-6	**MEDIO**	La información asociada al activo es **confidencial** y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría **considerablemente** a la empresa.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **50%**, pues la alteración de su integridad afectaría **considerablemente** a la empresa.	Se considera que como máximo el activo puede estar no disponible por **un día**, pues su carencia afectaría **considerablemente** a la empresa.
1-3	**BAJO**	La información asociada al activo es **de uso interno** y solo el personal de la empresa puede acceder a ella o **pública**, es decir que puede acceder cualquiera, pues su divulgación afectaría de manera **baja** a la empresa.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **95%**, pues la alteración de su integridad afectaría de manera **baja** a la empresa.	Se considera que como máximo el activo puede estar no disponible por **una semana o tiempo indefinido**, pues su carencia afectaría de manera **baja** a la empresa.

Fuente: Elaboración de los autores (2018)

El nivel de impacto del activo se obtiene al identificar el “Valor del activo” dentro de uno de los rangos de valor de la **Tabla 3.**

Tabla 3. Matriz de Impacto

ID	RANGO	VALOR		CRITERIO
3	7 - 10	ALTO	A	Valor alto
2	4 - 6	MEDIO	M	Valor medio
1	1 - 3	BAJO	B	Valor bajo

Fuente: Elaboración de los autores (2018)

Conforme a lo definido en los criterios de impacto de activos, los activos que pasan a la fase de evaluación de riesgos son solo aquellos activos de información cuyo nivel de impacto es **"ALTO" (Valorización de Activos)**

c. Evaluación de Riesgos

Para el cálculo del riesgo se debe considerar la probabilidad y el impacto del riesgo, ambos puntajes son multiplicados para obtener el riesgo total o inherente.

Probabilidad: Para calcular la probabilidad se debe determinar un número entre 1 a 4. **(Tabla 4.)**

Tabla 4. Criterios de probabilidad

ID	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
4	CASI SEGURO	El evento probablemente ocurre en la mayoría de las circunstancias	Más de una vez al año
3	PROBABLE	El evento probablemente ocurrirá en todas las circunstancias	Al menos una vez en los últimos 3 años
2	IMPROBABLE	El evento probablemente puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
1	RARO	El evento probablemente ocurre solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años

Fuente: Elaboración de los autores (2018)

Impacto: Para calcular el impacto se debe determinar un número entre 1 a 3. **(Tabla 5)**

Tabla 5. Criterios de probabilidad

ID	RANGO	DESCRIPCIÓN
3	**ALTO**	1. Afecta y daña de manera significativa la reputación de imagen, la misión e intereses de la organización. 2. Resulta pérdidas financieras de un alto costo y esfuerzo de los activos o recursos de la organización. 3. Afecta de manera la alta continuidad del inicio de los servicios brindados de la organización.
2	**MEDIO**	1. Afecta y daña la reputación de la imagen, la misión e intereses de la organización. 2. Resulta pérdidas financieras medianamente recuperable de los activos o recursos de la organización. 3. Afecta de manera media a la continuidad del inicio de los servicios brindados de la organización.
1	**BAJO**	1. Daño intrascendente a la reputación de la imagen, la misión e intereses de la organización. 2. Resulta pérdidas financieras mínimas de los activos o recursos en la organización. 3. No afecta a la continuidad del inicio de los servicios brindados de la organización.

Fuente: Elaboración de los autores (2018)

El valor del riesgo se calcula de acuerdo con la expresión matemática que se presenta a continuación:

$$(Nivel\ de\ Riesgo) = (Nivel\ de\ impacto) * (\frac{Probabilidad\ de}{ocurrencia\ del\ riesgo})$$

Para determinar el nivel de riesgo, se identifica el nivel de zona de riesgo dentro del rango indicado, haber utilizado la expresión matemática se obtuvo la siguiente **Tabla 6.**

Tabla 6. Zona de riesgos

PROBABILIDAD		IMPACTO		
		BAJO	MEDIO	ALTO
		1	**2**	**3**
RARO	**1**	1	2	3
IMPROBABLE	**2**	2	4	6
PROBABLE	**3**	3	6	9
CASI SEGURO	**4**	4	8	12

Fuente: Elaboración de los autores (2018)

Para visualizar la evaluación de Riesgos **(Anexo 20)**

d. Criterios de aceptación de riesgos

Una vez efectuado el análisis y la evaluación del riesgo, se debe decidir qué acciones se han de tomar con los activos que están sujetos a riesgos reales y significativos para la empresa. Para ello se puede aplicar una de las siguiente **Tabla 7:**

Tabla 7. Criterios de aceptación de riesgos

Medida frente al riesgo	
ASUMIR	Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas.
REDUCIR	Reducir la probabilidad o el impacto de ocurrencia mediante la implementación de controles de seguridad de la información. Se utiliza cuando al implementar el control trae beneficios mayores a la inversión de su implementación.
EVITAR	Eliminar la fuente del proceso que genera la amenaza. Se utiliza cuando el nivel de riesgo es alto y la actividad del proceso o sistema que lo genera no es de gran impacto en términos de negocio para la entidad, de modo que puede ser retirada funcionalmente.
TRANSFERIR	Transferir el impacto del riesgo a terceros (empresas aseguradoras o proveedores de servicio). Se utiliza cuando no se puede reducir la probabilidad de ocurrencia de un riesgo, pero el impacto es inminente.

Fuente: Elaboración de los autores (2018)

El criterio de aceptación de riesgos se realiza en base al nivel de riesgo evaluado según se detalla en la siguiente **Tabla 8:**

Tabla 8. Zona de riesgos

ID	RANGO	ZONA	CRITERIOS DE ACEPTACIÓN
B	1 - 2	Zona de riesgo baja	Asumir el riesgo
M	3 - 5	Zona de riesgo moderada	Asumir el riesgo, evaluar reducir el riego
A	6 - 8	Zona de riesgo alta	Reducir el riesgo, evitar, compartir el riesgo
E	9 - 12	Zona de riesgo extrema	Reducir el riesgo, evitar, compartir el riesgo

Fuente: Elaboración de los autores (2018)

e. Plan de Tratamiento de Riesgos

Una vez de haber definidos los criterios de aceptación de riesgos, se procede a realizar el plan de tratamiento de riesgos, es el paso en el que se tiene que moverse de la teoría a la práctica, mostrar resultados de todo lo planteado en ese plan. Para eso se define quién va a implantar, quién será el propietario del activo y quién es el responsable de dicho control, cuándo, qué presupuesto se necesita, etc. Además, este documento debe tener la aprobación de la alta dirección, ya que llevará mucho tiempo y esfuerzo dependiendo de la dificultad de aplicar dicho control y sin su compromiso no obtendrá los recursos necesarios.

ANEXO 15

LISTA DE INVENTARIO DE ACTIVOS DE INFORMACIÓN

ANEXO 15 LISTA DE INVENTARIO DE ACTIVOS DE INFORMACIÓN

LISTA DE INVENTARIO DE ACTIVOS DE INFORMACIÓN							
Ámbito	**Categoría**	**ID**	**Activo**	**Descripción**	**Proceso**	**Propietario / Responsable**	**Ubicación**
DATOS	[D] Datos	[D-001]	Datos del personal	Información acerca del personal de la empresa como nombres, apellidos, DNI, dirección, correo, cargo, puesto, grado, entre otros.	Gestión Recursos humanos	Recursos humanos	Servidor Nube
	[D] Datos	[D-002]	Control de salarios	Información de los contratos del personal como la lista de salario	Gestión Recursos humanos y Comercial	Recursos humanos	Servidor Nube
	[D] Datos	[D-003]	Datos de inventario de equipos	Información acerca del inventario de equipos como laptops, mouses, usb, discos duros, mochilas, cable de seguridad, pach, audífonos entre otros.	Gestión Logística	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-004]	Registro de certificaciones	Información acerca de las certificaciones del personal de la empresa	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-005]	Formatos de entrevista de candidatos	Información acerca de los postulantes que quieren trabajar en la empresa.	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física

Ámbito	Categoría	ID	Activo	Descripción	Proceso	Propietario / Responsable	Ubicación
DATOS	[D] Datos	[D-006]	Lista de asistencias	Información acerca de las asistencias del personal para el control de seguimiento	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-007]	Solicitud de permisos	Información acerca del personal que pide permiso por motivos de salud, compensación, intercambio de fechas entre otros.	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-008]	Informe técnico sobre el personal	Información acerca de reportes que se deben presentar a los gerentes	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-009]	Memorándum	Información acerca de avisos de llamada de atención, descuentos o entre otros.	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-010]	Registro de inclusión y exclusión de EPS	Información del ingreso y exclusión del personal a la EPS	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-011]	Formato cálculo de crédito de EPS	Cuadro de costos para calcular el descuento de la EPS al personal	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[D] Datos	[D-012]	Informe técnico sobre facturación y cobranzas	Información acerca de los montos pendientes a facturar y cobrar	Gestión de Contabilidad y Finanzas	Finanzas	Servidor Nube / Ubicación Física
	[D] Datos	[D-013]	Registros de órdenes de compras y facturas	Información acerca de las ordenes de compras y facturas de nuestros clientes	Gestión de Contabilidad y Finanzas	Finanzas	Servidor Nube
	[D] Datos	[D-014]	Registro de notas de créditos	Información acerca de las facturas anuladas	Gestión de Contabilidad y Finanzas	Finanzas	Servidor Nube

Ámbito	Categoría	ID	Activo	Descripción	Proceso	Propietario / Responsable	Ubicación
DATOS	[D] Datos	[D-015]	Formato de seguimiento de OC y facturas	Formato sobre el estado de las OC's emitidas y facturas por cobrar	Gestión de Contabilidad y Finanzas	Finanzas	Servidor Nube
	[D] Datos	[D-016]	Préstamos financieros	Información acerca de los préstamos que se realiza a los empleados y la socia empresa	Gestión de Contabilidad y Finanzas	Finanzas	Servidor Nube
	[D] Datos	[D-017]	Registro de caja chica	Información de los ingresos y gastos de la empresa	Gestión de Contabilidad y Finanzas	Contabilidad	Servidor Nube
	[D] Datos	[D-018]	Registro de cuentas por pagar	Información de las facturas que faltan por pagar	Gestión de Contabilidad y Finanzas	Contabilidad	Servidor Nube
	[D] Datos	[D-019]	Formato de movilidad	Formato para que los empleados soliciten movilidad	Gestión de Contabilidad y Finanzas	Contabilidad	Servidor Nube
	[D] Datos	[D-020]	Formato de gestión de oportunidades	Formato en donde se encuentran todas las oportunidades de negocios	Comercial	Comercial	Servidor Nube
	[D] Datos	[D-021]	Formato de propuesta técnica y económica	Información de la propuesta comercial hacia los clientes	Comercial	Comercial	Servidor Nube
	[D] Datos	[D-022]	Reporte de Actas de aceptación	Informe de OC's con actas de aceptación por proyectos	Comercial	Comercial / Asistente comercial	Servidor Nube
	[D] Datos	[D-023]	Diseño técnico detallado	Estimación de los proyectos	Gestión de proyectos	Gestor de proyectos	Servidor Nube
	[D] Datos	[D-024]	Reporte de acceso de usuarios VNP	Lista de usuarios de acceso de VNP de los clientes	Gestión de proyectos	Gestor de proyectos	Servidor Nube
	[D] Datos	[D-025]	Formato de compensación de horas (carga de trabajo)	Información de las horas extras de los empleados	Gestión de proyectos	Gestor de proyectos	-

Ámbito	Categoría	ID	Activo	Descripción	Proceso	Propietario / Responsable	Ubicación
DATOS	[D] Datos	[D-026]	Reporte de estatus de proyectos	Información de los estados de proyectos de clientes	Gestión de proyectos	Gestor de proyectos	-
	[D] Datos	[D-027]	Reporte de estatus de Staff	Información de estado del staff	Gestión de proyectos	Gestor de proyectos	-
	[D] Datos	[D-028]	Reporte de cuadro de recursos	Información de recursos que están asignados en proyectos	Gestión de proyectos	Gestor de proyectos	-
	[D] Datos	[D-029]	Control de procedimiento	Información sobre todo los procesos internos de la empresa	Calidad	Recursos humanos y Calidad	Servidor Nube
	[D] Datos	[D-030]	Plan estratégico	Información importante donde visualiza la contextualidad de la empresa	Todos los procesos	Todos los responsables de las áreas	Servidor Nube / Ubicación Física
	[D] Datos	[D-031]	Control de políticas	Información de todas las políticas internas de la empresa	Gestión Recursos humanos	Recursos humanos	Servidor Nube
SERVICIOS	[S] Servicios	[S-001]	Internet	Servicio contratado al proveedor MOVISTAR	Todos los procesos	Logística	-
	[S] Servicios	[S-002]	Correo electrónico	Correo con dominio institucional @vfcons.com, este servicio es externo contratado por Xertica	Gestión Recursos humanos	Recursos humanos	Plataforma de Xertica
	[S] Servicios	[S-003]	Repositorio de versionamiento	Repositorio en donde guardan versión de desarrollo a proyectos	Prestación de servicios Telcos	Servicios Telcos	Servidor de Github
	[S] Servicios	[S-004]	Pagos a servicios a terceros	Información de nuestros proveedores	Gestión Recursos humanos y logística	Logística	Servidor Nube

Ámbito	Categoría	ID	Activo	Descripción	Proceso	Propietario / Responsable	Ubicación
SOFTWARE	[SW] Software	[SW-001]	Antivirus	Antivirus ESET NOD32 10 unidades licencias	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[SW] Software	[SW-002]	Licencias Office 365	Utilitarios como Microsoft Office, Visio, Project, Excel, Power Point 16 unidades licencias	Gestión Recursos humanos	Recursos humanos / Logística	Plataforma de Office 365
	[SW] Software	[SW-003]	Lista de instaladores de software	Sistemas operativos, programas, office,	Prestación de servicios Telcos	Logística / Servicios Telcos	Servidor Nube
HARDWARE	[HW] Hardware	[HW-001]	Laptops administrativos	5 unidades	Gestión de Recursos Humanos, finanzas, logística, contabilidad, calidad	Recursos humanos / Logística	Ubicación Física
	[HW] Hardware	[HW-002]	Laptops gerenciales	5 unidades	Gestión comercial	Recursos humanos / Logística	Ubicación Física
	[HW] Hardware	[HW-003]	Laptop de desarrollo	25 unidades	Prestación de servicios Telcos	Recursos humanos / Logística	Ubicación Física
EQUIPAMIENTO AUXILIAR	[AUX] Equipamiento auxiliar	[AUX-001]	Impresora	Impresora EPSON L375 1 unidad	Todos los procesos	Recursos humanos	Servidor Nube / Ubicación Física
	[AUX] Equipamiento auxiliar	[AUX-002]	Archivadores	Material para separar informaciones depende de su valorización	Gestión de Recursos humanos y Calidad	Recursos humanos	Ubicación Física
	[AUX] Equipamiento auxiliar	[AUX-003]	Armarios	Lugar en donde se guardan información confidencialidad de la empresa	Gestión de Recursos humanos y Calidad	Recursos humanos	Ubicación Física
	[AUX] Equipamiento auxiliar	[AUX-004]	Discos externos	Dispositivo para guardar información	Todos los procesos	Recursos humanos	Ubicación Física

Ámbito	Categoría	ID	Activo	Descripción	Proceso	Propietario / Responsable	Ubicación
EQUIPAMIENTO AUXILIAR	[AUX] Equipamiento auxiliar	[AUX-005]	USB's	Dispositivo para guardar información	Todos los procesos	Recursos humanos	Ubicación Física
	[AUX] Equipamiento auxiliar	[AUX-006]	Monitor	Material que usan internamente para presentaciones	Todos los procesos	Recursos humanos	Ubicación Física
	[AUX] Equipamiento auxiliar	[AUX-007]	Pizarra	Material que usan internamente para presentaciones	Todos los procesos	Recursos humanos	Ubicación Física
MEDIA	[M] Media	[M-001]	Documentación administrativa	Documento interna impresa en papel como contratos, currículos	Gestión Recursos humanos	Recursos humanos	Servidor Nube / Ubicación Física
	[M] Media	[M-002]	Documentación técnica	Manual de usuarios, procedimientos y configuraciones	Prestación de servicios Telcos	Servicios Telcos	-
	[M] Media	[M-003]	Documentación contable	Documento interno impresa como facturas, ordenes de compras, recibos	Gestión de Contabilidad y Finanzas	Contabilidad	Servidor Nube / Ubicación Física
REDES DE COMUNICACIÓN	[COM] Redes de comunicaciones	[COM-001]	Red de telefonía fijo	Teléfono fijo de la oficina principal	Todos los procesos	Recursos humanos	Ubicación Física
	[COM] Redes de comunicaciones	[COM-002]	Red Inalámbrica	Wifi para oficina y para la empresa contratista	Todos los procesos	Todos los responsables de las áreas	Ubicación Física
	[COM] Redes de comunicaciones	[COM-003]	Telefonía móvil	Celulares que son asignados para proyectos de desarrollo	Desarrollo de aplicaciones	Fábrica de Software	Ubicación Física
INSTALACIÓN	[I] Instalaciones	[I-001]	Oficina Miraflores	Todos los materiales y equipos que se encuentran en la oficina	Todos los proceso	Recursos humanos / Contabilidad	Ubicación Física

ANEXO 16

VALORIZACIÓN DE ACTIVOS

ANEXO 16 VALORIZACIÓN DE ACTIVOS

VALORIZACIÓN DE ACTIVOS

Ámbito	Categoría	ID	Activo	Criterios			Total	IMPACTO
				C	I	D		
DATOS	[D] Datos	[D-001]	**Datos del personal**	7	7	8	7	A
		[D-002]	**Control de salarios**	10	9	9	9	A
		[D-003]	Datos de inventario de equipos	4	4	4	4	M
		[D-004]	Registro de certificaciones	3	5	4	4	M
		[D-005]	Formatos de entrevista de candidatos	5	4	4	4	M
		[D-006]	Lista de asistencias	3	4	3	3	B
		[D-007]	Solicitud de permisos	4	4	4	4	M
		[D-008]	Informe técnico sobre el personal	7	6	3	5	M
		[D-009]	Memorándum	7	5	3	5	M
		[D-010]	Registro de inclusión y exclusión de EPS	4	6	6	5	M
		[D-011]	Formato cálculo de crédito de EPS	4	7	7	6	M
		[D-012]	Informe técnico sobre facturación y cobranzas	6	7	6	6	M
		[D-013]	**Registros de órdenes de compras y facturas**	7	10	8	8	A
		[D-014]	Registro de notas de créditos	6	3	4	4	M
		[D-015]	Formato de seguimiento de OC y facturas	7	7	6	7	M
		[D-016]	Préstamos financieros	5	6	4	5	M
		[D-017]	Registro de caja chica	6	6	7	6	M
		[D-018]	Registro de cuentas por pagar	7	5	7	6	M
		[D-019]	Formato de movilidad	5	3	4	4	M
		[D-020]	**Formato de gestión de oportunidades**	9	7	7	8	A

Ámbito	Categoría	ID	Activo	Criterios			Total	IMPACTO
				C	I	D		
DATOS	[D] Datos	[D-021]	**Formato de propuesta técnica y económica**	9	10	7	9	A
		[D-022]	**Reporte de actas de aceptación**	9	6	7	7	A
		[D-023]	**Diseño técnico detallado**	7	8	7	7	A
		[D-024]	**Reporte de acceso de usuarios VNP**	8	9	9	9	A
		[D-025]	Formato de compensación de horas (carga de trabajo)	5	6	7	6	M
		[D-026]	**Reporte de estatus de proyectos**	6	8	8	7	A
		[D-027]	Reporte de estatus de Staff	7	5	7	6	M
		[D-028]	Reporte de cuadro de recursos	7	5	7	6	M
		[D-029]	Control de procedimiento	4	9	6	6	M
		[D-030]	Plan estratégico	3	8	9	7	M
		[D-031]	**Control de políticas**	3	8	10	7	A
SERVICIOS	[S] Servicios	[S-001]	**Internet**	4	7	9	7	M
		[S-002]	**Correo electrónico**	7	6	7	7	M
		[S-003]	**Repositorio de versionamiento**	8	10	9	9	A
		[S-004]	Pagos a servicios a terceros	6	4	5	5	M
SOFTWARE	[SW] Software	[SW-001]	Antivirus	6	5	6	6	M
		[SW-002]	**Lista de instaladores de software**	7	9	10	9	A
HARDWARE	[HW] Hardware	[HW-001]	Laptops administrativos	6	7	7	7	M
		[HW-002]	Laptops gerenciales	6	7	7	7	M
		[HW-003]	**Laptops de desarrollo**	9	9	10	9	A
EQUIPAMIENTO AUXILIAR	[AUX] Equipamiento auxiliar	[AUX-001]	Impresora	1	2	2	2	B
		[AUX-002]	Archivadores	2	1	3	2	B
		[AUX-003]	Armarios	2	1	2	2	B
		[AUX-004]	Discos externos	6	7	6	6	M

Ámbito	Categoría	ID	Activo	Criterios			Total	IMPACTO
				C	I	D		
EQUIPAMIENTO AUXILIAR	[AUX] Equipamiento auxiliar	[AUX-005]	USB's	6	7	6	6	M
		[AUX-006]	Monitor	1	3	4	3	B
		[AUX-007]	Pizarra	1	2	3	2	B
MEDIA	[M] Media	[M-001]	Documentación administrativa	6	7	7	7	M
		[M-002]	**Documentación técnica**	7	9	10	9	A
		[M-003]	Documentación contable	5	5	7	6	M
REDES DE COMUNICACIÓN	[COM] Redes de comunicaciones	[COM-001]	Red de telefonía fijo	2	1	4	2	B
		[COM-002]	Red Inalámbrica	3	7	7	6	M
		[COM-003]	Telefonía móvil	5	5	6	5	M
INSTALACIÓN	[I] Instalaciones	[I-001]	**Oficina Miraflores**	8	6	9	8	A

ANEXO *17*

EVALUACIÓN DE RIESGOS

ANEXO 17 EVALUACIÓN DE RIESGOS

ANTES DE LA APLICACIÓN DE MEDIDAS DE SEGURIDAD

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN RECURSOS HUMANOS	Control de salarios	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT063	ALTO	3	PROBABLE	3	9	E
		ALT007	ALTO	3	IMPROBABLE	2	6	A
		EXT016	ALTO	3	PROBABLE	3	9	E
		ALT011	MEDIO	2	PROBABLE	3	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	MEDIO	2	IMPROBABLE	2	4	M
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	CASI SEGURO	4	12	E
		MOD001	MEDIO	2	IMPROBABLE	2	4	M
	Correo electrónico	ALT002	MEDIO	2	PROBABLE	3	6	A
		ALT015	MEDIO	2	PROBABLE	3	6	A
		ALT016	ALTO	3	IMPROBABLE	2	6	A
		ALT020	ALTO	3	IMPROBABLE	2	6	A
		ALT027	MEDIO	2	PROBABLE	3	6	A
	Datos del personal	ALT006	MEDIO	2	PROBABLE	3	6	A
		ALT011	MEDIO	2	PROBABLE	3	6	A
		ALT015	MEDIO	2	CASI SEGURO	4	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN RECURSOS HUMANOS	Datos del personal	ALT029	MEDIO	2	PROBABLE	3	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	BAJO	1	PROBABLE	3	3	M
		MOD021	BAJO	1	PROBABLE	3	3	M
		BAJ001	MEDIO	2	RARO	1	2	B
	Control de políticas	ALT011	ALTO	3	IMPROBABLE	2	6	A
		ALT015	ALTO	3	IMPROBABLE	2	6	A
		ALT030	ALTO	3	IMPROBABLE	2	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD014	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	MEDIO	2	RARO	1	2	B
GESTIÓN DE CALIDAD	Control de procedimiento	EXT001	ALTO	3	CASI SEGURO	4	12	E
		EXT047	ALTO	3	PROBABLE	3	9	E
		ALT011	MEDIO	2	PROBABLE	3	6	A
		ALT015	MEDIO	2	PROBABLE	3	6	A
		ALT031	MEDIO	2	PROBABLE	3	9	A
		BAJ001	BAJO	1	IMPROBABLE	2	2	B
	Persona	EXT002	ALTO	3	CASI SEGURO	4	12	E
		EXT015	ALTO	3	PROBABLE	3	9	E
	Toda la documentación información	ALT035	MEDIO	2	PROBABLE	3	6	A
	Oficina de Miraflores	MOD015	MEDIO	2	IMPROBABLE	2	4	M

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN COMERCIAL	Formato de gestión de oportunidades	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT010	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT027	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	CASI SEGURO	4	12	E
		EXT052	ALTO	3	PROBABLE	3	9	E
		EXT058	ALTO	3	PROBABLE	3	9	E
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	PROBABLE	3	9	E
	Propuesta técnica y económica	EXT005	ALTO	3	PROBABLE	3	9	E
		EXT011	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT027	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT052	ALTO	3	CASI SEGURO	4	12	E
		EXT057	ALTO	3	PROBABLE	3	9	E
		EXT059	ALTO	3	PROBABLE	3	9	E
		ALT028	ALTO	3	IMPROBABLE	2	6	A
	Reporte de actas de aceptación	MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD003	MEDIO	2	IMPROBABLE	2	4	M
		MOD004	MEDIO	2	IMPROBABLE	2	4	M

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN COMERCIAL	Reporte de actas de aceptación	MOD008	BAJO	1	CASI SEGURO	4	4	M
		MOD009	BAJO	1	CASI SEGURO	4	4	M
		MOD010	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	BAJO	1	IMPROBABLE	2	2	B
	Registro de gestión de oportunidades	ALT033	ALTO	3	IMPROBABLE	2	6	A
GESTIÓN DE PROYECTOS	Diseño técnico detallado	EXT001	ALTO	3	CASI SEGURO	4	12	E
		EXT012	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		ALT002	MEDIO	2	PROBABLE	3	6	A
		ALT013	MEDIO	2	CASI SEGURO	4	8	A
		ALT024	MEDIO	2	PROBABLE	3	6	A
		ALT029	MEDIO	2	CASI SEGURO	4	8	A
		MOD005	MEDIO	2	IMPROBABLE	2	4	M
		MOD018	MEDIO	2	IMPROBABLE	2	4	M
	Reporte de acceso de usuarios VPN/Token	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT013	ALTO	3	CASI SEGURO	4	12	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT018	ALTO	3	PROBABLE	3	9	E
		EXT019	ALTO	3	CASI SEGURO	4	12	E
		EXT028	ALTO	3	CASI SEGURO	4	12	E
		EXT029	ALTO	3	PROBABLE	3	9	E

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN DE PROYECTOS	Reporte de acceso de usuarios VPN/Token	EXT032	ALTO	3	CASI SEGURO	4	12	E
		EXT053	ALTO	3	CASI SEGURO	4	12	E
		EXT058	ALTO	3	CASI SEGURO	4	12	E
		ALT009	ALTO	3	IMPROBABLE	2	6	A
		ALT011	MEDIO	2	CASI SEGURO	4	8	A
		ALT025	ALTO	3	PROBABLE	3	9	E
	Persona	EXT002	ALTO	3	CASI SEGURO	4	12	E
		EXT015	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	CASI SEGURO	4	12	E
	Reporte de estatus de proyectos	EXT001	ALTO	3	PROBABLE	3	9	E
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD006	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	MEDIO	2	IMPROBABLE	2	4	M
		MOD012	BAJO	1	CASI SEGURO	4	4	M
		MOD019	BAJO	1	PROBABLE	3	3	M
GESTIÓN DE FINANZAS	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT017	ALTO	3	PROBABLE	3	9	E
	Registros de órdenes de compras y facturas	ALT002	ALTO	3	MEDIO	2	6	A
		ALT008	ALTO	3	MEDIO	2	6	A
		ALT013	ALTO	3	MEDIO	2	6	A
		ALT014	ALTO	3	MEDIO	2	6	A
		ALT015	MEDIO	2	PROBABLE	3	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
PRESTACIÓN DE SERVICIOS TELCOS Y LOGÍTISCA	Lista de instaladores de software	EXT001	ALTO	3	PROBABLE	3	9	E
		ALT001	MEDIO	2	PROBABLE	3	6	A
		ALT012	MEDIO	2	CASI SEGURO	4	8	A
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	CASI SEGURO	4	12	E
	Laptops de desarrollo	EXT022	ALTO	3	CASI SEGURO	3	9	E
		EXT054	ALTO	3	PROBABLE	3	9	E
		ALT001	ALTO	2	IMPROBABLE	2	6	A
		ALT004	ALTO	2	IMPROBABLE	2	6	A
		ALT012	ALTO	2	IMPROBABLE	2	6	A
		ALT017	ALTO	2	IMPROBABLE	2	6	A
	Oficina de Miraflores	EXT003	ALTO	3	CASI SEGURO	4	12	E
		EXT004	ALTO	3	PROBABLE	3	9	E
PRESTACIÓN DE SERVICIOS TELCOS	Repositorio de versionamiento	EXT001	ALTO	3	CASI SEGURO	4	12	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT031	ALTO	3	CASI SEGURO	4	12	E
		ALT010	ALTO	3	IMPROBABLE	2	6	A
		ALT026	MEDIO	2	CASI SEGURO	4	8	A
		MOD007	MEDIO	2	PROBABLE	2	4	M
		MOD013	MEDIO	2	PROBABLE	2	4	M
		MOD020	BAJO	1	PROBABLE	3	3	M
	Documentación técnica	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT014	ALTO	3	PROBABLE	3	9	E
		EXT027	ALTO	3	PROBABLE	3	9	E
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT052	ALTO	3	PROBABLE	3	9	E

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
PRESTACIÓN DE SERVICIOS TELCOS	Documentación técnica	EXT060	ALTO	3	PROBABLE	3	9	E
		ALT011	MEDIO	2	CASI SEGURO	4	8	A
		ALT019	MEDIO	2	PROBABLE	3	6	A
		MOD008	ALTO	3	PROBABLE	3	9	M
		BAJ002	BAJO	3	IMPROBABLE	2	2	B
	Persona	EXT002	ALTO	3	CASI SEGURO	4	12	E
	Laptops de desarrollo	EXT006	ALTO	3	PROBABLE	3	9	E
		EXT007	ALTO	3	PROBABLE	3	9	E
		EXT008	ALTO	3	PROBABLE	3	9	E
		EXT009	ALTO	3	CASI SEGURO	4	12	E
		EXT016	ALTO	3	PROBABLE	3	9	E
		EXT030	ALTO	3	PROBABLE	3	9	E
		EXT046	ALTO	3	CASI SEGURO	4	12	E
		ALT001	ALTO	3	IMPROBABLE	2	6	A
		ALT005	MEDIO	2	CASI SEGURO	4	8	A
	Lista de instaladores	ALT011	ALTO	3	IMPROBABLE	2	6	A
TODOS LOS PROCESOS	Oficina Miraflores	EXT003	ALTO	3	PROBABLE	3	9	E
		EXT037	ALTO	3	PROBABLE	3	9	E
		EXT056	ALTO	3	PROBABLE	3	9	E
		ALT001	ALTO	3	IMPROBABLE	2	6	A
		ALT018	ALTO	3	IMPROBABLE	2	6	A
		MOD015	ALTO	3	RARO	1	3	M

DESPUÉS DE LA APLICACIÓN DE MEDIDAS DE SEGURIDAD

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN RECURSOS HUMANOS	Control de salarios	EXT001	ALTO	3	RARO	1	3	M
		EXT028	ALTO	3	IMPROBABLE	2	6	A
		EXT058	ALTO	3	RARO	1	3	M
		EXT016	ALTO	3	IMPROBABLE	2	6	A
		ALT007	ALTO	3	RARO	1	3	M
		ALT011	MEDIO	2	PROBABLE	3	6	A
		MOD002	ALTO	3	RARO	1	3	M
		MOD009	BAJO	1	PROBABLE	3	3	M
	Persona	EXT002	MEDIO	2	IMPROBABLE	2	4	M
		EXT015	ALTO	3	IMPROBABLE	2	6	A
		EXT017	MEDIO	2	IMPROBABLE	2	4	M
		MOD001	MEDIO	2	PROBABLE	3	6	A
	Correo electrónico	ALT002	MEDIO	2	IMPROBABLE	2	4	M
		ALT015	ALTO	3	PROBABLE	3	9	E
		ALT016	MEDIO	2	IMPROBABLE	2	4	M
		ALT020	MEDIO	2	IMPROBABLE	2	4	M
		ALT027	MEDIO	2	IMPROBABLE	2	4	M
	Datos del personal	ALT006	ALTO	3	RARO	1	3	M
		ALT011	ALTO	3	RARO	1	3	M
		ALT015	ALTO	3	PROBABLE	3	9	E
		ALT029	MEDIO	2	IMPROBABLE	2	4	M

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN RECURSOS HUMANOS	Datos del personal	MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	ALTO	3	RARO	1	3	M
		MOD009	MEDIO	2	IMPROBABLE	2	4	M
		MOD021	BAJO	1	IMPROBABLE	2	2	B
		BAJ001	MEDIO	2	RARO	1	2	B
	Control de políticas	ALT011	ALTO	3	RARO	1	3	M
		ALT015	ALTO	3	IMPROBABLE	2	6	A
		ALT030	ALTO	3	RARO	1	3	M
		MOD002	ALTO	3	RARO	1	3	M
		MOD014	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	MEDIO	2	RARO	1	2	B
GESTIÓN DE CALIDAD	Control de procedimiento	EXT001	ALTO	3	IMPROBABLE	2	6	A
		EXT047	MEDIO	2	IMPROBABLE	2	4	M
		ALT011	ALTO	3	IMPROBABLE	2	6	A
		ALT015	ALTO	3	RARO	1	3	M
		ALT029	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	BAJO	1	RARO	1	1	B
	Persona	EXT002	MEDIO	2	IMPROBABLE	2	4	M
		EXT015	ALTO	3	IMPROBABLE	2	6	A
	Toda la documentación información	ALT030	MEDIO	2	PROBABLE	3	6	A
	Oficina de Miraflores	MOD015	ALTO	3	IMPROBABLE	2	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN COMERCIAL	Formato de gestión de oportunidades	EXT001	ALTO	3	RARO	1	3	M
		EXT010	ALTO	3	IMPROBABLE	2	6	A
		EXT016	MEDIO	2	IMPROBABLE	2	4	M
		EXT027	ALTO	3	RARO	1	3	M
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT052	ALTO	3	RARO	1	3	M
		EXT058	ALTO	3	IMPROBABLE	2	6	A
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
	Persona	EXT002	MEDIO	2	IMPROBABLE	2	4	M
		EXT015	ALTO	3	RARO	1	3	M
		EXT017	ALTO	3	IMPROBABLE	2	6	A
	Propuesta técnica y económica	EXT005	ALTO	3	IMPROBABLE	2	6	A
		EXT011	ALTO	3	IMPROBABLE	2	6	A
		EXT016	ALTO	3	RARO	1	3	M
		EXT027	MEDIO	2	RARO	1	2	B
		EXT028	ALTO	3	PROBABLE	3	9	E
		EXT052	ALTO	3	RARO	1	3	M
		EXT057	ALTO	3	PROBABLE	3	9	E
		EXT059	ALTO	3	IMPROBABLE	2	6	A
		ALT028	ALTO	3	IMPROBABLE	2	6	A
	Reporte de actas de aceptación	MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD003	MEDIO	2	IMPROBABLE	2	4	M
		MOD004	MEDIO	2	IMPROBABLE	2	4	M

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
GESTIÓN COMERCIAL	Reporte de actas de aceptación	MOD008	BAJO	1	CASI SEGURO	4	4	M
		MOD009	BAJO	1	CASI SEGURO	4	4	M
		MOD010	MEDIO	2	IMPROBABLE	2	4	M
		BAJ001	BAJO	1	IMPROBABLE	2	2	B
	Registro de gestión de oportunidades	ALT029	ALTO	3	IMPROBABLE	2	6	A
GESTIÓN DE PROYECTOS	Diseño técnico detallado	EXT001	ALTO	3	IMPROBABLE	2	6	A
		EXT012	ALTO	3	IMPROBABLE	2	6	A
		EXT016	ALTO	3	RARO	1	3	M
		EXT028	ALTO	3	IMPROBABLE	2	6	A
		ALT002	MEDIO	2	IMPROBABLE	2	4	M
		ALT013	MEDIO	2	IMPROBABLE	2	4	M
		ALT024	MEDIO	2	IMPROBABLE	2	4	M
		ALT029	MEDIO	2	IMPROBABLE	2	4	M
		MOD005	MEDIO	2	RARO	1	2	B
		MOD018	MEDIO	2	IMPROBABLE	2	4	M
	Reporte de acceso de usuarios VPN/Token	EXT001	ALTO	3	PROBABLE	3	9	E
		EXT013	ALTO	3	IMPROBABLE	2	6	A
		EXT016	ALTO	3	RARO	1	3	M
		EXT018	ALTO	3	IMPROBABLE	2	6	A
		EXT019	ALTO	3	IMPROBABLE	2	6	A
		EXT028	ALTO	3	IMPROBABLE	2	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
	Reporte de acceso de usuarios VPN/Token	EXT029	ALTO	3	PROBABLE	3	9	E
GESTIÓN DE PROYECTOS		EXT032	ALTO	3	IMPROBABLE	2	6	A
		EXT053	ALTO	3	IMPROBABLE	2	6	A
		EXT058	ALTO	3	IMPROBABLE	2	6	A
		ALT009	ALTO	3	RARO	1	3	M
		ALT011	MEDIO	2	IMPROBABLE	2	4	M
		ALT025	ALTO	3	IMPROBABLE	2	6	A
	Persona	EXT002	ALTO	3	RARO	1	3	M
		EXT015	ALTO	3	IMPROBABLE	2	6	A
		EXT017	ALTO	3	IMPROBABLE	2	6	A
	Reporte de estatus de proyectos	EXT001	ALTO	3	IMPROBABLE	2	6	A
		MOD002	MEDIO	2	IMPROBABLE	2	4	M
		MOD006	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
		MOD009	MEDIO	2	RARO	1	2	B
		MOD012	BAJO	1	CASI SEGURO	4	4	M
		MOD019	BAJO	1	PROBABLE	3	3	M
GESTIÓN DE FINANZAS	Persona	EXT002	ALTO	3	IMPROBABLE	2	6	A
		EXT017	ALTO	3	IMPROBABLE	2	6	A
	Registros de órdenes de compras y facturas	ALT002	ALTO	3	IMPROBABLE	2	6	A
		ALT008	ALTO	3	RARO	1	3	M
		ALT013	ALTO	3	RARO	1	3	M
		ALT014	ALTO	3	IMPROBABLE	2	6	A
		ALT015	MEDIO	2	IMPROBABLE	2	4	M

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
PRESTACIÓN DE SERVICIOS TELCOS Y LOGÍTISCA	Lista de instaladores de software	EXT001	ALTO	3	PROBABLE	3	9	E
		ALT001	MEDIO	2	PROBABLE	3	6	A
		ALT012	MEDIO	2	IMPROBABLE	2	4	M
	Persona	EXT002	ALTO	3	PROBABLE	3	9	E
		EXT015	ALTO	3	IMPROBABLE	2	6	A
	Laptops de desarrollo	EXT022	ALTO	3	RARO	1	3	M
		EXT054	ALTO	3	IMPROBABLE	2	6	A
		ALT001	ALTO	3	PROBABLE	3	9	E
		ALT004	MEDIO	2	IMPROBABLE	2	4	M
		ALT012	MEDIO	2	IMPROBABLE	2	4	M
		ALT017	MEDIO	2	IMPROBABLE	2	4	M
	Oficina de Miraflores	EXT003	ALTO	3	RARO	1	3	M
		EXT004	ALTO	3	RARO	1	3	M
PRESTACIÓN DE SERVICIOS TELCOS	Repositorio de versionamiento	EXT001	ALTO	3	IMPROBABLE	2	6	A
		EXT016	MEDIO	2	IMPROBABLE	2	4	M
		EXT031	ALTO	3	IMPROBABLE	2	6	A
		ALT010	ALTO	3	RARO	1	3	M
		ALT026	MEDIO	2	IMPROBABLE	2	4	M
		MOD007	MEDIO	2	RARO	1	2	B
		MOD013	MEDIO	2	IMPROBABLE	2	4	M
		MOD020	BAJO	1	IMPROBABLE	2	2	B
	Documentación técnica	EXT001	MEDIO	2	IMPROBABLE	2	4	M
		EXT014	MEDIO	2	PROBABLE	3	6	A

PROCESO	ACTIVO	ID DEL RIESGO	AMENAZA		OCURRENCIA		RIESGO	
			IMPACTO	VALOR	PROBABILIDAD	VALOR	TOTAL	ZONA DE RIESGO
PRESTACIÓN DE SERVICIOS TELCOS	Documentación técnica Persona	EXT027	ALTO	3	IMPROBABLE	2	6	A
		EXT028	ALTO	3	IMPROBABLE	2	6	A
		EXT052	ALTO	3	IMPROBABLE	2	6	A
		EXT060	MEDIO	2	IMPROBABLE	2	4	M
		ALT011	MEDIO	2	IMPROBABLE	2	4	M
		ALT019	MEDIO	2	IMPROBABLE	2	4	M
		MOD008	MEDIO	2	IMPROBABLE	2	4	M
		BAJ002	ALTO	3	IMPROBABLE	2	6	A
		EXT002	MEDIO	2	RARO	1	2	B
	Laptops de desarrollo	EXT006	ALTO	3	PROBABLE	3	9	E
		EXT007	ALTO	3	IMPROBABLE	2	6	A
		EXT008	ALTO	3	IMPROBABLE	2	6	A
		EXT009	ALTO	3	PROBABLE	3	9	E
		EXT016	ALTO	3	RARO	1	3	M
		EXT030	ALTO	3	IMPROBABLE	2	6	A
		EXT046	ALTO	3	CASI SEGURO	4	12	E
		ALT001	ALTO	3	PROBABLE	3	9	E
		ALT005	MEDIO	2	IMPROBABLE	2	4	M
	Lista de instaladores	ALT011	ALTO	3	RARO	1	3	M
TODOS LOS PROCESOS	Oficina Miraflores	EXT003	ALTO	3	PROBABLE	3	9	E
		EXT037	ALTO	3	PROBABLE	3	9	E
		EXT056	ALTO	3	PROBABLE	3	9	E
		ALT001	ALTO	3	PROBABLE	3	9	E
		ALT018	ALTO	3	IMPROBABLE	2	6	A
		MOD015	ALTO	3	IMPROBABLE	2	6	A

ANEXO 18

PLAN DE TRATAMIENTO DE RIESGOS

ANEXO 18 PLAN DE TRATAMIENTO DE RIESGOS

Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	2018 Abril	2018 May.	2018 Jun.	2018 Jul.	Resultado
6. Organización de la seguridad de la información	6.1.1	Control de salarios	EXT001	Descuido del responsable de no actualizar los datos y/o error al ingresar los datos correspondientes: - Errores en las boletas de pagos o en el costeo de recursos en los proyectos. -Equivocación o pérdida de tiempo al ejecutar los procedimientos de los procesos internos - Pérdidas de oportunidades de negocio. -Estimaciones de proyectos incorrectos. -Accesos no autorizados a los sistemas externos de los clientes. -Retrasos en los proyectos al no encontrar el software requerido o no estar con la versión reciente. -Confusión o retrasos en los proyectos con no contar con la última versión aceptada. -Retrasos en el desarrollo de los proyectos debido a la falta actualización de los manuales de procedimientos, técnicas.	EXTREMA	REDUCIR	Coordinadora de Recursos Humanos	**1. Memorandum (llamada de atención)** Documento en el cuál se comunicará al personal la actualización obligatoria de su información, así mismo este documento servirá como una llamada de atención al personal que infringe este control. **2. Aviso vía correo de actualización de información** Enviar un correo masivo indicando o haciendo recordar que deben actualizar su información, es decir subirla a la carpeta drive compartida de su área correspondiente. Además recordarles que deben hacer copias de respaldos a los equipos. **3. Ficha de puestos** Buscar a personas con conocimiento en seguridad de la información en caso de que no segregar la tarea de registrar, actualizar y evitar el mal uso de activos.	Gerente de Administración	1					TERMINADO
		Control de procedimiento					Coordinadora de Calidad		Gerente de Administración						
		Formato de gestión de oportunidades					Sub gerente del área comercial		Gerente Comercial						
		Diseño técnico detallado					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Reporte de acceso de usuarios VNP/ Tocken					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Reporte de estatus de proyectos					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Lista de instaladores de software					Encargado de Logística		Gerente de Administración						
		Repositorio de versionamiento					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
		Documentación técnica					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
	6.1.2	Persona	EXT002	Los encargados de áreas no supervisan a su personal con respecto a los accesos de usuarios ocasionando alteración o modificación de datos.	EXTREMA	REDUCIR	Todo el personal	**1. Organigrama de puestos** Identificar cuáles son los responsables de cada área para segregar tareas para evitar el uso incorrecto de los activos.	Encargado del área correspondiente	1					TERMINADO
	6.1.3	Oficina de Miraflores	EXT003	Posible accidente que se producen sin la intervención humana como incendios en las instalaciones, a demás accidentes como desastres naturales (Terremotos, sismos, tsunami, entre otros)	EXTREMA	TRANSFERIR	Encargado de Logística	**1. Proveedores de instalación de medidas de seguridad para oficinas.** Contar con una empresa externa que se encarge en la protección de incendios y además de asesoramiento al personal para que pueda desenvolverse adecuadamente ante un aviso de incendio. **2. Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)** Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros. **3.Lista de contacto de autoridades** Lista en la cual se encuentran las autoridades pertinentes a contactar de presentarse un incidente mayor.	Gerente de Administración	2					PENDIENTE
			EXT004	Además no cuentan con proveedores en donde haya intercambio de información para mejorar los asuntos de la seguridad de la información	EXTREMA	TRANSFERIR	Encargado de Logística		Gerente de Administración						

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
6. Organización de la seguridad de la información	6.1.5	Propuesta técnica y económica	EXT005	Fuga de información (accidental o intensional) pueden dañar la reputación de la empresa ya sea con fines maliciosos o beneficio propio debido a que no especifican en las propuestas. Fuga de información (accidental o intensional) pueden dañar la reputación de la empresa debido a que no cuentan con una política o un acuerdo del uso correcto de los dispositivos móviles.	EXTREMA	REDUCIR	Sub gerente del área comercial	**1. Procedimiento de propuestas** Agregar en términos y condiciones de las propuestas que la información brindada en las propuestas como el alcance, tiempo y costo sea condifencial y no divulgada con usuarios no autorizados tanto para la consultora como para el cliente. **2. El acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información expuesta en el correo institucional de los colaboradores para evitar fugas de información, acceso no autorizados. entre otros. **3. Política de seguridad de correo electrónico** Política para el uso correcto del correo electrónico, recalcando que la información es confidencial y no se debe usar para fines propios.	Gerente Comercial	1				TERMINADO
	6.2.2	Laptos de desarrollo	EXT006	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas, ocasionando fuga de información.	EXTREMA	REDUCIR	Encargado de Servicios Telcos	**1. Política de teletrabajo y penalidades.** Política para los colaboradores que trabajan en remoto o cuando se llevan las laptops para realizar actividades desde a fuera de la oficina. **2. Formato de entrega de equipos.** Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo.	Gerente de Serivicios Telcos	1				TERMINADO
			EXT007	Alteración intencionada del funcionamiento de sistemas de los clientes, persiguiendo un beneficio indirecto.	EXTREMA	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
			EXT008	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, ocasionando una fuga de información.	EXTREMA	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
			EXT009	Victimas de vandalismo, terrorismo que haga perder la información llevada en el activo.	EXTREMA	TRANSFERIR	Encargado de Servicios Telcos	**3. Contratar una empresa aseguradora (Póliza de equipos)** Contar con una empresa aseguradora que permita proteger los equipos electrónicos (computadoras, laptops, etc) contra robos, vandalismo o daños internos.	Gerente de Serivicios Telcos	2					PENDIENTE

											2018				
Cláusula del control ISO/IEC 27002	**Control ISO/IEC 27002**	**Activo**	**ID del Riesgo**	**Descripción del riesgo**	**Nivel de Riesgo**	**Estrategia de respuesta**	**Propietario del Riesgo**	**Plan de acción**	**Responsable del control**	**Grupo**	**Abril**	**May.**	**Jun.**	**Jul.**	**Resultado**
7. Seguridad de los recursos humanos	**7.1.2**	Formato de gestión de oportunidades	EXT010	Fuga de información (accidental o intensional) ocasionando pérdida de clientes y problemas financieros.	EXTREMA	REDUCIR	Sub gerente del área comercial	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. **2. Política de uso, manejo de informacion confidencial y pérdida de información VF** Definir los estandares para salvaguardar la información contra uso no autorizado, divulgación o revelación. **3. Agregar investigación de antecedentes al proceso de contratación del personal** En el procedimiento de contratación debe señalar en qué momento, quién y cómo se pedirán o realizarán las investigaciones de antecedentes penales de los futuros colaboradores debido a que se asignará información clasificada y confidencial.	Gerente Comercial	1					TERMINADO
		Propuesta técnica y económica	EXT011	Divulgar los datos personales afectaría al decreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores.	EXTREMA	REDUCIR	Sub gerente del área comercial		Gerente Comercial						
		Diseño técnico detallado	EXT012	Se modifica intensionalmente las estimaciones afectando retrasos de tiempo en los servicios.	EXTREMA	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Reporte de acceso de usuarios VNP/ Tocken	EXT013	Divulgar los accesos de usuarios VNP ocasionaría desconfianza de nuestros clientes al momento de utilizar sus sistemas y proceder con multas penales.	EXTREMA	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Documentación técnica	EXT014	Divulgar la documentación técnica afectaríala solución estrategica de nuestros servicios siendo una gran desventaja frente a nuestros competidores.	EXTREMA	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
	7.2.1	Persona	EXT015	No se cuentan con acuerdos con los colaboradores, proveedores y terceros ocacionando un daño considerable a la organización	EXTREMA	REDUCIR	Todos los encargados	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. **2. Política de proveedores** Política basada en establecer condiciones necesarias en caso de acceso a la información de la empresa por los proveedores.	Encargado del área correspondiente	1					TERMINADO

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
7. Seguridad de los recursos humanos	7.2.2	Control de salarios Formato de gestión de oportunidades Propuesta técnica y económica Diseño técnico detallado Reporte de acceso de usuarios VNP/ Laptops de desarrollo Repositorio de versionamiento	EXT016	Debido a que en la consultora no cuentan con una política o capacitación sobre la seguridad de la información sucede las siguientes incidencias: -Pérdida de la información (accidental o intensional) tanto física y/o digital. -Acceso de usuarios no autorizados en el control de salarios, formatos de gestión de oportunidades, propuestas para fines propios. -Alteración en el gestión de oportunidades, en los usuarios VPN, en el versionamiento, en los sistemas de los clientes, ocasionando pérdida en la cartera de clientes y perjuicio.	EXTREMA	REDUCIR	Coordinadora de Recursos Humanos Sub gerente del área comercial Sub gerente del área comercial Encargado de Gestión de proyectos Encargado de Gestión de proyectos Encargado de Servicios Telcos Encargado de Servicios Telcos	**1. Plan de capacitación y concientización** Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros.	Gerente de Administración Gerente Comercial Gerente Comercial Oficina de Gestión de proyectos Oficina de Gestión de proyectos Gerente de Serivicios Telcos Gerente de Serivicios Telcos	1					TERMINADO
	7.2.3	Persona	EXT017	No contaban con la clasificación de sasiones de acuerdo a la falta ocasionando pérdida de toma de decisión.	EXTREMA	REDUCIR	Todos los encargados	**1. Memorandum (llamada de atención)** Documento en la cuál se comunicará al personal la actualización obligatoria de su información, así mismo este documento sirvará como una llamada de atención a aquella personal que infringe este control. **2. Tipos de sanciones de acuerdo a la seguridad de la información** Contar con sanciones que infringe la seguridad de la información de la empresa y así tomar decisiones correctas al momento de aplicarlas.	Encargado del área correspondiente	1					TERMINADO
	7.3.1	Reporte de acceso de usuarios VNP/ Tocken	EXT018	Descuido del responsable de no realizar en constante actualización el acceso de usuarios VNP de los clientes	EXTREMA	REDUCIR	Encargado de Gestión de proyectos	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de los usuarios de VPN y que sanciones aquel personal que infringe este acuerdo. **2. Comunicado de terminación y cambio de empleo** Comunicar a todo el personal tanto a gerentes y colaboradores la terminación de un contrato de un personal para que estén informados y actualizados.	Oficina de Gestión de proyectos	1					TERMINADO
			EXT019	Tener acceso al reporte de acceso de usuarios VNP, puede ocasionar fugas de información, robo de información, fraudes.	EXTREMA	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
8. Gestión de activos	8.1.1	Todos los activos mencionados	EXT020	Carencia de inventario de activos ocasiona inseguridad de información, mala gestión financiera, pérdida de activos de alto impacto, entre otros.	EXTREMA	REDUCIR	Todos los encargados	**1. Inventario de activos** Inventariar los activos más relevantes en su ciclo de vida y documentar su importancia, además debe ser preciso y en constante actualización. Todo activo debe tener un propietario/responsable que valide que los activos están bien clasificados, ya que se deben revisar periódicamente y debe tener en cuenta los controles de seguridad aplicables a su activo	Encagado de la seguridad de la información	1					TERMINADO
	8.1.2		EXT021	Por ausencia del inventario de activos, no se conoce quienes son los propiertarios y/o responsables de los activos y riesgos	EXTREMA	REDUCIR	Todos los encargados								
	8.1.4	Laptos de desarrollo	EXT022	Carencia de recursos de equipos provoca carga de trabajo o prestación de servicios ocasionando atrasos en los proyectos. Carencia del procedimiento de disvinculación del personal ocasionando pérdida de recursos o demora en la entrega de material a los nuevos colaboradores.	EXTREMA	REDUCIR	Encargado de Logística / ServiciosTelcos	**1. Formato de entrega de equipos.** Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo. **2.Agregar el procedimiento de entrega de activos en el proceso de desvinculación del personal** En el proceso de desvinculación del personal se debe agragr el procedimiento en donde el personal debe retornar todos los activos de la consultora ya sea por contrato o acuerdo.	Gerente de Administración / Gerente de Servicios Telcos	1					TERMINADO
	8.2.1	Todos los activos mencionados	EXT023	Al no tener clasificada los activos de información, la empresa no sabe que activos son más revelantes de riesgos y cuáles no ocasionando inseguridad en sus activos.	EXTREMA	REDUCIR	Todos los encargados	**1. Clasificación y valorización de activos de información** Se debe valorizar los activos de acuerdo a los tres criterios: confidencialidad, integridad y disponibilidad, además la clasificación y valorizacion se deben actualizar cuando cambie su valor a lo largo de su ciclo de vida.	Encagado de la seguridad de la información	1					TERMINADO
	8.2.2		EXT024	No cuentan con etiquetado de información de sus activos, es decir que no identifican qué activo debe ser desarrollado e implementado.	EXTREMA	REDUCIR	Todos los encargados	**1. Procedimiento de control de información documentada** Tiene como objetivo describir las actividades para establecer, documentar, controlar y mantener los documentos (procedimientos, formatos, registros, etc), de acuerdo con los requisitos establecidos por la organización.	Encagado de la seguridad de la información						TERMINADO
	8.2.3		EXT025	No cuentan con procedimientos de desarrollo e implementación de activos.	EXTREMA	REDUCIR	Todos los encargados								

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
8. Gestión de activos	8.3.1	Laptos de desarrollo	EXT026	Por el debido uso de laptop para la realización de los servicios fuera de la oficina pueden ser victimas de vandalismo, terrorismo que haga perder la información llevada en el activo.	EXTREMA	REDUCIR	Encargado de Servicios Telcos	**1. Soporte técnico externo para el mantenimiento preventivo y correctivo de los equipos.** Contar con una empresa externa que permita realizar periódicamente mantenimiento, diagnóstico y reparación a los equipos informáticos **2. Inventario de equipos** En el inventario se encuentra la lista de los equipos, su estado, responsable, etc.	Gerente de Serivicios Telcos	2					PENDIENTE
	8.3.2	Formato de gestión de oportunidades	EXT027	Al no contar con procedimientos formales para la eliminación segura de elementos o información cuando ya no es necesaria, ocasionando fuga de información, pérdida de clientes, reputación, problemas financieros, retrasos en los proyectos, entre otros, ya que puede estar de manera visible para todo el personal.	EXTREMA	REDUCIR	Sub gerente del área comercial	**1. Procedimiento de destrucción o eliminación de documentos** Contar con procedimientos que permitan eliminar de forma segura de los documentos que contienen información que ya no sean necesarios para así evitar fugas de información de usuarios no autorizados.	Gerente Comercial	1					TERMINADO
		Propuesta técnica y económica					Sub gerente del área comercial		Gerente Comercial						
		Documentación técnica					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
9. Control de acceso	9.1.1	Control de salarios	EXT028	Carencia de una política de control de acceso ocasionando pérdida de información condifencial, disminución de cartera de clientes, fuga de talentos, desconfianza en los clientes.	EXTREMA	REDUCIR	Coordinadora de Recursos Humanos	**1. Política de control de acceso** Contar con una política en donde indique cuales son los responsables que deben tener acceso a las carpetas del drive y que información pueden acceder. **2. Plan de capacitación y concientización** Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros. **3. Árbol de carpeta para el acceso a usuarios** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de administración	1					TERMINADO
		Formato de gestión de oportunidades					Sub gerente del área comercial		Gerente Comercial						
		Propuesta técnica y económica					Sub gerente del área comercial		Gerente Comercial						
		Diseño técnico detallado					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Reporte de acceso de usuarios VNP/ Tocken					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Documentación técnica					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
	9.1.2	Reporte de acceso de usuarios VNP/ Tocken	EXT029	Acceso no autorizados al reporte de acceso de usuarios VPN, puede ocasionar fugas de información, robo de información, fraudes hacia nuestros clientes, entre otros.	EXTREMA	REDUCIR	Encargado de Gestión de proyectos	**1. Tipos de sanciones de acuerdo a la seguridad de la información** Contar con sanciones que infringe la seguridad de la información de la empresa y así tomar decisiones correctas al momento de aplicarlas.	Oficina de Gestión de proyectos	1					TERMINADO

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
9. Control de acceso	9.2.1	Laptos de desarrollo	EXT030	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas, alteració o fuga de información.	EXTREMA	REDUCIR	Encargado de Servicios Telcos	**1. Árbol de carpeta para el acceso a usuarios** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de Serivicios Telcos	1					TERMINADO
		Repositorio de versionamiento	EXT031	Consigue los accesos del activo sin tener autorización para ello, típicamente aprovechando un descuido del personal.	EXTREMA	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
	9.2.2	Reporte de acceso de usuarios VNP/ Tocken	EXT032	Divulgar los accesos de usuarios VPN ocasionaría desconfianza de nuestros clientes al momento de utilizar sus sistemas.	EXTREMA	REDUCIR	Encargado de Gestión de proyectos	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de los usuarios de VPN y que sanciones aquel personal que infringe este acuerdo.	Oficina de Gestión de proyectos	1					TERMINADO
	9.2.4	Laptos de desarrollo	EXT033	Alteración intencionada del funcionamiento de sistemas de los clientes, persiguiendo un beneficio indirecto.	EXTREMA	REDUCIR	Encargado de Servicios Telcos	**1. El acuerdo de confidencialidad de la seguridad de la información** Cláusula que señale la firma de compromiso de mantener la confidencialidad de la información brindada en forma secreta para la autenticación personal. **2.Política de seguridad de pantallas, escritorios limpios y contraseñas seguras** Política del correcto uso de equipos con respecto a la seguridad de la información como salvapantallas, escritorios limpios, contraseñas seguras.	Gerente de Serivicios Telcos	1					TERMINADO
	9.2.5	Todos los activos mencionados	EXT034	No cuentan con un directorio de acceso en donde indica quienes son los usuarios que tienen acceso a tal carpeta, lo que ocasiona pérdida de información confidencial.	EXTREMA	REDUCIR	Todos los encargados	**1. Árbol de carpeta para el acceso a usuarios** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas. **2. Aviso vía correo de actualización de información** Enviar un correo masivo indicando o haciendo recordar que deben actualizar su información, es decir subirla a la carpeta drive compartida de su área correspondiente. Además recordarles que deben hacer copias de respaldos a los equipos.	Encagado de la seguridad de la información	1					TERMINADO

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
9. Control de acceso	9.2.6	Todos los activos mencionados	EXT035	No cuentan con un procedimiento en que indique que los colaboradores que no pertenecen a la empresa hayan dejado los accesos o se haya disvinculado de los derechos de usuarios, esto ha ocasionado pérdida de información y divulgación a los competidores.	EXTREMA	REDUCIR	Todos los encargados	**1.Agregar el procedimiento de desvinculación de acceso a usuario en el proceso de desvinculación del personal** Tras la finalización del empleo, los derechos de acceso del personal a la información y activos asociados deberían eliminarse o suspender para evitar fugas de información.	Encagado de la seguridad de la información	1					TERMINADO
	9.3.1		EXT036	Toda información es visible para todos, a demás el uso de contraseñas es deseada baja causando divulgación entre los colaboradores.	EXTREMA	REDUCIR	Todos los encargados	**1. El acuerdo de confidencialidad de la seguridad de la información** Indica el compromiso de mantener la confidencialidad de la información brindada en forma secreta para la autenticación personal. **2.Política de seguridad de pantallas, escritorios limpios y contraseñas seguras** Política del correcto uso de equipos con respecto a la seguridad de la información como salvapantallas, escritorios limpios, contraseñas seguras.	Encagado de la seguridad de la información	1					TERMINADO
11. Seguridad física y ambiental	11.1.4	Oficina de Miraflores	EXT037	Posible accidente que se producen sin la intervención humana como incendios en las instalaciones, a demás accidentes como desastres naturales (Terremotos, sismos, tsunami, entre otros)	EXTREMA	TRANSFERIR	Encargado Empresa contratista	**1. Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)** Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros.	Encargado Empresa contratista	2					PENDIENTE
	11.2.1	Laptos de desarrollo	EXT038	Afecta a la disponibilidad del activo para la realización de trabajos, debido excesivo calor, frío, humedad, etc.	EXTREMA	TRANSFERIR	Todos los encargados	**1. Soporte técnico externo para el mantenimiento preventivo y correctivo de los equipos** Contar con una empresa externa que permita realizar periódicamente mantenimiento, diagnóstico y reparación a los equipos informáticos (laptops, impresoras, monitores, cargadores, entre otros)	Gerente de todas las áreas involucradas	2					PENDIENTE
			EXT039	El atacante consigue el acceso al activo sin tener autorización aprovechando un descuido del personal responsable.	EXTREMA	REDUCIR	Todos los encargados	**2.Política de seguridad de pantallas, escritorios limpios y contraseñas seguras** Política del correcto uso de equipos con respecto a la seguridad de la información como salvapantallas, escritorios limpios, contraseñas seguras.	Gerente de todas las áreas involucradas	1					TERMINADO
			EXT040	Suciedad en los equipos debido al mal uso por parte de los colaboradores ocasionando futuros retrasos en el trabajo.	EXTREMA	REDUCIR	Todos los encargados	**3. Directrices para comer beber y fumar en las instalaciones de la oficina** Contar con directrices donde indique lo que se debe o no se debe hacer en las instalaciones de la oficina y no afectar a los activos.	Gerente de todas las áreas involucradas						TERMINADO

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
11. Seguridad física y ambiental	11.2.4	Laptos de desarrollo	EXT041	Los equipos actualmente no cuentan con un mantenimiento de equipos	EXTREMA	TRANSFERIR	Todos los encargados	**1. Formato de entrega de equipos** Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo. **2. Plan de capacitación y concientización** Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros. **3.Política de seguridad de pantallas, escritorios limpios y contraseñas seguras** Política del correcto uso de equipos con respecto a la seguridad de la información como salvapantallas, escritorios limpios, contraseñas seguras. **4. Política de teletrabajo y penalidades** Política para los colaboradores que trabajan en remoto o cuando se llevan las laptops para realizar actividades desde a fuera de la oficina.	Gerente de todas las áreas involucradas	1					TERMINADO
	11.2.5		EXT042	Los colaboradores se llevan los equipos debido a que la mayoría trabajan en la misma empresa contratista o en su casa pero no cuentan con un acuerdo que diga la seguridad del equipo.	EXTREMA	REDUCIR	Todos los encargados		Gerente de todas las áreas involucradas						TERMINADO
	11.2.6				EXTREMA	REDUCIR	Todos los encargados		Gerente de todas las áreas involucradas						TERMINADO
	11.2.7		EXT043	No cuentan con un procedimiento en donde indique que hacer con los equipos que están libres si se pueden reutilizar o no.	EXTREMA	REDUCIR	Todos los encargados		Gerente de todas las áreas involucradas						TERMINADO
	11.2.8		EXT044	La mayoria de los colaboradores dejan sus laptops de manera visible sin suspenderlo lo que ocasiona pérdida de información.	EXTREMA	REDUCIR	Todos los encargados		Gerente de todas las áreas involucradas						TERMINADO
	11.2.9		EXT045	La mayoria de los colaboradores tiene en la pantalla visible de archivos e información confidencial no cuentan con pantalla limpia.	EXTREMA	REDUCIR	Todos los encargados		Gerente de todas las áreas involucradas						TERMINADO
12. Seguridad de operaciones	12.1.1	Laptos de desarrollo	EXT046	No realizan copias de respaldos ni mantenimiento de equipos causando problemas al querer buscar información o ejecutar un servicio.	EXTREMA	REDUCIR	Encargado de Servicios Telcos	**1. Soporte técnico externo para el mantenimiento preventivo y correctivo de los equipos** Contar con una empresa externa que permita realizar periódicamente mantenimiento, diagnóstico y reparación a los equipos informáticos (laptops, impresoras, monitores, cargadores, entre otros)	Gerente de Serivicios Telcos	2					PENDIENTE
	12.1.2	Control de procedimiento	EXT047	No cuentan con una gestión de cambio en los procesos internos y de negocio de la empresa, ocasionando desconocimiento del personal y eventos imprevistos	EXTREMA	REDUCIR	Coordinadora de Calidad	**1. Gestión de cambio** Contar con una gestión de cambio para que ayude a la organización a adaptar exitosamente nuevas formas o tecnologías de hacer negocio y mejorar los procesos internos.	Gerente de Administración	2					PENDIENTE
	12.2.1	Laptos de desarrollo	EXT048	No cuentan con un control del uso de los software's instalados, debido a que el mismo personal se instalan causando daño a los equipos.	EXTREMA	REDUCIR	Todos los encargados	**1. Control de software's instalados** Tener un control de los software's autorizados para evitar daños en los equipos y fugas de información.	Gerente de todas las áreas involucradas	2					PENDIENTE

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
12. Seguridad de operaciones	12.3.1	Laptos de desarrollo	EXT049	No se realizan copias de respaldos de los equipos ni tienen un backup de los servicios que han sido brindados.	EXTREMA	REDUCIR	Todos los encargados	**1. Aviso vía correo de actualización de información** Enviar un correo masivo indicando o haciendo recordar que deben actualizar su información, es decir subirla a la carpeta drive compartida de su área correspondiente. Además recordarles que deben hacer copias de respaldos a los equipos.	Gerente de todas las áreas involucradas	1					TERMINADO
	12.6.1		EXT050	No cuentan con una gestión de vulnerabilidad debido a que no contaban con un inventario de activos por la cuál no evaluaban para ver que las vulnerabilidades, causando amenazas y riesgos.	EXTREMA	REDUCIR	Todos los encargados	**1. Evaluación de riesgos** Cuadro de evaluación de los activos de información de alto impacto de la organización. **2. Clasificación y valorización de activos de información** Se debe valorizar los activos de acuerdo a los tres criterios: confidencialidad, integridad y disponibilidad, a demás la clasificación y valorizacion se deben actualizar cuando cambie su valor a lo largo de su ciclo de vida.	Gerente de todas las áreas involucradas	1					TERMINADO
12. Seguridad de operaciones	12.6.2	Laptos de desarrollo	EXT051	No cuentan con un control del uso de los software's instalados, debido a que el mismo personal se instalan causando daño a los equipos.	EXTREMA	REDUCIR	Todos los encargados	**1. Control de software's instalados** Tener un control de los software's autorizados para evitar daños en los equipos y fugas de información. **2. Creación de perfil de usuarios** Crear perfiles de usuarios al momento de asignar un equipo, solo algunos usuarios tendrán acceso al usuario "administrador" y otros solo "usuario" para restringir la instalación de software's no autorizados.	Gerente de todas las áreas involucradas	2					PENDIENTE
13. Seguridad de las comunicaciones	13.2.4 13.2.2	Formato de gestión de oportunidades	EXT052	Fuga de información (accidental o intencional) pueden ocasionar pérdida de clientes y problemas financieros. Divulgar información relevante lo cual ocasiona una gran desventaja frente a nuestros competidores.	EXTREMA	REDUCIR	Sub gerente del área comercial	**1. Acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos.	Gerente Comercial	1					TERMINADO
		Propuesta técnica y económica					Sub gerente del área comercial		Gerente Comercial						
		Documentación técnica					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
		Reporte de acceso de usuarios VNP/ Tocken	EXT053	Acceso de usuarios no autorizados en visualizar los reportes de acceso de usuarios VNP para fines maliciosos o beneficio propio. Divulgar los accesos de usuarios VNP ocasionaría desconfianza de nuestros clientes al momento de utilizar sus sistemas.	EXTREMA	REDUCIR	Encargado de Gestión de proyectos		Gerente de proyectos						

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
15. Relaciones con los proveedores	15.1.1 15.1.2 15.1.3	Formato de gestión de oportunidades	EXT054	Fuga de información al no tener indentificado y documentado los tipos de proveedores que puedan acceder a nuestra información.	EXTREMA	REDUCIR	Sub gerente del área comercial	**1. Política de proveedores** Política basada en establecer condiciones necesarias en caso de acceso a la información de la empresa por los proveedores. **2. Acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información de la organización brindada y recibida por ambas partes para cimplir con los requisitos de la seguridad de la información.	Gerente Comercial	1					TERMINADO
16. Gestión de inicidentes de la seguridad de información	16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.6 16.1.7	Todos los activos mencionados	EXT055	Carencia de la identificación de responsables y procedimientos de la gestión de incidentes Ausencia de un medio establecido para la comunicación de incidentes. Ausencia de reportes de incidentes. Ineficiente de evaluación y decisión sobre los incidentes identificados. Tardía respuesta a los incidentes de seguridad Inexistente evidencia de historicos de incidentes	EXTREMA	REDUCIR	Coordinadora de Calidad	**1. Procedimiento de gestión de incidentes** Este procedimiento tiene como objetivo la gestión adecuada de los incidentes reportados, es decir, identificarlos, evaluarlos, ejecutar acciones para corregirlos y mantener un informe de estos para futuras revisiones.	Gerente de Administración	1					TERMINADO
17. Aspectos de seguridad de la información en la gestión de continuidad del negocio	17.1.1 17.1.2 17.1.3	Laptops de desarrollo Oficina de Miraflores	EXT056	Incidentes que se producen sin intervención humana tales como: inundaciones, incendios, entre otros. Incidentes que se producen como desastres naturales: rayos, tormentas, terremotos, tsunami, entre otros. Pueden ser victimas de vandalismo, robo, terrorismo que haga lleve a perder la información llevada en el activo.	EXTREMA	TRANSFERIR	Todo el personal	**1. Plan de continuidad de la seguridad de la información** Tiene como objetivo preservar la seguridad de información en la empresa ante situaciones adversas. **2. Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)** Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros. **3. Contratar una empresa aseguradora (Póliza de equipos)** Contar con una empresa aseguradora que permita proteger los equipos electrónicos (computadoras, laptops, etc) contra robos, vandalismo o daños internos.	Gerente de Administración	2					PENDIENTE PENDIENTE PENDIENTE

											2018				
Cláusula del control ISO/IEC 27002	**Control ISO/IEC 27002**	**Activo**	**ID del Riesgo**	**Descripción del riesgo**	**Nivel de Riesgo**	**Estrategia de respuesta**	**Propietario del Riesgo**	**Plan de acción**	**Responsable del control**	**Grupo**	**Abril**	**May.**	**Jun.**	**Jul.**	**Resultado**
18. Cumplimiento	**18.1.1**	Propuesta técnica y económica	EXT057	Fuga de información (accidental o intensional) pueden dañar la reputación de la empresa ya sea con fines maliciosos o beneficio propio.	**EXTREMA**	REDUCIR	Sub gerente del área comercial	**1. Cláusula de requisitos contractuales y legislación aplicable** Se requiere ingresar una cláusula en la propuesta técnica y económica, revisada por la asesora legal, la cual asegure el cumplimiento de los requisitos contractuales y legislación vigente.	Gerente Comercial	1					**TERMINADO**
	18.1.3	Control de salarios	EXT058	Pérdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup. Acceso de usuarios no autorizados para beneficio propio o fines maliciosos.	**EXTREMA**	REDUCIR	Coordnadora de Recursos Humanos	**1. Procedimiento de control de información documentada** Tiene como objetivo describir las actividades para establecer, documentar, controlar y mantener los documentos (procedimientos, formatos, registros, etc), de acuerdo con los requisitos establecidos por la organización.	Gerente de Administración	1					**TERMINADO**
		Formato de gestión de oportunidades					Sub gerente del área comercial		Gerente Comercial						
		Reporte de acceso de usuarios VPN/ Tocken					Encargado de Gestión de proyectos		Gerente de proyectos						
		Propuesta técnica y económica	EXT059	Divulgar los datos personales afectaría al decreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores.	**EXTREMA**	REDUCIR	Sub gerente del área comercial		Gerente Comercial						
		Documentación técnica	EXT060	Divulgar la documentación técnica afectaríala solución estrategica de nuestros servicios siendo una gran desventaja frente a nuestros competidores.	**EXTREMA**	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
6. Organización de la seguridad de la información	**6.1.3**	Lista de instaladores de software	ALT001	Averias debido al fallo de equipos o desactualizaciones de los instaladores de programas ocasionando pérdida de tiempo en el desarrollo de los proyectos. Afecta a la disponibilidad del activo para la realización de los proyectos de servicios por polvo, suciedad, entre otros. Afecta a la disponibilidad del activo para la realización de los proyectos de servicios debido a los fallos de los equipos y/o programas. Afecta a la disponibilidad del activo para la realización de los proyectos de servicios debido excesivo calor, frío, humedad, etc. Posible inccidente que se producen sin la intervención humana como inundaciones, cortocircuito.	**ALTA**	REDUCIR	Encargado de Logística	**1. Actualizaciones de los drivers o instaladores** Cronograma de actualizaciones de drivers o instaladores de los programas que son necesarios para el desarrollo de los proyectos.	Gerente de Administración	2					**PENDIENTE**
		Laptos de desarrollo				TRANSFERIR	Encargado de Servicios Telcos Encargado de Logística	**2. Soporte técnico externo para el mantenimiento preventivo y correctivo de los equipos.** Contar con una empresa externa que permita realizar periódicamente mantenimiento, diagnóstico y reparación a los equipos informáticos (laptops, impresoras, monitores, cargadores, entre otros)	Gerente de Serivicios Telcos Gerente de Administración	2					**PENDIENTE**
		Oficina de Miraflores				TRANSFERIR	Encargado Empresa contratista	**3. Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)** Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros.	Gerente de todas las áreas involucradas	2					**PENDIENTE**

Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	2018				Resultado
											Abril	May.	Jun.	Jul.	
6. Organización de la seguridad de la información	6.2.1	Registros de ordenes de compras y facturas	ALT002	Fuga de información (accidental o intencional) pueden ocasionar pérdida de clientes, problemas financieros, desconfianza en los clientes, debido a que no cuentan con una política o un acuerdo del uso correcto de los dispositivos móviles.	ALTA	REDUCIR	Coordinadora de Finanzas	**1. El acuerdo de confidencialidad de la seguridad de la información** Cláusula que señale el uso correcto de la información expuesta en el correo institucional de los colaboradores para evitar fugas de información, acceso no autorizados. **2. Política de seguridad de correo electrónico** Política para el uso correcto del correo electrónico, recalcando que la información es confidencial y no se debe usar para fines propios.	Gerente de Administración	1					TERMINADO
		Diseño técnico detallado					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Correo electrónico					Encargado de todo el personal		Gerente de Administración						
	6.2.2	Laptos de desarrollo	ALT003	Descuido del colaborado en tener en malas condiciones el equipo o de no notificar alguna incidencia.	ALTA	REDUCIR	Encargado de Logística	**1. Política de teletrabajo y penalidades.** Política para los colaboradores que trabajan en remoto o cuando se llevan las laptops para realizar actividades desde a fuera de la oficina. **2. Formato de entrega de equipos.** Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo.	Gerente de Administración	1					TERMINADO
			ALT004	Uso no previsto para interesés personales como juegos, programas personales, afectando la disponibilidad, integridad y condifencialidad.	ALTA	REDUCIR	Encargado de Logística / ServiciosTelcos		Gerente de Administración / Servicios Telcos						
			ALT005	El atacante consigue el acceso al activo sin tener autorización aprovechando un descuido del personal responsable.	ALTA	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
7. Seguridad de los recursos humanos	7.1.1	Datos del personal	ALT006	Divulgar los datos personales afectaría al secreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores.	ALTA	REDUCIR	Coordinadora de Recursos Humanos	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de la información de datos del personal para evitar fugas de talentos. **2. Política de uso, manejo de informacion confidencial y pérdida de información VF** Definir los estandares para salvaguardar la información contra uso no autorizado, divulgación o revelación. **3. Agregar investigación de antecedentes al proceso de contratación del personal** En el procedimiento de contratación debe señalar en qué momento, quién y cómo se pedirán o realizarán las investigaciones de antecedentes penales de los futuros colaboradores debido a que se asignará información clasificada y confidencial.	Gerente de Administración	1					TERMINADO

												2018				
Cláusula del control ISO/IEC 27002	**Control ISO/IEC 27002**	**Activo**	**ID del Riesgo**	**Descripción del riesgo**	**Nivel de Riesgo**	**Estrategia de respuesta**	**Propietario del Riesgo**	**Plan de acción**	**Responsable del control**	**Grupo**	**Abril**	**May.**	**Jun.**	**Jul.**	**Resultado**
7. Seguridad de los recursos humanos	**7.1.2**	Control de salarios	ALT007	Revelar los datos de salarios generando una inquietud entre los empleados.	**ALTA**	REDUCIR	Coordinadora de Recursos Humanos	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados.	Gerente de Administración	1					**TERMINADO**
		Registros de ordenes de compras y facturas	ALT008	Fuga de información (accidental o intensional) pueden ocasionar pérdida de clientes y problemas financieros.	**ALTA**	REDUCIR	Coordinadora de Finanzas		Gerente de Administración						
		Reporte de acceso de usuarios VNP	ALT009	Fuga de información (accidental o intensional) pueden dañar la confianza de nuestro clientes al momento de que usen sus sistemas por personas no autorizadas.	**ALTA**	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Repositorio de versionamiento	ALT010	Divulgar el repositorio de versionamiento afectaría la información confidencial de los proyectos realizados siendo una gran desventaja frente a nuestros competidores.	**ALTA**	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
7. Seguridad de los recursos humanos	**7.2.2**	Datos del personal	ALT011	Debido a que en la consultora no cuentan con una política o capacitación sobre la seguridad de la información sucede las siguientes incidencias: -Alteración y modificación en la lista personal, control de salarios el pago de planilla, la gestión de oportunidades, instaladores de software afectando pérdida de clientes, riesgos en costo financieros, mala gestión en los costos de proyectos, entre otros. -Modificación intensionalmente del registro de ordenes de compras y facturas, en la gestión de oportunidades afectando retrasos en los reportes financieros y posibles propuestas de negociación. -Divulgación los datos personales afectando al secreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores. -Pérdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup, puede ocasionar pérdida de tiempo al realizar las gestiones administrativas, los procesos internos, entregas de proyectos, gestión de permiso de usuarios VPN y retrasos al realizar soluciones de servicios.	**ALTA**	REDUCIR	Coordinadora de Recursos Humanos	**1. Plan de capacitación y concientización** Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros. **2. Politica de seguridad de la información** Política en que todo colaborador debe saber los objetivos planteados que se deben cumplir de acuerdo a la confidencialidad, integridad y disponibilidad de la seguridad de la información. **3. Arbol de carpeta para el acceso a usuarios.** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de Administración	1					**TERMINADO**
		Control de salarios					Coordinadora de Recursos Humanos		Gerente de Administración						
		Control de políticas					Coordinadora de Recursos Humanos		Gerente de Administración						
		Control de procedimiento					Coordinadora de Calidad		Gerente de Administración						
		Registros de ordenes de compras y facturas					Coordinadora de Finanzas		Gerente de Administración						
		Formato de gestión de oportunidades					Sub gerente del área comercial		Gerente Comercial						
		Propuesta técnica y económica					Sub gerente del área comercial		Gerente Comercial						
		Reporte de acceso de usuarios VNP					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Lista de instaladores de software					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
		Documentación técnica					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						

											2018				
Cláusula del control ISO/IEC 27002	**Control ISO/IEC 27002**	**Activo**	**ID del Riesgo**	**Descripción del riesgo**	**Nivel de Riesgo**	**Estrategia de respuesta**	**Propietario del Riesgo**	**Plan de acción**	**Responsable del control**	**Grupo**	**Abril**	**May.**	**Jun.**	**Jul.**	**Resultado**
8. Gestión de activos	**8.1.3**	Lista de instaladores de software	ALT012	Uso no previsto para interesés personales como juegos, programas personales afectando la disponibilidad, integridad y condifencialidad siendo un uso no aceptable de sus activos.	**ALTA**	REDUCIR	Encargado de Logística	**1. Política de uso, manejo de informacion confidencial y pérdida de información VF** Definir los estandares para salvaguardar la información contra uso no autorizado, divulgación o revelación. **2. Formato de entrega de equipos.** Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo.	Gerente de Administración	1					**TERMINADO**
		Laptos de desarrollo					Encargado de Logística / ServiciosTelcos		Gerente de Administración / Servicios Telcos						
	8.3.2	Registros de ordenes de compras y facturas	ALT013	Al no contar con procedimientos formales para la eliminación segura de elementos o información cuando ya no es necesaria, ocasionando fuga de información, problemas financieros, desconfianza entre los gerentes y colaboradores.	**ALTA**	REDUCIR	Coordinadora de Finanzas	**1. Procedimiento de destrucción o eliminación de documentos** Contar con procedimientos que permitan eliminar de forma segura de los documentos que contienen información que ya no sean necesarios para así evitar fugas de información de usuarios no autorizados.	Gerente de Administración	1					**TERMINADO**
		Diseño técnico detallado					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
	8.3.3	Registros de ordenes de compras y facturas	ALT014	Divulgar por terceros el registro de facturas afecta al decreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores. Retrasos en las entregas de facturas a clientes debido a la mala gestión.	**ALTA**	TRANSFERIR	Coordinadora de Finanzas	**1. Contratar una empresa externa de mensajería** Contar con una empresa que se encargue de mensajería segura y confiable para los documentos que se necesiten ser trasladados.	Gerente de Administración	2					**PENDIENTE**
9. Control de acceso	**9.1.1**	Datos del personal	ALT015	Carencia de una política de control de acceso ocasionando fugas de talentos, políticas sin autorización, retrasos o fuga de información, pérdida financieros, pérdida en desarrollo de proyectos, mal uso del correo electrónico.	**ALTA**	REDUCIR	Coordinadora de Recursos Humanos	**1. Política de control de acceso** Contar con una política en donde indique cuales son los responsables que deben tener acceso a las carpetas del drive y que información pueden acceder **2. Árbol de carpeta para el acceso a usuarios** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de administración	1					**TERMINADO**
		Control de políticas			**ALTA**	REDUCIR	Coordinadora de Recursos Humanos		Gerente de administración						
		Control de procedimiento					Coordinadora de Calidad		Gerente de administración						
		Registros de ordenes de compras y facturas					Coordinadora de Finanzas		Gerente de administración						
		Lista de instaladores de software					Encargado de Logística		Gerente de administración						
		Correo electrónico					Coordinadora de Recursos Humanos		Gerente de administración						

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
9. Control de acceso	9.2.1	Correo electrónico	ALT016	Uso del correo para fines propios o robo de información	ALTA	REDUCIR	Coordinadora de Recursos Humanos	**1. Política de seguridad de correo electrónico** Política para el uso correcto del correo electrónico, recalcando que la información es confidencial y no se debe usar para fines propios.	Gerente de administración	1					TERMINADO
	9.2.3	Laptos de desarrollo	ALT017	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas, porque puede ocasionar fuga de información.	ALTA	REDUCIR	Encargado de Servicios Telcoss / Encargado de Logística	**1. Política de control de acceso** Cláusula donde indique el control de derechos acceso privilegiados asociados a cada proceso que la asignación de usuario debe estar restringida y controlada.	Gerente de Serivicios Telcos / Gerencia de administración	1					TERMINADO
11. Seguridad física y ambiental	11.2.2	Oficina de Miraflores	ALT018	Cuentan con fallos de alimentación de energía, electricidad, calefacción, ventilador, aire acondicionado, entre otros.	ALTA	TRANSFERIR	Encargado Empresa contratista	**1. Proveedor externo en instalaciones de suministros** Contar con un proveedor que se encargue de las instalaciones de suministro (energía, electricidad, calefacción, ventiladores o aire acondicionado, entre otros) que aseguren que estén en correcto funcionamiento y asi evitar problemas en el área laboral.	Encargado de seguridad de la información	2					PENDIENTE
12. Seguridad de operaciones	12.1.1	Documentación técnica	ALT019	No cuentan con manuales de usuarios, procedimientos y configuraciones ya sea de los instaladores de los software's que utilizan o soluciones de los servicios pasados.	ALTA	REDUCIR	Encargado de Servicios Telcos	**1. Manuales, procedimientos y configuraciones** Contar con manuales de usuarios para los software's utilizados, además procedimientos y configuraciones de los servicios pasados ya sea por los sistemas de nuestros clientes.	Gerente de Serivicios Telcos	2					PENDIENTE
13. Seguridad de las comunicaciones	13.2.3	Correo electrónico	ALT020	Uso del correo para fines propios o robo de información	ALTA	REDUCIR	Coordinadora de Recursos Humanos	**1. Política de seguridad de correo electrónico** Política para el uso correcto del correo electrónico, recalcando que la información es confidencial y no se debe usar para fines propios.	Gerente de Administración	1					TERMINADO

Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	2018				Resultado
											Abril	May.	Jun.	Jul.	
13. Seguridad de las comunicaciones	13.2.4 13.2.2	Control de salarios	ALT021	Revelar los datos de salarios generando una inquietud entre los empleados.	ALTO	REDUCIR	Coordinadora de Recursos Humanos	**1. Acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos.	Gerente de Administración	1					TERMINADO
		Registros de ordenes de compras y facturas	ALT022	Fuga de información (accidental o intensional) pueden ocasionar pérdida de clientes y problemas financieros. Divulgar el registro de ordenes de compras y facturas afecta al decreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores.	ALTO	REDUCIR	Coordinadora de Finanzas		Gerente de Administración						
		Formato de gestión de oportunidades	ALT023	Tener acceso al documento sin ninguna autorización puede ocasionar robo de oportunidades de servicios.	ALTO	REDUCIR	Sub gerente comercial		Gerente Comercial						
		Diseño técnico detallado	ALT024	Fuga de información (accidental o intensional) pueden dañar confianza entre la empresa y usuarios autorizados ya sea para beneficios propios.	ALTO	REDUCIR	Encargado de Gestión de proyectos		Gerente de proyectos						
		Reporte de acceso de usuarios VNP	ALT025	Fuga de información (accidental o intensional) pueden dañar la confianza de nuestro clientes al momento de que usen sus sistemas personas no autorizadas.	ALTO	REDUCIR	Encargado de Gestión de proyectos		Gerente de proyectos						
		Repositorio de versionamiento	ALT026	Divulgar el repositorio de versionamiento afectaría la información confidencial de los proyectos realizados siendo una gran desventaja frente a nuestros competidores.	ALTO	REDUCIR	Encargado de Servicios Telcos		Gerente de Servicios Telcos						
		Correo electrónico	ALT027	Uso del correo para fines propios o robo de información	ALTO	REDUCIR	Coordinadora de Recursos Humanos		Gerente de Administración						
18. Cumplimiento	18.1.1	Propuesta técnica y económica	ALT028	Pérdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup, puede ocasionar pérdida de tiempo de entregas de proyectos.	ALTA	REDUCIR	Sub gerente del área comercial	**1. Cláusula de requisitos contractuales y legislación aplicable** Se requiere ingresar una cláusula en la propuesta técnica y económica, revisada por la asesora legal, la cual asegure el cumplimiento de los requisitos contractuales y legislación vigente.	Gerente Comercial	1					TERMINADO

Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	2018 Abril	2018 May.	2018 Jun.	2018 Jul.	Resultado
18. Cumplimiento	18.1.3	Datos del personal	ALT029	Acceso de usuarios no autorizados en tener la lista del personal para fines propios. Divulgar los datos personales afectaría al secreto comercial de la empresa siendo una gran desventaja frente a nuestros competidores. Pérdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup, puede ocasionar pérdida de tiempo al realizar las gestiones administrativas.	ALTA	REDUCIR	Coordinadora de Recursos Humanos	**1. Procedimiento de control de información documentada** Tiene como objetivo describir las actividades para establecer, documentar, controlar y mantener los documentos (procedimientos, formatos, registros, etc), de acuerdo con los requisitos establecidos por la organización.	Gerente de Administración	1					TERMINADO
		Control de políticas					Coordinadora de Recursos Humanos		Gerente de Administración						
		Control de procedimiento					Coordinadora de Calidad		Gerente de Administración						
		Registros de ordenes de compras y facturas					Coordinadora de Finanzas		Gerente de Administración						
		Registro de gestión de oportunidades					Sub gerente del área comercial		Gerente Comercial						
		Diseño técnico detallado					Encargado de Gestión de proyectos		Gerente de proyectos						
	18.2.1	Toda la documentación referente a la seguridad de información	ALT030	Incumplimiento de políticas, controles, procedimientos implementados para la seguridad de la información	ALTA	REDUCIR	Coordinadora de Calidad	**1. Tipos de sanciones de acuerdo a la seguridad de la información** Contar con tipos de sanciones en reglamento interno que infringe la seguridad de la información de la empresa y así tomar decisiones correctas al momento de aplicarlas. **2. Revisión de la seguridad de información** Establecer la revisión de la seguridad de información periódica para identificar oportunidades de mejora.	Gerente de Administración	1					TERMINADO
	18.2.2									1					
6. Organización de la seguridad de la información	6.1.4	Persona	MOD001	No contar con una asesoría o apoyo en seguridad de la información	MODERADA	REDUCIR	Todos los encargados	**1. Lista de contacto con grupos de interés en seguridad de la información** Lista en la cual se encuentran los grupos de interés pertinentes a contactar de presentarse alguna inquietud respecto a la seguridad de la información en la empresa.	Encargado del área correspondiente	2					PENDIENTE
	6.2.1	Datos del personal	MOD002	Fuga de información (accidental o intensional) pueden ocasionar daños de reputación, fugas de talentos, descofianzas de gerentes hacia los colaboradores debido a que no cuentan con una política o un acuerdo del uso correcto de los dispositivos móviles. Solo la política de seguridad de la información es de acceso interno y/o externo.	MODERADA	REDUCIR	Coordinadora de Recursos Humanos	**1. El acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información expuesta en el correo institucional de los colaboradores para evitar fugas de información, accesos no autorizados, entre otros.	Gerente de Administración	1					TERMINADO
		Control de salarios					Coordinadora de Recursos Humanos		Gerente de Administración						
		Control de políticas					Coordinadora de Recursos Humanos		Gerente de Administración						
		Reporte de actas de aceptación					Sub gerente del área comercial		Gerente Comercial						
		Reporte de estatus de proyectos					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						

Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	2018			Resultado
											Abril	May.	Jun.	Jul.	
7. Seguridad de los recursos humanos	7.1.2	Reporte de actas de aceptación	MOD003	Fuga de información (accidental o intensional) pueden dañar confianza entre la empresa y usuarios autorizados ya sea para beneficios propios.	MODERADA	REDUCIR	Sub gerente del área comercial	**1. El acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados.	Gerente Comercial	1					TERMINADO
			MOD004	El reporte de actas de aceptación es divulgada solo al personal comercial, finanzas y gerencial.	MODERADA	REDUCIR	Sub gerente del área comercial		Gerente Comercial						
		Diseño técnico detallado	MOD005	El diseño técnico detallado son de conocimiento para todo el personal de prestación de servicios.	MODERADA	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Reporte de estatus de proyectos	MOD006	Alteración en los reportes de estatus de proyectos causando un perjuicio y reportes no confiables a la gerencia.	MODERADA	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Repositorio de versionamiento	MOD007	Fuga de información (accidental o intensional) pueden dañar los proyectos que se tienen avanzados al momento de reemplazar una versión no actualizada.	MODERADA	REDUCIR	Encargado de Servicios Telcos		Gerente de Serivicios Telcos						
7. Seguridad de los recursos humanos	7.2.2	Datos del personal	MOD008	Debido a que en la consultora no cuentan con una política o capacitación sobre la seguridad de la información sucede las siguientes incidencias: -Fuga de información (accidental o intensional) pueden dañar la reputación de la empresa ya sea con fines maliciosos o económicos. -Pérdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup, puede ocasionar mal seguimiento financiero, mala gestión en el seguimiento de oportunidades, entre otros. -Modificación intensionalmente del reporte de actas de aceptación, en el reporte de estatus de proyectos, la lista del personal afectando el cobro de los servicios dados, en la gestión documentaria (sunat, ministerios de trabajo, entre otros)	MODERADA	REDUCIR	Coordinadora de Recursos Humanos	**1. Plan de capacitación y concientización** Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros. **2. Política de seguridad de la información** Política en que todo colaborador debe saber los objetivos planteados que se deben cumplir de acuerdo a la confidencialidad, integridad y disponibilidad de la seguridad de la informaciόm. **3. Arbol de carpeta para el acceso a usuarios.** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de Administración	1					TERMINADO
		Registros de ordenes de compras y facturas					Coordinadora de Finanzas		Gerente de Administración						
		Formato de gestión de oportunidades					Sub gerente del área comercial		Gerente Comercial						
		Reporte de actas de aceptación					Sub gerente del área comercial		Gerente Comercial						
		Reporte de estatus de proyectos					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Documentación técnica					Encargado de Servicios Telcos		Gerente de Serivicios Telcos						

												2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
8. Gestión de activos	8.3.2	Datos del personal	MOD009	Al no contar con procedimientos formales para la eliminación segura de elementos o información cuando ya no es necesaria, ocasionando fuga de información, reputación de la consultora, mal manejo de información, desconfianza entre la empresa y los colaboradores.	MODERADA	REDUCIR	Coordinadora de Recursos Humanos	**1. Procedimiento de destrucción o eliminación de documentos** Contar con procedimientos que permitan eliminar de forma segura de los documentos que contienen información que ya no sean necesarios para así evitar fugas de información de usuarios no autorizados.	Gerente de Administración	1					TERMINADO
		Control de salarios					Coordinadora de Recursos Humanos		Gerente de Administración						
		Reporte de actas de aceptación					Sub gerente del área comercial		Gerente Comercial						
		Reporte de estatus de proyectos					Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
	8.3.3	Reporte de actas de aceptación	MOD010	El reporte de actas de aceptación divulgada por usuarios no autorizados.	MODERADA	REDUCIR	Sub gerente del área comercial	**1. Contratar una empresa externa de mensajería** Contar con una empresa que se encargue de mensajería segura y confiable para los documentos que se necesiten ser trasladados.	Gerente Comercial	2					PENDIENTE
9. Control de acceso	9.1.1	Reporte de actas de aceptación	MOD011	El reporte de actas de aceptación solo tienen acceso al personal comercial, finanzas y gerencial.	MODERADA	REDUCIR	Sub gerente del área comercial	**1. Política de control de acceso** Contar con una política en donde indique cuales son los responsables que deben tener acceso a las carpetas del drive y que información pueden acceder	Gerente Comercial	1					TERMINADO
		Reporte de estatus de proyectos	MOD012	Acceso de usuarios no autorizados en tener los estatus de proyectos para fines propios.	MODERADA	REDUCIR	Encargado de Gestión de proyectos		Oficina de Gestión de proyectos						
		Repositorio de versionamiento	MOD013	Acceso de usuarios no autorizados en poder utilizar el repositorio para fines propios.	MODERADA	REDUCIR	Encargado de Servicios Telcos		Gerente de Servicios Telcos						
	9.2.5	Control de políticas	MOD014	El riesgo es moderada debido a que todas las políticas son de acceso al persona en general	MODERADA	ASUMIR	Coordinadora de Recursos Humanos	**1. Carpeta pública para el personal donde visualicen las políticas internas.** Contar con una carpeta pública en donde se encuentren todas las políticas de la empresa para su conocimiento de todo el personal.	Gerente de Administración	1					TERMINADO
11. Seguridad física y ambiental	11.1.2	Oficina de Miraflores	MOD015	Las áreas de la consultora no cuentan con controles de entrada, debido a que poca vez vienen usuarios externos, la mayoría pertenece a la consultora. A demás actualmente se encuentra en remodelación de lugar.	MODERADA	TRANSFERIR	Encargado de todas las áreas	**1. Establecer controles de seguridad cuando se trasladen en la siguiente oficina** Contar con controles de seguridad como tarjetas de autenticación como tarjetas de control de acceso con número único por cada personal y acceso a las áreas correspondientes.	Gerente de todas las áreas involucradas	2					PENDIENTE
	11.1.3						Encargado de todas las áreas		Gerente de todas las áreas involucradas						

											2018				
Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Activo	ID del Riesgo	Descripción del riesgo	Nivel de Riesgo	Estrategia de respuesta	Propietario del Riesgo	Plan de acción	Responsable del control	Grupo	Abril	May.	Jun.	Jul.	Resultado
13. Seguridad de las comunicaciones	13.2.4 13.2.2	Control de salarios	MOD016	Fuga de información (accidental o intensional) pueden dañar la reputación de la empresa ya sea con fines maliciosos o económicos.	MODERADA	REDUCIR	Coordinadora de Recursos Humanos	**1. Acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos.	Gerente de Administración	1					TERMINADO
		Control de políticas	MOD017	Dependiendo del tipo de política puede ser de acceso interno y/o externo.	MODERADA	REDUCIR	Coordinadora de Recursos Humanos		Gerente de Administración						
		Reporte de actas de aceptación	MOD018	Fuga de información (accidental o intensional) pueden dañar confianza entre la empresa y usuarios autorizados ya sea para beneficios propios. Divulgación del reporte de actas de aceptación es divulgada a otro personal que no sea del área de comercial, finanzas o gerencial.	MODERADA	REDUCIR	Sub gerente del área comercial		Gerente Comercial						
		Diseño técnico detallado	MOD019	Divulgación del diseño técnico detallado a otro personal que no es del área de prestación de servicios.	MODERADA	REDUCIR	Encargado de Gestión de proyectos		Gerente de Proyectos						
		Reporte de estatus de proyectos	MOD020	Los reportes de estatus de proyectos son de conocimiento para todo el comercial, finanzas y gerencial.	MODERADA	REDUCIR	Encargado de Gestión de proyectos		Gerente de Proyectos						
		Repositorio de versionamiento	MOD021	Fuga de información (accidental o intensional) pueden dañar los proyectos que se tienen avanzados al momento de reemplazar una versión no actualizada.	MODERADA	REDUCIR	Encargado de Servicios Telcos		Gerente de Servicios Telcos						
18. Cumplimiento	18.1.4	Datos del personal	MOD022	Se modifica intensionalmente la lista personal afectando la gestión documentaria (sunat, sunafil, ministerio de trabajo entre otros)	MODERADA	REDUCIR	Coordinadora de Recursos Humanos	**1. Acuerdo de confidencialidad de la seguridad de la información.** Indica el uso correcto de la información de datos del personal para evitar fugas de talentos.	Gerente de Administración	1					TERMINADO

											2018				
Cláusula del control ISO/IEC 27002	**Control ISO/IEC 27002**	**Activo**	**ID del Riesgo**	**Descripción del riesgo**	**Nivel de Riesgo**	**Estrategia de respuesta**	**Propietario del Riesgo**	**Plan de acción**	**Responsable del control**	**Grupo**	**Abril**	**May.**	**Jun.**	**Jul.**	**Resultado**
7. Seguridad de los recursos humanos	**7.2.2**	Datos del personal	BAJ001	Debido a que en la consultora no cuentan con una polîtica o capacitación sobre la seguridad de la información sucede las siguientes incidencias: -Pérdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup, puede ocasionar pérdida de tiempo al realizar propuestas, pago de planilla, gestión documentaria, control de acesso al vpn, entre otros. -Alteración intensionalmente ocaciona conflictos o problemas legales y complicaciones al correr con los procesos internos, retrasos de pagos.	**BAJA**	REDUCIR	Coordinadora de Recursos Humanos	**<u>1. Plan de capacitación y concientización</u>** Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros. **<u>2. Politica de seguridad de la información</u>** Polîtica en que todo colaborador debe saber los objetivos planteados que se deben cumplir de acuerdo a la confidencialidad, integridad y disponibilidad de la seguridad de la informaciôm. **<u>3. Arbol de carpeta para el acceso a usuarios.</u>** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de Administración	1				**TERMINADO**
		Control de polîticas					Coordinadora de Recursos Humanos		Gerente de Administración						
		Control de procedimiento					Coordinadora de Calidad		Gerente de Administración						
		Reporte de actas de aceptación					Sub gerente del área comercial		Gerente Comercial						
13. Seguridad de las comunicaciones	**13.2.4 13.2.2**	Documentación técnica	BAJ002	Posible robo de documentación técnica de los proyectos en donde se encuentra los procedimientos, manuales de usuarios de los servicios realizados.	**BAJA**	REDUCIR	Encargado de Servicios Telcos	**<u>1. Acuerdo de confidencialidad de la seguridad de la información</u>** Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos.	Gerente de Servicios Telcos	1					**TERMINADO**

ANEXO 19

DECLARACIÓN DE APLICABILIDAD

ANEXO 19 DECLARACIÓN DE APLICABILIDAD

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir qué controles son adecuados para implementar en VF CONSULTING S.A.C. cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos empleados de VF CONSULTING S.A.C que cumplen una función dentro del SGSI.

2. DEFINICIONES Y ACRÓNIMOS

SGSI: Sistema de Gestión de Sistema de Información.

3. DOCUMENTOS Y REGISTROS

No aplica.

4. APLICABILIDAD DE LOS CONTROLES

Son aplicables los siguientes controles del Anexo A de la norma ISO/IEC 27001:

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
5.1 Dirección de la gerencia para la seguridad de la información			
A.5.1.1	Políticas para seguridad de la información	SI	Es necesario establecer una "Política de Seguridad de Información", ya que es un requisito para establecer el SGSI. Además, sirve como base para el establecimiento del SGSI.
A.5.1.2	Revisión de políticas para seguridad de la información	SI	Es necesario contar con una "Política de Seguridad de Información" que sea revisada y aprobada por la Alta Dirección para asegurar que sea la adecuada para la organización.
6.1 Organización Interna			
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	SI	En la consultora no cuentan con roles definidos en seguridad de información, es necesario definirlos para tener identificados quienes serán los encargados de las actividades y así evitar sobrecargas de actividades.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.6.1.2	Segregación de deberes	SI	Es necesario segregar funciones entre los roles de la consultora, de esta manera evitar la sobrecarga de tareas y la ineficiente ejecución de los procesos.
A.6.1.3	Contacto con autoridades	SI	Es necesario que exista un documento de contactos con autoridades en donde se indique cómo y cuándo se debería informar de los incidentes de la seguridad de la Información.
A.6.1.4	Contacto con grupos de interés especial	SI	Es necesario que exista contactos con grupos de interés especial, foros, asociaciones o entidades que incentiven y apliquen la seguridad de información
A.6.1.5	Seguridad de la información en gestión de proyectos	SI	Actualmente la empresa cuenta con una metodología de gestión de proyectos, pero no están alineadas con los objetivos de la seguridad de la información ya que no existe una política de seguridad de información. Es necesario incluir los objetivos de la política de seguridad de Información en el método de la gestión de proyectos.
6.2 Dispositivos móviles y teletrabajo			
A.6.2.1	Política sobre dispositivos móviles	SI	Actualmente la empresa no asigna dispositivos móviles a los empleados para uso de trabajo, pero si autoriza la vinculación del correo institucional en los dispositivos propios de los empleados. Por esa razón, es necesario definir una política o acuerdo sobre el uso correcto de la información expuesta en el correo institucional.
A.6.2.2	Teletrabajo	SI	La empresa ya que es una consultora de servicios, la mayoría de sus empleados realizan sus actividades en las oficinas contratistas de los clientes. Es por eso que se necesita una política de teletrabajo.
7.1 Antes del Empleo			
A.7.1.1	Investigación de antecedentes	SI	En el área de RRHH, y como parte del proceso de selección y reclutamiento no se tiene mapeado los antecedentes penales y policiales de cada uno de los candidatos a un puesto laboral. Es por esa razón que es necesario realizar una búsqueda o investigación más exhaustiva si el puesto laboral tiene mayor rango.
A.7.1.2	Términos y condiciones de empleo	SI	Como parte de las cláusulas del contrato firmado por los colaboradores no se tiene establecido una de confidencialidad hacia la empresa; tampoco no se establece la confidencialidad respectiva a los datos personales del trabajador; es por ello que es necesario incluir ciertas cláusulas que cumplan con la ley de Protección de datos Personales.
7.2 Durante el empleo			
A.7.2.1	Gestión de responsabilidades	SI	Es necesario hacer que los colaboradores apliquen la seguridad de información con relación a las políticas y procedimientos de la empresa.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	Actualmente la empresa no toma en cuenta algunos aspectos de seguridad de información en la cultura organizacional, es por ello que es necesario que todos los colaboradores de la organización deban recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.
A.7.2.3	Proceso disciplinario	SI	Es necesario que haya sanciones para aquellos colaboradores que cometan una violación a la seguridad o que hayan incumplido con la política de seguridad de información aprobada.
7.3 Finalización del empleo o cambio en el puesto de trabajo			
A.7.3.1	Terminación o cambio de condiciones del empleo	SI	Una vez que culmine el contrato de un colaborador, las responsabilidades de seguridad de la información y funciones deben seguir vigentes después del término o cambio de empleo. Asimismo, estas responsabilidades deben ser definidas, y comunicas al trabajador o contratista.
8.1 Responsabilidad de los Activos			
A.8.1.1	Inventario de activos	SI	Es necesario realizar un listado de activos de información en la organización, con el fin de hacer seguimiento y monitorearlos.
A.8.1.2	Propiedad de los activos	SI	Es necesario realizar un listado de activos de información en la organización, con el fin de hacer seguimiento y monitorearlos, asimismo se especifican las propiedades de cada uno.
A.8.1.3	Uso aceptable de los activos	SI	Actualmente la empresa no cuenta con una regla del correcto uso de activos de información, es por eso que es necesario realizarlo y ser difundido correctamente.
A.8.1.4	Devolución de activos	SI	Actualmente la empresa no cuenta con un procedimiento de devolución de activos, es por eso que se debe definir en un procedimiento para la devolución de los activos de la organización que están en posesión de algún colaborador cuando termine su contrato.
8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información	SI	De acuerdo al inventario de activos de información se debe clasificar en términos de su importancia aplicando en los tres criterios de la seguridad de la información.
A.8.2.2	Etiquetado de la información	SI	Actualmente no se ha definido un procedimiento para etiquetar o clasificar los activos de información, por eso es necesario identificarlos con etiquetas de nomenclatura y tener una lista maestra para saber que activos de información se tiene por cada área.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.8.2.3	Manejo de activos	SI	Actualmente no se ha definido un procedimiento para etiquetar o clasificar los activos de información, por eso es necesario identificarlos con etiquetas de nomenclatura y tener una lista maestra para saber que activos de información se tiene por cada área y si pertenecen a la empresa o no.
8.3 Manipulación de los soportes			
A.8.3.1	Gestión de medios removibles	SI	El uso de laptop para la realización de los servicios fuera de la oficina central requiere que estos tipos de activos sean protegidos y asegurados.
A.8.3.2	Eliminación de medios	SI	Actualmente no se cuenta con procedimientos formales para la eliminación segura de elementos o información cuando ya no es necesaria, es por esa razón que se necesita tener un procedimiento en donde indique si el elemento o información no contiene información confidencial y proceda a ser eliminada.
A.8.3.3	Transferencia de medios físicos	SI	Actualmente en la empresa todas las laptops son entregadas al personal, pero no se ha tenido un control correcto. Es por eso que es necesario un control de registro de materiales que se haya entregado a cada colaborador y que se comprometa a cuidar y regresarlos cuando no esté en uso.
9.1 Requisitos de la empresa para el control de acceso			
A.9.1.1	Política de control de acceso	SI	No cuentan con políticas actualizadas con respecto al control de acceso, es por eso que es necesario ya que en la impresa se tiene demasiada información de alta importancia.
A.9.1.2	Acceso a redes y a servicios de red	SI	Debido a que actualmente la empresa cuenta con acceso de VPN de los clientes para el desarrollo de los servicios, es necesario contar con una política de acceso seguro de VPN's.
9.2 Gestión de acceso de usuario			
A.9.2.1	Registración y baja de usuarios	SI	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
A.9.2.2	Concesión de acceso de usuarios	SI	No hay un procedimiento en el que se abastezcan de usuarios de acceso. Actualmente solo se cuenta con la plataforma de Google Suite en donde se tiene un control de acceso a los correos institucionales.
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	Es necesario realizar un procedimiento documentado, en el cual se indique que cada jefe de área, debe solicitar los permisos adecuados para cada colaborador que se le autorice.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	SI	Es necesario establecer lineamientos para la adecuada gestión de autenticación de usuarios.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.9.2.5	Revisión de los derechos de acceso del usuario	SI	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
A.9.2.6	Eliminación o ajuste de derechos de acceso	SI	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
9.3 Responsabilidades del usuario			
A.9.3.1	Uso de información secreta de autenticación	SI	No hay una cultura de seguridad en los colaboradores de la organización, esto hace que las vulnerabilidades se vean expuestas, es por ello que es necesario que cada trabajador sea responsable de su usuario y contraseña.
9.4 Control de acceso a sistema y aplicación			
A.9.4.1	Restricción al acceso a la información	NO	No aplica debido a que actualmente la empresa es una consultora de servicios Telcos y lo realizan en las empresas contratista, además no se tiene un área de desarrollo de software, es decir no cuentan todavía con sistemas internos todo es manual.
A.9.4.2	Procedimiento de registro en el terminal	NO	
A.9.4.3	Sistema de gestión de claves	NO	
A.9.4.4	Uso de programas de utilidad privilegiada	NO	
A.9.4.5	Control de acceso al código fuente del programa	NO	
10.1. Controles criptográficos			
A.10.1.1	Política del uso de controles criptográficos	NO	No aplica debido a que por ahora no está tomando en cuenta los controles criptográficos para el alcance del SGSI.
A.10.1.2	Gestión clave	NO	
11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	NO	No aplica debido a que actualmente la empresa se encuentra en remodelación de lugar, por ahora se está trabajando la parte administrativa en un edificio de 6to piso y mayormente se trabaja en las empresas contratista.
A.11.1.2	Controles físicos de ingreso	SI	Actualmente la empresa como encuentra en un edificio de 6to piso, pero como se tiene información valiosa no cuenta con controles de entrada y acceso al personal como cerraduras, alarmas, etc.
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones	SI	Actualmente la empresa se encuentra en un edificio de 6to piso y está separado por áreas, pero no se cuenta con controles de entrada y acceso al personal como barras, alarmas, cerraduras, etc.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.11.1.4	Protección contra amenazas externas y ambientales	SI	No se cuenta con un reglamento o asesoramiento para evitar daños causados por juego, inundación, etc.
A.11.1.5	Trabajo en áreas seguras	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
A.11.1.6	Áreas de entrega y carga	NO	
11.2 Seguridad de los equipos			
A.11.2.1	Emplazamiento y protección de los equipos	SI	Actualmente los equipos no saben dónde ubicarlo ni cómo protegerlos de los riesgos ambientales por eso es necesario establecer políticas del uso correcto de los equipos.
A.11.2.2	Servicios de suministro	SI	Establecer políticas para definir acuerdos de servicio de soporte a las demás áreas.
A.11.2.3	Seguridad en el cableado	NO	No aplica por que actualmente la empresa no cuenta con cableado.
A.11.2.4	Mantenimiento de equipo	SI	Es necesario establecer lineamientos para realizar regularmente el mantenimiento de los servidores.
A.11.2.5	Remoción de activos	SI	Actualmente los colaboradores se llevan las laptops fuera de las instalaciones de la oficina debido al teletrabajo.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	Actualmente no se cuenta con medidas de seguridad de las laptops y materiales entregados fuera de las instalaciones.
A.11.2.7	Disposición o reutilización de equipos	SI	No existen políticas que especifican que los equipos, información y otras aplicaciones no deben ser retirados fuera de la organización, sin previa autorización y tampoco se cuenta con un procedimiento de copia de seguridad, back up antes de ser reutilizada.
A.11.2.8	Equipo de usuario desatendido	SI	No existe una política de aseguramiento en los equipos desentendido.
A.11.2.9	Política de escritorio limpio y pantalla limpia	SI	Es necesario establecer lineamientos para realizar mantener un escritorio limpio y pantalla limpia.
12.1 Procedimientos y responsabilidades operacionales			
A.12.1.1	Procedimientos documentados de operación	SI	Establecer lineamientos para garantizar que la información esté disponible.
A.12.1.2	Gestión de cambios	SI	Debido a que no aplicaban la seguridad de información no contaban con procedimiento de gestión de cambios de incidentes es por eso que es necesario que se tenga una gestión de cambios para identificar y controlar los incidentes.
A.12.1.3	Gestión de capacidad	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
A.12.1.4	Separación de ambientes de desarrollo, prueba y operacionales	NO	

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
12.2 Protección contra el software malicioso (malware)			
A.12.2.1	Controles contra software malicioso	SI	Actualmente no existen políticas de seguridad con respecto al uso de correo electrónico, respecto a páginas de internet de contenido dudoso.
12.3 Copias de seguridad de la información			
A.12.3.1	Copia de seguridad de la información	SI	Actualmente los colaboradores no realizan back up del desarrollo de su trabajo, por eso e**s** necesario establecer políticas de respaldo de información, realización de back up.
12.4 Registro de eventos			
A.12.4.1	Registro de eventos	NO	No se aplica debido a que en la empresa no cuentan con sistemas, está a futuro establecer sistemas para acelerar los procesos internos.
A.12.4.2	Protección de la información del registro	NO	
A.12.4.3	Registros del administrador y operador	NO	
A.12.4.4	Sincronización de relojes	NO	
12.5 Control del software operacional			
A.12.5.1	Instalación de software en sistemas operativos	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
12.6 Gestión de vulnerabilidad técnica			
A.12.6.1	Gestión de vulnerabilidades técnicas	SI	Actualmente no cuenta con un inventario de activos en donde indiquen que vulnerabilidades se ha tenido hasta el momento, es por eso que es necesario identificar los riesgos asociados y qué medidas tomar.
a.12.6.2	Restricciones sobre instalación de software	SI	No existen políticas de restricción de software para personal no autorizado, debido a que se le asigna las laptops nuevas, los mismos colaboradores se encargan de crear su usuario (administrador) y ellos lo manejan.
12.7 Consideraciones para la auditoria de los sistemas de información			
A.12.7.1	Controles de auditoría sobre los sistemas de información	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
13.1 Gestión de la seguridad de la red			
A.13.1.1	Controles de red	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información y de red.
A.13.1.2	Seguridad de los servicios de red	NO	
A.13.1.3	Segregación en redes	NO	
13.2 Transferencia de información			
A.13.2.1	Procedimientos y políticas sobre transferencia de información	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información y de red.
A.13.2.2	Acuerdos sobre transferencia de información	SI	Es necesario establecer acuerdos para el intercambio de información del negocio entre todos de la organización y los terceros.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.13.2.3	Mensajes electrónicos	SI	Es necesario establecer políticas sobre la transferencia de información.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	SI	Existen políticas de confidencialidad de información en la organización por parte de nuestros clientes, pero interno están en proceso.
14.1 Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificación de los requerimientos de seguridad de la información	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información.
A.14.1.2	Seguridad de servicios de aplicación en redes públicas	NO	
A.14.1.3	Protección de transacciones de servicios de aplicaciones	NO	
14.2 Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
A.14.2.2	Procedimientos para control en cambio de sistema	NO	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	NO	
A.14.2.4	Restricciones sobre los cambios en los paquetes de software	NO	
A.14.2.5	Principios de ingeniería para sistema seguro	NO	
A.14.2.6	Ambiente de desarrollo seguro	NO	
A.14.2.7	Desarrollo externalizado	NO	
A.14.2.8	Prueba de seguridad del sistema	NO	
A.14.2.9	Prueba de aceptación del sistema	NO	
14.3 Datos de prueba			
A.14.3.1	Protección de datos de prueba	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
15.1 Seguridad de la información en las relaciones con los proveedores			
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	SI	Establecer condiciones para el caso de acceso a activos de información mediante el servicio.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	SI	Es necesario establecer políticas con los proveedores, llegar a un acuerdo del uso correcto de almacenar, comunicar, tratar, acceder o proporcionar la información brindada y recepcionada.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	Es necesario que los acuerdos con los proveedores deban incluir requisitos para evitar riesgos de seguridad de la información.
15.2 Gestión de entrega de servicios del proveedor			
A.15.2.1	Monitoreo y revisión de los servicios de proveedores	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
A.15.2.2	Gestión de cambios en los servicios de proveedores	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
16.1 Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos	SI	Se requiere identificar responsabilidades y un procedimiento para la gestión de incidentes.
A.16.1.2	Reporte de eventos en la seguridad de la información	SI	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación. Asimismo, se deben mantener procesos actualizados.
A.16.1.3	Reporte de debilidades en la seguridad de la información	SI	Se requieren reportes sobre los incidentes identificados para poder evaluar si es un problema o no.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	SI	Establecer pasos a seguir según las decisiones tomadas para la seguridad de la información, para tener una idea clara de qué hacer.
A.16.1.5	Respuesta ante incidentes de seguridad de la información	SI	Es necesario saber a quién comunicar los incidentes de la seguridad de información y dar respuesta al contacto responsable.
A.16.1.6	Aprendizaje a partir de los incidentes en la seguridad de la información	SI	Es necesario cuantificar y supervisar los tipos, volúmenes y costos de los incidentes de seguridad de la información para evaluarlos y aprender de estos.
A.16.1.7	Recolección de evidencia	SI	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación.
17.1 Continuidad de seguridad de la información			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Es necesario determinar las necesidades de la seguridad de la información.

ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección
A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	Es necesario establecer, documentar, implementar y mantener los procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	Es necesario verificar y revisar la continuidad de la seguridad de la información.
17.2 Redundancias			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI.
18.1 Cumplimiento con requisitos legales y contractuales			
A.18.1.1	Identificación de legislación y requerimientos contractuales aplicables	SI	Se requiere ingresar una cláusula en la propuesta técnica y económica, revisada por la asesora legal, la cual asegure el cumplimiento de los requisitos contractuales y legislación vigente.
A.18.1.2	Derechos de propiedad intelectual	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, además en la empresa no se cuentan con sistemas de información.
A.18.1.3	Protección de registros	SI	Es necesario tener un procedimiento de control documentada para tener registrado y mapeado toda información y así evitar pérdida, alteración, falsificación, entre otros.
A.18.1.4	Privacidad y protección de información personalmente identificable	SI	Es necesario establecer un acuerdo de confidencialidad sobre la privacidad de las personas y la protección de datos de carácter personal de la organización.
A.18.1.5	Regulación de controles criptográficos	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, además en la empresa no se cuentan con sistemas de información.
18.2 Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información	SI	Es necesario realizar una revisión periódica de la seguridad de la información.
A.18.2.2	Cumplimiento con las políticas y estándares de seguridad	SI	Es necesario que los encargados de cada área se aseguren que todos los procedimientos de la seguridad se estén cumpliendo tanto políticas y controles, en todo caso aplicar sanciones.
A.18.2.3	Revisión de cumplimiento técnico	NO	No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información.

ANEXO 20

PLAN DE CAPACITACIÓN Y CONCIENTIZACIÓN

ANEXO 20 PLAN DE CAPACITACIÓN Y CONCIENTIZACIÓN

1. OBJETIVO, ALCANCE Y RESPONSABLES

El objetivo del presente plan es capacitar y concientizar al personal de VF CONSULTING S.A.C para que alcance las competencias necesarias para mejorar la seguridad de la información, para ello describimos las actividades, cronograma y presupuesto necesarios.

El compromiso empieza desde la alta gerencia y se extiende al personal dentro del proceso core y los procesos involucrados, para el cumplimiento de la implementación del SGSI.

2. DEFINICIONES Y ACRONIMOS

SGSI: Sistema de gestión de seguridad de la información.

3. DOCUMENTOS Y REGISTROS

- Lista de asistencia
- Informe de plan de capacitación y concientización

4. ACTIVIDADES

4.1. CHARLA DE SEGURIDAD DE LA INFORMACIÓN

Se realizará una charla presencial de concientización en seguridad de la información, cuyo detalle se muestra a continuación:

TEMARIO:

- ¿Qué es la seguridad de información?
- Diferencia entre seguridad de información y seguridad informática
- Ejemplos de inseguridad de información
- Activos de información importantes
- Medidas protección
- Campaña de seguridad de la información
- Conclusiones

Las charlas se dictarán a la siguiente audiencia:

- 01 charla de concientización en seguridad de la información

✓ **Audiencia**: Todo el personal de VF CONSULTING S.A.C

- ✓ **Cantidad de personas**: 25 personas aprox.
- ✓ **Duración de la capacitación**: 01 hora aprox.

Al iniciar y finalizar la charla se realizarán unos exámenes rápidos sobre la seguridad de la información, para tener una idea del impacto en el personal sobre esta charla. Además, se les brindará una constancia de participación en la charla.

4.2. CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Se realizarán capacitaciones presenciales sobre algunos temas en seguridad de la información, cuyo detalle se muestra a continuación:

TEMARIO:

- ¿Qué es el SGSI?
- Beneficios del SGSI
- Procedimiento de control de información documentada
- Gestión de riesgos
- Controles de seguridad de información
- Gestión de incidentes
- Auditoria interna
- Conclusiones y recomendaciones.

Las charlas se dictarán a los siguientes grupos de audiencia:

- 01 charla de capacitación en seguridad de la información
- ✓ **Audiencia**: Responsables de cada proceso.
- ✓ **Cantidad de personas**: 5 personas aprox.
- ✓ **Duración de la capacitación**: 01 hora aprox.

4.3. CAMPAÑA DE SEGURIDAD DE LA INFORMACIÓN

Es una campaña que tiene por finalidad crear una cultura de seguridad de la información al personal de VF, a través de diversas actividades tales como; salvapantallas, boletines electrónicos, folletos, trípticos, posters y afiches alusivos a la seguridad de la información.

De esta forma, la campaña busca que el personal de VF se familiarice de forma rápida con la seguridad de la información.

La campaña está dirigido a los siguientes grupos de audiencia:

- ✓ **Audiencia:** Todo el personal de VF Consulting.
- ✓ **Cantidad de personas**: 25 personas aprox.
- ✓ **Duración de la campaña:** 1 semana constante y luego se realizará cada 2 meses periódicamente.

La campaña debe desarrollarse en 3 etapas:

a. <u>Diseño de la campaña</u>

Esta etapa consiste en el diseño y desarrollo de los insumos necesarios para llevar a cabo la campaña de concientización de seguridad de la información. A continuación, se listan las actividades a realizarse en esta etapa:

- Diseño de un logo y lema para la seguridad de información.
- Diseño y elaboración de 3 modelos de salvapantallas alusivos a la seguridad de la información.
- Diseño y elaboración de 3 modelos de Poster y/o Afiches alusivos a la seguridad de la información.
- Diseño y elaboración de trípticos o folletos para el caso de personal externo.

b. <u>Promoción de la campaña</u>

Esta etapa consiste en la promoción de la campaña de concientización de seguridad de la información, a través de las siguientes actividades:

- Difusión de los Poster y/o Afiches alusivos a la campaña, a través del correo electrónico.

c. <u>Ejecución de la campaña</u>

Esta etapa consiste en llevar a cabo la campaña de seguridad de la información, la cual consiste en las siguientes actividades:

- Difusión del logo y lema de seguridad de la información.
- Despliegue de las salvapantallas en todos los computadores de los colaboradores de VF.

- Despliegue de los posters y/o afiches de seguridad de la información en la oficina de VF.
- Entrega de los trípticos o folletos físicos para el caso de personal externo.

5. CRONOGRAMA

	IMPLEMENTACIÓN DEL PLAN DE CAPACITACIÓN Y CONCIENTIZACIÓN	8 días	jue 03/05/18	sáb 12/05/18		RECURSOS
	CAMPAÑA DE SEGURIDAD DE LA INFORMACIÓN	**5 días**	**jue 03/05/18**	**mar 08/05/18**		
3	**Diseño de la campaña**	**2 días**	**jue 03/05/18**	**vie 04/05/18**		
4	Diseño de un logo y lema	1 día	jue 03/05/18	jue 03/05/18		CRRHH
5	Diseño y elaboración de 3 modelos de salvapantallas	1 día	jue 03/05/18	jue 03/05/18		ASI, CRRHH
6	Diseño y elaboración de 3 modelos de Poster y/o Afiches	1 día	vie 04/05/18	vie 04/05/18	5	ASI, CRRHH
7	Diseño y elaboración de trípticos o folletos	1 día	vie 04/05/18	vie 04/05/18	5	ASI, CRRHH
8	**Promoción de la campaña**	**2 días**	**sáb 05/05/18**	**lun 07/05/18**		
9	Difusión de los Poster y/o Afiches	2 días	sáb 05/05/18	lun 07/05/18	7	CC, CRRHH
10	**Ejecución de la campaña**	**1 día**	**mar 08/05/18**	**mar 08/05/18**		
11	Difusión del logo y lema	1 día	mar 08/05/18	mar 08/05/18	9	JP, CRRHH
12	Despliegue del salvapantallas	1 día	mar 08/05/18	mar 08/05/18	9	JP, CRRHH
13	Despliegue de los posters y/o afiches	1 día	mar 08/05/18	mar 08/05/18	9	JP, CRRHH
14	Entrega de los trípticos o folletos físicos	1 día	mar 08/05/18	mar 08/05/18	9	JP, ASI
15	**CHARLA DE SEGURIDAD DE LA INFORMACIÓN**	**2 días**	**mié 09/05/18**	**sáb 12/05/18**		
16	**Preparación de Charla de concientización**	**1 día**	**mié 09/05/18**	**mié 09/05/18**		
17	Realizar presentación (ppt) para la charla	1 día	mié 09/05/18	mié 09/05/18	14	JP, ASI
18	Preparación del recurso que dará la charla	1 día	mié 09/05/18	mié 09/05/18	14	JP, ASI, CRRHH, CC
19	Realizar charla de concientización	1 día	sáb 12/05/18	sáb 12/05/18	18	JP, ASI, CRRHH, CC
20	**CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN**	**3 días**	**mié 09/05/18**	**sáb 12/05/18**		
21	**Preparación de Capacitación de la seguridad de información**	**1 día**	**mié 09/05/18**	**mié 09/05/18**		
22	Realizar presentación (ppt) para la capacitación	1 día	mié 09/05/18	mié 09/05/18	14	JP, ASI
23	Preparación del recurso que dará la capacitación	1 día	mié 09/05/18	mié 09/05/18	14	JP, ASI
24	Realizar capacitación de seguridad de la información	1 día	sáb 12/05/18	sáb 12/05/18	18	JP, ASI

Fig. 1. Cronograma del plan de capacitación y concientización
Fuente: Elaboración de los autores

6. PRESUPUESTO

Tabla 1. Presupuesto para charla y capacitación

	EMPRESA	DESCRIPCIÓN	CANTIDAD	MONTO TOTAL S/.
COFFEE BREAK	COLMENA PRODUCCIONES	- Sandwich cocktail (2) - Bocadito dulce (1) - Bebidas	30 personas	S/ 564.00
IMPRESIONES Y FOLLETOS	GRÁFICA	- Impresión: 01 millar de folletos - Calidad: Full color - Tamaño: A4	01 millar	S/ 100.00
		COSTO TOTAL		**S/ 664.00**

Fuente: Elaboración de los autores

ANEXO 21

LISTA DE ASISTENCIA PARA LA CHARLA

ANEXO 21 LISTA DE ASISTENCIA PARA LA CHARLA

VF CONSULTING	**LISTA DE ASISTENCIA**

Nombre del Curso:	CHARLA DE SEGURIDAD DE INFORMACION		
Nombre del expositor:	YVONNE MECHAN, KATHERIN DE LA SOTA, FIOR SARMIENTO Y VANESSA SOVERO		
Fecha:	12/05/2018	**Horario:** 9:30 A.M.	11:30 A.M.

N°	Apellidos y nombres	Cargo	Firma
1	Frank Luis Vilela Carrasco	Analista Técnico	
2	Barreto Saldaña David Enrique	Analista Mediación	
3	Marcelo Leonardo, V. Ke.	Analista Programador	
4	Raul Castro Alvarado	Analista BSCS	
5	Jorge Segura Díaz	Analista Programador	
6	JIMMY JUAREZ CHILLCCE	PMO / G. PROYECTOS	
7	ERIKA RONCHE INGA	Analista	
8	Elizaguirre Mamani Sandra	Analista Programador	
9	Andrés Ezequiel Bonilla	Analista Programador	
10	Roca Márquez Ángela Luz	G. Comercial	
11	BRYANS HALASQUEZ	Analista.	
12	Giancfranco Cáceres Soto	Analista	
13	Javier Villanueva Rangel	Analista	
14			
15			
16			
17			
18			
19			
20			

VF CONSULTING	LISTA DE ASISTENCIA

N°	Apellidos y nombres	Cargo	Firma
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			

NOMBRE Y FIRMA
COORDINADORA DE CALIDAD

NOMBRE Y FIRMA
COORDINADORA DE RRHH

NOMBRE Y FIRMA
ANALISTA DE SEGURIDAD DE INFORMACION

NOMBRE Y FIRMA
JEFE DE PROYECTOS

ANEXO 22 LISTA DE ASISTENCIA PARA CAPACITACIÓN

VF CONSULTING SAC	LISTA DE ASISTENCIA

Nombre del Curso:	CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN		
Nombre del expositor:	YVONNE MECHAN Y KATHERIN DE LA SOTA		
Fecha:	12/05/2018	**Horario:** 11:30 A.M.	01:00 P.M

N°	Apellidos y nombres	Cargo	Firma
1	Segovia Díaz, Jorge E.	Analista Programador	
2	Roca Márquez Angela	G. Comercial	
3	FLOR SARMIENTO DEL VALLE	COORDINADORA DE CALIDAD	
4	SOVERO TORRES VANESSA A.	COORDINADORA DE RRHH	
5	JIMMY JUAREZ CHILLCCE	PMO / G. PROYECTOS	
6			
7			
8			
9			
10			

NOMBRE Y FIRMA
ANALISTA DE SEGURIDAD DE INFORMACIÓN

NOMBRE Y FIRMA
JEFE DE PROYECTOS

ANEXO 23

EVIDENCIA DE LA CHARLA Y CAPACITACIÓN

ANEXO 23 EVIDENCIA DE LA CHARLA Y CAPACITACIÓN

FOTO DE LA CHARLA DE SEGURIDAD DE INFORMACIÓN REALIZADA

FOTO DE LA CAPACITACIÓN DE INFORMACIÓN REALIZADA

AFICHE DE LA CAMPAÑA DE SEGURIDAD DE INFORMACIÓN

SALVAPANTALLA DE LA CAMPAÑA DE SEGURIDAD DE INFORMACIÓN

ANEXO 24

PLAN DE IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

ANEXO 24 PLAN DE IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

1. Objetivo

El objetivo del plan es de implementar todas las medidas de seguridad del Sistema de Gestión de la Seguridad de Información en VF CONSULTING S.A.C., bajo la norma ISO/IEC 27001:2013.

2. Alcance del proyecto

Se ha definido que este plan como alcance todas las medidas de seguridad contempladas en el “segundo grupo” en el documento del Plan de tratamiento de riesgos.

3. Alcance NO contemplado

En este proyecto no contempla ninguna medida de seguridad no mencionada en el Plan de tratamiento de riesgos, ni los del “primer grupo” ya que estos ya fueron implementados.

4. Medidas de seguridad

4.1 Instalación de medidas de seguridad para la oficina

Se debe contar con una empresa, la cual se encargará de la instalación de un sistema de alarma contra incendios, además del asesoramiento al personal para que pueda desenvolverse adecuadamente ante un aviso de incendio en la oficina. Para ello, tenemos el costo de la implementación considerando la cotización obtenida de la empresa **SYSCONI S.A.C.**, en la **Tabla 1**. Además, se identificó como responsable de esta medida a la Coordinadora de logística.

Tabla 1. Costo total de la implementación

Descripción	Valor Nuevos Soles S/
Kit Sistema de alarma contra incendios +sensores de humo	S/ 2,879.00
Instalación	S/ 1,000.00
Asesoramiento al personal	S/ 200.00
Total de la implementación	**S/ 4,079.00**

Fuente: Elaboración propia

4.2 Seguro contra desastres naturales y no naturales

Se debe contar con una empresa, la cual se encargará de proteger la oficina contra incendios, daño malicioso, vandalismo, terremoto, huelgas, inundaciones, cortocircuitos, entre otros. Para ello se cotizó un Seguro para PYME de la empresa **Pacífico**, sobre ello se indica el costo en la **Tabla 2** y se identificó como responsable de la medida a la Coordinadora de Logística.

Tabla 2. Costo total de la implementación

Descripción	Valor Nuevos Soles S/
Seguro para PYME (Incluye laptops)	S/ 150.00
Costo total mensual	**S/ 150.00**

Fuente: Elaboración propia

4.3 Póliza de equipos electrónicos

Se debe contar con una empresa, la cual se encargará de proteger los equipos electrónicos contra perdida y daño físico accidental. Para ello se cotizó un Seguro de todo riesgo de equipo electrónico de la empresa **MAPFRE**, sobre ello se indica el costo en la **Tabla 3** y se identificó como responsable de la medida a la Coordinadora de Logística.

Tabla 3. Costo total de la implementación

Descripción	Valor Nuevos Soles S/
Seguro de todo riesgo de equipo electrónico	S/ 200.00
Costo total mensual	**S/ 200.00**

Fuente: Elaboración propia

4.4 Sanciones de acuerdo con la seguridad de la información

Se debe contar con sanciones claras y específicas, en el reglamento interno, a favor de la seguridad de la información de la empresa, y a su vez estas deben ser comunicadas y explicadas. Para ello se identificó como responsable de la medida al Oficial de seguridad de información que se encargará de que se cumplan las sanciones establecidas por la empresa.

4.5 Soporte técnico para el mantenimiento preventivo y correctivo de los equipos

Se debe contar con el soporte técnico de una empresa, la cual se encargará del mantenimiento, diagnóstico y reparación de los equipos (laptops, impresoras, monitores, cargadores, entre otros) periódicamente. Para ello se cotizó este servicio en la empresa **Informática Samanez,** sobre ello se indica el costo en la **Tabla 4** y se identificó como responsable de la medida a la Coordinadora de Logística.

Tabla 4. Costo total de la implementación

Descripción	Valor Nuevos Soles S/
Mantenimiento de equipos (bimestral)	S/ 300.00
Diagnóstico de equipos	S/ 0.00
Reparación de equipos (trimestral)*	S/ 300.00
Costo total	**S/ 600.00**

Fuente: Elaboración propia

***Costo por daños comunes y que no incluyan cambio de piezas.**

4.6 Control del software instalado

Se debe contar con el control del software autorizado para evitar daños en los equipos y fugas de información. Para ello se realizará una lista de todos los softwares necesarios para el desarrollo del trabajo, y deberá actualizarse según sea necesario. Como la empresa recién se está automatizando, por el momento se hará de forma manual hasta implementar un sistema de logística que contempla los datos necesarios para el control. Además, se identificó como responsable de la medida a la Coordinadora de Logística.

4.7 Creación de perfil de usuarios

Se debe contar con perfiles de usuarios al momento de asignar un equipo a un recurso, dependiendo de las configuraciones que requiera; es decir, crear un perfil de “administrador”, siendo ellos los únicos responsables de las instalaciones, actualizaciones del equipo autorizado y otro perfil “local” que son creados en el equipo cuando un usuario inicia sesión pero que no pueden alterar, ni instalar programas sin la autorización de la persona encargada, en este caso la Coordinadora de Logística.

4.8 Mensajería segura de entrega de Courier

Se debe contar con una empresa encargada de la mensajería segura de entrega y recojo, la cual se encargará de enviar documentos (facturas, contratos), productos, entre otras cosas. Para ello se cotizó el servicio a la empresa **Glovo,** sobre ello se indica el costo en la **Tabla 5** y se identificó como responsable de la medida a la Coordinadora de Logística.

Tabla 5. Costo total de la implementación

Descripción	Valor Nuevos Soles S/
Express Courier - documentos	S/ 10.00
Express Courier - productos	S/ 25.00
Costo total	**S/ 35.00**

Fuente: Elaboración propia

***Variación del costo por tamaño y peso del producto.**

4.9 Instalación de suministros

Se debe contar con una empresa encargada de las instalaciones de suministros (energía, electricidad, calefacción, ventiladores, aire acondicionado, entro otros) para la nueva oficina de la empresa. Para ello se cotizó a la empresa **Coorporación ELECTROAGUSA** sobre ello se indica los costos brindados en la **Tabla 6** y se identificó como responsable de la medida a la Coordinadora de Logística.

Tabla 6. Servicios brindados

Descripción	Valor Nuevos Soles S/
Servicio de electricidad	S/ 850.00
Servicio de gasfitería	S/ 356.00
Bombas de aguas	S/ 275.00
Ventiladores	S/ 198.00
Calefacción y aire acondicionado	S/ 756.00
Instalación	S/ 65.00

Fuente: Elaboración propia

4.10 Manuales, procedimientos y configuraciones

Se debe contar con manuales, procedimientos y configuraciones de los servicios que se han realizado en la empresa por parte de nuestros clientes para futuros servicios. Para ello se identificó como responsable de la medida al Oficial de

seguridad de información y con la ayuda de la coordinadora de Calidad para que se cumplan en la realización de estos documentos, además de asegurar que toda información manejada debe estar en la nube, en la carpeta compartida dependiendo de la carpeta de acceso.

4.11 Controles de seguridad en la nueva oficina

Se debe contar con controles de seguridad para la nueva oficina que se trasladará a fines de año, como tarjetas de autenticación, control de ingreso, cámaras de vigilancias, entre otros. Para ello se cotizó el servicio a dos empresas, la primera a **Electrotec** y **DCG Innovation,** sobre ello se indica el costo en la **Tabla 7** y se identificó como responsable de la medida a la Coordinadora de Logística.

Tabla 7. Costo total de la implementación

Descripción	Valor Nuevos Soles S/
Tarjetas de autenticación c/u	S/ 20.00
4 Cámaras de vigilancias	S/ 880.00
Sistema de control de ingreso	S/ 1105.00
Costo total	S/ 2,005.00

Fuente: Elaboración propia

4.12 Revisión de la seguridad de la información

Se debe establecer la revisión de la seguridad de la información para poder identificar las oportunidades de mejoras, para eso se realizará un cronograma de revisión bimestral que el encargado Oficial de la Seguridad de la información asegure que se cumple dicho cronograma y que audite si toda la documentación con respecto a la seguridad de la información se esté cumpliendo.

4.13 Lista de contactos de autoridades

Se debe realizar una lista de contactos de autoridades pertinentes a presentar algún incidente mayor, para eso el encargado Oficial de la Seguridad de la información asegurará que se cuente con esta lista y sea visible para toda la organización para cualquier emergencia.

4.14 Lista de contactos con grupos de interés en seguridad de la información

Se debe realizar una lista de contactos con grupos de interés que estén relacionado a la seguridad de la información para alguna inquietud de incidentes de seguridad, para eso la Coordinadora de Recursos Humanos se encargará de contactar a los proveedores en este caso Cámara del Comercio, Nexsys, empresas proveedoras que realizan charlas, eventos, conferencias con respecto a la seguridad de la información en las empresas.

5. Tiempo estimado del proyecto

	PROYECTO - IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD	28 días	lun 02/07/18	jue 02/08/18		RECURSOS
	GRUPO 2	**28 días**	**lun 02/07/18**	**jue 02/08/18**		
3	**Instalación de medidas de seguridad para la oficina**	**4 días**	**lun 02/07/18**	**jue 05/07/18**		
4	Instalación de sistema de alarma	2 días	lun 02/07/18	mar 03/07/18		CRRHH
5	Asesoramiento al personal	2 días	mié 04/07/18	jue 05/07/18	4	CRRHH
6	**Seguro contra desastres naturales y no naturales**	**1 día**	**mar 10/07/18**	**mar 10/07/18**		
7	Contratar seguro para PYME	1 día	mar 10/07/18	mar 10/07/18	5	CRRHH
8	**Póliza de equipos electrónicos**	**1 día**	**mar 17/07/18**	**mar 17/07/18**		
9	Contratar seguro de todo riesgo de equipo electrónico	1 día	mar 17/07/18	mar 17/07/18	7	CRRHH
10	**Sanciones de acuerdo con la seguridad de la información**	**3 días**	**mar 24/07/18**	**jue 26/07/18**		
11	Incluir sanciones en el reglamento interno	1 día	mar 24/07/18	mar 24/07/18		CRRHH
12	Comunicar sanciones	2 días	mié 25/07/18	jue 26/07/18	11	CRRHH
13	**Soporte técnico para el mantenimiento preventivo y correctivo de los equipos**	**1 día**	**lun 30/07/18**	**lun 30/07/18**		
14	Contratar servicio de mantenimiento preventivo y correctivo	1 día	lun 30/07/18	lun 30/07/18	9	ASI
15	**Control de software instalado**	**2 días**	**mié 01/08/18**	**jue 02/08/18**		
16	Realizar lista de software a instalar	2 días	mié 01/08/18	jue 02/08/18	14	CRRHH
17	**Creación de perfil de usuarios**	**14 días**	**mie 01/08/18**	**jue 16/08/18**		
18	Crear perfil de usuarios en los equipos	14 días	mie 01/08/18	jue 16/08/18	16	CRRHH
19	**Mensajería segura de entrega de Courier**	**2 día**	jue 02/08/18	vie 03/08/18		
20	Contratar servicio de mensajería segura	2 día	jue 02/08/18	vie 03/08/18	11	CRRHH
21	**Manuales, procedimientos y configuraciones**	**5 días**	jue 02/08/18	mar 05/08/18		
22	Realizar manuales, procedimientos y configuraciones	5 días	jue 02/08/18	mar 05/08/18	14	CC
23	**Revisión de la seguridad de la información**	**5 días**	lun 13/08/18	vie 17/08/18		
24	Revisar la seguridad de la información	5 días	lun 13/08/18	vie 17/08/18	14,16	ASI
25	**Instalación de suministros**	**15 días**	lun 13/08/18	mie 29/08/18		
26	Contratar servicio de suministros para la nueva oficina	15 días	lun 13/08/18	mie 29/08/18	7	CRRHH
27	**Control de seguridad en la nueva oficina**	**7 días**	jue 16/08/18	jue 23/08/18		
28	Instalar de controles de seguridad	7 días	jue 16/08/18	jue 23/08/18	26	ASI
29	**Lista de contactos de autoridades**	**1 día**	lun 20/08/18	lun 20/08/18		
30	Realizar la lista de contactos de autoridades	1 día	lun 20/08/18	lun 20/08/18	7,9,14	ASI
31	**Lista de contactos con grupos de interés en seguridad de la información**	**2 días**	mar 21/08/18	mie 22/08/18		
32	Realizar la lista de contactos con grupos de interés	2 días	mar 21/08/18	mie 22/08/18	30	ASI

Fig. 1. Cronograma de proyecto
Fuente: Elaboración propia

ANEXO 25

ESTADO DE DOCUMENTOS

ANEXO 25 ESTADO DE DOCUMENTOS

DOCUMENTO	DESCRIPCIÓN	APROBADO POR:	ESTADO
Memorándum (llamada de atención)	Documento en la cual se comunica al personal la actualización obligatoria de su información, así mismo este documento sirve como una llamada de atención a aquel personal que infringe este control.	Gerente de Administración	ACTUALIZADO
Organigrama de puestos	Documento en el cual se actualizó y se identificó los responsables de cada área para segregar tareas para evitar el uso incorrecto de los activos.	Gerente de Administración	ACTUALIZADO
Ficha de puestos	Documento que se identifica personas con conocimiento en seguridad de la información en caso de que no segregar la tarea de registrar, actualizar y evitar el mal uso de activos.	Gerente de Administración	NUEVO
Procedimiento de propuestas	Se agregó los términos y condiciones de la información brindada en las propuestas como el alcance, tiempo y costo sea confidencial y no divulgada con usuarios no autorizados tanto para la consultora y el cliente.	Gerente Comercial	ACTUALIZADO
El acuerdo de confidencialidad de la seguridad de la información	Documento que señala el uso correcto de la información expuesta en el correo institucional de los colaboradores para evitar fugas de información, accesos no autorizados, que señale el uso correcto de la información de brindados al personal al inicio y durante su contratación, que señale el uso correcto de los usuarios de VPN y que sanciones aquel personal que infringe este acuerdo.	Gerente de Administración	NUEVO
Política de seguridad de correo electrónico	Política para el uso correcto del correo electrónico, recalcando que la información es confidencial y no se debe usar para fines propios.	Gerente de Administración	NUEVO
Política de teletrabajo y penalidades	Política para los colaboradores que trabajan en remoto o cuando se llevan las laptops para realizar actividades desde a fuera de la oficina.	Gerente de Administración	NUEVO
Formato de entrega de equipos	Documento que en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuándo se entregó el equipo.	Gerente de Administración	ACTUALIZADO
Política de uso, manejo de información confidencial y pérdida de información VF	Política que identifica los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación.	Gerente de Administración	ACTUALIZADO

DOCUMENTO	DESCRIPCIÓN	APROBADO POR:	ESTADO
Política de proveedores	Política basada en establecer condiciones necesarias en caso de acceso a la información de la empresa por los proveedores.	Gerente Comercial	NUEVO
Política de seguridad de la información	Política en que todo colaborador debe saber los objetivos planteados que se deben cumplir de acuerdo con la confidencialidad, integridad y disponibilidad de la seguridad de la información.	Gerente de Administración	ACTUALIZADO
Árbol de carpeta para el acceso a usuarios	Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas.	Gerente de Administración	NUEVO
Tipos de sanciones de acuerdo con la seguridad de la información	Documento de los tipos de sanciones que se encuentra en el reglamento interno, en donde si se infringe la seguridad de la información de la empresa se debe tomar decisiones correctas al momento de aplicarlas.	Gerente de Administración	ACTUALIZADO
Inventariado de activos	Lista y documento de Inventario de activos más relevantes en su ciclo de vida y su importancia. A demás, todo activo debe tener su propio propietario que aseguren que los activos estén bien clasificados, que se deben revisar en un determinado tiempo.	Todos los encargados de las áreas	NUEVO
Clasificación y valorización de activos de información	Valorización de los activos de acuerdo con los tres criterios: confidencialidad, integridad y disponibilidad, además la clasificación y valorización se deben actualizar cuando cambie su valor a lo largo de su ciclo de vida.	Todos los encargados de las áreas	NUEVO
Agregar el procedimiento de entrega de activos en el proceso de desvinculación del personal	En el proceso de desvinculación del personal se agregó el procedimiento en donde el personal debe retornar todos los activos de la consultora ya sea por contrato o acuerdo.	Gerente de Administración	ACTUALIZADO
Procedimiento de destrucción o eliminación de documentos	Procedimientos que permitan eliminar de forma segura de los documentos que contienen información que ya no sean necesarios para así evitar fugas de información de usuarios no autorizados.	Todos los encargados de las áreas	NUEVO
Política de control de acceso	Política en donde indique cuales son los responsables que deben tener acceso a las carpetas del drive y que información pueden acceder.	Todos los encargados de las áreas	NUEVO
Política de seguridad de pantallas, escritorios limpios y contraseñas seguras	Política que especifica la seguridad de los activos de información con las contraseñas de autenticidad para verificar la identidad de los usuarios.	Gerente de Administración	NUEVO

DOCUMENTO	DESCRIPCIÓN	APROBADO POR:	ESTADO
Agregar el procedimiento de desvinculación de acceso a usuario en el proceso de desvinculación del personal	Se agregó en el procedimiento de desvinculación del personal, cuando en la finalización del empleo los derechos de acceso del personal a la información y activos asociados deben a eliminarse o suspenderse para evitar fugas de información.	Gerente de Administración	ACTUALIZADO
Agregar investigaciones de antecedentes el proceso de contratación del personal	En el proceso de contratación se agregó el procedimiento de investigaciones de antecedentes penales de los futuros colaboradores debido a que se asignará información clasificada y confidencial.	Gerente de Administración	ACTUALIZADO
Procedimiento de gestión de incidentes	Procedimiento de la gestión adecuada de los incidentes reportados, es decir, identificarlos, evaluarlos, ejecutar acciones para corregirlos y mantener un informe de estos para futuras revisiones.	Gerente de Administración	NUEVO
Cláusula de requisitos contractuales y legislación aplicable	Cláusula en la propuesta técnica y económica, revisada por la asesora legal, la cual asegure el cumplimiento de los requisitos contractuales y legislación vigente.	Gerente Comercial	NUEVO
Procedimiento de control de información documentada	Descripción de las actividades para establecer, documentar, controlar y mantener los documentos (procedimientos, formatos, registros, etc.), de acuerdo con los requisitos establecidos por la organización.	Gerente de Administración	NUEVO

FUENTE: ELABORACIÓN DE LOS AUTORES (2018)

FUENTES DE CONSULTA

Abad M. (2015). Cómo gestionar la seguridad de la información (según ISO 27001: 2013) en una PYME del sector de las tecnologías de la información y la comunicación. (Tesis de pregrado). Universidad de VALLADOLID, Valladolid, España.

AENOR (2014). UNE-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). *AENORmás.*

AENOR PERÚ (2015) Para la certificación de ISO, el Perú es un mercado muy reducido. *Gestión*.

Arévalo J., Bayona R. y Rico D. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura*, 19(46), 123-134.

Baca, V. (2016). Diseño de un sistema de gestión de la seguridad de la información para la Unidad de Gestión Educativa Local Chiclayo. *Ingeniería: Ciencia, Tecnología e Innovación*, *3*(1), 42-57.

Berríos C. y Rocha M. (2015). Propuesta de un modelo de sistema de gestión de la seguridad de la información en una PYME basado en la norma ISO/IEC 27001 (Tesis de pregrado). Universidad Peruana de Ciencias Aplicadas, Lima, Perú.

BSI group. (2013). Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013.

Burgos J. y Campos P. (2013) Modelo para Seguridad de Información en TIC. *Bío Bío, 8*, 234-253

Calder A. (2013) Información de seguridad y ISO 27001. *Libro Verde de Gobierno de TI.*

Cardenas L., Martinez H., y Becerra L. (2016). Gestión de seguridad de la información: Revisión bibliográfica. *El profesional de la información, 25*(6), 931-948.

Centro de Desarrollo Industrial (2017). Organizaciones que obtuvieron reconocimiento a Sistema de Gestión certificados. *CDI.*

Chaparro, M. (2016) Elaboración de un plan de implementación de la ISO/IEC 27001:2013 para la unidad GST (Tesis Maestría). Universitat Oberta de Catalunya, Barcelona, España.

Charlet, L. (2017). The ISO Survey of Management System Standard Certifications 2016. *ISO.*

Cruz J. (2014) Plan de un Sistema de Gestión de Seguridad de la información para una entidad pública (tesis de pregrado). Universidad San Martín de Porres, Lima, Perú.

Gomez L. y Fernández P. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. *AERNOS ediciones.*

GTDI (2017). Número de certificados ISO/IEC 27001 en Perú en el año 2016. *Tecnologías de la Información y Consultoría.*

INCIBE (2016). Seguridad en el dialecto del jefe. *Newsletter Subcription.*

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2013) ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos. Suiza: ISO.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2014). ISO/IEC 27000:2014 Tecnología de Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de Información - Descripción y vocabulario. Suiza: ISO.

ISOTools (2015). Las normas ISO más empleadas a nivel mundial. *Software de Gestión para la excelencia empresarial.*

ISO (2017) *ISO/IEC 27001 - data per country and sector 2006 to 2016 Functions*

Jimeno J. (2013) El ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming una mejora continua. PDCA Home.

Meza A. (2016). Propuesta para la implementación de un Sistema de Gestión de Seguridad de la Información aplicando la Norma ISO 27001 para industriales (Tesis de pregrado). Universidad de Guayaquil Facultad de Ingeniería Industrial, Guayaquil, Ecuador.

Miranda K. (2013). Guía Metodológica para implementar un Sistema de Gestión de Seguridad en Instituciones. (Tesis de Maestría). Universidad de Piura, Piura, Perú.

Monsalve J., Aponte F., y Chaves D. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Facultad de Ingeniería*, *23*(37), 65-72.

Moody G., Siponen M., y Pahnila S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1), *285-311.*

Nieves A. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013. (Tesis de pregrado). Institución Universitaria Politécnico Grancolombiano, Bogotá, Colombia.

Rojo A. (2017). Top 10 de certificaciones en Normas ISO a nivel mundial. *SBQ Consultores.*

Sánchez A. (2013). Diseño de un Sistema de Gestión de la Seguridad de la Información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito (Tesis de pregrado). Pontificia Universidad Católica del Ecuador, Quito, Ecuador.

Sánchez L., Villafranca D., Fernández E. y Piattini M. (2014) MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES. *ResearchGate,* 4.

Santos, D. (2016). Establecimiento, implementación y mejorar de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2013, para una empresa consultora de software (tesis de pregrado). Universidad Pontificia Católica del Perú, Lima, Perú.

SGSI (2014). Un cambio en la Integración de los Sistemas de Gestión. *Blog especializado en Sistemas de Gestión de Seguridad de la Información.*

Solarte F., Enriquez E. y Banavides M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL, 28*(5), 492-507.

Suarez, S. (2015) Análisis y diseño de un Sistema de Gestión de Seguridad Informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad Informática de la infraestructura tecnológica de la Organización (tesis Pregrado). Universidad Nacional Abierta y a Distancia, Bogotá, Colombia.

Valencia F. y Orozco M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 2700. *Risti*, 22, 73-88.

Zully Justino S. (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 pregrado). Pontificia Universidad Católica del Perú, Lima, Perú.

27001 Academy (2018). ¿Qué es norma ISO 27001? *Online Consultation Center.*