



**FACULTAD DE INGENIERÍA, ARQUITECTURA Y  
URBANISMO**

**ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA  
DE SISTEMAS**

**TESIS**

**MEJORA DE PROCESO DE GESTIÓN DE RIESGO  
DE TECNOLOGÍA DE LA INFORMACIÓN  
UTILIZANDO LA NORMA ISO / IEC 27001:2013  
PARA UNA EMPRESA CONSTRUCTORA PERUANA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO  
DE SISTEMAS**

**Autor:**

**Bach. Rodríguez Juárez José Antonio  
ORCID: <https://orcid.org/0000-0002-5364-0947>**

**Asesor:**

**Mag. William Atalaya Urrutia  
ORCID: <https://orcid.org/0000-0002-2761-4868>**

**Línea de Investigación:**

**Infraestructura, Tecnología y Medio Ambiente**

**Pimentel – Perú 2020**

**MEJORA DE PROCESO DE GESTIÓN DE RIESGO DE TECNOLOGÍA DE LA  
INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA  
EMPRESA CONSTRUCTORA PERUANA**

**Aprobación de la Tesis**

---

**Mag. Jaime Arturo Bravo Ruiz  
Presidente del Jurado de Tesis**

---

**Ing, David, Bances Saavedra  
Secretario del jurado de Tesis**

---

**Mag. William Atalaya Urrutia  
Vocal del Jurado de Tesis**

## **DEDICATORIA**

Dedico de manera especial esta tesis a Dios por haberme dado la salud y bienestar familiar y haberme permitido realizarme profesionalmente, a la memoria de mi querida madre Lady que desde el cielo cuida de mí y en todo momento la llevo conmigo, pues es quien me dio mis principales cimientos para mi desarrollo profesional, en mi madre tengo el espejo en el cual me quiero reflejar por sus virtudes infinitas y su bondadoso corazón siempre me llevo a admirarla cada día más.

## **AGRADECIMIENTO**

A mis abuelos Magda y Juan, a quienes agradezco por su amor y comprensión y ser mis guías para la realización de mis sueños, por sus enseñanzas y consejos diarios que me permitieron realizarme como persona. Le doy las gracias a mi familia esposa Vilma y a mi hijo José Adriel por ser el motivo para salir adelante dándome el apoyo y compañía en todo momento. Así mismo a mis estimados profesores durante mi vida universitaria y asesores por la paciencia y su constante apoyo durante el desarrollo de esta tesis.

## **Resumen**

La presente tesis se desarrolla en una empresa constructora peruana ubicada en la región sur del Perú, el cual contiene los procesos engranados con tecnologías de información (TI). Se enfoca principalmente en los riesgos asociados a la totalidad de sus procesos y a su interacción con los usuarios de la organización. Todo ello bajo el enfoque de la norma ISO/IEC 27001:2013.

Como línea base, se dio inicio con la aplicación de una encuesta a diferentes usuarios de la organización, con el objetivo de conocer la real situación de los procesos de TI en toda la organización y cuáles son las oportunidades de mejora existentes.

Se procede con el análisis de riesgo de tecnología de la información mediante la metodología MageriT que nos permite evaluar un correcto análisis del nivel de criticidad de los riesgos a los cuales está expuesto la organización, tanto a nivel de procesos como de activos. Luego de culminado el análisis se procederá a proponer la implementación de oportunidades de mejora para tratar la gestión de los riesgos.

Finalmente, se describen conclusiones y recomendaciones que se pueden desprender del trabajo de investigación desarrollado.

**Palabras Clave:** Tecnologías de la información, Riesgos en procesos, ISO/IEC 27001:2013.

## **Abstract**

This thesis is developed in a Peruvian construction company located in the southern region of Peru, which contains the processes linked to information technology (IT). And it focuses mainly on the risks associated with all of its processes and its interaction with users in the organization. All this under the focus of ISO/IEC 27001:2013.

As a baseline, it began with the application of a survey to different users of the organization, with the aim of knowing the real situation of IT processes throughout the organization and what are the opportunities for improvement that exist.

We proceed with the risk analysis of Information Technology using the MageriT methodology that allows us to evaluate a correct analysis of the level of criticality of the risks to which the organization is exposed, both at the level of processes and assets. And after the analysis is completed, we will proceed to propose the implementation of improvement opportunities to deal with risk management.

Finally, they describe conclusions and recommendations that can be derived from the research work developed.

**Keywords:** IT, risk management implementation, ISO/IEC 27001:2013.

## Índice

<b>I. INTRODUCCIÓN.....</b>	<b>1</b>
<b>1.1. Planteamiento del Problema.....</b>	<b>2</b>
<b>1.2. Antecedentes de estudio. ....</b>	<b>7</b>
1.2.1. A nivel internacional. ....	7
1.2.2. A nivel nacional.....	9
<b>1.3. Abordaje teórico.....</b>	<b>10</b>
1.3.1. Riesgos para la tecnología de la información.....	11
1.3.2. Gestión de la Tecnología de información.....	13
1.3.3. Norma ISO/IEC 27001:2013.....	13
1.3.4. Principios.....	14
1.3.5. Estructura del Modelo.....	15
1.3.6. Evaluación del riesgo de la seguridad de la información. ....	16
1.3.7. Tratamiento del riesgo de seguridad de la información.....	17
1.3.8. Metodologías.....	18
<b>1.4. Formulación del problema.....</b>	<b>23</b>
<b>1.5. Justificación e importancia del estudio.....</b>	<b>23</b>
<b>1.6. Objetivos .....</b>	<b>24</b>
1.6.1. Objetivo general .....	24
1.6.2. Objetivos específicos .....	24
<b>1.7. Limitaciones. ....</b>	<b>25</b>
1.7.1. Delimitación de la Investigación.....	25
<b>II. MATERIAL Y MÉTODO .....</b>	<b>26</b>
<b>2.1. Tipo de estudio y diseño de la investigación. ....</b>	<b>26</b>
2.1.1. Diseño de la investigación. ....	26
<b>2.2. Escenario de estudio.....</b>	<b>27</b>
2.2.1. Enfoque seleccionado. ....	27
2.2.2. Objeto de estudio.....	27
<b>2.3. Caracterización de Sujetos.....</b>	<b>30</b>
<b>2.4. Técnicas e instrumentos de recolección de datos. ....</b>	<b>30</b>
2.4.1. Metodología, estrategias y herramientas para seleccionar data. .....	30

2.4.2. Instrumentos de seleccionar data.....	31
2.4.3. Validación del instrumento.....	31
2.5. Procedimientos para la recolección de datos.....	33
2.6. Procedimiento de análisis de datos.....	34
2.7. Criterios éticos.....	34
2.8. Criterios de rigor científico.....	34
<b>III. REPORTE DE RESULTADOS .....</b>	<b>35</b>
3.1. Análisis y discusión de resultados.....	35
3.1.1. Resultados en tablas y figuras.....	35
3.1.2. Relación de preguntas a ser aplicadas en el cuestionario. ....	39
3.1.3. Discusión de resultados.....	55
3.2. Consideraciones finales.....	56
3.3. Generalidades de la Propuesta.....	56
3.3.1. Fase I – Identificar los procesos para la gestión de riesgos....	63
3.3.2. Fase II – Declaración de Aplicabilidad de los controles del Anexo “A” - Norma ISO/IEC 27001:2013.....	64
3.3.3. Fase III – Realizar una Línea Base de los dominios del Anexo “A” de la norma ISO / IEC 27001:2013.....	65
3.3.4. Fase IV – Desplegar una metodología adecuada para la evaluación y administración de riesgos.....	81
3.3.5. Fase V: Definición de Planes de Acción para mitigar los riesgos.....	220
3.4. Conclusiones y recomendaciones.....	243
3.4.1. Conclusiones.....	243
3.4.2. Recomendaciones.....	245
<b>REFERENCIAS .....</b>	<b>246</b>
<b>ANEXOS.....</b>	<b>254</b>



## **I. INTRODUCCIÓN**

La presente investigación define un problema expresado como ¿cómo se analizan los riesgos en tecnología de la información mediante la Norma ISO/IEC 27001:2013 en una empresa constructora peruana?; la importancia se radica en analizar los riesgos tecnológicos de la información cuando se utiliza la Norma ISO/IEC 27001:2013; las cuales, definitivamente mejorarán una primera etapa de la gestión de TI en una empresa que desarrolla proyectos de gran envergadura en el sector construcción.

El principal antecedente está relacionado con la investigación titulada “Procedimiento de estudio y evaluación de riesgos aplicados a la seguridad informática mediante la norma ISO/IEC 27001”, persigue como fin analizar el grupo de riesgos asociados con tecnologías de la información utilizando la Norma ISO/IEC 27001:2013; y para lo cual se recabó el parecer de los colaboradores de la organización.

A nivel nacional destaca la investigación “Modelo de Tecnologías de la Información y la Comunicación en una compañía constructora”, tuvo como centro su trabajo en el estudio de los requerimientos de comunicaciones de las organizaciones que tienen como rubro la construcción, estableciendo un modelo de gestión, dando las bases de TICs necesarias, con un enfoque eficiente y rentable económicamente. Al basarse en las necesidades de mantener actualizado los subprocesos de interlocución de las compañías dedicadas a la industria de la construcción. Se procedió a elaborar un prototipo hipotético para gestionar la comunicación, elaborando y organizando métodos estándar con las cuantificaciones requeridas que generen un resultado óptimo en el proceso y proporcionan a la organización un esquema de la información eficaz y eficiente, teniendo como consecuencia la sucesión de progresos significativos para la empresa. Las mejoras del atributo observada impactan en los productos, en la dirección con los abastecedores, el clima en el trabajo o productividad económica, etc.

Finalmente, por medio de la simulación realizada se obtuvo como conclusiones los beneficios del establecimiento del modelo propuesto en la empresa, los cuales se generan a partir del 1º año desde su implementación, originando un aumento en los réditos generales que supera el 5% interanual.

En conclusión, adjuntamos el concepto básico de la única variable, evaluación de los riesgos en las tecnologías de la información, es que la eventualidad de la complicación, variación, o problemas en la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, origine pérdidas financieras a la organización. Es una de las partes de riesgo operacional.

### **1.1. Planteamiento del Problema.**

A nivel internacional, administrar las tecnologías de la información es cada vez más relevante; es por ello que las empresas optan por utilizar estándares que los ayuden a gestionar de forma más eficiente minimizando riesgos y siendo un generador de valor para la empresa.

La norma ISO/IEC 27001 es ampliamente difundida a nivel mundial. De acuerdo con la última encuesta realizada por iso.org, países como Japón (8945 certificados), Reino Unido (3367 certificados), India (2902 certificados), China (2618 certificados) y Alemania (1338 certificados) son los países líderes en adoptar esta metodología con el objetivo de administrar los sistemas de Seguridad en TI. En seguida, mostraremos la situación de la adopción de la norma ISO 27001 en la región.

De acuerdo con lo manifestado por (Ortiz, 2014), en donde se menciona que en México muchos especialistas coinciden acerca de los procesos de administración para la seguridad de TI, con un bajo nivel de uso de internet y la carencia de personal capacitado son factores que dificultan a pymes orientadas al negocio de la construcción puedan incluir tecnología en sus actividades diarias. La consultora KPMG desarrolló un estudio donde exponen que, en promedio, el 45% y 50% de los beneficiarios de los servicios de cloud computing tienen como una importante inquietud la seguridad de la

información. González explica que la intención de las compañías a invertir en tecnología demuestra que apoyan este tipo de soluciones mientras sean de impacto económico moderado. Sin embargo, si la tecnología es muy compleja el requerimiento de personal especializado, ausente en las Pymes, incrementarían el coste. El coste para implementar es una de las principales dificultades para que las medianas y pequeñas empresas en América del Sur inviertan en tecnologías de la información, confirmó César Cernudo, vicepresidente regional de ventas de Microsoft, en el pasado Microsoft World Partner Conference, que ocurrió en Toronto, Canadá.

Lo que manifiesta (Mendoza , 2015), en donde se menciona que en la cultura mexicana, el ISO 27001 concibe a la administración de la seguridad TI como un plan de constante mejora que da protección a la información de las organizaciones y en última instancia, al negocio, donde se exponen una variedad de problemáticas en la seguridad de TI en organizaciones de diferente tamaño. El cambio constante influye en el riesgo de seguridad de TI con gran impacto, donde las amenazas son desarrolladas y vulnerabilidades son descubiertas, en todos los ámbitos. Ante este escenario, existe el enfoque que tiene como foco la idea de que sólo es cuestión de tiempo para padecer las consecuencias de dichas amenazas. Lo más importante es el nivel de preparación para atender los diferentes incidentes, en conjunto con medidas preventivas y proactivas las cuales contribuyen a disminuir la posibilidad de que ocurran y dan la impresión correspondiente, así como las acciones correctivas necesarias para solventar los problemas.

(Parot, 2014), en su obra en donde realizó un estudio sobre el uso de TI en la construcción; en la cual se entrevista a Drago Eterovic, Gerente para el Cono Sur de la división de soluciones de negocios de Microsoft - Colombia, indica que en la actualidad existen muchas empresas pequeñas dedicadas al rubro de construcción, las cuales solo cuentan con una PC para la gestión de planillas. "Sin embargo, la llegada de conglomerados extranjeras obliga a trabajar con estándares internacionales y para eso el uso de TI es fundamental". De acuerdo con Eduardo Quinlan, presidente de Unysoft

empresa que diseña y comercializa sistemas especializados para los rubros de ingeniería, constructoras e inmobiliarias ubicadas en Chile, a pesar del histórico atraso en TI en el sector de construcción, el contexto global de los negocios motiva ir más allá. "El negocio con compañías multinacionales ha obligado a las constructoras locales a entregar un servicio acorde con los estándares a nivel mundial".

En nuestro país, (Quezada, 2018), indicó que en España el entorno es cada vez más digital, eso nos trae grandes beneficios, sin embargo, mientras más dependemos de la tecnología, también se incrementará el número de amenazas cibernéticas que acechan. Éstas varían de pequeñas acciones que van desde un robo de contraseñas, pasando por una posesión de equipo, hasta desastres catastróficos, como la pérdida o secuestro total de los datos. Con amenazas cada vez más avanzadas, los directivos corporativos están viendo la importancia de la seguridad cibernética. Hoy en día existe el desafío para el CISO, que es discutir los problemas del negocio que causan los desafíos de seguridad (y no solo aquellos que implican cuestiones relacionadas a la tecnología). Además de ser un buen líder, también debe poner en funcionamiento procesos de administración para la seguridad de la información que generalmente radica en detectar proactivamente las amenazas. De igual forma debe hacer énfasis en los aspectos que deben ser considerados antes de la implementación de la ISO 27001, particularmente durante las fases de planificación y operación.

Los niveles de seguridad de TI en Lima, de acuerdo con (Flores Cano, 2018), son escasos, acompañado de una baja conciencia de internet y ausencia de profesionales idóneos son factores que disminuyen en la adopción de TI en sus procesos en la industria de la construcción. En particular, en esta industria es más difícil cambiar la cultura de "así se ha hecho siempre". El cambio de paradigmas es un proceso de naturaleza difícil debido a que estos cambios tecnológicos implican un cambio de paradigma. Otra variable es el costo económico de estas mejoras ya que muchas empresas tomarían la decisión de asignar recursos económicos si la tecnología demuestra ser solución de

problemas, con una relación conveniente de costo beneficio. En cambio, la TI se muestra como un tema complicado con la participación de personal especializado, ausente en las empresas pequeñas, incrementando sus costos. Para los empresarios debería ser importante evaluar el reintegro de la inversión a mediano y largo plazo, y no concentrarse en el costo actual de TI.

Para (Giraldo, 2016), nos indica que en Lima si es posible ver inversión en tecnologías básicas, pero el sector de construcción aun no adopta plataformas de gestión de TI orientadas a su rubro debido a la falta de conocimiento de los resultados positivos en la implementación de estas. En una entrevista brindada por Benjamín Archila, gerente general de la firma Consensus, comenta sobre la importancia en las constructoras la gestión en base a nuevas TI: "Una de las herramientas principales debería ser el uso de un ERP, el cual permite interconectar todos los departamentos de la organización que permitirá, por ejemplo, conocer los niveles de stock, en cuestión de segundos, que se requiere para alguna actividad específica programada".

De acuerdo con un informe presentado en (Diario Gestión, 2014), en el cual en un artículo se indicó que en Lima está tomando fuerza la revolución de las TI sea cual sea el rubro y el negocio de la construcción no está exento de esto. En nuestro país, las grandes empresas enfocadas en la construcción y asesores en arquitectura están bajo este nuevo impulso, empleando el estándar Building Information Modeling (BIM) enfocados en el crecimiento global de acciones de crecimiento de un proyecto de infraestructura. "Esta es una idea cuyo foco se sustenta en el proceso de creación de infraestructura, desde una manufacturera hasta una empresa generadora de energía. Esta idea es común en el sector construcción, el cual se enfoca en unificar a TI y a establecer procesos, brindando consecuencias reales", expone Alejandro de León, country manager de América Latina de Autodesk. Así, este grupo de aportes de TI y software se implementan desde el diseño de una obra hasta el cierre y mantenimiento del mismo. Poniendo foco en la obra y la administración del abastecimiento de materiales o el cálculo de interferencia.

A nivel regional en la empresa Colvias S.A.C., ubicada en el departamento de Moquegua, encontramos un conjunto de riesgos relacionados con el planeamiento estratégico inexistente en el negocio, lo que implica una ausencia de hoja de ruta estratégica para la gestión.

En el departamento de TI de la sede ubicada en Moquegua, se puede observar que la información es vulnerable ante los riesgos propios del negocio, lo cual puede ocasionar la pérdida de información estratégica de la organización tanto en la realización de proyectos y para la administración en las demás actividades de la empresa.

Otro problema frecuente está relacionado con los proveedores; dado que esta situación, es necesario establecer el nivel de influencia de los proveedores en los procesos de TI, de encontrarse riesgos importantes, se procederá a analizar los procedimientos actuales con el objetivo de detectarlos y analizarlos; y de ser posible, eliminarlos, o en otra circunstancia, minimizar su influencia.

Otro problema sensible representa la falta de capital humano con el conocimiento necesario; la organización carece de una ventaja comercial, que permita obtener una cualidad sobre los competidores en el rubro del sector de construcción ante los clientes, que hoy en día les importa mantener de carácter seguro la información.

El rápido crecimiento de la organización, viene hacer un problema mayor debido que mayormente no existe el tiempo para hacer una pausa e identificar los procedimientos asociados a sus procesos; siendo así numerosas ocasiones los trabajadores desconocen que es lo que se tiene que hacer, cuando y quien debe de realizarlo; por lo que, en consecuencia, hacen tener respuestas lentas frente a los cambios del sector.

Finalmente, y por lo anteriormente expuesto observamos que en la empresa Colvias S.A.C., no se cuenta con una estrategia que facilite identificar los

riesgos que ponen en peligro la seguridad de la información; por lo que, es de suma importancia proteger los activos en sus tres dimensiones de integridad, confidencialidad y disponibilidad que se maneja dentro de la organización.

## **1.2. Antecedentes de estudio.**

### **1.2.1. A nivel internacional.**

En la investigación desarrollada por (Benavides Sepúlveda & Blandón Jaramillo, 2018), la cual se titula “Modelo procesos de administración de seguridad de la información en organizaciones dedicadas a la educación”, obtuvo como objetivo general definir el nivel de cumplimiento de la IED relacionado en su totalidad con lo solicitado por la NTC ISO/IEC 27001. Finalmente, su conclusión fue establecer un patrón de procesos de administración de seguridad de la información en base a la norma NTC ISO/IEC 27001 para IED's de conocimiento general, proporcionando un marco de referencia para que se cumpla el Decreto Único Reglamentario 1078/2015 parte de “seguridad y confidencialidad de la información”, lo cual permite dar cumplimiento a lo ordenado por el Decreto 1526/2002 del MEN, en cuestiones de calidad en la información y la responsabilidad de las organizaciones territoriales de llevar a cabo auditorías por lo menos una vez al año a los matriculados y al personal docente apoyando en la preparación de las IED's para estos procesos de verificación.

El trabajo de investigación realizado por (Widhi Candra, Candra Briloyant, & Rebeca Tamba, 2017), la cual se denomina “Planificación de SGSI referenciado en ISO/IEC 27001:2013 mediante el proceso de jerarquía analítica en su fase análisis de brechas, tuvo como objetivo planificar la seguridad de la información, cómo adquirir precisión en la etapa de análisis de brechas. De acuerdo con la guía de implementación de los procesos de administración de seguridad de la información (SGSI) basada en ISO/IEC 27001:2013, la planificación del SGSI posee 5 fases. Estas fases son: delimitar el intervalo, analizar brechas, hacer evaluación de riesgos, establecer el control y el objetivo y plantear la política y el procedimiento del SGSI. La etapa de análisis de brechas se requiere para

evaluar la posición actual de la organización hacia la implementación del SGSI. Esta investigación sugirió el uso de AHP para determinar qué control de seguridad de la información se relaciona más a los requerimientos y objetivos de una organización.

Los autores (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015), cuya investigación se titula “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática bajo la norma ISO/IEC 27001”, enfocó el trabajo en el desarrollo de capacidades en ingenieros de sistemas, las cuales les permite diagnosticar, estar en capacidad para poner en funcionamiento los proceso de seguridad de la información – SGSI relacionado con el estándar ISO/IEC 27001 y los controles planteados en la norma ISO/IEC 27002. Sus conclusiones luego del análisis y evaluación de los riesgos plantean medidas de control en seguridad que permitan la integración futura dentro de un SGSI que acceda a dar respuesta a los requerimientos de seguridad de TI acorde a sus necesidades.

Para (Montiel Acosta, 2015), en el trabajo denominado “Sistema de Seguridad de la Información de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil siguiendo la Norma NTE INEN ISO/IEC 27001 – 2013”, tuvo como objetivo minimizar las consecuencias de los riesgos en la infraestructura de red, el centro de cómputo y de más áreas críticas del CISC - CINT. El presente proyecto de tesis se consideró para su investigación la modalidad de proyecto factible, la misma que ayudará en el método de estudio de esta, reconociendo así la factibilidad de la investigación. El instrumento se aplicará a 356 personas. Concluyendo, el estudio de la norma ISO/IEC 27001, se tuvo la oportunidad formar un contexto más detallado sobre seguridad de la información, donde se da a conocer metodologías, herramientas, estándares, etc., con el objetivo de lograr la meta.



### **1.2.2. A nivel nacional.**

Con el estudio realizado por (Santos Llanos, 2016), en su tesis titulada “Promulgar, aplicación, Mantenimiento y mejora de un Sistema de Gestión de seguridad de la Información, basado en la ISO/IEC 27001:2013, en una organización de asesoría de Software”, se enfocó en desarrollar un SGSI en una entidad de asesoría en desarrollo y calidad de software, empleando como normativa el estándar ISO/IEC 27001:2013; esta investigación busca entender, simular el ambiente y las necesidades de seguridad de información en una organización que desarrolla software. Las conclusiones elaboradas indican que este patrón hace que cuente con un modelo de mejora continua, que provee de forma permanente una gestión idónea de la seguridad de su información.

Para (Maceli Simon, 2017), a través de su proyecto denominado “Innovación tecnológica en la industria de la construcción peruana: Situación actual y Diagnóstico”, estableciendo la situación actual en el Perú en aspectos como la innovación tecnológica en el sector de la construcción del Perú. El autor definió el estado real en temas de innovación del rubro de construcción en el Perú y da una opinión en base al marco teórico, realizando reuniones con independientes y organizaciones, identificando puntos débiles del manejo actual del conocimiento y las pérdidas en las oportunidades de innovar. Finalmente, se demostró la aplicación en las organizaciones españolas entrevistadas.

Este modelo generó interés por la posibilidad de asimilación en la realidad peruana, analizando los diferentes contextos de ambos países, identificando e incorporando 09 parámetros de más (distintos a los propuestos en el patrón) en la reunión semielaborada que se desarrolló con miembros de organizaciones nacionales, generando un amplio grado de acuerdos con las personas consultadas acerca de los parámetros del modelo, tomando como ciertas 15 del total.

De acuerdo con (Talavera Álvarez, 2015), en la investigación titulada, “Diseño de un Proceso de Administración de Seguridad de la Información para un organismo público de Salud de acuerdo con la ISO/IEC 27001:2013”, tenía como meta realizar el diseño de un proceso de administración de seguridad de la información para un organismo de salud del estado, según la NTP ISO/IEC 27001:2013. Concluyo que la brecha más importante es en cuanto a seguridad de la información, carencia que se debe resolver previamente a hacer parte a la gerencia en las etapas del plan. Estas últimas deben ser definida con motivo de la implementación del SGSI institucional, gestionándolo como un proyecto institucional, de forma que se cuente con la ayuda de la alta dirección.

Para (Berríos Mesía & Rocha Cam, 2015), en su proyecto de investigación denominado “Propuesta de un Patrón de procesos de administración de la Seguridad de la Información en una Pyme basado en la Norma ISO/IEC 27001”, elaboró una idea de plan para un SGSI en una pequeña y mediana empresa, que se basa en el grupo de normas ISO/IEC 27000. Empleando el modelo SMESEC que cuenta con tres secciones: Gobierno y Gestión, Operación y Controles. Concluyó que, el patrón SMESEC da respuesta a la interrogante por la ausencia de un SGSI en las pequeñas y medianas empresas en el Perú, ya que es posible plasmar este sistema de administración en las PYMES, establecer y mantener un ambiente razonablemente seguro de tal forma que se salvaguarde la confiabilidad, disponibilidad e integridad de la información.

### **1.3. Abordaje teórico.**

Según Valencia-Duque (Valencia-Duque & Orozco-Alzate, 2017), la puesta en marcha de un grupo de actividades de administración de un SGSI de acuerdo al grupo de normas de la ISO/IEC 27000, se busca cumplir con cuatro puntos importantes: (a) el cumplimiento de lo determinado por ISO/IEC 27001; (b) con los puntos de control de seguridad presentes en la ISO/IEC 27002; (c) con el bosquejo de riesgos de la ISO/IEC 27005; (d) con las etapas sugeridas en la ISO/IEC 27003. Obteniendo como respuesta una metodología que responde

al cómo emprender un proyecto de este nivel de importancia en el contexto actual de las empresas y basado en estándares reconocidos a nivel internacional.

Para (Arévalo-Ascanio, Bayona-Trillos, & Rico-Bautista, 2015), con el fin de dar más información y conocer las principales variables del rubro productivo, desarrollaron un estudio descriptivo que se basó en la promoción de métodos de gestión alienados con estándares propios y foráneos. Con lo obtenido se obtuvo los datos correspondientes a la fase tecnológica de las organizaciones, proponiendo la aplicación de herramientas de la norma ISO 27001:2005 para el análisis de sistemas de información, usando tecnologías de información acordes a las entidades de investigación, que cuidan su recurso más valioso la información.

Según (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015), es básico el desarrollo de destrezas en los ingenieros de sistemas, a partir de las cuales se logre dirigir proyectos de análisis, planteamiento y definir los procesos de seguridad de la información – SGSI según la NTP ISO/IEC 27001 y los procesos de control planteados en la norma ISO/IEC 27002. Empleando una encuesta a los colaboradores del área de TI y los beneficiarios de los sistemas, estableciendo con ello el diagnóstico de seguridad actual. Después se utilizará una lista de chequeo basado en la NTP, para chequear que existen parámetros de control de seguridad en las actividades organizacionales. Por último y según los valores obtenidos del análisis y verificación de los riesgos, se plantean parámetros de control en seguridad para que se unifiquen hacia el futuro como parte de un SGSI que satisfaga los requisitos de seguridad informática y de datos según lo necesario.

### **1.3.1. Riesgos para la tecnología de la información.**

En los tiempos actuales las organizaciones de mayor envergadura, saben que la información es un activo valioso que depende del uso de la tecnología para ser exitosas y lograr continuidad en el negocio. Su objetivo

al emplear sistemas de seguridad de la información y de los sistemas de procesamiento es la evaluación y la gestión de riesgos.

La contingencia que se dan a raíz de: (a) la interrupción, (b) alteración, (c) problemas con la arquitectura de TI, (d) procesos de datos (e) registros de la información, (f) grupo de subprocesos de TI; provoca pérdidas financieras a las instituciones, el cual es considerado como uno de los componentes de riesgo operacional. (Superintendencia de Bancos, 2017).

El riesgo tecnológico consta de las siguientes dimensiones:

- Gobierno de TI: Brechas de conocimiento del personal de TI, estrategias de seguimiento a metas y rotación del personal.
- Infraestructura de TI: Nivel de integración del hardware, tráfico de información, uso de tecnologías.
- Sistemas de Información: Integración de los sistemas, nivel transaccional.
- Continuidad de Operaciones de TI: Alineamiento con el negocio y dependencia con terceros.
- Seguridad de TI: Vulnerabilidad de marco de seguridad.

El análisis de riesgos, se enfoca en un proceso iterativo dado los cambios de las condiciones del alcance en la mejora continua de las empresas. La administración de riesgos provee una metodología sistemática que permite elaborar un plan, identificar la amenazas, analizarlas, evaluarlas, tratarlas y monitorear sus riesgos los cuales están asociados con la actividad, función o proceso, que se realiza la organización para poder reducir pérdidas e incrementar sus oportunidades. Venegas & Pardo (2014).

### **1.3.2. Gestión de la Tecnología de información.**

Para las TI, debe hacerse referencia a ITIL. En donde ITIL son las siglas de “Information Technology Infrastructure Library” y constituyen un marco de referencia sobre buenas prácticas para la gestión de las TI de aceptación mundial.

(Peña Calvo, 2015), Indicó que los objetivos principales de las ITIL son 2:

- General: construir soluciones innovadoras para ordenar las metas de la organización con los de la tecnología de la información.
- Específicos: Proporcionar un completo y coherente conjunto de las mejores prácticas relacionadas con la materia.

Lograr la eficacia en la organización a través de la eficiencia en el uso de las nuevas tecnologías.

Reducir la dependencia del personal clave de sistemas determinando y definiendo procedimientos, funciones y roles para el mantenimiento del SI.

#### **Sus principales características son:**

- Se puede usar a todo tipo de organizaciones.
- Tiene un bagaje puesto que ha sido creado en los años 80 y mejorado desde entonces.
- Actualización permanente.
- Es una guía no propietaria.

### **1.3.3. Norma ISO/IEC 27001:2013.**

De acuerdo con (Peña Calvo, 2015), indica que la NTP ISO/IEC 27001, es un parámetro relativo a la seguridad de la información publicada en 2005 por International Standardization Normalization. En el 2013 se actualizó, siendo ISO/IEC 27001:2013. Por ello, este reglamento

determina los requerimientos precisos para su definición, propuesta, mantenimiento y mejora de un SGSI. Utiliza como herramienta el “Ciclo de Deming” o PDCA (Plan – Do – Check – Act).

De acuerdo con la definición de (Carpentier, 2016), la norma ISO/IEC 27001, sirve como referencia en materia de seguridad de los sistemas de información, debido que principalmente define una estructura en la aplicación de procesos de gestión de la seguridad de la información (ISO 27005), siendo considerada como el brazo de seguridad en TI de los reglamentos de calidad ISO 9001.

Por otro lado; (Carpentier, 2016), sustentó que la NTP ISO/IEC 27001:2013 es principal por la definición de necesidades para CMSI (procesos de administración de la seguridad de la información). Corresponde al principio de certificación de las organizaciones.

La ISO 27001 está respaldada por una familia de normas de mejores prácticas relacionadas, cada una de las cuales proporciona una directriz adicional sobre un aspecto concreto de la administración de la seguridad de la información. Este grupo de reglas está creciendo y desarrollándose continuamente. Para (Calder, 2017), la ISO 27001 reconoce implícitamente que la seguridad de la información y un SGSI deberían formar parte integral de cualquier sistema de control interno creado como parte de los procedimientos del gobierno corporativo. La norma encaja con el enfoque adoptado en el Reino Unido por la Directriz sobre gestión del riesgo de FRC.

#### **1.3.4. Principios.**

Para (Atehortúa, Bustamante, & Valencia, 2008), expusieron que de la norma ISO 27001 pueden lograrse las siguientes partes como principios para el modelo:

- Valor de la información: considerada como un recurso importante para un alto desempeño y permanencia en el negocio de la empresa, donde asegurar la data y los sistemas que lo procesan con esta son el objetivo primigenio de la organización.
- Enfoque de sistemas: La implementación de un grupo de procesos que cubran estas labores metódicamente, documentado y en base a metas fijas en seguridad y un examen de los riesgos a los que se exponen la data de una organización.

### **1.3.5. Estructura del Modelo.**

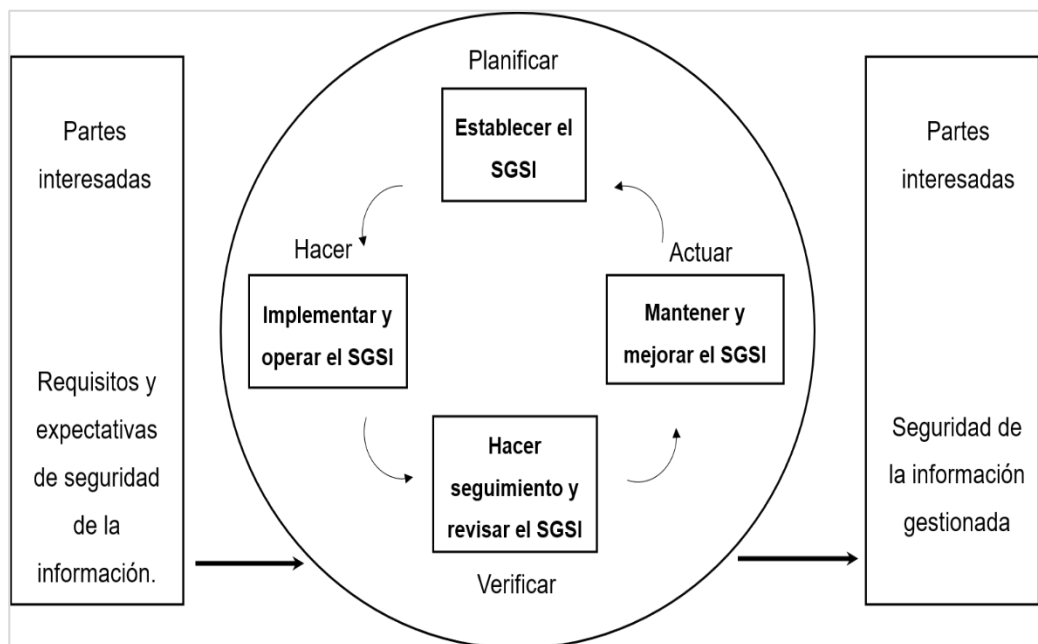
Según (Atehortúa, Bustamante, & Valencia, 2008), la norma ISO 27001 cuenta con una estructura orientada al Ciclo de Deming, en el cual las etapas son planificar, hacer, verificar y actuar. La planificación surge con la declaración del alcance, se determinan las actividades de la empresa donde se aplicará el sistema. Por lo general se eligen los procesos con mayor riesgo en la administración de la información. Como siguiente es necesario preparar y difundir una política de administración de la seguridad de la información, para establecer los lineamientos rectores de la organización a considerar hacia los posibles problemas con la data, incorporando requerimientos de la ley, relacionados a contrato y propios en la empresa.

La caracterización de los riesgos de la información en relación con las posibles amenazas y los puntos vulnerables de una organización en sus dimensiones de confidencialidad, seguridad y disponibilidad de la información viene a hacer el eje central de una planificación del SGSI. Siendo así que la identificación, análisis y valoración de estos riesgos nos permitirá definir los planes de acción, que nos ayudará a llevar los riesgos identificados hasta un nivel aceptable o manejable por la organización. La implementación se basa en poner en práctica los planes de acción definidos. Contiene también la documentación de la aplicación y el cumplimiento de los procedimientos necesarios, así como la formación y

la sensibilización de los colaboradores de la organización en referencia a seguridad de la información.

La etapa de verificación contiene la medición del desempeño, la eficacia de los controles implementados, esto a través de la realización de auditorías internas al SGSI y la verificación del mismo por parte de la gerencia. Siendo así que estas acciones nos llevan a una mejora continua la cual incluye actualizaciones de planes, procedimientos, etc. de seguridad de la información.

Por lo tanto; (Atehortúa, Bustamante, & Valencia, 2008), muestran la siguiente figura que representa gráficamente el diseño del sistema de administración de la seguridad de la información:



*Figura 1.* Modelo de Sistema de Administración de Seguridad de la Información. Fuente: (Atehortúa, Bustamante, & Valencia, 2008).

### 1.3.6. Evaluación del riesgo de la seguridad de la información.

(ISO 27001, 2013), especifica que “la organización requiere establecer una metodología para la gestión del riesgo de seguridad de la información” (p.4).



Dicho proceso debe desarrollarse de la siguiente forma:

- Se debe determinar y conservar criterios de riesgo de seguridad de la información que deben contener:
  - Parámetros que me permitan aceptar los riesgos.
  - Parámetros para la realización de los exámenes de riesgos de seguridad de la información.
  
- Asegurarse en las pruebas de seguridad de la información desarrollados repetitivamente generen resultados consistentes, válidos y que se puedan comparar.
  
- Ubicar las dificultades asociadas a seguridad de la información.
  
- Analizar dichos riesgos.
  
- Estimar los riesgos que se asocian a seguridad de la información.

#### **1.3.7. Tratamiento del riesgo de seguridad de la información.**

(ISO 27001, 2013), manifiesta: “La entidad deberá brindar la definición y el marco de aplicación para un proceso para tratar los riesgos de seguridad de la información” (p.5).

Dicho proceso se desarrollará así:

- Elegir las opciones convenientes para los riesgos asociados con seguridad de la información, tomando en cuenta lo obtenido en el examen de los riesgos.
  
- Establecer los controles necesarios para poner en funcionamiento la opción de tratamiento elegida.

### **1.3.8. Metodologías.**

#### **1.3.8.1. Prince2.**

(Turkley, 2010), describe la metodología mencionando el método MOR (Management of Risk), que presenta métodos genéricos para la gestión de riesgos, que consisten en lo siguiente:

- Entender el alcance del proyecto.
- Incluir partes interesadas (usuarios, proveedores y equipos).
- Suministrar informes regulares de los riesgos.
- Concretar catálogos y responsabilidades de los riesgos.

Según, (Turkley, 2010), se establece un modelo consistente en 5 fases (identificar, evaluar, planificar, implementar y comunicar), además encomienda que se tenga un portafolio estratégico en el cual se deban establecer los procedimientos para la gestión de riesgo para cada proyecto.

Paso 01 – Identificar: Completar el documento de estrategia de Gestión del Proyecto, luego identificar los riesgos (amenazas y oportunidades) que puedan afectar al proyecto.

Paso 02 – Evaluar: Evaluar los riesgos según su probabilidad e impacto en los objetivos del proyecto.

Paso 03 – Planificar: Disponer las respuestas puntualizadas a las amenazas.

Paso 04 – Implementar: Se lleva a desarrollar las respuestas planificadas citadas en el paso de Planificación.

Paso 05 – Comunicación: Se salvaguarda la comunicación entre las partes interesadas.

### 1.3.8.2. MagerIT.

(Esquema nacional de seguridad, 2012), menciona sobre la metodología MagerIT (Metodología de Análisis y Gestión de Riesgos de Sistemas de Información), la cual fue desarrollada y promovida por el Consejo Superior de Administración Electrónica (CSAE) en contestación a la percepción de que la Administración Pública que de forma progresiva obedece a los sistemas de información con el fin de conseguir sus objetivos. MagerIT, es rectamente coherente con el uso de las TI y comunicaciones, que presume algunos beneficios indiscutibles para los usuarios, asimismo da lugar a la gestión de los riesgos a través de mecanismos de control en seguridad de la información que brinden confianza a los usuarios en diferentes medios.

(Esquema nacional de seguridad, 2012), permite que el proceso de gestión de riesgos se implemente dentro de un contexto de trabajo ayudando a los órganos de gobierno a tomar medidas teniendo en cuenta los riesgos producidos por el uso de las TI; respondiendo a la sección 4.4 “Implementar la Gestión de Riesgo” – ISO 31000.

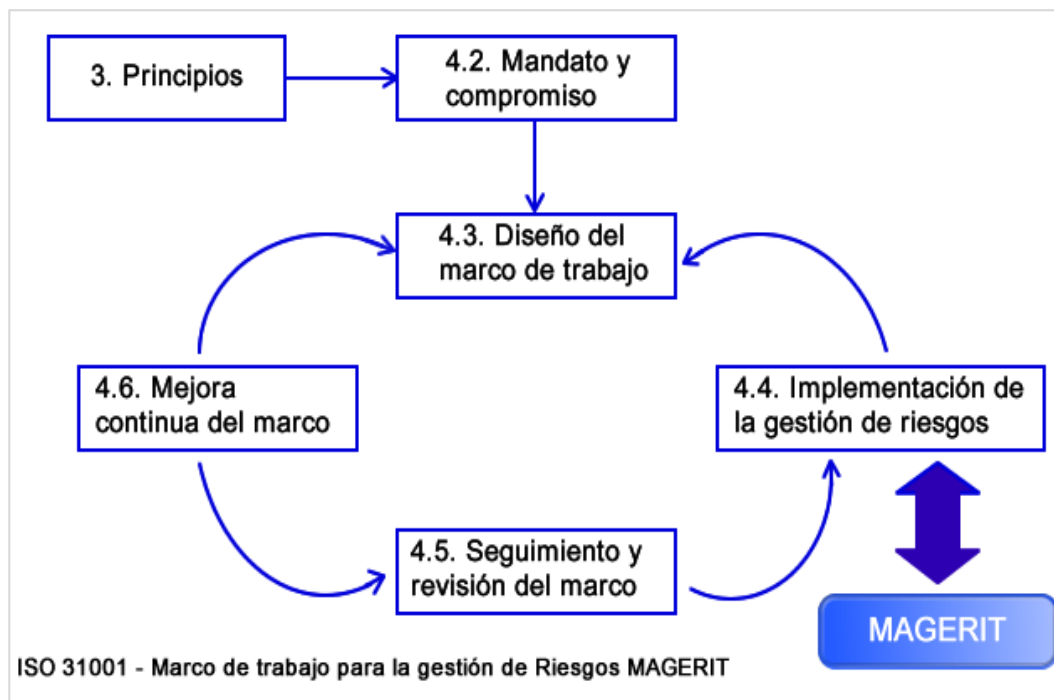


Figura 2. Marco de trabajo para la gestión de riesgos. Fuente: (Amutio, Candau, & Mañas, 2012).

(Esquema nacional de seguridad, 2012), establece la existencia de varios acercamientos en relación con la dificultad de evaluar los riesgos sobrellevados por los sistemas de TI, las guías informales, acercamientos metódicos y herramientas de soporte, son algunas de ellas con las cuales indagan objetivar una evaluación de riesgos para saber el nivel de seguridad o inseguridad se encuentran. La complejidad del problema viene a ser un gran reto a la cual se afrontan; por lo que, se persigue un acercamiento metódico que no dé cabida a una improvisación y más aún dependa de un análisis absurdo.

### **Objetivos:**

#### **Directos:**

Los dueños de los procesos en las organizaciones, deben de ser juiciosos con la presencia de los riesgos y la penuria de controlarlos.

Fomentar un procedimiento sistemático que permita analizar los riesgos originados del uso de las TIC.

Identificar y planear un tratamiento oportuno para conservar un control de los riesgos.

#### **Indirectos:**

La organización deberá de prepararse para los diversos procesos de evaluación, auditoría, certificación o acreditación.

#### **1.3.8.3. RiskIT.**

(Isaca.org, 2019), la metodología RiskIT tiene como origen en ISACA, líder internacional y reconocido como provisor de nociones, certificaciones, soporte y formación en seguridad y resguardo de sistemas de información, gobierno organizacional, gobierno de TI, al igual que riesgos y una obediencia coherente con TI.

Hoy en día en un mundo globalizado, la gestión de riesgo es una práctica estratégica para toda organización, lo que hace a la metodología RiskIT esté destinada a un público objetivo amplio. RiskIT, nos proporciona información de cómo aplicar los principios de gestión de riesgos de una organización - ERM (Enterprise Risk Management), las normas y marcos como COSO ERM y AS/NZ 4360, a las TI. Esta metodología está definida y basada en una serie de guías basadas en los principios aceptados en ERM, que permitirá a las TI una eficaz gestión de los riesgos.

Para la gestión de riesgos bajo el marco de RiskIT, se ha creado un modelo de proceso similar a COBIT y Val IT, que se parte en tres secciones: Gobernanza del riesgo, evaluación del riesgo y la respuesta del riesgo, cada uno de estos con sus 3 subprocesos:

Gobierno del Riesgo (GR):

RG1 Implantar y conservar una vista de riesgo común.

RG2 Integrar con ERM.

RG3 Tomar decisiones conscientes de los riesgos del negocio.

Evaluación del riesgo (RE):

RE1 Recolección de datos.

RE2 Análisis de datos.

RE3 Conservar el perfil de riesgo.

Respuesta de Riesgo (RR):

RR1 Riesgo articulado.

RR2 Manipular el riesgo.

RR3 Reaccionar a acontecimientos.

#### **1.3.8.4. Mehari.**

(Barrera & Rodríguez, 2014), la metodología MEHARI, fue desarrollada en el año 1996 por CLUSIF (Club de la Seguridad de Información de Francia). Mehari nos permite que los principales riesgos que pueda

percibir una organización en su contexto sean evaluados cuantitativa o cualitativamente, según corresponda.

Mediante un grupo de elementos y herramientas que se encuentran concretamente bajo el mando de la seguridad de la información según los requisitos ISO/IEC 27005:2008, Mehari define como principal objetivo brindar una metodología para la estimación y gestión de riesgos.

Entre los aspectos esenciales de Mehari son: Definir una metodología de riesgo, valoración de la eficacia de las políticas de seguridad y capacidad para valorar y simular los niveles de riesgo. Mehari, usa auditoria para identificar las vulnerabilidades, en las cuales evalúa las situaciones de riesgo y se deducen sus contextos. Además, cuenta con tres módulos: análisis o tasación de riesgos, valoración de seguridad y análisis de amenazas, los cuales pueden seleccionarse teniendo como línea base las políticas y estrategias corporativas a fin de plantear mecanismos de control que permita controlar la seguridad de la información (Barrera & Rodríguez, 2014).

#### **1.3.8.5. Octave**

La metodología Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation), desarrollada por el SEI (Software Engineering Institute – EE. UU). Se enfoca necesariamente en el riesgo y no en la tecnología como otras metodologías, haciéndola un poco más complicada a diferencia de las otras. Su implementación es ideal en organizaciones con un mayor número de 300 colaboradores y se encuentra dividida en 3 etapas: Fase 1 – Identificación de amenazas basada en los activos, Fase 2 – Identificar las vulnerabilidades de los activos y Fase 3 – Desplegar mecanismos de control en base a los riesgos identificados. (Hurtado, 2018).

Según, (Barrera & Rodríguez, 2014), Octave propone un plan para mitigar los riesgos dentro en una organización partiendo desde una correcta

evaluación de riesgos en TI, asimismo busca concientizar a toda la organización respecto a una cultura en seguridad de la información.

Octave, a través de diversos procesos, como realizar una correcta evaluación de los activos asignándoles un valor estimado para la organización, analiza y estudia la infraestructura de la información; considerándose como una técnica de alineación, proyección, categorización y consultoría en seguridad de TI, logrando su desarrollo en las 3 fases mencionadas anteriormente. Octave permite obtener los siguientes beneficios identificación, evaluación de riesgos y plantear estrategias de protección para mitigar los riesgos de seguridad de la información, estos beneficios orientan a la Organización a una mejor gestión de los riesgos. En conclusión, Octave viene hacer un método operativo direccionado a resultados, el cual permite obtener un plan a corto plazo (2-3 meses de su iteración) y posteriormente un plan estratégico a largo plazo (6 – 12 meses), que permitirá mitigar los riesgos identificados. (Barrera & Rodríguez, 2014).

#### **1.4. Formulación del problema.**

¿En qué medida el uso de la norma ISO/IEC 27001:2013 contribuirá en mejorar los procesos de gestión de riesgos de tecnologías de la información para una empresa constructora peruana?

#### **1.5. Justificación e importancia del estudio.**

La presente indagación es relevante porque analiza los riesgos tecnológicos de la información cuando utilizamos la Norma ISO/IEC 27001:2013; las cuales definitivamente mejorarán la administración básica en las TI en una organización que desarrolla proyectos de gran envergadura en el sector construcción.

El estudio tiene implicancia social para justificar el orden de una organización de mediano tamaño para ordenar los procesos de gestión en la oficina de TI

y en consecuencia favorece el bienestar de los colaboradores en este tipo de empresa.

Esta tesis tiene valor teórico, debido a que es contributiva en el conocimiento científico para los conceptos de análisis de riesgos para la tecnología de la información y el conocimiento y práctica de las Norma ISO/IEC 27001:2013 brindando aportes los cuales se pueden presentar en congresos científicos y publicar en revistas especializadas en gestión de la construcción.

Tiene valor práctico, porque los instrumentos que se pueden emplear en este estudio pueden ser útiles en otras investigaciones del mismo rubro con resultados diferenciales entre ellos.

Su valor metodológico, es importante porque la propuesta del estudio puede analizar de manera eficiente los riesgos tecnológicos y generar mejora continua de los procesos de gestión en Colvias S.A.C.

## **1.6. Objetivos**

### **1.6.1. Objetivo general**

Desplegar una metodología para mejorar los procesos de Gestión de Riesgos de Tecnologías de la Información mediante el uso de la norma ISO/IEC 27001:2013 para una empresa constructora peruana.

### **1.6.2. Objetivos específicos**

- a) Identificar los procesos de gestión de riesgo de Tecnología de la Información.
- b) Realizar un diagnóstico situacional de los estados actuales de los controles de seguridad de la información de la norma ISO / IEC 27001:2013 de la empresa.
- c) Identificar los activos de seguridad de la información.



- d) Desplegar una metodología adecuada para la evaluación y administración de los riesgos para una empresa constructora peruana.
- e) Diseñar una propuesta de implementación de los mecanismos de control que permitirán dar respuesta a los riesgos identificados.

### **1.7.Limitaciones.**

- Sólo se realizará en las oficinas ubicadas en Moquegua.
- Se utilizará la información que la empresa brinde para el análisis correspondiente.

#### **1.7.1. Delimitación de la Investigación.**

El presente trabajo de investigación fue realizado en la ciudad de Moquegua, para ello se analizó la administración de riesgos de las actividades que forman parte de TI en la empresa; así como su interacción con otras áreas de la organización.

## **II. MATERIAL Y MÉTODO**

### **2.1. Tipo de estudio y diseño de la investigación.**

La forma para desarrollar la investigación se puede dividir en 02 categorías, el primero relacionado con el objetivo de estudio, y el segundo por los procedimientos que serán empleados.

Bajo los conceptos anteriormente descritos, el presente trabajo de investigación, dado que uno de los objetivos del estudio es del tipo cualitativa, ya que se trabajará con información recopilada de la empresa, con la cual se medirá la situación en estos momentos sobre la gestión asociada con riesgos del grupo de subprocesos asociados con TI. Y de acuerdo con los procedimientos empleados, el trabajo es de campo, ya que la información se recoge mediante la observación y aplicando un cuestionario para recoger data relevante de los procesos de TI de la empresa.

#### **2.1.1. Diseño de la investigación.**

En lo referente al diseño, para nuestro caso de estudio, el tipo de diseño de investigación que será empleado es el denominado diseño de investigación descriptivo, dado que se ubicará en una categoría que nos proporcionará una visión integral de nuestro caso de estudio.

Para el desarrollo del diseño, se están considerando las siguientes etapas:

Etapa preliminar: En esta etapa se define: la población y la muestra a considerar, el diseño del cuestionario (incluye las preguntas y la escala de calificación de cada pregunta).

Etapa de aplicación: Aquí se procede a la aplicación de la encuesta a los colaboradores que componen la muestra elegida; luego se realiza una verificación de las encuestas aplicadas (que hayan sido llenadas

completamente, que la escala elegida sea acorde con la percepción de cada usuario, etc.).

Etapa posterior a la aplicación: En esta parte, se procede a ingresar los datos para procesarlos, preparar los informes e interpretar los resultados obtenidos.

## **2.2. Escenario de estudio.**

Para el caso de estudio, vamos a considerar como población a todos los procesos de la empresa constructora Colvias S.A.C.

La muestra será representada por las unidades funcionales de la empresa que interactúan con el subproceso de TI.

### **2.2.1. Enfoque seleccionado.**

Caso de Estudio: Empresa constructora Colvias S.A.C, el cual es una empresa que tiene como sede situada en la ciudad de Moquegua, el cual aún no cuenta con un sistema de gestión de riesgos asociados a sus procesos de TI; debido a ello, es necesario desarrollar una propuesta de administración de riesgos en el grupo de subprocesos de tecnologías de la información de acuerdo con los parámetros de la norma ISO/IEC 27001:2013.

### **2.2.2. Objeto de estudio.**

Colvias S.A.C. – Sede Moquegua.

Colvias S.A.C. es una empresa constructora peruana dedicada al desarrollo de proyectos de infraestructura en el Perú.

### **Misión.**

Contribuir a la modernización del país, a la movilidad de las personas y al desarrollo de las comunidades, brindando soluciones de infraestructura innovadoras y de calidad.

**Visión.**

Ser una de las compañías líderes en la construcción y mantenimiento de la infraestructura pública y privada en el Perú.

**Valores.**

- Confianza
- Respeto
- Excelencia
- Creatividad
- Espíritu de equipo
- Rectitud

**Servicios que realiza.**

- Obras de infraestructura vial.
- Obras de infraestructura Urbana.
- Construcción y mantenimiento de obras civiles.
- Movimiento de tierras.
- Construcción de PADS.
- Construcción de Pozas.
- Construcción de plataformas.
- Infraestructura para minería.
- Infraestructura Aeroportuaria
- Obras hidráulicas.
- Túneles.
- Redes de acueducto y alcantarillado.

Mapa de procesos.

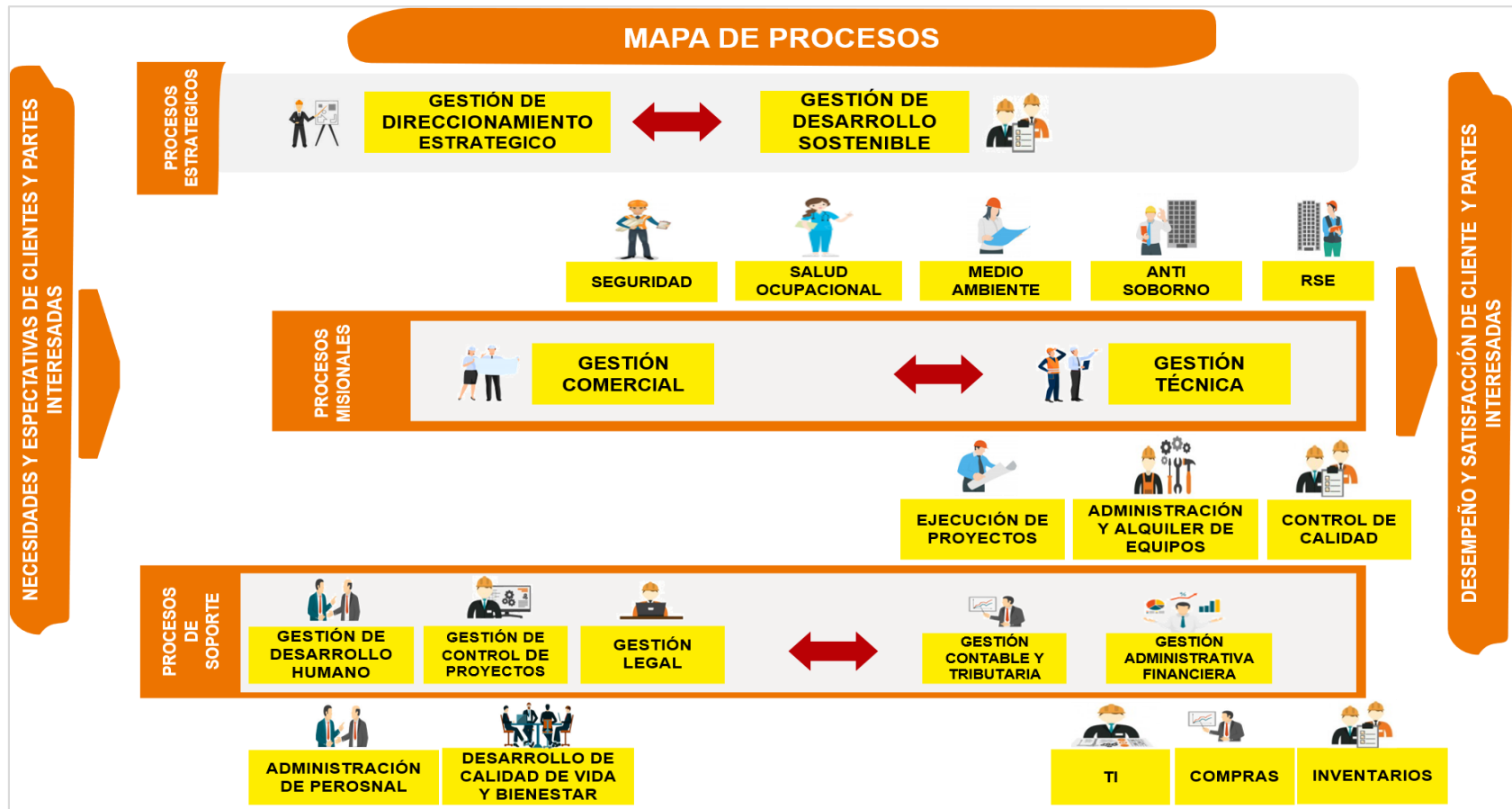


Figura 3. Mapa de Procesos. Fuente: Colvias S.A.C.

### **Objetivos generales:**

- **Objetivo 01:** Lograr el crecimiento, mejorando la eficacia de los procesos y garantizando la rentabilidad de la organización.
- **Objetivo 02:** Incrementar la satisfacción del cliente con respecto a nuestros productos y servicios.
- **Objetivo 03:** Cumplir con la normatividad y reglamentación vigente.
- **Objetivo 04:** Promover una buena calidad de vida laboral, potenciando y manteniendo nuestro recurso humano.
- **Objetivo 05:** Actuar con responsabilidad social y ética.

### **2.3. Caracterización de Sujetos.**

Los sujetos participantes de la presente investigación corresponden a las unidades organizacionales de la empresa Colvias S.A.C – Moquegua que interactúa con el subproceso de TI de la organización.

### **2.4. Técnicas e instrumentos de recolección de datos.**

#### **2.4.1. Metodología, estrategias y herramientas para seleccionar data.**

La herramienta para la toma y selección de datos es la encuesta, ya que esta nos permitirá recoger información de la muestra representativa de la población a considerar.

Para un mayor detalle del tipo de entrevista a realizar, el tipo de encuesta a utilizar es la denominada “auto administrado”, en el cual, la encuesta se proporciona directamente a los miembros de la muestra; por el cuestionario a utilizar, las preguntas son del tipo “cerradas”, ya que se le brinda a los encuestados opciones muy puntuales para responder.

Para la recolección y procesamiento de la data, se utilizará un formato de entrevistas y una hoja de cálculo para el procesamiento de la información.

#### 2.4.2. Instrumentos de seleccionar data.

- **Cuestionario para identificar la situación de los procesos de TI**, se usará para orientar la atención en lo que necesitamos observar o analizar referenciado en el anexo 03.
- **Formatos de procesamiento de datos obtenidos en las encuestas**, con esto se pretende tener un formato estandarizado para el registro y posterior análisis de los datos.

#### 2.4.3. Validación del instrumento.

En la presente investigación se procederá a evaluar el instrumento de la recolección de datos y la propuesta a través de un juicio de expertos; los expertos que realizaron la validación del instrumento (entrevistas) fueron los siguientes:

Tabla 1.

*Jueces expertos de validez de contenido.*

<b>Jueces expertos</b>	<b>Grado</b>	<b>Apellidos y Nombres</b>	<b>CIP</b>
JUEZ 01	Ingeniero de Sistemas	Luis Chavarria Aragón	166401
JUEZ 02	Ingeniero de Sistemas	Hilda Milagros Santacruz Quiroz	202709
JUEZ 03	Ingeniero de Sistemas	Carlos Alberto Sánchez Acosta	193176

*Nota:* Se muestra los ingenieros de sistemas que conformaron el equipo de jueces expertos en la validación del instrumento. Fuente: Elaboración propia.

Para el cálculo del coeficiente de validez del instrumento (entrevista), se realizó haciendo uso el método Delphi.

Cálculo del Coeficiente de Validez por cuestión (pregunta):

$$C_p = \sum_{i=1}^n J_{ip}$$

Dónde:  $J_{ip}$  es el rango asociado a la evaluación del juez experto "i" de la pregunta "p".

Cálculo del Coeficiente de Validez:

$$Cv = \frac{\bar{Jz}}{K}$$

Dónde:

Jz: es la media aritmética del puntaje obtenido por pregunta de los jueces expertos.

K: es la constante (puntaje deseado = 25).

En la siguiente tabla número 02, se muestra el resumen de evaluación por los expertos. Las calificaciones para los criterios de validación se detallan en la hoja de juicio de experto (anexo 06) con respecto al contenido del instrumento.

Tabla 2.

*Calificación para el instrumento de los jueces expertos.*

<b>Pregunta Evaluada</b>	<b>Juez 01</b>	<b>Juez 02</b>	<b>Juez 03</b>	<b>Puntaje Deseado</b>	<b>Coeficiente de Validez</b>
Pregunta "a"	25	25	25	25	1.00
Pregunta "b"	23	21	25	25	0.92
Pregunta "c"	25	23	23	25	0.95
Pregunta "d"	25	25	21	25	0.95
Pregunta "e"	25	23	23	25	0.95
Pregunta "f"	25	25	23	25	0.97
Pregunta "g"	23	23	25	25	0.95
Pregunta "h"	25	23	21	25	0.92
Pregunta "i"	23	25	21	25	0.92
Pregunta "j"	23	21	23	25	0.89



Pregunta "k"	23	23	21	25	0.89
Pregunta "l"	23	21	19	25	0.84
Pregunta "m"	25	23	23	25	0.95
Pregunta "n"	25	25	25	25	1.00

*Nota:* Se muestra la puntuación de las preguntas del instrumento validado por los jueces expertos, para obtener el coeficiente de validez es el cálculo de la media aritmética de la columna "Coeficiente de Validez". Fuente: Elaboración Propia.

Validez = Media Aritmética (Coeficiente de validez).

Validez = 0.94.

De la evaluación realizada se obtiene una validez del 0.94, según escala de validez el instrumento (entrevista) tiene como resultado "MUY ALTO", de acuerdo con el criterio de los jueces expertos.

Tabla 3.

*Escala de validez.*

Rango	Criterio de Validez
0.01 - 0.20	Muy bajo
0.21 - 0.60	Bajo
0.61 - 0.80	Moderado
0.81 - 0.90	Alto
0.91 - 1	Muy Alto

*Nota:* Se muestra la escala para los criterios de validez. Fuente: Elaboración Propia.

## 2.5. Procedimientos para la recolección de datos.

Para el procedimiento de toma de data se utilizará como referente el análisis documentario, el cual consiste en la clasificación y revisión de los documentos de gestión que la empresa utiliza, dichos documentos pueden ser:

- Procedimientos e instructivos de trabajo.

- Políticas u objetivos de los sistemas de gestión que la organización posee.
- Información respecto a los posibles riesgos que se pueden evidenciar en el proceso de TI.
- Plan estratégico y procedimientos de TI.

## **2.6. Procedimiento de análisis de datos.**

La Información será recolectada mediante los instrumentos de recolección de los datos, serán revisados, validados y además interpretado de acuerdo a los fines planteados en la investigación.

Para el análisis de la información se utilizarán histogramas, los cuales mostrarán los resultados de cada una de las preguntas del cuestionario planteado; además, se utilizarán promedio ponderados y análisis de Pareto para la presentación de la información y la interpretación del mismo.

## **2.7. Criterios éticos.**

Son criterios que valen como base para argumentar muchos de los preceptos éticos y valoraciones puntuales de las acciones humanas. Como los principios que son aceptados de manera general dentro de nuestros usos y costumbres.

## **2.8. Criterios de rigor científico.**

El trabajo de investigación a desarrollar, el cual se relaciona con una propuesta de implementación de la gestión de riesgos en los procesos de TI, se realizará siguiendo una metodología y los juicios científicos establecidos, logrando así garantizar la calidad de la propuesta de implementación. De esta forma, se logra una coherencia metodológica durante el desarrollo de la presente investigación.

### III. REPORTE DE RESULTADOS

#### 3.1. Análisis y discusión de resultados.

##### 3.1.1. Resultados en tablas y figuras.

Para el desarrollo de la presente investigación se desarrollará un cuestionario a los colaboradores de la organización, con el objetivo de conocer la realidad que tiene la institución respecto a la gestión de TI.

Este cuestionario nos permitirá; definir el nivel de riesgo que se encuentran los procesos de TI de Colvias S.A.C.

En la tabla número 04, se muestra la relación de los trabajadores de la organización que serán encuestados con el objetivo de tener un diagnóstico acerca de cómo los procesos de TI interactúan con los usuarios.

Además, en los cuadros se determina si el colaborador será elegido para responder la encuesta

Tabla 4.

*Lista de cargos encuestados de la organización.*

Área Funcional	Perfil de Cargo	Encuestado (SI/NO)
	Director de RR.HH	SI
	Coordinador de RR.HH	SI
	Generalista de RR.HH	SI
Desarrollo Humano	Asistente de RR.HH	SI
	Asistente Social	SI
	Auxiliar de RR.HH	SI
	Tareador	NO

	Director Administrativo Financiero de Proyecto	SI
	Jefe Administrativo de Obra	SI
	Coordinador Administrativo e Inventarios	SI
	Coordinador de Tecnología de la Información	SI
Administración y Finanzas	Supervisor Administrativo	SI
	Asistente de Compras	SI
	Almacenero	SI
	Auxiliar Contable	SI
	Auxiliar de Alimentos	NO
	Auxiliar de Almacén	NO
	Auxiliar de Limpieza	NO
	Coordinador de Oficina Técnica	SI
	Ingeniero de Oficina Técnica	SI
	Ingeniero de Planeamiento y Control	SI
	Ingeniero de Topografía	SI
Oficina Técnica	Especialista en Gestión Documentaria y Seguimiento de Contratos	SI
	Cadista	SI
	Auxiliar de Oficina Técnica	NO
	Auxiliar Topógrafo	NO
	Nivelador	NO
	Jefe de Control de Proyectos	SI

	Ingeniero de Control de Proyecto	SI
Control de Proyectos	Supervisor de Rendimiento de Maquinaria	SI
	Asistente de Oficina Técnica	SI
	Jefe de Control de Calidad	SI
CONTROL DE CALIDAD	Asistente de Control de Calidad	SI
	Auxiliar de Control de Calidad	NO
	Laboratorista	NO
	Director de construcción General	SI
	Director de Proyecto	SI
	Gerente de Construcción	SI
	Residente de Obra	SI
	Secretaria de Obra	SI
Construcción	Abogado de Obra	SI
	Jefe de Campo	SI
	Jefe de Planta	SI
	Ingeniero de Campo	SI
	Ingeniero de Perforación y Voladura	SI
	Supervisor de Campo	SI
	Capataz	NO
	Coordinador de Equipos	NO
Equipos	Ingeniero de equipos	SI
	Auxiliar de equipos	SI

	Auxiliar de operador de grúa	NO
	Conductor de Vehículo Liviano	NO
	Conductor de Vehículo Pesado	NO
	Electricista	NO
	Mecánico	NO
	Auxiliar Mecánico	NO
	Director de Desarrollo Sostenible	SI
	Jefe de Gestión SSO	SI
	Jefe de Desarrollo Sostenible	SI
	Jefe de SSO	SI
	Jefe Ambiental	SI
	Coordinador Coach Motivacional	SI
Desarrollo Sostenible	Médico Ocupacional de Obra	SI
	Médico Asistencial	SI
	Supervisor SSO	SI
	Asistente SSO	SI
	Enfermero Ocupacional	NO
	Conductor Paramédico	NO
	Supervisor Ambiental	SI
	Asistente de Gestión Integral	SI

---

*Nota:* Se muestra la lista de cargos de los colaboradores de la constructora Colvias S.A.C, que participaron en el llenado del cuestionario (anexo 03). Fuente: Elaboración Propia.

Según con los datos mostrados en la tabla número 04, se puede mostrar que son 70 los colaboradores de la empresa. De los cuales, se ha elegido a 51 personas para que respondan la encuesta para establecer la línea base respecto a la gestión de los riesgos asociados con los procesos de TI.

Los datos de las 04 primeras tablas mostradas, se puede mostrar la siguiente tabla resumen:

Tabla 5.

*Cuadro resumen – cantidad de colaboradores seleccionados.*

<b>Categoría de Respuestas</b>	<b>Numero de Respuestas</b>	<b>Porcentaje de Participación</b>
SI	51	73%
NO	19	27%
TOTAL	70	100%

*Nota:* Se muestra los resultados en porcentaje de la participación de los colaboradores en el cuestionario (anexo 03). Fuente: Elaboración Propia.

De la tabla número 05, se desprende que el 73% de los colaboradores serán encuestados, y con ello, se establecerá la situación actual de los riesgos asociados a los procesos de TI.

### **3.1.2. Relación de preguntas a ser aplicadas en el cuestionario.**

La lista de preguntas a utilizar serán las siguientes:

- a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?
- b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?

- c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?
- d) ¿Usted necesita el uso de contraseña para acceder a información segura?
- e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?
- f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?
- g) ¿Usted cree que realiza un correcto manejo de los servicios que brinda el departamento de TI?
- h) ¿Es usted consciente en lo significativo que es tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?
- i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?
- j) ¿Sabe usted lo importante que es ejecutar copias de seguridad de la información en determinados periodos ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?
- k) ¿Sabe usted si la empresa tiene implementado un SGSI en los procesos de TI?
- l) ¿Cree usted que la implantación de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?
- m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?



n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar respecto a lo significativo en seguridad de la información?

Mediante las siguientes gráficas, se mostrarán los resultados que se desprenden una vez aplicada la encuesta:

a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?

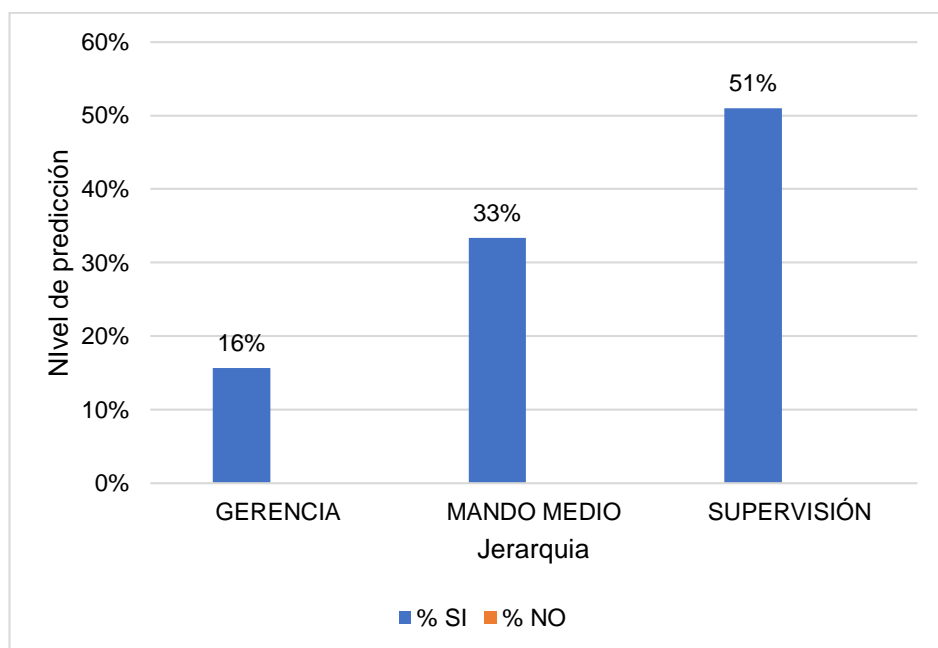


Figura 4. Tasa de respuestas de la pregunta a. Fuente: Elaboración Propia.

Tabla 6.

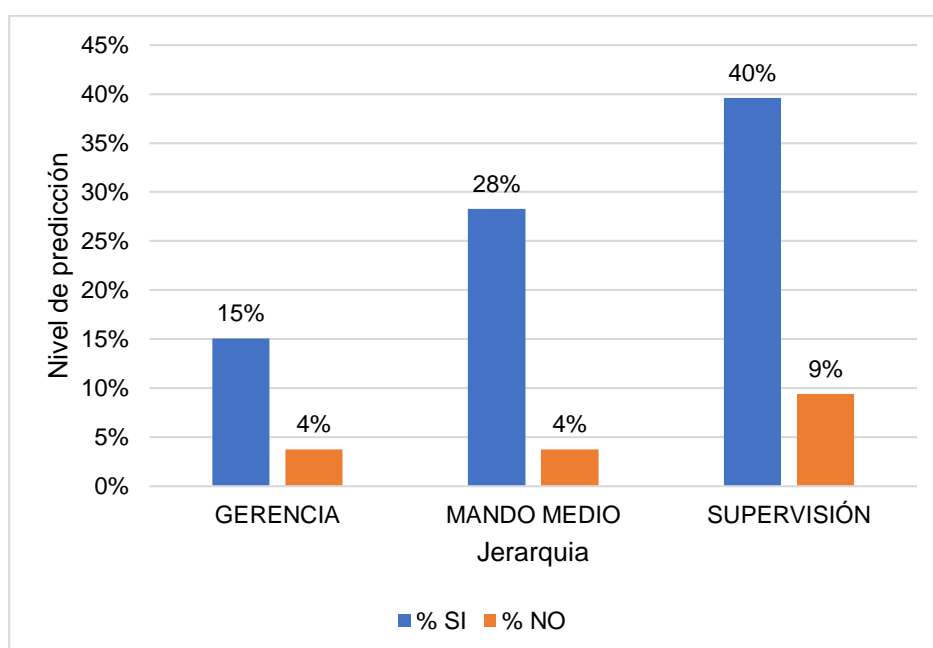
Cuadro resumen – Tasa de respuestas – pregunta a.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	17	26	51
NO	0	0	0	0
% SI	16%	33%	51%	100%
% NO	0%	0%	0%	0%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta a. Fuente: Elaboración Propia.

De la primera pregunta de la encuesta, podemos decir que el 100% de los entrevistados tiene asignado un equipo informático para sus labores asignadas.

b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?



*Figura 2.* Tasa de respuestas – pregunta b. Fuente: Elaboración Propia.

Tabla 7:

*Cuadro resumen – Tasa de respuestas – pregunta b.*

RANGO	GERENCIA	MANDO MEDIO	SUPERVISIÓN	TOTAL
SI	8	15	21	44
NO	2	2	5	9
% SI	15%	28%	40%	83%
% NO	4%	4%	9%	17%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta b. Fuente: Elaboración Propia.

De la segunda pregunta de la encuesta, podemos decir que el 83% de los entrevistados tiene conocimiento de los programas informáticos asignados para sus labores asignadas, siendo el mayor porcentaje en los niveles jerárquicos de mando medio y al nivel de supervisión.

c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?

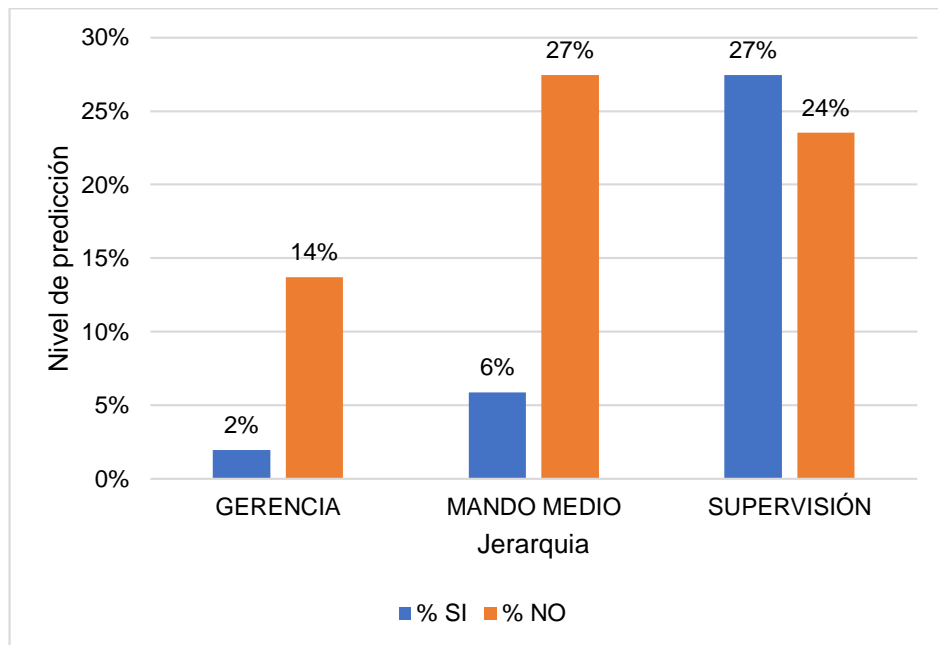


Figura 3. Tasa de respuestas – pregunta c. Fuente: Elaboración Propia.

Tabla 8:

Cuadro resumen – Tasa de respuestas – pregunta c.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	1	3	14	18
NO	7	14	12	33
% SI	2%	6%	27%	35%
% NO	14%	27%	24%	65%

Nota: Resultados según grupo de jerarquía de la organización para la pregunta c. Fuente: Elaboración Propia.

De la tercera pregunta de la encuesta, podemos decir que el 65% de los entrevistados no reporta al área de TI acerca de los equipos informáticos en desuso que tiene bajo su cuidado, y este porcentaje es mayor a nivel jerárquico de mando medio.

d) ¿Usted necesita el uso de contraseña para acceder a información segura?

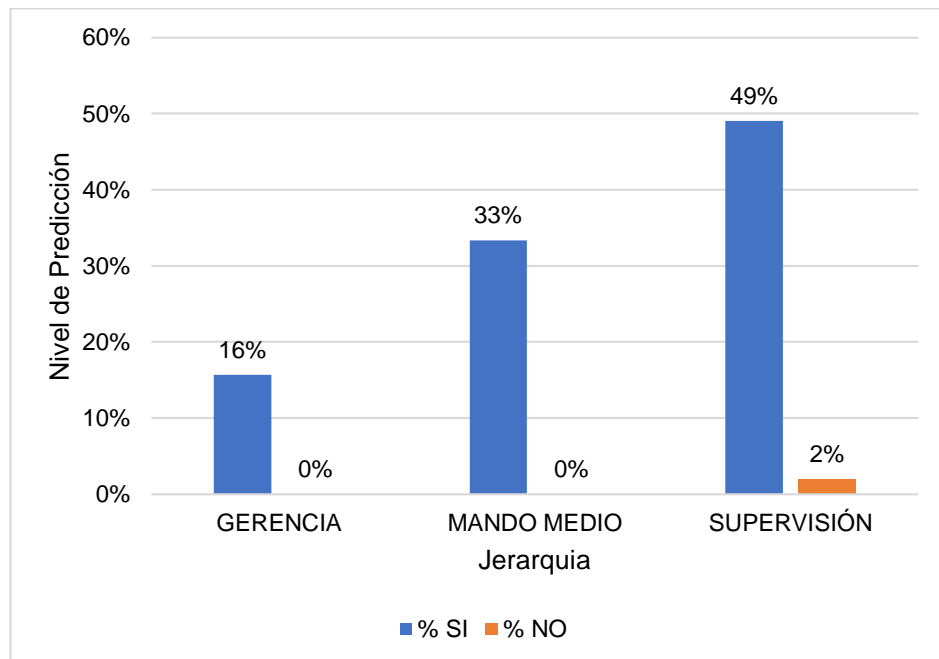


Figura 4. Tasa de respuestas – pregunta d. Fuente: Elaboración Propia.

Tabla 9.

Cuadro resumen – Tasa de respuestas – pregunta d.

RANGO	GERENCIA	MANDO MEDIO	SUPERVISIÓN	TOTAL
SI	8	17	25	50
NO	0	0	1	1
% SI	16%	33%	49%	98%
% NO	0%	0%	2%	2%

Nota: Resultados según grupo de jerarquía de la organización para la pregunta d. Fuente: Elaboración Propia.

De la cuarta pregunta de la encuesta, podemos decir que el 98% de los entrevistados necesita del uso de una contraseña para acceder a una información segura y este porcentaje es mayor a nivel jerárquico de supervisión y mando medio.

e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?

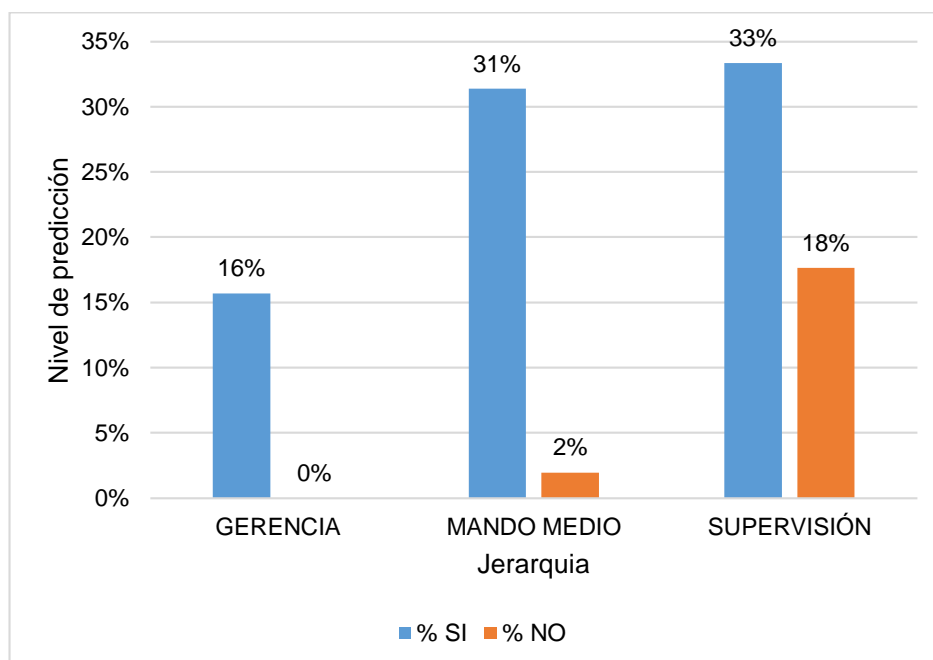


Figura 5. Tasa de respuestas – pregunta e. Fuente: Elaboración Propia.

Tabla 10.

Cuadro resumen – Tasa de respuestas – pregunta e.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	16	17	41
NO	0	1	9	10
% SI	16%	31%	33%	80%
% NO	0%	2%	18%	20%

Nota: Resultados según grupo de jerarquía de la organización para la pregunta e. Fuente: Elaboración Propia.

De la quinta pregunta de la encuesta, podemos decir que el 80% de los entrevistados considera que es importante realizar el cambio de contraseña con frecuencia, dicho porcentaje se hace más evidente en los colaboradores que son del nivel jerárquico de supervisión y mando medio.

f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?

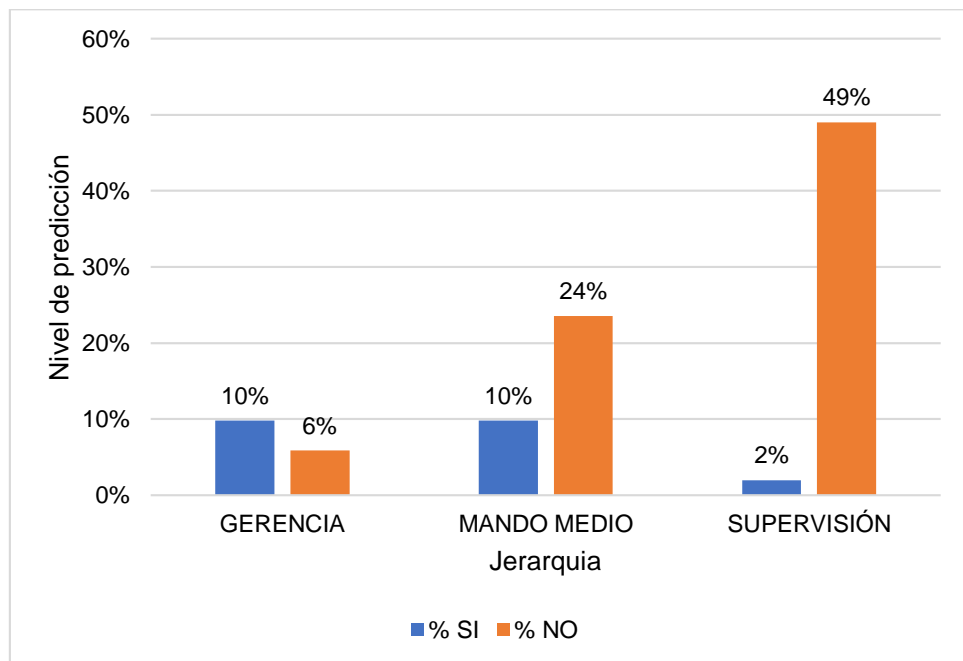


Figura 6. Tasa de respuestas – pregunta f. Fuente: Elaboración Propia.

Tabla 11.

Cuadro resumen – Tasa de respuestas – pregunta f.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	5	5	1	11
NO	3	12	25	40
% SI	10%	10%	2%	22%
% NO	6%	24%	49%	78%

Nota: Resultados según grupo de jerarquía de la organización para la pregunta f. Fuente: Elaboración Propia.

De la sexta pregunta de la encuesta, podemos decir que el 78% de los entrevistados no conoce a quien reportar en caso suceda algún incidente informático, dicho porcentaje se hace más evidente en los colaboradores que son del nivel jerárquico de supervisión y mando medio.

g) ¿Usted cree que realiza un correcto manejo de los servicios que brinda el departamento de TI?

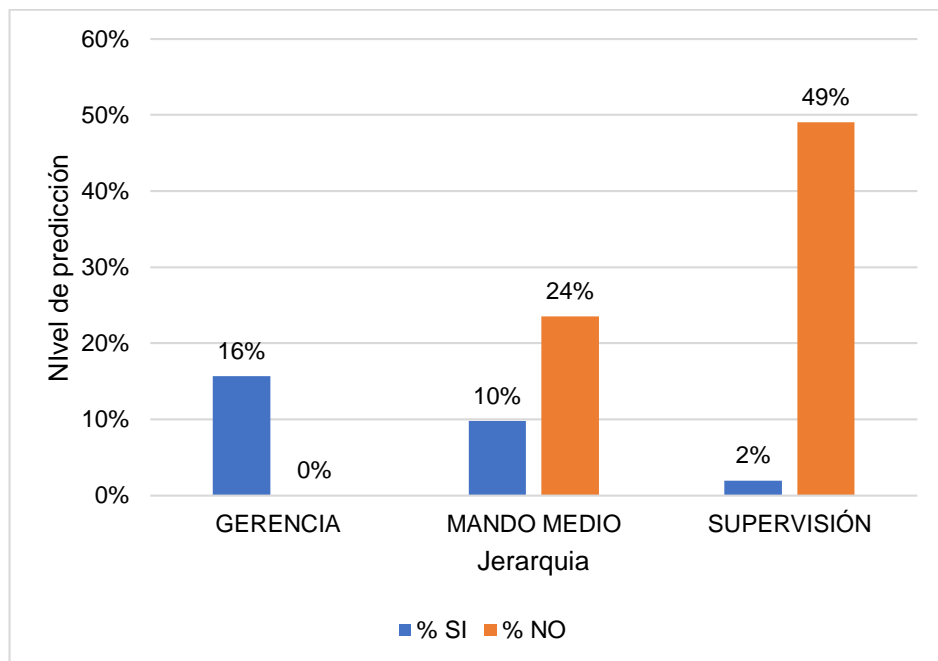


Figura 7. Tasa de respuestas – pregunta g. Fuente: Elaboración Propia.

Tabla 12.

Cuadro resumen – Tasa de respuestas – pregunta g.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	5	1	14
NO	0	12	25	37
% SI	16%	10%	2%	27%
% NO	0%	24%	49%	73%

Nota: Resultados según grupo de jerarquía de la organización para la pregunta g. Fuente: *Elaboración Propia*.

De la séptima pregunta de la encuesta, podemos decir que el 73% de los entrevistados no considera que realizan un uso correcto los servicios que brinda TI, dicho porcentaje se hace más evidente en los colaboradores que son del nivel de supervisión.

h) ¿Es usted consciente en lo significativo que es tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?

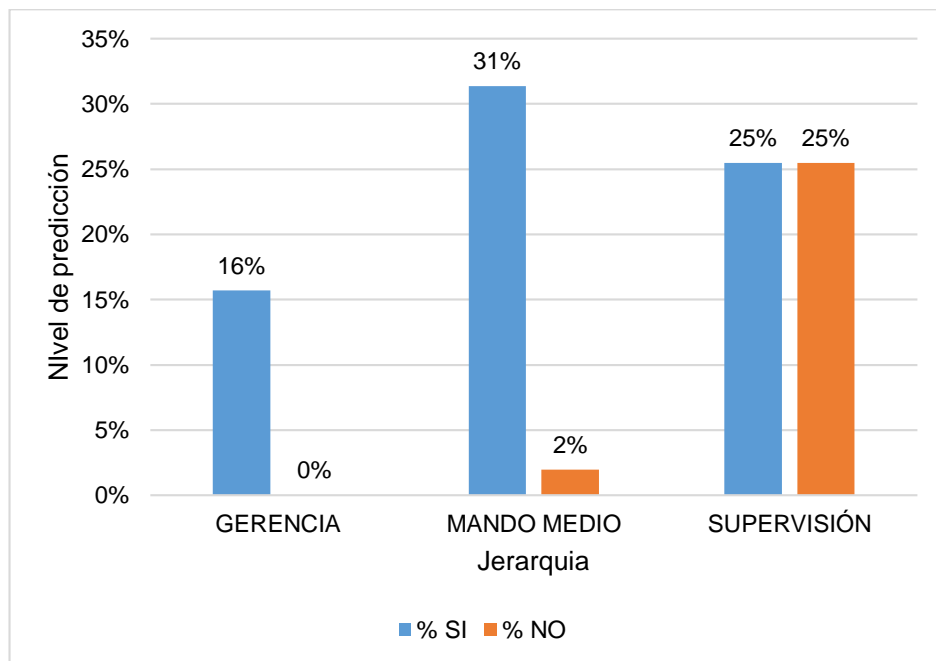


Figura 8. Tasa de respuestas – pregunta h. Fuente: Elaboración Propia.

Tabla 13.

Cuadro resumen – Tasa de respuestas – pregunta h.

RANGO	GERENCIA	MANDO MEDIO	SUPERVISIÓN	TOTAL
SI	8	16	13	37
NO	0	1	13	14
% SI	16%	31%	25%	73%
% NO	0%	2%	25%	27%

Nota: Resultados para la pregunta h. Fuente: Elaboración Propia.



De la octava pregunta de la encuesta, podemos decir que el 73% de los entrevistados es consiente sobre la importancia de tomar medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignaos, dicho porcentaje se hace más evidente en los colaboradores que son del nivel mando de supervisión.

i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?

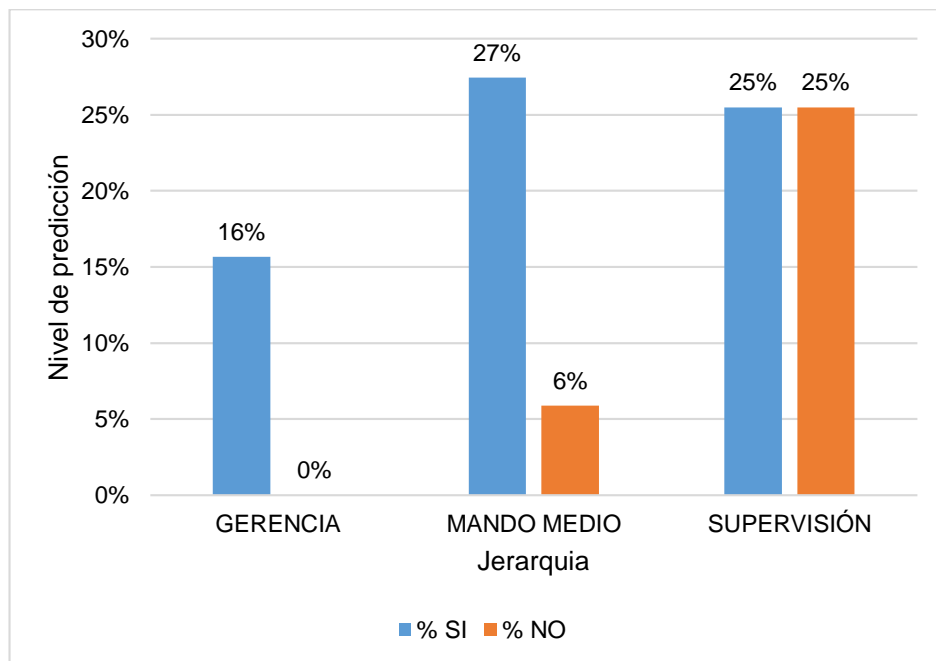


Figura 9. Tasa de respuestas – pregunta i. Fuente: Elaboración Propia.

Tabla 14.

Cuadro resumen – Tasa de respuestas – pregunta i.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	14	13	35
NO	0	3	13	16
% SI	16%	27%	25%	69%
% NO	0%	6%	25%	31%

Nota: Resultados según grupo de jerarquía de la organización para la pregunta i. Fuente: Elaboración Propia.

De la novena pregunta de la encuesta, podemos decir que el 69% de los entrevistados consideran que es importante realizar actualizaciones de los antivirus de los equipos de cómputo asignados, dicho porcentaje se hace más evidente en los colaboradores que son del nivel mando de supervisión.

j) ¿Sabe usted lo importante que es ejecutar copias de seguridad de la información en determinados periodos ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?

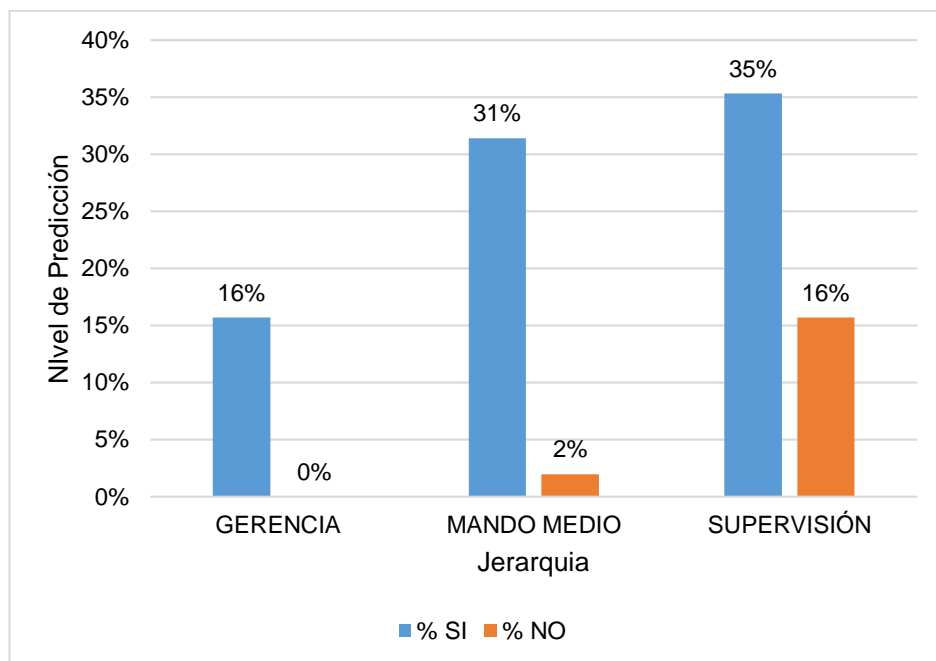


Figura 10. Tasa de respuestas – pregunta j. Fuente: Elaboración Propia.

Tabla 15.

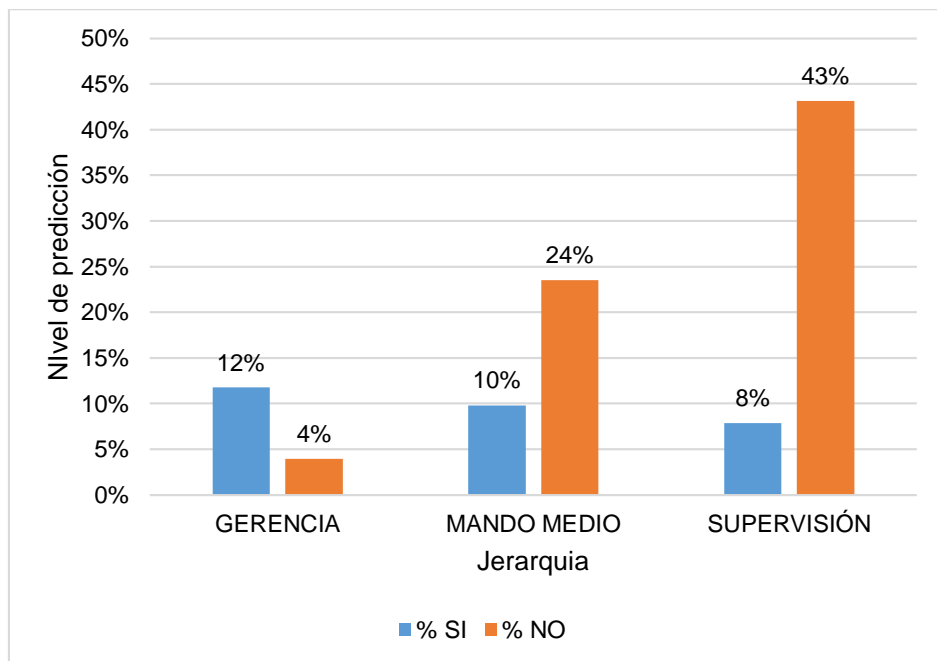
Cuadro resumen – Tasa de respuestas – pregunta j.

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	1	8	19	28
NO	7	9	7	23
% SI	2%	16%	37%	55%
% NO	14%	18%	14%	45%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta j. Fuente: *Elaboración Propia*.

De la décima pregunta de la encuesta, podemos decir que el 55% no es consciente de lo significativo que es realizar copias de seguridad periódicamente que permita resguardar la información ante algún siniestro, dicho porcentaje se hace más evidente en los colaboradores que son del nivel mando medio y supervisión.

k) ¿Sabe usted si la empresa tiene implementado un SGSI en los procesos de TI?



*Figura 11.* Tasa de respuestas – pregunta k. Fuente: *Elaboración Propia*.

Tabla 16.

*Cuadro resumen – Tasa de respuestas – pregunta k.*

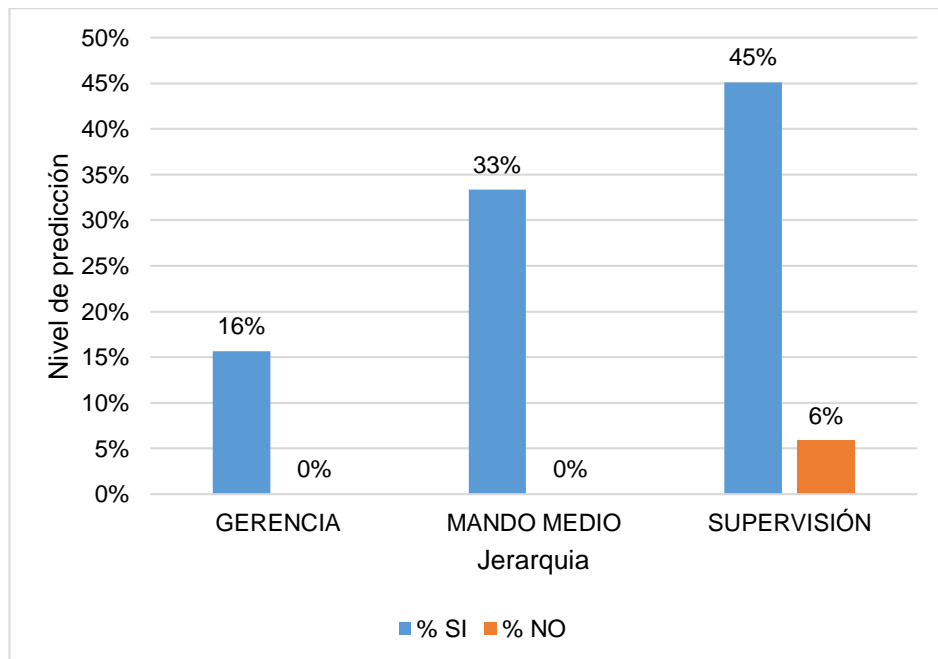
Rango	Gerencia	Mando Medio	Supervisión	Total
SI	6	5	4	15
NO	2	12	22	36
% SI	12%	10%	8%	29%

% NO            4%            24%            43%            71%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta k. Fuente: Elaboración Propia.

De la décimo primera pregunta de la encuesta, podemos decir que el 71% desconoce si se tiene implementado un SGSI en la organización, dicho porcentaje se hace más evidente en los colaboradores que son del nivel mando de supervisión.

l) ¿Cree usted que la implantación de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?



*Figura 12.* Tasa de respuestas – pregunta I. Fuente: Elaboración Propia.

Tabla 17.

*Cuadro resumen – Tasa de respuestas – pregunta I.*

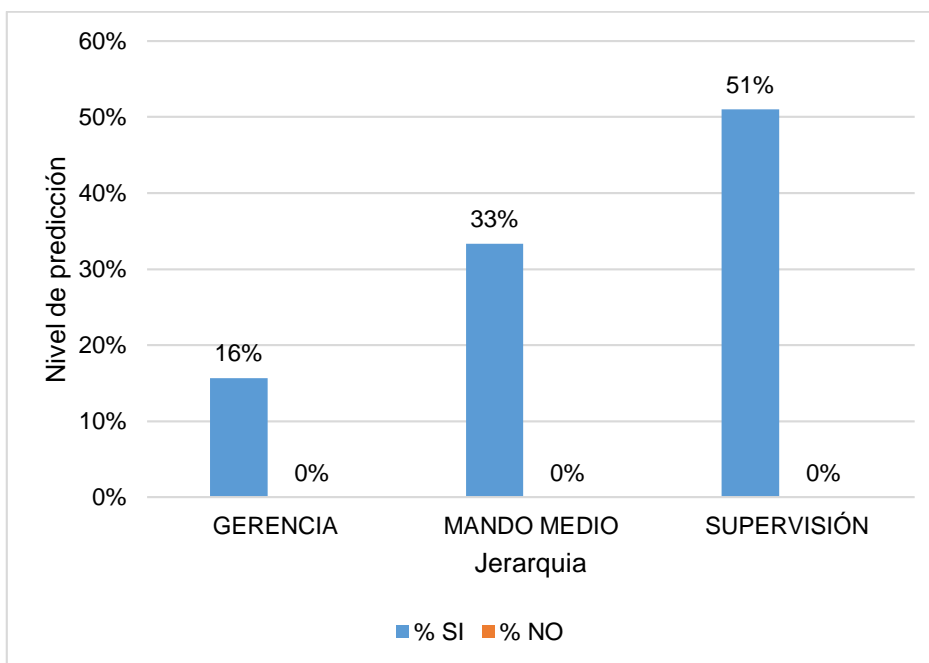
Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	17	23	48
NO	0	0	3	3

% SI	16%	33%	45%	94%
% NO	0%	0%	6%	6%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta I. Fuente: Elaboración Propia.

De la décimo segunda pregunta de la encuesta, podemos decir que el 94% de los entrevistados están convencidos que mediante la implementación de un SGSI será posible mejorar la seguridad de la información que utilizan para el desenvolvimiento de sus actividades diarias.

m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?



*Figura 13.* Tasa de respuestas – pregunta m. Fuente: Elaboración Propia.

Tabla 18.

*Cuadro resumen – Tasa de respuestas – pregunta m.*

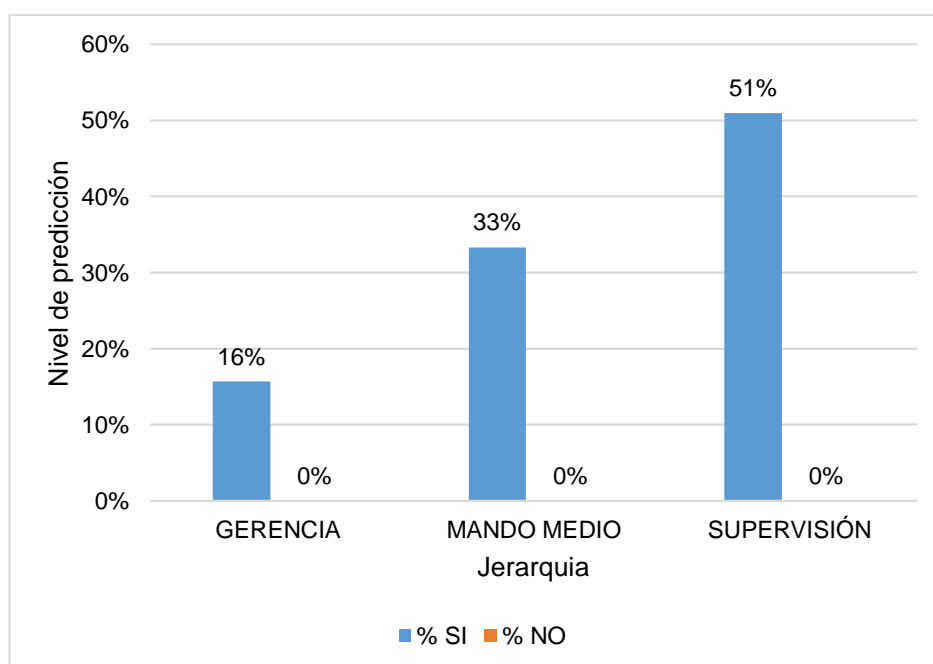
Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	17	26	51

NO	0	0	0	0
% SI	16%	33%	51%	100%
% NO	0%	0%	0%	0%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta m. Fuente: Elaboración Propia

De la décimo tercera pregunta de la encuesta, podemos decir que el total de los entrevistados está de acuerdo con el desarrollo de un SGSI.

n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar respecto a lo significativo en seguridad de la información?



*Figura 14.* Tasa de respuestas – pregunta n. Fuente: Elaboración Propia.

Tabla 19.

*Cuadro resumen – Tasa de respuestas – pregunta n.*

Rango	Gerencia	Mando Medio	Supervisión	Total
SI	8	17	26	51
NO	0	0	0	0

% SI	16%	33%	51%	100%
% NO	0%	0%	0%	0%

*Nota:* Resultados según grupo de jerarquía de la organización para la pregunta n. Fuente: Elaboración Propia.

De la décimo cuarta pregunta de la encuesta, el total de los entrevistados está de acuerdo con la implantación de actividades que ayuden a sensibilizar sobre la importancia en seguridad de la información.

### **3.1.3. Discusión de resultados.**

Se puede observar que los entrevistados están a favor de la implementación de una metodología que gestione adecuadamente los riesgos asociados con la información y con los equipos tecnológicos que utilizan los colaboradores para sus actividades diarias.

En punto en el cual hay controversia es en cuanto al nivel de cuidado y conciencia que los colaboradores tienen respecto al cuidado de los equipos, de la información y la forma como deben actuar en caso de algún tipo de siniestro que pueda ocurrir con los equipos tecnológicos a su cargo, ya que se puede observar que no consideran importante la actualización de los antivirus, y además de ello, no son conscientes de la importancia de realizar copias de respaldo periódicas para mitigar riesgos ante la pérdida de la información.

En conclusión, es sustancial y prioritario la implementación de la gestión de riesgos asociados a los procesos de TI, lo cual permitirá en un futuro la implementación de un SGSI. Además de ello, será necesario desarrollar un programa de sensibilización para los usuarios, con el objetivo de que tomen conciencia de la importancia de la actualización de los antivirus y de una gestión integrada de los riesgos, y como se asocian e interactúan con la información y los equipos que tienen a su cuidado para el desarrollo de sus labores cotidianas.

### **3.2. Consideraciones finales.**

En la actualidad se observa que la gestión de riesgos se encuentra dentro del proceso delimitado por el ciclo de Deming (PDCA), cumpliendo un ciclo de vida. Para el caso del sujeto de estudio empresa constructora peruana Colvias S.A.C., surgió un dilema: ¿De las metodologías que existentes para la gestión de riesgos en la industria cual sería la más adecuada a utilizar como guía?

Teniendo como guía el estudio realizado por (Solarte, Enríquez y Benavidez, 2015), en el cual establece una secuencia de pasos para verificar la existencia de controles de seguridad, pruebas de software y monitoreo de los sistemas de información, esto ayudara a realizar una correcta evaluación del riesgo, permitiéndonos conocer el estado actual de la organización, identificando las causas, vulnerabilidades y posteriormente proponer medidas de control que ayuden a mitigar los riesgos; para el análisis se ha creído conveniente inicialmente comprender los dominios mencionados en el Anexo "A" de la norma ISO / IEC 27001.

### **3.3. Generalidades de la Propuesta.**

Previo al desarrollo de la propuesta se sostuvo reuniones con el responsable de TI y la alta dirección de la empresa constructora peruana Colvias SAC, con quienes se trabajó siguiendo el modelo de estudio realizado por (Jonathan Carrillo Sánchez, 2013), quien define una guía para la selección de la metodología de la gestión de riesgos; se ha creído conveniente presentar la siguiente tabla número 17 que se describe las principales características como: nombre de la metodología, abreviatura, país de origen y la descripción de su abreviatura de las metodologías CMMI, PRINCE2, PMBOK, RISK IT, OCTAVE, COBIT y MAGERIT.



Tabla 20.

*Metodologías que Gestionan el Riesgo.*

<b>Metodología</b>	<b>Descripción</b>	<b>Organización</b>	<b>País de origen</b>
CMMI	Capability Maturity Model	SEI (Software Engineering Institute)	EE.UU.
	Integration Project Management Body of Knowledge	PMI (Project Management Institute)	
PMBOK	Projects IN Controlled Environments	OGC (Office of Government Commerce)	Reino Unido
PRINCE2	Control Objectives for Information and related Technology	ISACA (Information Systems Audit and Control Association) & ITGI (IT Governance Institute)	EE.UU:
COBIT	Risk IT Model	ISACA (Information Systems Audit and Control Association)	EE.UU.
RISK IT	Operationally Critical Threat, Asset and Vulnerability Evaluation	Carnegie Mellon SEI (Software Engineering Institute) y CERT (Computer	EE.UU.
OCTAVE			

MAGERIT	Metodología de Análisis y Gestión de Riesgos de IT	Emergency Response Team)	MAP (Ministerio de Administraciones Públicas)	España
---------	--	--------------------------	---	--------

*Nota:* Metodologías de la gestión de riesgo a evaluación. Fuente: Elaboración Propia.

Posteriormente para poder identificar las principales fortalezas de las metodologías se ha definido los siguientes elementos de tecnología de la información; en las siguientes tablas 21 y 22 se describirán los elementos de TI:

Tabla 21.  
*Elementos de TI.*

Abreviatura	Descripción
(HW)	Hardware
(SW)	Software
(D)	Datos
(COM)	Redes y Comunicación
(P)	Personal
(F)	Financiero
(S)	Servicios de Terceros
(L)	Legal

*Nota:* Identificación de los elementos de tecnología de la información de la organización. Fuente: Elaboración Propia.

Tabla 22.

*Descripción de los elementos de TI.*

<b>Elementos de TI</b>	<b>Descripción</b>
Hardware (HW)	Son todos los equipos informáticos, bienes materiales, que brinden el soporte directo e indirecto de los servicios que presta la organización. También se considerará los dispositivos que permiten el almacenamiento de la información.
Software (SW)	Programas informáticos que facilitan el manejo de datos.
Datos (D)	Son todos los datos que materializan la información.
Redes y Comunicaciones (COM)	Son las redes de comunicación que permiten intercambiar datos.
Personal (P)	Es el personal relacionado con los sistemas de información, así como también los usuarios internos y externos.
Legal (L)	Son los contratos, licencias, derecho intelectual, reglamentos internos de trabajo, impuestos, etc.
Financiero (F)	Se considera a los procesos involucrados con la estimación, presupuestar y controlar los costos que se contemplan en la gestión de un proyecto teniendo como referencia el presupuesto aprobado.
Servicios de Terceros (S)	Servicios auxiliares que son necesarios para poder satisfacer las necesidades de la organización.

*Nota:* Descripción breve de los elementos de TI. Fuente: Elaboración Propia

Para poder calificar las metodologías en relación a los elementos de TI se propone una escala cuantitativa y cualitativa:

Tabla 23.

*Escala de valoración.*

<b>Descripción</b>	<b>Nivel de puntuación</b>	<b>Escala de Medición (EM)</b>	<b>Rango de Selección</b>
No existe correspondencia con el elemento de TI evaluado.	NO CUMPLE	$0 < EM < 0.5$	<b>INSATISFAC TORIO (I)</b>
Existe una aproximación con el elemento de TI evaluado.	CUMPLE PARCIALMENTE	$0.5 < EM < 0.75$	
Se alcanza una correspondencia con el elemento de TI evaluado, sin embargo, este puede diferir en algún aspecto.	ADECUADO	$0.75 < EM < 1$	<b>SATISFACT ORIO (S)</b>
Existe evidencia que si cumple con el elemento de TI evaluado.	CUMPLE	$EM \geq 1$	

*Nota:* Escala de valoración para la evaluación de los elementos de TI.

Fuente: Elaboración Propia.

Teniendo las metodologías a evaluar y una escala de valorización se realizó una matriz de evaluación de las metodologías según sus elementos de TI, en la cual se definirá los valores adecuados y a través de la siguiente fórmula

se definirá la escala de medición final, que ayudará a identificar la metodología adecuada para la organización:

$$\frac{1}{ETI} \sum VTI$$

Donde:

ETI: Número total de elementos de TI evaluados.

VTI: Representa cada valor asignado en los elementos de TI, según metodología evaluada.

Tabla 24.

*Evaluación de las metodologías según elementos de TI.*

Metodología	HW	SW	D	COM	P	F	S	L	Escala de Medición (EM)	Nivel de Puntuación (NP)	Rango de Selección
CMMI	0.5	0.75	0.75	0.5	0.5	0.25	0.5	0	0.47	No Cumple	I
RISK IT	0.75	0.75	0.8	0.75	0.8	0.5	0.8	0.6	0.72	Cumple parcialmente	I
PRINCE 2	0.6	0.6	0.6	0.6	0.6	0.25	0.8	0.25	0.54	Cumple Parcialmente	I
PMBOK	0.6	0.6	0.6	0.6	0.8	0.8	0.6	0	0.58	Cumple Parcialmente	I
COBIT	0.8	0.8	0.8	0.8	0.8	0.7	0.8	0.7	0.78	Adecuado	S
<b>MAGERIT</b>	<b>0.8</b>	<b>0.8</b>	<b>0.8</b>	<b>0.8</b>	<b>0.8</b>	<b>0.8</b>	<b>0.8</b>	<b>0.8</b>	<b>0.80</b>	<b>Adecuado</b>	<b>S</b>
OCTAVE	0.8	0.8	0.8	0.8	0.8	0.6	0.8	0.8	0.78	Adecuado	S

Fuente: Elaborado por coordinador de TI – Colvias S.A.C.

Tomando como base la evaluación realizada en la tabla número 24 observamos que la metodología MAGERIT alcanza un nivel satisfactorio al momento de gestionar los riesgos en los elementos de TI; por lo que, juntamente con el coordinador de TI de la organización se desplegara la metodología MAGERIT para la Gestión de Riesgo dentro de la organización. Asimismo, para el análisis se ha creído conveniente realizar una línea base de los dominios de la ISO 27001 lo cual servirá para implantar en lo futuro la norma ISO/IEC 27001:2013 en la organización. Para el desarrollo de la presente investigación se deben seguir las siguientes fases:

- Fase I: Identificar los procesos para la gestión de riesgos.
- Fase II: Declaración de aplicabilidad de los controles Anexo “A” -norma ISO / IEC 27001:2013.
- Fase III: Realizar una Línea Base de los dominios del Anexo “A” de la norma ISO / IEC 27001:2013.
- Fase IV: Desplegar una metodología adecuada para la tasación y administración de riesgos.
- Fase V: Definición de Planes de Acción que ayuden a mitigar los riesgos.

### **3.3.1. Fase I – Identificar los procesos para la gestión de riesgos.**

En esta fase se determinó los procesos para la gestión de riesgos, bajo los principios de la administración de riesgos prevista en la norma ISO 31001, en la cual se considera cinco procesos de gestión mencionados en la siguiente tabla:

Tabla 25:

*Procesos para la gestión de riesgos.*

<b>Ítem</b>	<b>Proceso</b>	<b>Descripción</b>
P.1	Definir el contexto	Toda organización tiene un entorno interno y externo, dentro del entorno interno se tiene a la misión, visión, políticas, objetivos, estrategias, roles, responsabilidades, etc.

---

		Mientras que en el entorno externo se tiene las regulaciones legales aplicables, economía, política, cultura, etc.
P.2	Análisis de riesgos	Toda organización es necesario identificar los activos de la información que se requieren proteger, mediante una evaluación de riesgos.
P.3	Tratamiento de riesgos	Toda organización debe establecer el tratamiento de los riesgos e implementar las acciones correctivas a tomar para mitigar los riesgos identificados y lograr reducirlos a riesgos aceptables para la organización.
P.4	Monitorear y revisar	Toda organización debe establecer un control de cambios, con el fin de definir acciones a seguir ante los cambios, así logrando que la gestión este continuamente actualizada. Con respecto al monitoreo se busca asegurar una constante revisión sobre la gestión de riesgo.
P.5	Comunicación y consulta	Toda organización debe establecer un plan de comunicación a nivel interno y externo, como medio de uso para la comunicación se sugieren cartas circulares, capacitaciones, campañas, etc.

---

*Nota:* Descripción de los 5 procesos. Fuente: Elaboración Propia.

### **3.3.2. Fase II – Declaración de Aplicabilidad de los controles del Anexo “A” - Norma ISO/IEC 27001:2013.**

En la fase II, se elaboró una matriz la cual incluye todos los controles mencionados en el Anexo “A” de la norma ISO/IEC 27001:2013, en el cual Colvias SAC selecciona y justifica la exclusión o su aplicabilidad de los controles del anexo A, los cuales tendrán las justificaciones siguientes para su justificación:



- a) Requerimientos Legales (RL).
- b) Compromisos Contractuales (CC).
- c) Requerimientos para la continuidad del negocio (CN).
- d) Resultado del Análisis de riesgo (RAR).

En el anexo 04 se detalla la declaración de aplicabilidad propuesta.

### **3.3.3. Fase III – Realizar una Línea Base de los dominios del Anexo “A” de la norma ISO / IEC 27001:2013.**

Para los sistemas de información la gestión de los riesgos es muy importante para gestionar adecuadamente las posibles amenazas ante la pérdida de información de la organización; además nos ayuda a detectar oportunidades de mejora que permitan mejorar la gestión de la información y de los activos relacionados a los procesos de TI de la empresa constructora.

En la Fase III, a través de los 14 dominios del Anexo “A” de la ISO/IEC 27001:2013 se realizará una evaluación inicial y con ayuda del modelo de Capacidad y Madurez (CMM - Capability Maturity Model), se identificará el nivel de madurez actual de la organización asociados a los procesos de la gestión de riesgos identificados en la Fase I; el modelo CMM fue desarrollado por la universidad Carnegie-Mellon para el SEI (Software Engineering Institute). Posteriormente se realizará la identificación de los activos los cuales serán valorizados en sus 3 dimensiones básicas (Confidencialidad, Integridad y Disponibilidad).

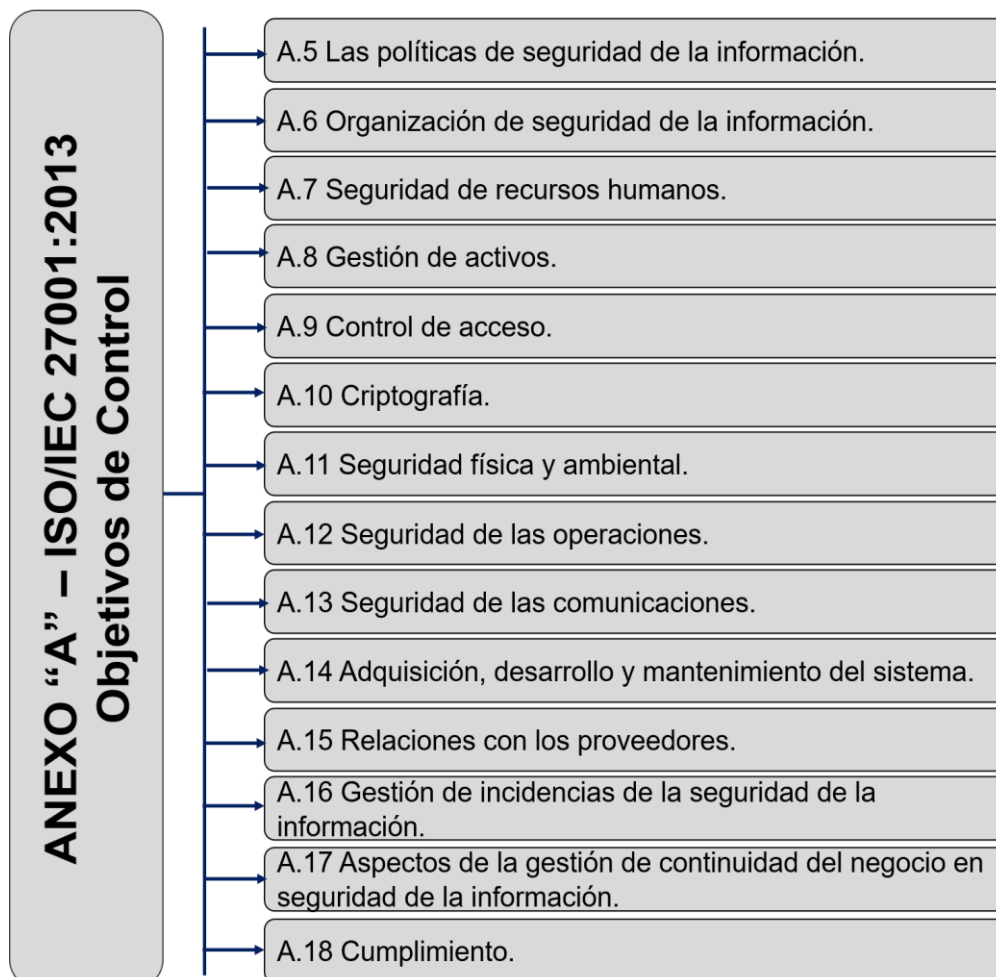


Figura 15. Dominios ISO/IEC 27001:2013. Fuente: ISO / IEC 27001:2013.

### 3.3.3.1. Nivel de Madurez (Modelo CMM).

En una organización para los responsables de la seguridad de la información es muy significativo definir los grados de madurez del funcionamiento de la organización, para el cual en este caso de estudio se realizará bajo el modelo de CMM, el cual manifiesta niveles de madurez en su diseño como en el contenido, siendo una plataforma evolutiva previamente definida para el logro constante de los procesos organizacionales. Con este modelo, podremos averiguar el nivel de implantación actual de los dominios de la ISO/IEC 27001:2013, podemos ver los niveles en la siguiente tabla:

Tabla 26.

*Modelo de Capacidad de Madurez – CMM.*

<b>Nivel-CMM</b>	<b>Efectividad %</b>	<b>Estado</b>	<b>Descripción</b>
<b>L0</b>	<b>0%</b>	<b>Inexistente</b>	Carencia completa de cualquier proceso conocido. El éxito de los procesos se basa en el esfuerzo del personal, en algunos casos no existente procedimientos o son localizados en otras áreas concretas.
<b>L1</b>	<b>10%</b>	<b>Inicial/Ad-hoc</b>	Existe una metodología de trabajo basada en la experiencia. Cada individuo tiene sus respectivas
<b>L2</b>	<b>50%</b>	<b>Repetible, pero intuitivo</b>	responsabilidades y solo él se encargará de darles el cumplimiento. Cada persona cuenta con conocimientos únicos, haciendo que se dependa de su grado de conocimiento. Los procesos de la organización están implantados,
<b>L3</b>	<b>90%</b>	<b>Proceso definido</b>	documentados y comunicados, haciendo que la organización entera participé en el proceso.

			Existen indicadores numéricos y estadísticos para el seguimiento de la evolución de los procesos.
<b>L4</b>	<b>95%</b>	<b>Gestionado y Medible</b>	Los trabajos son automatizados por la tecnología disponible, se tienen herramientas para mejorar la calidad y la eficiencia Existe una constante mejora en los procesos.
<b>L5</b>	<b>100%</b>	<b>Optimizado</b>	Teniendo como base los criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
<b>L6</b>	<b>N/A</b>		No aplica

*Nota:* Descripción de los grados de madurez para la metodología CMM  
Fuente: Modelo de Capacidad de Madurez – CMM.

### **3.3.3.2. Análisis del Modelo de Madurez de Capacidad (CMM) y GAP bajo los dominios de la norma ISO/IEC 27001:2013.**

En la tabla número 27 se evalúa el cumplimiento de los objetivos de control de los dominios definidos en el anexo “A” – ISO / IEC 27001:2013.

Tabla 27.

*Análisis del modelo de la capacidad y madurez (CMM) en los dominios del Anexo "A" dominios de la ISO/IEC 27001:2013.*

<b>Dominios ISO/IEC 27001:2013</b>		<b>Nivel - CMM</b>	<b>% Obtenido</b>
A.5	Las políticas de seguridad de información		10%
A.5.1	Dirección de gerencia para la seguridad de la información		
	A.5.1.1 Políticas para seguridad de la información	L1	10%
	A.5.1.2 Revisión de las políticas de seguridad de la Información	L1	10%
A.6	Organización de seguridad de la información		27%
A.6.1	Organización interna		
	A.6.1.1 Los roles y las responsabilidades de seguridad de información	L1	10%
	A.6.1.2 La segregación de funciones	L1	10%
	A.6.1.3 El contacto con las autoridades	L2	50%
	A.6.1.4 El contacto con los grupos de interés especial	L1	10%
	A.6.1.5 Seguridad de la información en gestión de proyectos	I1	10%
A.6.2	Dispositivos móviles y trabajo a distancia		
	A.6.2.1 Política dispositivo móvil	L2	50%
	A.6.2.2 Trabajo a distancia	L2	50%

A.7	Seguridad de recursos humanos		23%
A.7.1	Previo al empleo		
	A.7.1.1 Investigación de antecedentes	L2	50%
	A.7.1.2 Términos y condiciones de empleo	L2	50%
A.7.2	Durante el empleo		
	A.7.2.1 Responsabilidades de gestión	L1	10%
	A.7.2.2 Concientización, educación y entrenamiento en la seguridad de información	L1	10%
	A.7.2.3 Proceso disciplinario	L1	10%
A.7.3	Finalización o cambio de empleo		
	A.7.3.1 Terminación o cambio de responsabilidades laborales	L1	10%
A.8	Gestión de activos		29%
A.8.1	Responsabilidad para activos		
	A.8.1.1 Inventario de activos	L2	50%
	A.8.1.2 La propiedad de los activos	L2	50%
	A.8.1.3 Uso aceptable de los activos	L1	10%
	A.8.1.4 Retorno de los activos	L2	50%
A.8.2	Clasificación de la información		
	A.8.2.1 Clasificación de la información	L2	50%
	A.8.2.2 Etiquetado de información	L1	10%
	A.8.2.3 Manejo de activos	L2	50%

A.8.3	Manejo Medios		
A.8.3.1	Gestión de medios extraíbles	L1	10%
A.8.3.2	Eliminación de los medios de comunicación	L0	0%
A.8.3.3	Transferencia de medios Físicos	L1	10%
A.9	Control de acceso		41%
A.9.1	Requisitos del negocio del control de acceso		
A.9.1.1	Política de control de acceso	L1	10%
A.9.1.2	Acceso a redes y servicios de red	L2	50%
A.9.2	Gestión de acceso a usuarios		
A.9.2.1	Registro de usuarios y de la matrícula	L2	50%
A.9.2.2	Acceso a provisionamiento usuario	L2	50%
A.9.2.3	Gestión de derechos de acceso privilegiados	L2	50%
A.9.2.4	Gestión de la información de autenticación de secreto de usual	L2	50%
A.9.2.5	Revisión de los derechos de acceso de usuario	L1	10%
A.9.2.6	Retiro o ajuste de los derechos de acceso	L2	50%
A.9.3	Responsabilidades del usuario		
A.9.3.1	Uso de la información secreta de autenticación	L1	10%

A.9.4	Control de acceso de aplicación y sistema		
A.9.4.1	Restricción de acceso Información	L2	50%
A.9.4.2	Inicio de sesión de segura procedimientos	L2	50%
A.9.4.3	Sistema de gestión de contraseña	L2	50%
A.9.4.4	Uso de programas de utilidad privilegiados	L2	50%
A.9.4.5	Control de acceso a código fuente del programa	L6	N/A
A.10	Criptografía		0%
A.10.1	Controles criptográficos		
A.10.1.1	Política sobre el uso de controles criptográficos	L0	0%
A.10.1.2	Gestión de claves	L0	0%
A.11	Seguridad física y ambiental		29%
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	L0	0%
A.11.1.2	Controles de entrada físicas	L1	10%
A.11.1.3	Protección de oficinas, habitaciones e instalaciones	L1	10%
A.11.1.4	Protección contra amenazas externas y ambientales	L2	50%
A.11.1.5	Trabajar en zonas seguras	L1	10%
A.11.1.6	Áreas de entrega y carga	L6	N/A



A.11.2	Equipo		
	A.11.2.1 Localización del equipo y protección	L2	50%
	A.11.2.2 Utilidades Apoyo	L2	50%
	A.11.2.3 Seguridad Cableado	L2	50%
	A.11.2.4 El mantenimiento del equipo	L1	10%
	A.11.2.5 La eliminación de los activos	L2	50%
	A.11.2.6 Seguridad de equipo y activos fuera de las instalaciones	L1	10%
	A.11.2.7 Eliminación segura o la reutilización de los equipos	L2	50%
	A.11.2.8 Equipos de usuario desatendida	L2	50%
	A.11.2.9 Claro escritorio y política pantalla clara	L1	10%
A.12	Seguridad de las operaciones		34%
A.12.1	Responsabilidades y procesamientos operacionales		
	A.12.1.1 Procedimientos operativos Documentados	L1	10%
	A.12.1.2 Gestión del cambio	L2	50%
	A.12.1.3 Gestión de la capacidad	L2	50%
	A.12.1.4 Separación de desarrollo, pruebas y entornos operativos	L2	50%
A.12.2	Protección del malware o programas maliciosos		

	A.12.2.1 Controles contra el malware	L3	90%
A.12.3	Backup o código de seguridad		
	A.12.3.1 Información copia de seguridad	L3	90%
A.12.4	Registro y monitoreo		
	A.12.4.1 Registro Evento - Event logging	L0	0%
	A.12.4.2 Protección de información de registro	L1	10%
	A.12.4.3 Administrador y registros del operador	L1	10%
	A.12.4.4 Sincronización del reloj	L2	50%
A.12.5	Control de software operacional		
	A.12.5.1 Instalación de software en los sistemas operativos	L1	10%
A.12.6	Gestión vulnerabilidad Técnica		
	A.12.6.1 Gestión de vulnerabilidades técnicas	L0	0%
	A.12.6.2 Restricciones sobre la instalación de software	L2	50%
A.12.7	Consideraciones sobre la auditoría de sistemas de información		
	A.12.7.1 Información controles de auditoría de sistemas	L1	10%
A.13	Seguridad en las Comunicaciones		47%
A.13.1	Gestión de la seguridad Red		
	A.13.1.1 Controles red	L2	50%
	A.13.1.2 Seguridad de los servicios de red	L2	50%

	A.13.1.3 Segregación en redes	L3	90%
A.13.2	La transferencia de información		
	A.13.2.1 Las políticas y los procedimientos de transferencia de información	L0	0%
	A.13.2.2 Acuerdos en la transferencia de información	L0	0%
	A.13.2.3 La mensajería electrónica	L2	50%
	A.13.2.4 Confidencialidad o acuerdos de confidencialidad	L3	90%
A.14	Adquisición, desarrollo y mantenimiento del sistema.		23%
A.14.1	Requisitos de seguridad de los sistemas de información		
	A.14.1.1 Análisis de los requisitos de seguridad y la especificación	L1	10%
	A.14.1.2 Protección de los servicios de aplicación en las redes públicas	L2	50%
	A.14.1.3 Protección de las transacciones de servicios de aplicaciones	L0	0%
A.14.2	Seguridad en los procesos de desarrollo y de apoyo		
	A.14.2.1 Política de desarrollo seguro	L6	N/A
	A.14.2.2 Procedimientos de control de cambios del sistema	L2	50%

	A.143.2.3 Revisión técnica de aplicaciones después de la plataforma de funcionamiento	L2	50%
	A.14.2.4 Restricciones sobre los cambios en los paquetes de software	L6	N/A
	A.14.2.5 Sistema seguro principios de ingeniería	L2	50%
	A.14.2.6 Seguro entorno de desarrollo	L6	N/A
	A.14.2.7 Desarrollo Outsourced	L6	N/A
	A.14.2.8 Pruebas de seguridad Sistema	L0	0%
	A.14.2.9 Pruebas de aceptación del sistema	L0	0%
A.14.3	Datos de prueba		
	A.14.3.1 Protección de datos de prueba	L0	0%
A.15	Relaciones con los proveedores		24%
A.15.1	Seguridad de la información en relaciones con los proveedores		
	A.15.1.1 La política de seguridad de la información para relaciones con los proveedores	L0	0%
	A.15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores	L1	10%
	A.15.1.3 Tecnología de la comunicación Información y cadena de suministro	L1	10%

	A.15.2	Gestión de la prestación de servicios Proveedor		
		A.15.2.1 Monitoreo y revisión de los servicios de proveedores	L2	50%
		A.15.2.2 Gestión de cambios en los servicios de proveedores	L2	50%
A.16		Gestión de incidencias de la seguridad de la información		4%
		Gestión de incidentes de		
A.16.1		seguridad de la información y mejoras		
		A.16.1.1 Responsabilidades y procedimientos	L0	0%
		A.16.1.2 Presentación de informes de programas de seguridad de información	L1	10%
		A.16.1.3 Reporte de debilidades de seguridad de información	L0	0%
		A.16.1.4 Evaluación de y decisión sobre los eventos de seguridad de información	L1	10%
		A.16.1.5 Respuesta a incidentes de seguridad de información	L1	10%
		A.16.1.6 Aprendiendo de los incidentes de seguridad de la información	L0	0%
		A.16.1.7 Collection of evidence - El acopio de pruebas	L0	0%
A.17		Aspectos de la gestión de continuidad del negocio en seguridad de la información		0%

A.17.1	Continuidad en la seguridad de la información		
	A.17.1.1 Planificación		
	continuidad seguridad de la información	L0	0%
	A.17.1.2 Implementación de la información, su continuidad y seguridad	L0	0%
	A.17.1.3 Verificar, revisar y evaluar la información de seguridad de continuidad	L0	0%
A.17.2	Redundancias		
	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	L0	0%
A.18	Cumplimiento		38%
A.18.1	Cumplimiento con los requisitos legales y contractuales		
	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	L2	50%
	A.18.1.2 Los derechos de propiedad intelectual	L3	90%
	A.18.1.3 Protección de los registros	L2	50%
	A.18.1.4 Privacidad y protección de datos personales	L3	90%
	A.18.1.5 Reglamento de controles criptográficos	L0	0%
A.18.2	Información revisiones de seguridad		

A.18.2.1 Revisión independiente de seguridad de la información	L0	0%
A.18.2.2 Cumplimiento con las políticas y estándares de seguridad	L1	10%
A.18.2.3 Revisión de cumplimiento técnico	L1	10%

*Nota:* Resultados del análisis de la capacidad y madurez de los dominios del Anexo “A” de la norma ISO/IEC 27001:2013 en la organización.  
Fuente: Elaboración propia.

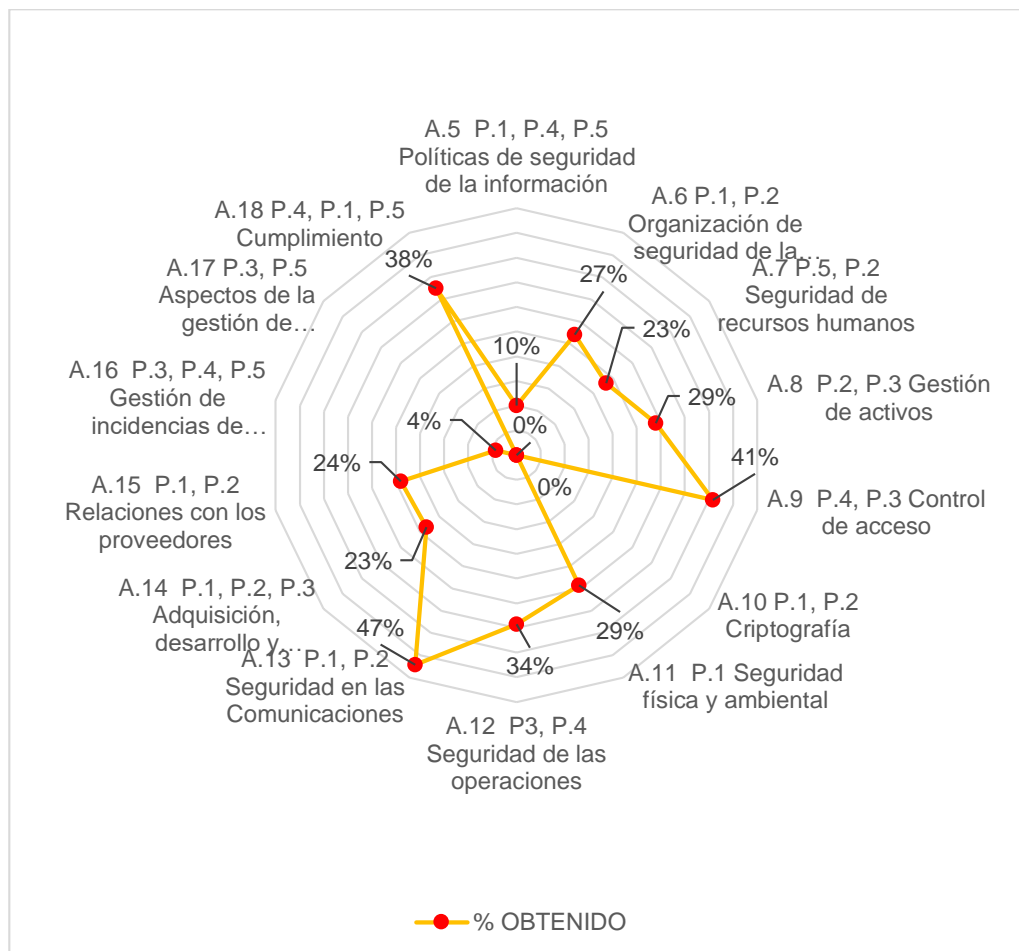
Tabla 28.

*Análisis del Modelo de la Madurez de la Capacidad (CMM).*

<b>Id. Dominio</b>	<b>Dominio</b>	<b>Nivel - CMM</b>	<b>% Obtenido</b>
A.5	Las políticas de seguridad de información	L1	10%
A.6	Organización de seguridad de la información	L1	27%
A.7	Seguridad de recursos humanos	L1	23%
A.8	Gestión de activos	L1	29%
A.9	Control de acceso	L1	41%
A.10	Criptografía	L0	0%
A.11	Seguridad física y ambiental	L1	29%
A.12	Seguridad de las operaciones	L1	34%
A.13	Seguridad en las Comunicaciones	L1	47%
A.14	Adquisición, desarrollo y mantenimiento del sistema.	L1	23%
A.15	Relaciones con los proveedores	L1	24%

A.16	Gestión de incidencias de la seguridad de la información	L1	4%
A.17	Aspectos de la gestión de continuidad del negocio en seguridad de la información	L0	0%
A.18	Cumplimiento	L1	38%

*Nota:* Resumen del análisis del Modelo de la Madurez de la Capacidad (CMM) de la ISO/IEC 27001:2013 en referencia a la tabla 27, asociados a los procesos identificados en la Fase I. Fuente: Elaboración propia.



*Figura 16.* Análisis GAP del Anexo “A” de la ISO/IEC 27001:2013 en la organización. Fuente: Elaboración propia.



En la figura 16 (análisis GAP), se puede concluir que el 76% de los controles estipulados en el Anexo "A" de la norma ISO / IEC 27001:2013, no se encuentran implementados en la organización y el 24% restantes no se encuentran gestionados o son defectuosos.

### 3.3.4. Fase IV – Desplegar una metodología adecuada para la evaluación y administración de riesgos.

Siguiendo con la continuidad de la investigación y de la metodología MagerIT, se procede con el inicio de la cuarta fase, donde se identificarán los activos y posteriormente a las amenazas que están expuestos, las cuales se clasifican en 04 grupos (MAGERIT Libro II, 2013), las cuales se mostraran en la tabla número 30.

Las fases de trabajo de la metodología MAGERIT se definen en el siguiente gráfico:

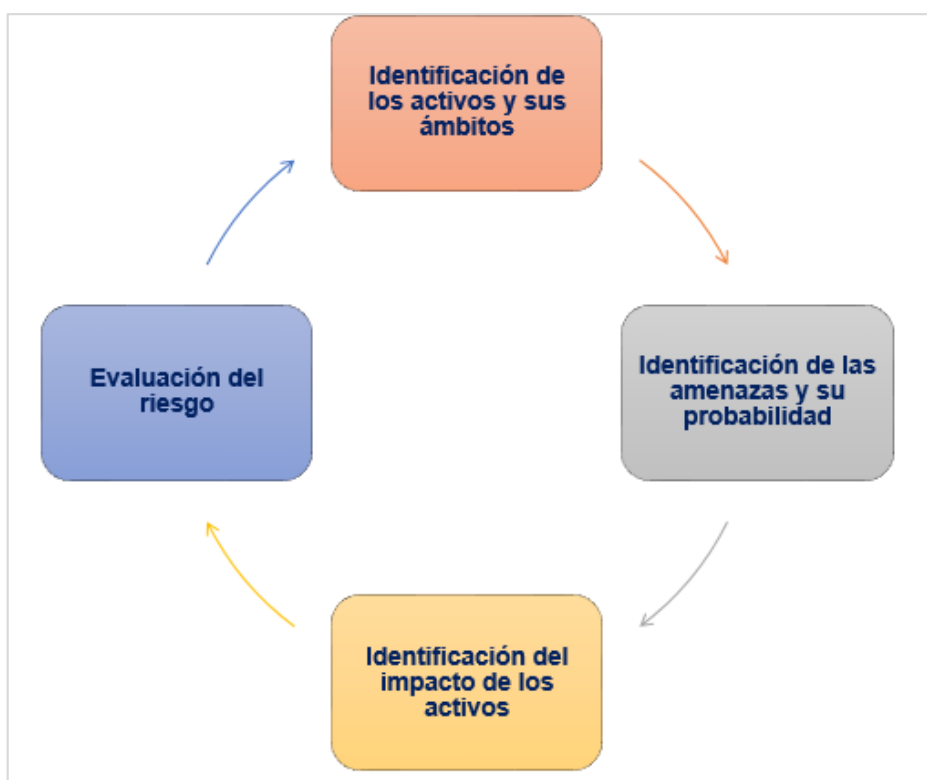


Figura 17. Esquema de trabajo de la metodología MAGERIT.  
Fuente: MAGERIT V3.

### 3.3.4.1. Inventario de Activos

Se comenzará por definir el ámbito de los activos de la organización según la definición que propone MagerIT en su Libro I, posteriormente se mencionaran los activos más relevantes seleccionados para el análisis de riesgos en la presente investigación, se encuentran resumidos en las siguientes tablas:

Tabla 29.

*Ámbitos de los activos.*

<b>Ítem Ámbito</b>	<b>Nombre del Ámbito</b>	<b>Descripción del Ámbito</b>
<b>[D]</b>	Datos	Son todos los datos que materializan la información
<b>[K]</b>	Claves Criptográficas	Sistemas que permiten la protección o autenticación de la información
<b>[S]</b>	Servicios de Terceros	Servicios auxiliares que son necesarios para poder constituir el sistema.
<b>[SW]</b>	Software	Programas informáticos que facilitan el manejo de datos
<b>[HD]</b>	Hardware	Equipos tecnológicos que permiten hospedar datos, programas y servicios
<b>[SINF]</b>	Soportes de Información	Son los dispositivos que permiten el almacenamiento de datos
<b>[EAUX]</b>	Equipos Auxiliares	Son los equipos que complementan el material informático
<b>[COM]</b>	Redes de Comunicación	Son las redes de comunicación que permiten intercambiar datos.

<b>[L]</b>	Infraestructura Física	Son instalaciones que permiten acoger los equipos tecnológicos (informáticos y comunicaciones)
<b>[P]</b>	Recurso Humano	Es el personal que opera y/o explota todos los elementos anteriormente mencionados.

*Nota:* Descripción de los ámbitos de los activos para la organización. Fuente: Elaboración propia.

Tabla 30.  
*Inventario de Activos.*

<b>Ámbito</b>	<b>Activo</b>
[D.1]	Registros de actividades de software
[D.2]	Información de Desarrollo Humano
[D.3]	Información de Administración y Finanzas
[D.4]	Información de Control de Proyectos Constructivos
[D.5]	Información de Control de Calidad
[D.6]	Información de Equipos
[D.7]	Información de Desarrollo Sostenible
[D.8]	Copias de Respaldo
[D.9]	Archivos de Datos de Configuración
[D.10]	Archivos de Contraseñas
[K.1]	Resguardo de la Información
[K.2]	Resguardo de las comunicaciones
[K.3]	Cifrado de soportes de la información
[S.1]	Canal de internet

- [S.2] Correo electrónico
- [S.3] Acceso remoto a usuario local
- [SW.1] Navegadores WEB
- [SW.2] Sistemas Operativos
- [SW.3] Aplicativos de ofimática
- [SW.4] Clientes de correo electrónico
- [SW.5] Gestor de máquinas virtuales
- [SW.6] Sistema de BD
- [SW.7] Sistema de gestión de backups
- [SW.7] Sistema de referenciación geográfica
- [SW.8] Sistema de pagos asociados
- [SW.9] Aplicativo para el diseño de arquitectura, mecánico y la cartografía
- [SW.10] Antivirus
- [SW.11] Desarrollo de Software a medida subcontratado
- [HD.1] Servidor
- [HD.2] Computador de escritorio
- [HD.3] Computador portátil (laptop)
- [HD.4] Móviles / Radios de comunicación
- [HD.5] DRONES
- [HD.6] Periféricos (Impresoras, escáneres, proyectores, etc.)
- [HD.7] Servidores de respaldo (backup)
- [HD.8] Router
- [HD.9] Switch

- [HD.10] Módems
- [HD.11] Puntos de acceso inalámbrico
- [HD.12] Antenas de comunicación
- [SINF.1] Discos virtuales
- [SINF.2] Memorias USB
- [SINF.3] Discos duros externos
- [EAUX.1] Equipos de alimentación eléctrica
- [EAUX.2] UPS
- [EAUX.3] Equipo de aire acondicionado
- [EAUX.4] Cableado eléctrico
- [EAUX.5] Cableado de comunicaciones (UTP)
- [COM.1] Comunicaciones de Radio
- [COM.2] Redes inalámbricas
- [COM.3] Telefonía móvil
- [COM.4] Redes LAN
- [COM.5] Internet
  - [L.1] Oficinas - Moquegua
  - [L.2] Oficinas - Campamento Minero
  - [L.3] Container
  - [L.4] Equipos móviles terrestres (camionetas, volquetes, equipos de línea amarilla)
  - [L.5] Plantas operativas (concreto, asfalto, etc.)
- [P.1] Usuarios Externos
- [P.2] Usuarios internos
- [P.4] Proveedores

[P.5] Sub Contratistas

[P.6] Clientes

[P.7] Administradores de los Sistemas de información

---

*Nota:* Descripción de los activos. Fuente: Elaboración propia

### 3.3.4.2. Valoración de los activos.

Una vez identificado los activos de la organización, se procederá con su valoración de cada uno de los activos de acuerdo con el daño que pueda causar en ellos, mediante la escala que propone la metodología MagerIT en su libro III, asimismo se complementara con una estimación cualitativa y cuantitativa definida en términos económicos para la organización.

Tabla 31:

*Criterio de valoración de los activos.*

<b>Nivel</b>	<b>Costo (daño al activo y/o proceso)</b>	<b>Definición</b>
<b>Muy alta - (E)</b>	US\$ 100,000.00 ≤ Pérdida	Pérdidas económicas altas del activo de alto valor; o Pérdidas que exceden los \$100,000.00 US\$; o Impacto mayor no planificado en el presupuesto y programa del proyecto.
<b>Alta (D)</b>	US\$ 10,001 ≤ Pérdida < US\$ 100,000.00	Pérdida o Daños del activo que no pueden reemplazarse con facilidad; o Pérdidas que exceden los \$10,001.00 - \$ 100,000.00; o Impacto que afecta considerablemente al proyecto.
<b>Media (C)</b>	US\$ 5,001.00 ≤ Pérdida < US\$ 10,000.00	Pérdida o Daños del activo que pueden reemplazarse con facilidad; o Pérdidas que exceden los \$5,001.00 y US\$

		10,000.00; o Impacto leve no planificado en el presupuesto del proyecto.
	US\$ 1,000 <=	
<b>Baja (B)</b>	Pérdida < US\$ 5,000	Daños del activo que pueden reemplazarse con facilidad; o Pérdidas que exceden los 1,000 y menor a US\$ 5,000; Impacto del activo que afecta imperceptiblemente al presupuesto del proyecto.
<b>Muy Baja (A)</b>	Pérdidas < US\$ 1,000.00	Daños del activo que pueden reemplazarse con facilidad; o Pérdidas menor a \$ 1,000.00; Impacto del activo que apenas afecta al presupuesto del proyecto.

---

*Nota:* Valoración del daño de los activos propuesto en el Libro III de la metodología MAGERIT. Fuente: Elaboración propia.

### **3.3.4.3. Dimensiones de seguridad.**

Para la valoración de los activos se tiene que realizar de forma autónoma para cada activo en sus tres dimensiones básicas de seguridad (confidencialidad (C), integridad (I) y disponibilidad (D)), asimismo se identifica el impacto o daño que se podría causar a la organización por algún incidente de seguridad asociado a cada una de las dimensiones de seguridad citadas.

(MAGERIT V3, 2012), las siguientes preguntas nos ayudara a establecer los niveles de impacto asociados con cada activo en cada dimensión de seguridad:

**Confidencialidad (C):** ¿Qué daño originaría a la organización si el activo lo conociera quien no debe?

**Integridad (I):** ¿Qué daño produciría a la organización si el activo estuviese dañado, corrupto o alterado sin autorización?

**Disponibilidad (D):** ¿Qué perjuicio produciría a la organización el no tener el activo o no poder utilizarlo cuando se requiera?

En tabla número 32 se procede a realizar la valoración cualitativa de los activos en función a un valor numérico y escala del daño:

Tabla 32.  
*Escala de daños de los activos.*

<b>Valor Numérico</b>	<b>Valor Descriptivo</b>	<b>Criterio</b>
<b>10</b>	Muy Alto	Daño muy grave
<b>7-9</b>	Alto	Daño grave
<b>4-6</b>	Medio	Daño importante
<b>1-3</b>	Bajo	Daño menor
<b>0</b>	Despreciable	Daño Irrelevante

*Nota:* Valoración cualitativa de los activos según su escala de daño.

Fuente: Elaboración propia.

En la tabla número 33 se define la criticidad de los activos en sus 03 dimensiones básicas de seguridad Confidencialidad (C), Integridad (I) y Disponibilidad (D):

Tabla 33.  
*Valoración de los activos según su dimensión (Confidencialidad, Integridad y Disponibilidad)*

<b>Ámbito</b>	<b>Activo</b>	<b>C</b>	<b>I</b>	<b>D</b>	<b>Valor</b>
[D.1]	Registros de actividades de software	3	4	3	MEDIO



[D.2]	Información de Desarrollo Humano	7	7	6	ALTO
[D.3]	Información de Administración y Finanzas	8	8	7	ALTO
[D.4]	Información de Control de Proyectos Constructivos	10	10	8	MUY ALTO
[D.5]	Información de Control de Calidad	8	8	7	ALTO
[D.6]	Información de Equipos	7	7	6	ALTO
[D.7]	Información de Desarrollo Sostenible	8	8	8	ALTO
[D.8]	Copias de Respaldo	10	10	10	MUY ALTO
[D.9]	Archivos de Datos de Configuración	6	6	6	MEDIO
[D.10]	Archivos de Contraseñas	8	6	8	ALTO
[K.1]	Resguardo de la Información	8	8	8	ALTO
[K.2]	Resguardo de las comunicaciones	8	8	6	ALTO
[K.3]	Cifrado de soportes de la información	10	10	8	MUY ALTO
[S.1]	Canal de internet	10	10	9	MUY ALTO
[S.2]	Correo electrónico	10	10	10	MUY ALTO
[S.3]	Acceso remoto a usuario local	8	8	8	ALTO
[SW.1]	Navegadores WEB	8	8	7	ALTO
[SW.2]	Sistemas Operativos	8	9	8	ALTO
[SW.3]	Aplicativos de ofimática	6	6	4	MEDIO

[SW.4]	Clientes de correo electrónico	10	8	8	MUY ALTO
[SW.5]	Gestor de máquinas virtuales	8	8	6	ALTO
[SW.6]	Sistema de BD	10	10	8	MUY ALTO
[SW.7]	Sistema de gestión de backups	9	9	9	ALTO
[SW.7]	Sistema de referenciación geográfica	5	5	5	MEDIO
[SW.8]	Sistema de pagos asociados	9	9	9	ALTO
[SW.9]	Aplicativo para el diseño de arquitectura, mecánico y la cartografía	3	3	3	BAJO
[SW.10]	Antivirus	9	9	9	ALTO
[SW.11]	Desarrollo de Software a medida subcontratado	9	9	9	ALTO
[HD.1]	Servidor	10	10	10	MUY ALTO
[HD.2]	Computador de escritorio	6	6	6	MEDIO
[HD.3]	Computador portátil (laptop)	6	6	6	MEDIO
[HD.4]	Móviles / Radios de comunicación	6	6	6	MEDIO
[HD.5]	DRONES	8	8	8	ALTO
[HD.6]	Periféricos (Impresoras, escáneres, proyectores, etc.)	3	3	3	BAJO
[HD.7]	Servidores de respaldo (backup)	10	10	9	MUY ALTO
[HD.8]	Router	8	8	8	ALTO
[HD.9]	Switch	8	8	8	ALTO
[HD.10]	Módems	6	6	6	MEDIO

[HD.11]	Puntos de acceso inalámbrico	6	6	6	MEDIO
[HD.12]	Antenas de comunicación	6	6	6	MEDIO
[SINF.1]	Discos virtuales	6	6	6	MEDIO
[SINF.2]	Memorias USB	3	3	3	BAJO
[SINF.3]	Discos duros externos	6	5	5	MEDIO
[EAUX.1]	Equipos de alimentación eléctrica	3	1	3	BAJO
[EAUX.2]	UPS	3	1	3	BAJO
[EAUX.3]	Equipo de aire acondicionado	3	1	3	BAJO
[EAUX.4]	Cableado eléctrico	3	1	3	BAJO
[EAUX.5]	Cableado de comunicaciones (UTP)	3	1	3	BAJO
[COM.1]	Comunicaciones de Radio	4	4	4	MEDIO
[COM.2]	Redes inalámbricas	7	7	7	ALTO
[COM.3]	Telefonía móvil	7	7	7	ALTO
[COM.4]	Redes LAN	7	7	7	ALTO
[COM.5]	Internet	8	8	8	ALTO
[L.1]	Oficinas - Moquegua	4	4	4	MEDIO
[L.2]	Oficinas - Campamento Minero	4	4	4	MEDIO
[L.3]	Container	4	4	4	MEDIO
[L.4]	Equipos móviles terrestres (camionetas, volquetes, equipos de línea amarilla)	4	4	4	MEDIO
[L.5]	Plantas operativas (concreto, asfalto, etc.)	7	7	7	ALTO
[P.1]	Usuarios Externos	5	5	5	MEDIO

[P.2]	Usuarios internos	8	8	8	ALTO
[P.4]	Proveedores	8	8	8	ALTO
[P.5]	Sub Contratistas	5	5	5	MEDIO
[P.6]	Clientes	8	8	8	ALTO
[P.7]	Administradores de los Sistemas de información	8	8	8	ALTO

*Nota:* Se define la criticidad de los activos en sus tres dimensiones básicas. Fuente: Elaboración propia.

Tabla 34.  
*Tipos de amenazas que afectan a los activos en la organización.*

<b>Grupo</b>	<b>Amenaza</b>
	N.1 Incendio (Fuego)
Desastres Naturales <b>[N]</b>	N.2 Daños ocasionados por el agua
	N.3 Climas adversos
	N.4 Eventos sísmicos
De Origen Industrial <b>[I]</b>	I.1 Incendio (Fuego)
	I.2 Daños ocasionados por el agua
	I.3 Sobretensiones eléctricas
	I.4 Accidentes de tránsito
	I.5 Contaminación mecánica (Polución, vibraciones)
	I.6 Fallo de origen del Hardware o Software
	I.7 Pérdida del suministro eléctrico
	I.8 Deficiencias en la climatización de las instalaciones

	I.9 Fallo de los medios de comunicaciones
	I.10 Soporte de almacenamiento de la información (Hardware) degradado
	E.1 Errores no intencionado por parte de los usuarios
	E.2 Errores no intencionados por parte del administrador
	E.3 Inadecuado registro de actividades (Log)
	E.4 Error en los datos de configuración
	E.5 Deficiencias de la organización
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)
	E.7 Error de secuencia
Errores y Fallos No Intencionados	E.8 Perturbación no intencionado de la información
<b>[E]</b>	E.9 Eliminación no intencional de la información
	E.10 Fugas de información
	E.11 SW Vulnerables
	E.12 Errores de actualización de las aplicaciones (software)
	E.13 Errores de mantenimiento y/o actualizaciones del hardware
	E.14 Extravió de equipos
	E.15 Personal no disponible
Ataques Intencionados	A.1 Manipulación de registro de actividades (Log)
<b>[A]</b>	A.2 Manipulación de la configuración
	A.3 Usurpación de identidad de los usuarios

- A.4 Abuso de acceso del nivel de privilegios
- A.5 Uso de los recursos de los activos para fines no previstos
- A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)
- A.7 Alteración de datos
- A.8 Accesos no autorizados
- A.9 Monitorización del tráfico
- A.10 Denegación de acciones
- A.11 Interceptación de la información (Escucha pasiva)
- A.12 Alteración deliberada de la información
- A.13 Eliminación de la información
- A.14 Divulgación de la información
- A.15 Alteración de software (programas)
- A.16 Sabotaje del hardware
- A.17 Robo
- A.18 Ataque destructivo del hardware o soportes
- A.19 Ocupación enemiga
- A.20 Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc.)
- A.21 Extorsión
- A.22 Ingeniería Social

---

*Nota:* Tipos de amenazas que pueden afectar a los activos, según metodología MAGERIT V3. Fuente: Elaboración Propia.

Después de realizada las coordinaciones con los dueños de los procesos y el encargado de tecnología de información de la organización se identificaron las amenazas que afectan a la organización (Tabla 36); posteriormente se determina el grado de probabilidad de materialización de la amenaza, se utilizó la siguiente escala de tiempo cimentada en la cantidad de incidencias en un periodo de un año, se muestra en la tabla número 35:

Tabla 35.  
*Escala de valoración de frecuencia (Vulnerabilidad – Probabilidad de Ocurrencia).*

<b>Valor</b>	<b>Rango</b>	<b>Condición</b>
<b>1</b>	Muy Alta (MA)	Su ocurrencia es diaria
<b>0.033</b>	Alta (A)	Su ocurrencia es una vez al mes
<b>0.011</b>	Media (M)	Su ocurrencia es una vez cada trimestre
<b>0.005</b>	Baja (B)	Su ocurrencia es cada semestre
<b>0.003</b>	Muy Baja (MB)	Su ocurrencia es una vez al año

*Nota:* Valoración de la frecuencia según su escala de ocurrencia en el tiempo. Fuente: Elaboración Propia.

Tabla 36.  
*Probabilidad de ocurrencia de la amenaza identificada.*

<b>Grupo</b>	<b>Amenaza</b>	<b>Nivel de Probabilidad (NP)</b>
Desastres Naturales [N]	N.1 Incendio (Fuego)	0.003
	N.2 Daños ocasionados por el agua	0.003

	N.3 Climas adversos	0.011
	N.4 Eventos sísmicos	0.003
De Origen Industrial <b>[I]</b>	I.1 Incendio (Fuego)	0.003
	I.2 Daños ocasionados por el agua	0.003
	I.3 Sobretensiones eléctricas	0.005
	I.4 Accidentes de transito	0.005
	I.5 Contaminación mecánica (Polución, vibraciones)	0.011
	I.6 Fallo de origen del Hardware o Software	0.005
	I.7 Pérdida del suministro eléctrico	0.033
	I.8 Deficiencias en la climatización de las instalaciones	0.005
	I.9 Fallo de los medios de comunicaciones	0.033
	I.10 Soporte de almacenamiento de la información (Hardware) degradado	0.003
Errores y Fallos No Intencionados <b>[E]</b>	E.1 Errores no intencionado por parte de los usuarios	0.033
	E.2 Errores no intencionados por parte del administrador	0.003
	E.3 Inadecuado registro de actividades (Log)	0.005
	E.4 Error en los datos de configuración	0.005



	E.5 Deficiencias de la organización	0.011
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033
	E.7 Error de secuencia	0.005
	E.8 Perturbación no intencionado de la información	0.011
	E.9 Eliminación no intencional de la información	0.033
	E.10 Fugas de información	1
	E.11 SW Vulnerables	0.011
	E.12 Errores de actualización de las aplicaciones (software)	0.011
	E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011
	E.14 Extravió de equipos	0.033
	E.15 Personal no disponible	1
Ataques Intencionados <b>[A]</b>	A.1 Manipulación de registro de actividades (Log)	0.005
	A.2 Manipulación de la configuración	0.033
	A.3 Usurpación de identidad de los usuarios	0.011
	A.4 Abuso de acceso del nivel de privilegios	1

A.5 Uso de los recursos de los activos para fines no previstos	1
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1
A.7 Alteración de datos	0.011
A.8 Accesos no autorizados	0.033
A.9 Monitorización del trafico	0.005
A.10 Denegación de acciones	1
A.11 Interceptación de la información (Escucha pasiva)	1
A.12 Alteración deliberada de la información	1
A.13 Eliminación de la información	1
A.14 Divulgación de la información	1
A.15 Alteración de software (programas)	0.011
A.16 Sabotaje del hardware	0.005
A.17 Robo	0.033
A.18 Ataque destructivo del hardware o soportes	0.011
A.19 Ocupación enemiga	0.005
A.20 Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc.)	0.033

A.21 Extorsión	0.005
A.22 Ingeniería Social	0.033

*Nota:* Valoración del nivel de probabilidad de ocurrencia de la amenaza identificada en la organización. Fuente: Elaboración Propia.

Una vez se haya obtenido las amenazas identificadas, se procede a señalar la probabilidad de ocurrencia, para ello fue necesario realizar una evaluación lógica y física dentro de la organización. Por lo tanto, se dialogó con los dueños de los procesos y responsable de TI. En la siguiente tabla se describe los activos y sus amenazas consideradas y aprobadas por la organización:

Tabla 37.

*Probabilidad de la amenaza identificada por activo en sus tres dimensiones.*

Ámbito	Activo	Amenaza	Frecuencia	C	I	D
[D.1]	Registros de actividades de software		1	60 %	60 %	70 %
		E.1 Errores no intencionado por parte de los usuarios	0.033	60 %	60 %	60 %
		E.2 Errores no intencionados por parte del administrador	0.003	60 %	60 %	60 %
		E.3 Inadecuado registro de actividades (Log)	0.005	-	50 %	-

E.4 Error en los datos de configuración	0.005	-	50 %	-
E.8 Perturbación no intencionado de la información	0.011	-	60 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	70 %
E.10 Fugas de información	1	60 %	-	-
A.1 Manipulación de registro de actividades (Log)	0.005	-	60 %	-
A.2 Manipulación de la configuración	0.033	50 %	50 %	50 %
A.3 Usurpación de identidad de los usuarios	0.011	50 %	50 %	50 %
A.4 Abuso de acceso del nivel de privilegios	1	50 %	50 %	50 %
A.8 Accesos no autorizados	0.033	60 %	60 %	-
A.12 Alteración deliberada de la información	1	-	60 %	-
A.13 Eliminación de la información	1	-	-	60 %
A.14 Divulgación de la información	1	60 %	-	-

---

	Información		40	40	50
[D.2]	de Desarrollo Humano	1	%	%	%
	E.1 Errores no intencionado por parte de los usuarios	0.033	40%	40%	40%
	E.2 Errores no intencionados por parte del administrador	0.003	40%	40%	40%
	E.3 Inadecuado registro de actividades (Log)	0.005	-	20%	-
	E.4 Error en los datos de configuración	0.005	-	20%	-
	E.8 Perturbación no intencionado de la información	0.011	-	40%	-
	E.9 Eliminación no intencional de la información	0.033	-	-	50%
	E.10 Fugas de información	1	20%	-	-
	A.1 Manipulación de registro de actividades (Log)	0.005	-	20%	-
	A.2 Manipulación de la configuración	0.033	20%	20%	20%
	A.3 Usurpación de identidad de los usuarios	0.011	30%	30%	30%

	A.4 Abuso de acceso del nivel de privilegios	1	40 %	40 %	40 %
	A.8 Accesos no autorizados	0.033	30 %	30 %	-
	A.12 Alteración deliberada de la información	1	-	40 %	-
	A.13 Eliminación de la información	1	-	-	50 %
	A.14 Divulgación de la información	1	20 %	-	-
[D.3]	Información de Administración y Finanzas	1	60 %	70 %	70 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	50 %	50 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	40 %	40 %	20 %
	E.3 Inadecuado registro de actividades (Log)	0.005	-	40 %	-
	E.4 Error en los datos de configuración	0.005	-	40 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	50 %	-

	E.9 Eliminación no intencional de la información	0.033	-	-	70 %
	E.10 Fugas de información	1	60 %	-	-
	A.1 Manipulación de registro de actividades (Log)	0.005	-	40 %	-
	A.2 Manipulación de la configuración	0.033	60 %	60 %	60 %
	A.3 Usurpación de identidad de los usuarios	0.011	60 %	60 %	60 %
	A.4 Abuso de acceso del nivel de privilegios	1	50 %	50 %	50 %
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	70 %	-
	A.13 Eliminación de la información	1	-	-	70 %
	A.14 Divulgación de la información	1	40 %	-	-
	<hr/>				
	Información de Control de Proyectos Constructivos				
[D.4]		1	60 %	80 %	70 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	50 %	70 %	40 %

E.2 Errores no intencionados por parte del administrador	0.003	50 %	50 %	40 %
E.3 Inadecuado registro de actividades (Log)	0.005	-	40 %	-
E.4 Error en los datos de configuración	0.005	-	40 %	-
E.8 Perturbación no intencionado de la información	0.011	-	80 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	70 %
E.10 Fugas de información	1	60 %	-	-
A.1 Manipulación de registro de actividades (Log)	0.005	-	50 %	-
A.2 Manipulación de la configuración	0.033	40 %	80 %	50 %
A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	30 %
A.4 Abuso de acceso del nivel de privilegios	1	60 %	60 %	-
A.8 Accesos no autorizados	0.033	60 %	60 %	-



	A.12 Alteración deliberada de la información	1	-	60 %	-
	A.13 Eliminación de la información	1	-	-	60 %
	A.14 Divulgación de la información	1	60 %	-	-
	Información de Control de Calidad	1	70 %	90 %	70 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	70 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	50 %	50 %	50 %
	E.3 Inadecuado registro de actividades (Log)	0.005	-	30 %	-
	E.4 Error en los datos de configuración	0.005	-	60 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	90 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	60 %
	E.10 Fugas de información	1	50 %	-	-

	A.1 Manipulación de registro de actividades (Log)	0.005	-	50 %	-
	A.2 Manipulación de la configuración	0.033	70 %	80 %	70 %
	A.3 Usurpación de identidad de los usuarios	0.011	50 %	50 %	40 %
	A.4 Abuso de acceso del nivel de privilegios	1	60 %	60 %	-
	A.8 Accesos no autorizados	0.033	60 %	60 %	-
	A.12 Alteración deliberada de la información	1	-	60 %	-
	A.13 Eliminación de la información	1	-	-	60 %
	A.14 Divulgación de la información	1	60 %	-	-
[D.6]	Información de Equipos	1	50 %	60 %	60 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	50 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	40 %	40 %	40 %
	E.3 Inadecuado registro de actividades (Log)	0.005	-	40 %	-

E.4 Error en los datos de configuración	0.005	-	40 %	-
E.8 Perturbación no intencionado de la información	0.011	-	50 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	60 %
E.10 Fugas de información	1	50 %	-	-
A.1 Manipulación de registro de actividades (Log)	0.005	-	50 %	-
A.2 Manipulación de la configuración	0.033	50 %	50 %	40 %
A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	30 %
A.4 Abuso de acceso del nivel de privilegios	1	50 %	50 %	-
A.8 Accesos no autorizados	0.033	50 %	50 %	-
A.12 Alteración deliberada de la información	1	-	60 %	-
A.13 Eliminación de la información	1	-	-	60 %
A.14 Divulgación de la información	1	20 %	-	-

---

	Información		60	60	80
[D.7]	de Desarrollo Sostenible	1	%	%	%
	E.1 Errores no intencionado por parte de los usuarios	0.033	50%	60%	50%
	E.2 Errores no intencionados por parte del administrador	0.003	40%	40%	40%
	E.3 Inadecuado registro de actividades (Log)	0.005	-	30%	-
	E.4 Error en los datos de configuración	0.005	-	40%	-
	E.8 Perturbación no intencionado de la información	0.011	-	50%	-
	E.9 Eliminación no intencional de la información	0.033	-	-	50%
	E.10 Fugas de información	1	50%	-	-
	A.1 Manipulación de registro de actividades (Log)	0.005	-	40%	-
	A.2 Manipulación de la configuración	0.033	50%	50%	50%
	A.3 Usurpación de identidad de los usuarios	0.011	40%	40%	40%

	A.4 Abuso de acceso del nivel de privilegios	1	50 %	50 %	-
	A.8 Accesos no autorizados	0.033	50 %	50 %	-
	A.12 Alteración deliberada de la información	1	-	60 %	-
	A.13 Eliminación de la información	1	-	-	80 %
	A.14 Divulgación de la información	1	60 %	-	-
[D.8]	Copias de Respaldo	1	60 %	90 %	90 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	60 %
	E.2 Errores no intencionados por parte del administrador	0.003	60 %	60 %	60 %
	E.3 Inadecuado registro de actividades (Log)	0.005	-	40 %	-
	E.4 Error en los datos de configuración	0.005	-	50 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	90 %	-

	E.9 Eliminación no intencional de la información	0.033	-	-	90%
	E.10 Fugas de información	1	60%	-	-
	A.1 Manipulación de registro de actividades (Log)	0.005	-	50%	-
	A.2 Manipulación de la configuración	0.033	50%	70%	60%
	A.3 Usurpación de identidad de los usuarios	0.011	50%	50%	50%
	A.4 Abuso de acceso del nivel de privilegios	1	50%	50%	-
	A.8 Accesos no autorizados	0.033	50%	50%	-
	A.12 Alteración deliberada de la información	1	-	90%	-
	A.13 Eliminación de la información	1	-	-	90%
	A.14 Divulgación de la información	1	60%	-	-
[D.9]	Archivos de Datos de Configuración	1	30%	40%	40%
	E.1 Errores no intencionado por parte de los usuarios	0.033	30%	40%	30%

E.2 Errores no intencionados por parte del administrador	0.003	30 %	40 %	30 %
E.3 Inadecuado registro de actividades (Log)	0.005	-	40 %	-
E.4 Error en los datos de configuración	0.005	-	40 %	-
E.8 Perturbación no intencionado de la información	0.011	-	40 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	40 %
E.10 Fugas de información	1	30 %	-	-
A.1 Manipulación de registro de actividades (Log)	0.005	-	40 %	-
A.2 Manipulación de la configuración	0.033	30 %	40 %	30 %
A.3 Usurpación de identidad de los usuarios	0.011	20 %	40 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	30 %	20 %	-
A.8 Accesos no autorizados	0.033	20 %	30 %	-

	A.12 Alteración deliberada de la información	1	-	40 %	-
	A.13 Eliminación de la información	1	-	-	30 %
	A.14 Divulgación de la información	1	10 %	-	-
[D.10]	Archivos de Contraseñas	1	40 %	30 %	40 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	30 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	30 %	20 %	30 %
	E.3 Inadecuado registro de actividades (Log)	0.005	-	30 %	-
	E.4 Error en los datos de configuración	0.005	-	30 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	20 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	20 %
	E.10 Fugas de información	1	40 %	-	-



	A.1 Manipulación de registro de actividades (Log)	0.005	-	20 %	-
	A.2 Manipulación de la configuración	0.033	20 %	20 %	20 %
	A.3 Usurpación de identidad de los usuarios	0.011	30 %	30 %	30 %
	A.4 Abuso de acceso del nivel de privilegios	1	20 %	20 %	-
	A.8 Accesos no autorizados	0.033	30 %	20 %	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.13 Eliminación de la información	1	-	-	20 %
	A.14 Divulgación de la información	1	20 %	-	-
[K.1]	Resguardo de la Información	1	50 %	50 %	50 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	40 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	30 %	30 %	20 %
	E.8 Perturbación no intencionado de la información	0.011	-	40 %	-

	E.9 Eliminación no intencional de la información	0.033	-	-	40 %
	E.10 Fugas de información	1	50 %	-	-
	A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	30 %
	A.4 Abuso de acceso del nivel de privilegios	1	50 %	40 %	30 %
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	50 %	-
	A.13 Eliminación de la información	1	-	-	50 %
	A.14 Divulgación de la información	1	40 %	-	-
[K.2]	Resguardo de las comunicaciones	1	40 %	40 %	40 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	20 %
	E.2 Errores no intencionados por parte del administrador	0.003	30 %	30 %	20 %

	E.8 Perturbación no intencionado de la información	0.011	-	40 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	40 %
	E.10 Fugas de información	1	40 %	-	-
	A.3 Usurpación de identidad de los usuarios	0.011	40 %	30 %	30 %
	A.4 Abuso de acceso del nivel de privilegios	1	30 %	40 %	30 %
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	40 %	-
	A.13 Eliminación de la información	1	-	-	40 %
	A.14 Divulgación de la información	1	40 %	-	-
[K.3]	Cifrado de soportes de la información	1	50 %	50 %	60 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	40 %	30 %
	E.2 Errores no intencionados por	0.003	50 %	50 %	30 %

	parte del administrador				
	E.8 Perturbación no intencionado de la información	0.011	-	40 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	50 %
	E.10 Fugas de información	1	40 %	-	-
	A.3 Usurpación de identidad de los usuarios	0.011	40 %	30 %	40 %
	A.4 Abuso de acceso del nivel de privilegios	1	30 %	40 %	30 %
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	50 %	-
	A.13 Eliminación de la información	1	-	-	60 %
	A.14 Divulgación de la información	1	50 %	-	-
[S.1]	Canal de internet	1	50 %	60 %	70 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	40 %	40 %
	E.2 Errores no intencionados por	0.003	30 %	30 %	30 %

parte del administrador				
E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	40 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	60 %
E.10 Fugas de información	1	30 %	-	-
A.3 Usurpación de identidad de los usuarios	0.011	30 %	40 %	30 %
A.4 Abuso de acceso del nivel de privilegios	1	30 %	40 %	30 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.7 Alteración de datos	0.011	-	30 %	-
A.8 Accesos no autorizados	0.033	50 %	50 %	-
A.10 Denegación de acciones	1	-	20 %	-
A.12 Alteración deliberada de la información	1	-	60 %	-
A.13 Eliminación de la información	1	-	-	70 %

		A.14 Divulgación de la información	1	40 %	-	-
[S.2]	Correo electrónico		1	30 %	30 %	40 %
		E.1 Errores no intencionado por parte de los usuarios	0.033	30 %	30 %	30 %
		E.2 Errores no intencionados por parte del administrador	0.003	20 %	30 %	20 %
		E.7 Error de secuencia	0.005	-	30 %	-
		E.8 Perturbación no intencionado de la información	0.011	-	30 %	-
		E.9 Eliminación no intencional de la información	0.033	-	-	40 %
		E.10 Fugas de información	1	30 %	-	-
		A.3 Usurpación de identidad de los usuarios	0.011	30 %	30 %	20 %
		A.4 Abuso de acceso del nivel de privilegios	1	30 %	30 %	20 %
		A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %

	A.7 Alteración de datos	0.011	-	20 %	-
	A.8 Accesos no autorizados	0.033	20 %	20 %	-
	A.10 Denegación de acciones	1	-	10 %	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.13 Eliminación de la información	1	-	-	40 %
	A.14 Divulgación de la información	1	30 %	-	-
[S.3]	Acceso remoto a usuario local	1	20 %	30 %	30 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	30 %	30 %
	E.2 Errores no intencionados por parte del administrador	0.003	20 %	30 %	20 %
	E.7 Error de secuencia	0.005	-	30 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	30 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	30 %

	E.10 Fugas de información	1	20 %	-	-
	A.3 Usurpación de identidad de los usuarios	0.011	20 %	30 %	20 %
	A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %
	A.7 Alteración de datos	0.011	-	20 %	-
	A.8 Accesos no autorizados	0.033	20 %	20 %	-
	A.10 Denegación de acciones	1	-	10 %	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.13 Eliminación de la información	1	-	-	30 %
	A.14 Divulgación de la información	1	20 %	-	-
[SW.1]	Navegadores WEB	1	50 %	40 %	50 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
	E.1 Errores no intencionado por	0.033	20 %	30 %	20 %



parte de los usuarios				
E.2 Errores no intencionados por parte del administrador	0.003	10 %	20 %	10 %
E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc)	0.033	50 %	40 %	50 %
E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	30 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	30 %
E.10 Fugas de información	1	20 %	-	-
E.11 SW Vulnerables	0.011	20 %	20 %	20 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	20 %	20 %
A.3 Usurpación de identidad de los usuarios	0.011	20 %	30 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	30 %	30 %	20 %

	A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
	A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc)	1	30 %	40 %	40 %
	A.7 Alteración de datos	0.011	-	20 %	-
	A.8 Accesos no autorizados	0.033	30 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	40 %	-
	A.13 Eliminación de la información	1	-	-	30 %
	A.14 Divulgación de la información	1	30 %	-	-
	A.15 Alteración de software (programas)	0.011	30 %	40 %	30 %
[SW.2]	Sistemas Operativos	1	40 %	60 %	60 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	30 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	20 %
	E.2 Errores no intencionados por	0.003	10 %	10 %	10 %

parte del administrador				
E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc)	0.033	30 %	40 %	30 %
E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	20 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	60 %
E.10 Fugas de información	1	20 %	-	-
E.11 SW Vulnerables	0.011	30 %	40 %	20 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	20 %	10 %
A.3 Usurpación de identidad de los usuarios	0.011	20 %	30 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	10 %

	A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	40 %	50 %	40 %
	A.7 Alteración de datos	0.011	-	40 %	-
	A.8 Accesos no autorizados	0.033	30 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	60 %	-
	A.13 Eliminación de la información	1	-	-	60 %
	A.14 Divulgación de la información	1	40 %	-	-
	A.15 Alteración de software (programas)	0.011	40 %	50 %	40 %
[SW.3]	Aplicativos de ofimática	1	30 %	30 %	30 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	20 %
	E.2 Errores no intencionados por parte del administrador	0.003	10 %	10 %	10 %
	E.6 Propagación de SW malicioso	0.033	20 %	30 %	20 %

(virus, troyanos, spyware, etc.)				
E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	20 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	20 %
E.10 Fugas de información	1	20 %	-	-
E.11 SW Vulnerables	0.011	30 %	30 %	20 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	20 %	10 %
A.3 Usurpación de identidad de los usuarios	0.011	20 %	20 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	10 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	20 %	30 %	20 %

	A.7 Alteración de datos	0.011	-	30 %	-
	A.8 Accesos no autorizados	0.033	20 %	20 %	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.13 Eliminación de la información	1	-	-	30 %
	A.14 Divulgación de la información	1	20 %	-	-
	A.15 Alteración de software (programas)	0.011	20 %	20 %	20 %
[SW.4]	Cientes de correo electrónico	1	40 %	60 %	60 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	30 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	20 %
	E.2 Errores no intencionados por parte del administrador	0.003	10 %	10 %	10 %
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc)	0.033	20 %	30 %	20 %

E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	40 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	50 %
E.10 Fugas de información	1	30 %	-	-
E.11 SW Vulnerables	0.011	30 %	30 %	20 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	20 %	20 %
A.3 Usurpación de identidad de los usuarios	0.011	30 %	20 %	30 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	10 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	30 %	30 %	20 %
A.7 Alteración de datos	0.011	-	40 %	-

	A.8 Accesos no autorizados	0.033	30 %	30 %	-
	A.12 Alteración deliberada de la información	1	-	60 %	-
	A.13 Eliminación de la información	1	-	-	60 %
	A.14 Divulgación de la información	1	40 %	-	-
	A.15 Alteración de software (programas)	0.011	30 %	40 %	30 %
[SW.5]	Gestor de máquinas virtuales	1	30 %	40 %	40 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	10 %	10 %	10 %
	E.2 Errores no intencionados por parte del administrador	0.003	10 %	10 %	20 %
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	20 %	30 %	20 %
	E.7 Error de secuencia	0.005	-	20 %	-



E.8 Perturbación no intencionado de la información	0.011	-	30 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	40 %
E.10 Fugas de información	1	30 %	-	-
E.11 SW Vulnerables	0.011	30 %	30 %	30 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	20 %	20 %
A.3 Usurpación de identidad de los usuarios	0.011	30 %	20 %	30 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc)	1	30 %	30 %	20 %
A.7 Alteración de datos	0.011	-	40 %	-
A.8 Accesos no autorizados	0.033	30 %	30 %	-

	A.12 Alteración deliberada de la información	1	-	40 %	-
	A.13 Eliminación de la información	1	-	-	40 %
	A.14 Divulgación de la información	1	30 %	-	-
	A.15 Alteración de software (programas)	0.011	30 %	30 %	30 %
[SW.6]	Sistema de BD	1	40 %	80 %	80 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	50 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	40 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	30 %	30 %	30 %
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	40 %	50 %	40 %
	E.7 Error de secuencia	0.005	-	40 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	60 %	-

E.9 Eliminación no intencional de la información	0.033	-	-	80 %
E.10 Fugas de información	1	40 %	-	-
E.11 SW Vulnerables	0.011	40 %	40 %	40 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	40 %	40 %
A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	40 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	30 %	30 %	30 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	40 %	40 %	40 %
A.7 Alteración de datos	0.011	-	60 %	-
A.8 Accesos no autorizados	0.033	40 %	40 %	-
A.12 Alteración deliberada de la información	1	-	80 %	-

	A.13 Eliminación de la información	1	-	-	80 %
	A.14 Divulgación de la información	1	40 %	-	-
	A.15 Alteración de software (programas)	0.011	40 %	40 %	40 %
[SW.7]	Sistema de gestión de backups	1	50 %	70 %	80 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	70 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	50 %	40 %
	E.2 Errores no intencionados por parte del administrador	0.003	30 %	50 %	30 %
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	40 %	50 %	40 %
	E.7 Error de secuencia	0.005	-	30 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	70 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	80 %

E.10 Fugas de información	1	50 %	-	-
E.11 SW Vulnerables	0.011	40 %	50 %	40 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	40 %	40 %
A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	40 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	30 %	30 %	30 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	50 %	50 %	50 %
A.7 Alteración de datos	0.011	-	60 %	-
A.8 Accesos no autorizados	0.033	40 %	40 %	-
A.12 Alteración deliberada de la información	1	-	70 %	-
A.13 Eliminación de la información	1	-	-	80 %
A.14 Divulgación de la información	1	50 %	-	-

	A.15 Alteración de software (programas)	0.011	40 %	40 %	40 %
[SW.8]	Sistema de referenciación geográfica	1	50 %	60 %	70 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	50 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	50 %	50 %
	E.2 Errores no intencionados por parte del administrador	0.003	30 %	50 %	30 %
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	40 %	50 %	50 %
	E.7 Error de secuencia	0.005	-	40 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	60 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	70 %
	E.10 Fugas de información	1	40 %	-	-
	E.11 SW Vulnerables	0.011	40 %	50 %	40 %

E.12 Errores de actualización de las aplicaciones (software)	0.011	-	40 %	50 %
A.3 Usurpación de identidad de los usuarios	0.011	20 %	20 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	30 %	30 %	30 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	30 %	50 %	50 %
A.7 Alteración de datos	0.011	-	60 %	-
A.8 Accesos no autorizados	0.033	40 %	40 %	-
A.12 Alteración deliberada de la información	1	-	60 %	-
A.13 Eliminación de la información	1	-	-	70 %
A.14 Divulgación de la información	1	50 %	-	-
A.15 Alteración de software (programas)	0.011	30 %	30 %	30 %

---

[SW.9]	Sistema de pagos asociados	1	60 %	70 %	80 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	70 %
	E.1 Errores no intencionado por parte de los usuarios	0.033	50 %	60 %	50 %
	E.2 Errores no intencionados por parte del administrador	0.003	40 %	50 %	40 %
	E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	50 %	70 %	50 %
	E.7 Error de secuencia	0.005	-	50 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	70 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	70 %
	E.10 Fugas de información	1	50 %	-	-
	E.11 SW Vulnerables	0.011	40 %	60 %	50 %
	E.12 Errores de actualización de	0.011	-	40 %	50 %



	las aplicaciones (software)				
	A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	30 %
	A.4 Abuso de acceso del nivel de privilegios	1	50 %	50 %	30 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	30 %	30 %	30 %
	A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	40 %	40 %	30 %
	A.7 Alteración de datos	0.011	-	70 %	-
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	70 %	-
	A.13 Eliminación de la información	1	-	-	80 %
	A.14 Divulgación de la información	1	60 %	-	-
	A.15 Alteración de software (programas)	0.011	40 %	40 %	30 %
<hr/>					
[SW.10]	Aplicativo para el diseño de	1	30 %	40 %	40 %

---

arquitectura,  
mecánico y la  
cartografía

I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	20 %
E.2 Errores no intencionados por parte del administrador	0.003	10 %	10 %	10 %
E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	20 %	30 %	20 %
E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	20 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	20 %
E.10 Fugas de información	1	20 %	-	-
E.11 SW Vulnerables	0.011	30 %	30 %	20 %
E.12 Errores de actualización de	0.011	-	20 %	10 %

las aplicaciones (software)				
A.3 Usurpación de identidad de los usuarios	0.011	20 %	20 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	10 %
A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc)	1	20 %	30 %	20 %
A.7 Alteración de datos	0.011	-	40 %	-
A.8 Accesos no autorizados	0.033	20 %	20 %	-
A.12 Alteración deliberada de la información	1	-	30 %	-
A.13 Eliminación de la información	1	-	-	40 %
A.14 Divulgación de la información	1	20 %	-	-
A.15 Alteración de software (programas)	0.011	20 %	20 %	20 %
[SW.11] Antivirus	1	40 %	50 %	50 %

I.6 Fallo de origen del Hardware o Software	0.005	-	-	50%
E.1 Errores no intencionado por parte de los usuarios	0.033	20%	50%	20%
E.2 Errores no intencionados por parte del administrador	0.003	10%	40%	20%
E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	20%	30%	20%
E.7 Error de secuencia	0.005	-	40%	-
E.8 Perturbación no intencionado de la información	0.011	-	40%	-
E.9 Eliminación no intencional de la información	0.033	-	-	50%
E.10 Fugas de información	1	20%	-	-
E.11 SW Vulnerables	0.011	40%	40%	40%
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	40%	30%

	A.3 Usurpación de identidad de los usuarios	0.011	20 %	20 %	20 %
	A.4 Abuso de acceso del nivel de privilegios	1	20 %	20 %	20 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
	A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc.)	1	40 %	40 %	40 %
	A.7 Alteración de datos	0.011	-	50 %	-
	A.8 Accesos no autorizados	0.033	30 %	30 %	-
	A.12 Alteración deliberada de la información	1	-	50 %	-
	A.13 Eliminación de la información	1	-	-	50 %
	A.14 Divulgación de la información	1	40 %	-	-
	A.15 Alteración de software (programas)	0.011	40 %	40 %	40 %
[SW.12]	Desarrollo de Software a medida subcontratado	1	50 %	70 %	80 %

I.6 Fallo de origen del Hardware o Software	0.005	-	-	70 %
E.1 Errores no intencionado por parte de los usuarios	0.033	40 %	50 %	40 %
E.2 Errores no intencionados por parte del administrador	0.003	30 %	50 %	30 %
E.6 Propagación de SW malicioso (virus, troyanos, spyware, etc.)	0.033	40 %	50 %	40 %
E.7 Error de secuencia	0.005	-	30 %	-
E.8 Perturbación no intencionado de la información	0.011	-	70 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	80 %
E.10 Fugas de información	1	50 %	-	-
E.11 SW Vulnerables	0.011	40 %	50 %	40 %
E.12 Errores de actualización de las aplicaciones (software)	0.011	-	40 %	40 %

	A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	40 %
	A.4 Abuso de acceso del nivel de privilegios	1	20 %	30 %	20 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	30 %	30 %	30 %
	A.6 Difusión de SW dañino (Virus, troyanos, spyware, etc)	1	50 %	50 %	50 %
	A.7 Alteración de datos	0.011	-	60 %	-
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	70 %	-
	A.13 Eliminación de la información	1	-	-	80 %
	A.14 Divulgación de la información	1	50 %	-	-
	A.15 Alteración de software (programas)	0.011	40 %	40 %	40 %
[HD.1]	Servidor	1	70 %	60 %	80 %
	N.1 Incendio (Fuego)	0.003	-	-	70 %

N.2 Daños ocasionados por el agua	0.003	-	-	70 %
N.3 Climas adversos	0.011	-	-	70 %
N.4 Eventos sísmicos	0.003	-	-	70 %
I.1 Incendio (Fuego)	0.003	-	-	70 %
I.2 Daños ocasionados por el agua	0.003	-	-	60 %
I.3 Sobretensiones eléctricas	0.005	-	-	50 %
I.4 Accidentes de transito	0.005	-	-	60 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	70 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	50 %
I.7 Perdida del suministro eléctrico	0.033	-	-	50 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	40 %
E.2 Errores no intencionados por parte del administrador	0.003	40 %	50 %	60 %



E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	50%
E.14 Extravió de equipos	0.033	70%	-	70%
A.4 Abuso de acceso del nivel de privilegios	1	40%	50%	50%
A.5 Uso de los recursos de los activos para fines no previstos	1	40%	40%	40%
A.8 Accesos no autorizados	0.033	40%	40%	-
A.16 Sabotaje del hardware	0.005	60%	60%	60%
A.17 Robo	0.033	60%	-	70%
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	80%

---

[HD.2]	Computador de escritorio	1	60%	40%	60%
	N.1 Incendio (Fuego)	0.003	-	-	60%
	N.2 Daños ocasionados por el agua	0.003	-	-	60%
	N.3 Climas adversos	0.011	-	-	60%

N.4 Eventos sísmicos	0.003	-	-	60 %
I.1 Incendio (Fuego)	0.003	-	-	60 %
I.2 Daños ocasionados por el agua	0.003	-	-	50 %
I.3 Sobretensiones eléctricas	0.005	-	-	40 %
I.4 Accidentes de tránsito	0.005	-	-	50 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	40 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	50 %
I.7 Perdida del suministro eléctrico	0.033	-	-	50 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	30 %
E.2 Errores no intencionados por parte del administrador	0.003	20 %	40 %	30 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	50 %
E.14 Extravió de equipos	0.033	30 %	-	60 %

A.4 Abuso de acceso del nivel de privilegios	1	30 %	30 %	30 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.8 Accesos no autorizados	0.033	20 %	20 %	-
A.16 Sabotaje del hardware	0.005	40 %	40 %	40 %
A.17 Robo	0.033	60 %	-	60 %
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	60 %

---

[HD.3]	Computador portátil (laptop)	1	60 %	40 %	60 %
	N.1 Incendio (Fuego)	0.003	-	-	60 %
	N.2 Daños ocasionados por el agua	0.003	-	-	60 %
	N.3 Climas adversos	0.011	-	-	60 %
	N.4 Eventos sísmicos	0.003	-	-	60 %
	I.1 Incendio (Fuego)	0.003	-	-	60 %

I.2 Daños ocasionados por el agua	0.003	-	-	50 %
I.3 Sobretensiones eléctricas	0.005	-	-	40 %
I.4 Accidentes de transito	0.005	-	-	50 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	40 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	50 %
I.7 Perdida del suministro eléctrico	0.033	-	-	50 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	30 %
E.2 Errores no intencionados por parte del administrador	0.003	20 %	40 %	30 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	50 %
E.14 Extravió de equipos	0.033	30 %	-	60 %
A.4 Abuso de acceso del nivel de privilegios	1	30 %	30 %	30 %

	A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
	A.8 Accesos no autorizados	0.033	20 %	20 %	-
	A.16 Sabotaje del hardware	0.005	40 %	40 %	40 %
	A.17 Robo	0.033	60 %	-	60 %
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	60 %
<hr/>					
[HD.4]	Móviles / Radios de comunicación	1	20 %	40 %	50 %
	N.1 Incendio (Fuego)	0.003	-	-	50 %
	N.2 Daños ocasionados por el agua	0.003	-	-	50 %
	N.3 Climas adversos	0.011	-	-	50 %
	N.4 Eventos sísmicos	0.003	-	-	50 %
	I.1 Incendio (Fuego)	0.003	-	-	50 %
	I.2 Daños ocasionados por el agua	0.003	-	-	50 %
	I.3 Sobretensiones eléctricas	0.005	-	-	30 %

I.4 Accidentes de tránsito	0.005	-	-	40 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	30 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	40 %
I.7 Pérdida del suministro eléctrico	0.033	-	-	50 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	20 %
E.2 Errores no intencionados por parte del administrador	0.003	20 %	40 %	40 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	40 %
E.14 Extravió de equipos	0.033	10 %	-	40 %
A.4 Abuso de acceso del nivel de privilegios	1	10 %	10 %	30 %
A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %
A.8 Accesos no autorizados	0.033	20 %	20 %	-

	A.16 Sabotaje del hardware	0.005	20 %	20 %	30 %
	A.17 Robo	0.033	20 %	-	40 %
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	50 %
<hr/>					
[HD.5]	DRONES	1	30 %	30 %	70 %
	N.1 Incendio (Fuego)	0.003	-	-	70 %
	N.2 Daños ocasionados por el agua	0.003	-	-	70 %
	N.3 Climas adversos	0.011	-	-	70 %
	N.4 Eventos sísmicos	0.003	-	-	70 %
	I.1 Incendio (Fuego)	0.003	-	-	70 %
	I.2 Daños ocasionados por el agua	0.003	-	-	70 %
	I.3 Sobretensiones eléctricas	0.005	-	-	60 %
	I.4 Accidentes de transito	0.005	-	-	60 %
	I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	50 %

I.6 Fallo de origen del Hardware o Software	0.005	-	-	50 %
I.7 Perdida del suministro eléctrico	0.033	-	-	40 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	50 %
E.2 Errores no intencionados por parte del administrador	0.003	30 %	30 %	40 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	40 %
E.14 Extravió de equipos	0.033	10 %	-	70 %
A.4 Abuso de acceso del nivel de privilegios	1	10 %	10 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	30 %	20 %	40 %
A.8 Accesos no autorizados	0.033	20 %	20 %	-
A.16 Sabotaje del hardware	0.005	20 %	20 %	30 %
A.17 Robo	0.033	20 %	-	70 %
A.18 Ataque destructivo del	0.011	-	-	70 %



hardware o  
soportes

Periféricos (Impresoras, escáneres, proyectores, etc.)			20	20	40
[HD.6]		1	%	%	%
	N.1 Incendio (Fuego)	0.003	-	-	40 %
	N.2 Daños ocasionados por el agua	0.003	-	-	40 %
	N.3 Climas adversos	0.011	-	-	40 %
	N.4 Eventos sísmicos	0.003	-	-	40 %
	I.1 Incendio (Fuego)	0.003	-	-	40 %
	I.2 Daños ocasionados por el agua	0.003	-	-	40 %
	I.3 Sobretensiones eléctricas	0.005	-	-	40 %
	I.4 Accidentes de transito	0.005	-	-	20 %
	I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	20 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %

I.7 Perdida del suministro eléctrico	0.033	-	-	20 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	20 %
E.2 Errores no intencionados por parte del administrador	0.003	20 %	20 %	30 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	30 %
E.14 Extravió de equipos	0.033	20 %	-	40 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	20 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.8 Accesos no autorizados	0.033	20 %	20 %	-
A.16 Sabotaje del hardware	0.005	20 %	20 %	30 %
A.17 Robo	0.033	20 %	-	40 %
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	40 %

---

	Servidores de		60	50	70
[HD.7]	respaldo (backup)	1	%	%	%
	N.1 Incendio (Fuego)	0.003	-	-	70 %
	N.2 Daños ocasionados por el agua	0.003	-	-	70 %
	N.3 Climas adversos	0.011	-	-	70 %
	N.4 Eventos sísmicos	0.003	-	-	70 %
	I.1 Incendio (Fuego)	0.003	-	-	70 %
	I.2 Daños ocasionados por el agua	0.003	-	-	70 %
	I.3 Sobretensiones eléctricas	0.005	-	-	40 %
	I.4 Accidentes de transito	0.005	-	-	50 %
	I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	40 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	30 %
	I.7 Perdida del suministro eléctrico	0.033	-	-	30 %
	I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	40 %

	E.2 Errores no intencionados por parte del administrador	0.003	30 %	20 %	30 %
	E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	30 %
	E.14 Extravió de equipos	0.033	60 %	-	70 %
	A.4 Abuso de acceso del nivel de privilegios	1	40 %	40 %	30 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
	A.8 Accesos no autorizados	0.033	30 %	40 %	-
	A.16 Sabotaje del hardware	0.005	30 %	50 %	50 %
	A.17 Robo	0.033	20 %	-	60 %
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	70 %
[HD.8]	Router	1	50 %	50 %	50 %
	N.1 Incendio (Fuego)	0.003	-	-	50 %

N.2 Daños ocasionados por el agua	0.003	-	-	50 %
N.3 Climas adversos	0.011	-	-	50 %
N.4 Eventos sísmicos	0.003	-	-	50 %
I.1 Incendio (Fuego)	0.003	-	-	50 %
I.2 Daños ocasionados por el agua	0.003	-	-	50 %
I.3 Sobretensiones eléctricas	0.005	-	-	40 %
I.4 Accidentes de transito	0.005	-	-	40 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	40 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	30 %
I.7 Perdida del suministro eléctrico	0.033	-	-	30 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	40 %
E.2 Errores no intencionados por parte del administrador	0.003	40 %	30 %	40 %

	E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	30 %
	E.14 Extravió de equipos	0.033	50 %	-	50 %
	A.4 Abuso de acceso del nivel de privilegios	1	40 %	40 %	30 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
	A.8 Accesos no autorizados	0.033	30 %	40 %	-
	A.16 Sabotaje del hardware	0.005	30 %	50 %	50 %
	A.17 Robo	0.033	20 %	-	50 %
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	50 %
[HD.9]	Switch	1	50 %	50 %	50 %
	N.1 Incendio (Fuego)	0.003	-	-	50 %
	N.2 Daños ocasionados por el agua	0.003	-	-	50 %
	N.3 Climas adversos	0.011	-	-	50 %

N.4 Eventos sísmicos	0.003	-	-	50 %
I.1 Incendio (Fuego)	0.003	-	-	50 %
I.2 Daños ocasionados por el agua	0.003	-	-	50 %
I.3 Sobretensiones eléctricas	0.005	-	-	40 %
I.4 Accidentes de tránsito	0.005	-	-	40 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	40 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	30 %
I.7 Perdida del suministro eléctrico	0.033	-	-	30 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	40 %
E.2 Errores no intencionados por parte del administrador	0.003	40 %	30 %	40 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	30 %
E.14 Extravió de equipos	0.033	50 %	-	50 %

A.4 Abuso de acceso del nivel de privilegios	1	40 %	40 %	30 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.8 Accesos no autorizados	0.033	30 %	40 %	-
A.16 Sabotaje del hardware	0.005	30 %	50 %	50 %
A.17 Robo	0.033	20 %	-	50 %
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	50 %
[HD.10] Módems	1	30 %	40 %	40 %
N.1 Incendio (Fuego)	0.003	-	-	40 %
N.2 Daños ocasionados por el agua	0.003	-	-	40 %
N.3 Climas adversos	0.011	-	-	40 %
N.4 Eventos sísmicos	0.003	-	-	40 %
I.1 Incendio (Fuego)	0.003	-	-	40 %
I.2 Daños ocasionados por el agua	0.003	-	-	40 %



I.3 Sobretensiones eléctricas	0.005	-	-	20 %
I.4 Accidentes de transito	0.005	-	-	20 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	20 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
I.7 Perdida del suministro eléctrico	0.033	-	-	20 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	20 %
E.2 Errores no intencionados por parte del administrador	0.003	20 %	30 %	20 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	30 %
E.14 Extravió de equipos	0.033	20 %	-	40 %
A.4 Abuso de acceso del nivel de privilegios	1	30 %	30 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %

	A.8 Accesos no autorizados	0.033	30 %	30 %	-
	A.16 Sabotaje del hardware	0.005	30 %	40 %	40 %
	A.17 Robo	0.033	20 %	-	40 %
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	40 %
[HD.11]	Puntos de acceso inalámbrico	1	20 %	20 %	20 %
	N.1 Incendio (Fuego)	0.003	-	-	20 %
	N.2 Daños ocasionados por el agua	0.003	-	-	20 %
	N.3 Climats adversos	0.011	-	-	20 %
	N.4 Eventos sísmicos	0.003	-	-	20 %
	I.1 Incendio (Fuego)	0.003	-	-	20 %
	I.2 Daños ocasionados por el agua	0.003	-	-	20 %
	I.3 Sobretensiones eléctricas	0.005	-	-	10 %
	I.4 Accidentes de transito	0.005	-	-	20 %
	I.5 Contaminación mecánica	0.011	-	-	20 %

(Polución, vibraciones)				
I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
I.7 Perdida del suministro eléctrico	0.033	-	-	20 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	20 %
E.2 Errores no intencionados por parte del administrador	0.003	10 %	10 %	20 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	20 %
E.14 Extravió de equipos	0.033	20 %	-	20 %
A.4 Abuso de acceso del nivel de privilegios	1	20 %	20 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %
A.8 Accesos no autorizados	0.033	20 %	20 %	-
A.16 Sabotaje del hardware	0.005	20 %	20 %	20 %
A.17 Robo	0.033	10 %	-	20 %

	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	20 %
[HD.12]	Antenas de comunicación	1	10 %	20 %	20 %
	N.1 Incendio (Fuego)	0.003	-	-	20 %
	N.2 Daños ocasionados por el agua	0.003	-	-	20 %
	N.3 Climas adversos	0.011	-	-	20 %
	N.4 Eventos sísmicos	0.003	-	-	20 %
	I.1 Incendio (Fuego)	0.003	-	-	20 %
	I.2 Daños ocasionados por el agua	0.003	-	-	20 %
	I.3 Sobretensiones eléctricas	0.005	-	-	10 %
	I.4 Accidentes de transito	0.005	-	-	20 %
	I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	20 %
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
	I.7 Perdida del suministro eléctrico	0.033	-	-	20 %

I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	20%
E.2 Errores no intencionados por parte del administrador	0.003	10%	10%	20%
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	20%
E.14 Extravió de equipos	0.033	10%	-	20%
A.4 Abuso de acceso del nivel de privilegios	1	10%	20%	20%
A.5 Uso de los recursos de los activos para fines no previstos	1	10%	10%	10%
A.8 Accesos no autorizados	0.033	10%	20%	-
A.16 Sabotaje del hardware	0.005	10%	20%	20%
A.17 Robo	0.033	10%	-	20%
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	20%

---

[SINF.1]	Discos virtuales	1	40%	30%	40%
----------	------------------	---	-----	-----	-----

N.1 Incendio (Fuego)	0.003	-	-	40 %
N.2 Daños ocasionados por el agua	0.003	-	-	40 %
N.3 Climas adversos	0.011	-	-	40 %
N.4 Eventos sísmicos	0.003	-	-	40 %
I.1 Incendio (Fuego)	0.003	-	-	40 %
I.2 Daños ocasionados por el agua	0.003	-	-	40 %
I.3 Sobretensiones eléctricas	0.005	-	-	30 %
I.4 Accidentes de transito	0.005	-	-	30 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	30 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	30 %
I.7 Perdida del suministro eléctrico	0.033	-	-	30 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	30 %
I.10 Soporte de almacenamiento de la información	0.003	-	-	30 %

(Hardware)				
degradado				
E.1 Errores no intencionado por parte de los usuarios	0.033	20 %	20 %	20 %
E.2 Errores no intencionados por parte del administrador	0.003	20 %	20 %	20 %
E.8 Perturbación no intencionado de la información	0.011	-	30 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	40 %
E.10 Fugas de información	1	40 %	-	-
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	30 %
E.14 Extravió de equipos	0.033	40 %	-	40 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.8 Accesos no autorizados	0.033	20 %	20 %	-
A.12 Alteración deliberada de la información	1	-	30 %	-

	A.13 Eliminación de la información	1	-	-	40 %
	A.14 Divulgación de la información	1	30 %	-	-
	A.16 Sabotaje del hardware	0.005	30 %	-	30 %
	A.17 Robo	0.033	30 %	-	40 %
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	40 %
[SINF.2]	Memorias USB	1	10 %	10 %	10 %
	N.1 Incendio (Fuego)	0.003	-	-	10 %
	N.2 Daños ocasionados por el agua	0.003	-	-	10 %
	N.3 Climas adversos	0.011	-	-	10 %
	N.4 Eventos sísmicos	0.003	-	-	10 %
	I.1 Incendio (Fuego)	0.003	-	-	10 %
	I.2 Daños ocasionados por el agua	0.003	-	-	10 %
	I.3 Sobretensiones eléctricas	0.005	-	-	10 %
	I.4 Accidentes de tránsito	0.005	-	-	10 %



I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	10 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	10 %
I.7 Perdida del suministro eléctrico	0.033	-	-	10 %
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	10 %
I.10 Soporte de almacenamiento de la información (Hardware) degradado	0.003	-	-	10 %
E.1 Errores no intencionado por parte de los usuarios	0.033	5%	5%	5%
E.2 Errores no intencionados por parte del administrador	0.003	5%	5%	5%
E.8 Perturbación no intencionado de la información	0.011	-	10 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	10 %
E.10 Fugas de información	1	10 %	-	-

	E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	10%
	E.14 Extravió de equipos	0.033	5%	-	10%
	A.5 Uso de los recursos de los activos para fines no previstos	1	5%	5%	5%
	A.8 Accesos no autorizados	0.033	5%	5%	-
	A.12 Alteración deliberada de la información	1	-	10%	-
	A.13 Eliminación de la información	1	-	-	10%
	A.14 Divulgación de la información	1	10%	-	-
	A.16 Sabotaje del hardware	0.005	10%	-	10%
	A.17 Robo	0.033	10%	-	10%
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	10%
[SINF.3]	Discos duros externos	1	20%	20%	20%
	N.1 Incendio (Fuego)	0.003	-	-	20%

N.2 Daños ocasionados por el agua	0.003	-	-	20 %
N.3 Climas adversos	0.011	-	-	20 %
N.4 Eventos sísmicos	0.003	-	-	20 %
I.1 Incendio (Fuego)	0.003	-	-	20 %
I.2 Daños ocasionados por el agua	0.003	-	-	20 %
I.3 Sobretensiones eléctricas	0.005	-	-	10 %
I.4 Accidentes de transito	0.005	-	-	10 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	10 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
I.7 Perdida del suministro eléctrico	0.033	-	-	5%
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	20 %
I.10 Soporte de almacenamiento de la información (Hardware) degradado	0.003	-	-	10 %

E.1 Errores no intencionado por parte de los usuarios	0.033	10 %	10 %	10 %
E.2 Errores no intencionados por parte del administrador	0.003	10 %	10 %	10 %
E.8 Perturbación no intencionado de la información	0.011	-	10 %	-
E.9 Eliminación no intencional de la información	0.033	-	-	20 %
E.10 Fugas de información	1	10 %	-	-
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	20 %
E.14 Extravió de equipos	0.033	20 %	-	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %
A.8 Accesos no autorizados	0.033	10 %	10 %	-
A.12 Alteración deliberada de la información	1	-	20 %	-
A.13 Eliminación de la información	1	-	-	20 %

A.14 Divulgación de la información	1	10 %	-	-
A.16 Sabotaje del hardware	0.005	10 %	-	10 %
A.17 Robo	0.033	10 %	-	20 %
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	20 %

---

[EAUX.1 ]	Equipos de alimentación eléctrica	1	10 %	10 %	20 %
	N.1 Incendio (Fuego)	0.003	-	-	20 %
	N.2 Daños ocasionados por el agua	0.003	-	-	20 %
	N.3 Climas adversos	0.011	-	-	20 %
	N.4 Eventos sísmicos	0.003	-	-	20 %
	I.1 Incendio (Fuego)	0.003	-	-	20 %
	I.2 Daños ocasionados por el agua	0.003	-	-	20 %
	I.3 Sobretensiones eléctricas	0.005	-	-	10 %
	I.4 Accidentes de tránsito	0.005	-	-	10 %
	I.5 Contaminación mecánica	0.011	-	-	10 %

(Polución, vibraciones)				
I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
I.7 Perdida del suministro eléctrico	0.033	-	-	5%
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	10 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	10 %
E.14 Extravió de equipos	0.033	10 %	-	10 %
A.5 Uso de los recursos de los activos para fines no previstos	1	10 %	10 %	10 %
A.8 Accesos no autorizados	0.033	0%	0%	-
A.16 Sabotaje del hardware	0.005	10 %	-	20 %
A.17 Robo	0.033	10 %	-	20 %
A.18 Ataque destrutivo del hardware o soportes	0.011	-	-	20 %

---

[EAUX.2 ] UPS	1	0%	0%	20 %
------------------	---	----	----	---------

N.1 Incendio (Fuego)	0.003	-	-	20 %
N.2 Daños ocasionados por el agua	0.003	-	-	20 %
N.3 Climas adversos	0.011	-	-	20 %
N.4 Eventos sísmicos	0.003	-	-	20 %
I.1 Incendio (Fuego)	0.003	-	-	20 %
I.2 Daños ocasionados por el agua	0.003	-	-	20 %
I.3 Sobretensiones eléctricas	0.005	-	-	10 %
I.4 Accidentes de transito	0.005	-	-	10 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	10 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	20 %
I.7 Perdida del suministro eléctrico	0.033	-	-	5%
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	10 %
E.13 Errores de mantenimiento y/o	0.011	-	-	10 %

actualizaciones del hardware

E.14 Extravió de equipos 0.033 0% - 10%

A.5 Uso de los recursos de los activos para fines no previstos 1 0% 0% 10%

A.8 Accesos no autorizados 0.033 0% 0% -

A.16 Sabotaje del hardware 0.005 0% - 20%

A.17 Robo 0.033 0% - 20%

A.18 Ataque destructivo del hardware o soportes 0.011 - - 20%

---

[EAUX.3 ] Equipo de aire acondicionado 1 0% 0% 20%

N.1 Incendio (Fuego) 0.003 - - 20%

N.2 Daños ocasionados por el agua 0.003 - - 20%

N.3 Climas adversos 0.011 - - 20%

N.4 Eventos sísmicos 0.003 - - 20%

I.1 Incendio (Fuego) 0.003 - - 20%



I.2 Daños ocasionados por el agua	0.003	-	-	20 %
I.3 Sobretensiones eléctricas	0.005	-	-	10 %
I.4 Accidentes de tránsito	0.005	-	-	10 %
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	10 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	0%
I.7 Perdida del suministro eléctrico	0.033	-	-	5%
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	10 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	0%
E.14 Extravió de equipos	0.033	0%	-	10 %
A.5 Uso de los recursos de los activos para fines no previstos	1	0%	0%	10 %
A.8 Accesos no autorizados	0.033	0%	0%	-
A.16 Sabotaje del hardware	0.005	0%	-	20 %

	A.17 Robo	0.033	0%	-	20%
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	20%
[EAUX.4 ]	Cableado eléctrico	1	0%	0%	20%
	N.1 Incendio (Fuego)	0.003	-	-	10%
	N.2 Daños ocasionados por el agua	0.003	-	-	10%
	N.3 Climas adversos	0.011	-	-	10%
	N.4 Eventos sísmicos	0.003	-	-	10%
	I.1 Incendio (Fuego)	0.003	-	-	10%
	I.2 Daños ocasionados por el agua	0.003	-	-	10%
	I.3 Sobretensiones eléctricas	0.005	-	-	10%
	I.4 Accidentes de transito	0.005	-	-	0%
	I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	10%
	I.6 Fallo de origen del Hardware o Software	0.005	-	-	0%

I.7 Perdida del suministro eléctrico	0.033	-	-	5%
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	10%
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	0%
E.14 Extravió de equipos	0.033	0%	-	10%
A.5 Uso de los recursos de los activos para fines no previstos	1	0%	0%	10%
A.8 Accesos no autorizados	0.033	0%	0%	-
A.16 Sabotaje del hardware	0.005	0%	-	20%
A.17 Robo	0.033	0%	-	20%
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	20%

---

[EAUX.5 ]	Cableado de comunicaciones (UTP)	1	0%	0%	20%
	N.1 Incendio (Fuego)	0.003	-	-	10%
	N.2 Daños ocasionados por el agua	0.003	-	-	10%

N.3 Climas adversos	0.011	-	-	10 %
N.4 Eventos sísmicos	0.003	-	-	10 %
I.1 Incendio (Fuego)	0.003	-	-	10 %
I.2 Daños ocasionados por el agua	0.003	-	-	10 %
I.3 Sobretensiones eléctricas	0.005	-	-	10 %
I.4 Accidentes de transito	0.005	-	-	0%
I.5 Contaminación mecánica (Polución, vibraciones)	0.011	-	-	10 %
I.6 Fallo de origen del Hardware o Software	0.005	-	-	0%
I.7 Perdida del suministro eléctrico	0.033	-	-	5%
I.8 Deficiencias en la climatización de las instalaciones	0.005	-	-	10 %
E.13 Errores de mantenimiento y/o actualizaciones del hardware	0.011	-	-	0%
E.14 Extravió de equipos	0.033	0%	-	10 %
A.5 Uso de los recursos de los	1	0%	0%	10 %

	activos para fines no previstos				
	A.8 Accesos no autorizados	0.033	0%	0%	-
	A.16 Sabotaje del hardware	0.005	0%	-	20%
	A.17 Robo	0.033	0%	-	20%
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	20%
[COM.1]	Comunicaciones de Radio	1	40%	60%	60%
	I.9 Fallo de los medios de comunicaciones	0.033	-	-	60%
	E.2 Errores no intencionados por parte del administrador	0.003	40%	60%	60%
	E.7 Error de secuencia	0.005	-	40%	-
	E.8 Perturbación no intencionado de la información	0.011	-	40%	-
	E.9 Eliminación no intencional de la información	0.033	-	50%	-
	E.10 Fugas de información	1	40%	-	-

	A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	20 %
	A.4 Abuso de acceso del nivel de privilegios	1	20 %	20 %	20 %
	A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
	A.7 Alteración de datos	0.011	-	40 %	-
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.9 Monitorización del trafico	0.005	30 %	-	-
	A.11 Interceptación de la información (Escucha pasiva)	1	40 %	-	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.14 Divulgación de la información	1	40 %	-	-
[COM.2]	Redes inalámbricas	1	50 %	50 %	50 %
	I.9 Fallo de los medios de comunicaciones	0.033	-	-	50 %
	E.2 Errores no intencionados por	0.003	40 %	50 %	50 %

parte del administrador				
E.7 Error de secuencia	0.005	-	40 %	-
E.8 Perturbación no intencionado de la información	0.011	-	40 %	-
E.9 Eliminación no intencional de la información	0.033	-	50 %	-
E.10 Fugas de información	1	40 %	-	-
A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	40 %	40 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.7 Alteración de datos	0.011	-	40 %	-
A.8 Accesos no autorizados	0.033	40 %	40 %	-
A.9 Monitorización del trafico	0.005	30 %	-	-
A.11 Interceptación de la información (Escucha pasiva)	1	40 %	-	-

		A.12 Alteración deliberada de la información	1	-	30 %	-
		A.14 Divulgación de la información	1	50 %	-	-
[COM.3]	Telefonía móvil		1	40 %	30 %	50 %
		I.9 Fallo de los medios de comunicaciones	0.033	-	-	50 %
		E.2 Errores no intencionados por parte del administrador	0.003	0%	0%	0%
		E.7 Error de secuencia	0.005	-	0%	-
		E.8 Perturbación no intencionado de la información	0.011	-	0%	-
		E.9 Eliminación no intencional de la información	0.033	-	30 %	-
		E.10 Fugas de información	1	30 %	-	-
		A.3 Usurpación de identidad de los usuarios	0.011	20 %	20 %	20 %
		A.4 Abuso de acceso del nivel de privilegios	1	20 %	20 %	20 %
		A.5 Uso de los recursos de los	1	10 %	10 %	10 %



	activos para fines no previstos				
	A.7 Alteración de datos	0.011	-	30 %	-
	A.8 Accesos no autorizados	0.033	10 %	20 %	-
	A.9 Monitorización del trafico	0.005	30 %	-	-
	A.11				
	Interceptación de la información (Escucha pasiva)	1	40 %	-	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.14 Divulgación de la información	1	40 %	-	-
[COM.4]	Redes LAN	1	50 %	50 %	50 %
	I.9 Fallo de los medios de comunicaciones	0.033	-	-	50 %
	E.2 Errores no intencionados por parte del administrador	0.003	40 %	50 %	50 %
	E.7 Error de secuencia	0.005	-	40 %	-
	E.8 Perturbación no intencionado de la información	0.011	-	40 %	-

E.9 Eliminación no intencional de la información	0.033	-	50 %	-
E.10 Fugas de información	1	40 %	-	-
A.3 Usurpación de identidad de los usuarios	0.011	40 %	40 %	20 %
A.4 Abuso de acceso del nivel de privilegios	1	40 %	40 %	20 %
A.5 Uso de los recursos de los activos para fines no previstos	1	20 %	20 %	20 %
A.7 Alteración de datos	0.011	-	40 %	-
A.8 Accesos no autorizados	0.033	40 %	40 %	-
A.9 Monitorización del trafico	0.005	30 %	-	-
A.11 Interceptación de la información (Escucha pasiva)	1	40 %	-	-
A.12 Alteración deliberada de la información	1	-	30 %	-
A.14 Divulgación de la información	1	50 %	-	-
[COM.5] Internet	1	40 %	60 %	60 %

I.9 Fallo de los medios de comunicaciones	0.033	-	-	60%
E.2 Errores no intencionados por parte del administrador	0.003	40%	60%	60%
E.7 Error de secuencia	0.005	-	40%	-
E.8 Perturbación no intencionado de la información	0.011	-	40%	-
E.9 Eliminación no intencional de la información	0.033	-	50%	-
E.10 Fugas de información	1	40%	-	-
A.3 Usurpación de identidad de los usuarios	0.011	40%	40%	20%
A.4 Abuso de acceso del nivel de privilegios	1	20%	20%	20%
A.5 Uso de los recursos de los activos para fines no previstos	1	20%	20%	20%
A.7 Alteración de datos	0.011	-	40%	-
A.8 Accesos no autorizados	0.033	40%	40%	-
A.9 Monitorización del trafico	0.005	30%	-	-

	A.11				
	Interceptación de la información (Escucha pasiva)	1	40 %	-	-
	A.12 Alteración deliberada de la información	1	-	30 %	-
	A.14 Divulgación de la información	1	40 %	-	-
[L.1]	Oficinas - Moquegua	1	50 %	40 %	80 %
	N.1 Incendio (Fuego)	0.003	-	-	80 %
	N.2 Daños ocasionados por el agua	0.003	-	-	80 %
	N.3 Climas adversos	0.011	-	-	80 %
	N.4 Eventos sísmicos	0.003	-	-	80 %
	I.1 Incendio (Fuego)	0.003	-	-	70 %
	I.2 Daños ocasionados por el agua	0.003	-	-	60 %
	I.3 Sobretensiones eléctricas	0.005	-	-	50 %
	E.8 Perturbación no intencionado de la información	0.011	-	0%	-
	E.9 Eliminación no intencional de la información	0.033	-	-	0%

	E.10 Fugas de información	1	20 %	-	-
	A.5 Uso de los recursos de los activos para fines no previstos	1	40 %	40 %	40 %
	A.8 Accesos no autorizados	0.033	40 %	40 %	-
	A.12 Alteración deliberada de la información	1	-	0%	-
	A.13 Eliminación de la información	1	-	-	0%
	A.14 Divulgación de la información	1	30 %	-	-
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	80 %
	A.19 Ocupación enemiga	0.005	50 %	-	50 %
[L.2]	Oficinas - Campamento Minero	1	50 %	50 %	80 %
	N.1 Incendio (Fuego)	0.003	-	-	80 %
	N.2 Daños ocasionados por el agua	0.003	-	-	80 %
	N.3 Climas adversos	0.011	-	-	80 %
	N.4 Eventos sísmicos	0.003	-	-	80 %

I.1 Incendio (Fuego)	0.003	-	-	80 %
I.2 Daños ocasionados por el agua	0.003	-	-	60 %
I.3 Sobretensiones eléctricas	0.005	-	-	50 %
E.8 Perturbación no intencionado de la información	0.011	-	0%	-
E.9 Eliminación no intencional de la información	0.033	-	-	0%
E.10 Fugas de información	1	30 %	-	-
A.5 Uso de los recursos de los activos para fines no previstos	1	50 %	50 %	50 %
A.8 Accesos no autorizados	0.033	40 %	40 %	-
A.12 Alteración deliberada de la información	1	-	0%	-
A.13 Eliminación de la información	1	-	-	60 %
A.14 Divulgación de la información	1	30 %	-	-
A.18 Ataque destrutivo del hardware o soportes	0.011	-	-	80 %

		A.19 Ocupación enemiga	0.005	50 %	-	50 %
[L.3]	Container		1	60 %	50 %	80 %
		N.1 Incendio (Fuego)	0.003	-	-	80 %
		N.2 Daños ocasionados por el agua	0.003	-	-	60 %
		N.3 Climas adversos	0.011	-	-	80 %
		N.4 Eventos sísmicos	0.003	-	-	60 %
		I.1 Incendio (Fuego)	0.003	-	-	80 %
		I.2 Daños ocasionados por el agua	0.003	-	-	60 %
		I.3 Sobretensiones eléctricas	0.005	-	-	70 %
		E.8 Perturbación no intencionado de la información	0.011	-	0%	-
		E.9 Eliminación no intencional de la información	0.033	-	-	60 %
		E.10 Fugas de información	1	30 %	-	-
		A.5 Uso de los recursos de los activos para fines no previstos	1	50 %	50 %	50 %

	A.8 Accesos no autorizados	0.033	50 %	50 %	-
	A.12 Alteración deliberada de la información	1	-	0%	-
	A.13 Eliminación de la información	1	-	-	50 %
	A.14 Divulgación de la información	1	50 %	-	-
	A.18 Ataque destructivo del hardware o soportes	0.011	-	-	80 %
	A.19 Ocupación enemiga	0.005	60 %	-	60 %
<hr/>					
[L.4]	Equipos móviles terrestres (camionetas, volquetes, equipos de línea amarilla)	1	60 %	50 %	80 %
	N.1 Incendio (Fuego)	0.003	-	-	80 %
	N.2 Daños ocasionados por el agua	0.003	-	-	60 %
	N.3 Climas adversos	0.011	-	-	80 %
	N.4 Eventos sísmicos	0.003	-	-	60 %
	I.1 Incendio (Fuego)	0.003	-	-	80 %



I.2 Daños ocasionados por el agua	0.003	-	-	60%
I.3 Sobretensiones eléctricas	0.005	-	-	50%
E.8 Perturbación no intencionado de la información	0.011	-	0%	-
E.9 Eliminación no intencional de la información	0.033	-	-	0%
E.10 Fugas de información	1	30%	-	-
A.5 Uso de los recursos de los activos para fines no previstos	1	50%	50%	50%
A.8 Accesos no autorizados	0.033	50%	50%	-
A.12 Alteración deliberada de la información	1	-	0%	-
A.13 Eliminación de la información	1	-	-	0%
A.14 Divulgación de la información	1	0%	-	-
A.18 Ataque destructivo del hardware o soportes	0.011	-	-	80%
A.19 Ocupación enemiga	0.005	60%	-	60%

	Plantas				
[L.5]	operativas (concreto, asfalto, etc.)	1	60 %	60 %	80 %
	N.1 Incendio (Fuego)	0.003	-	-	80 %
	N.2 Daños ocasionados por el agua	0.003	-	-	60 %
	N.3 Climas adversos	0.011	-	-	80 %
	N.4 Eventos sísmicos	0.003	-	-	60 %
	I.1 Incendio (Fuego)	0.003	-	-	80 %
	I.2 Daños ocasionados por el agua	0.003	-	-	60 %
	I.3 Sobretensiones eléctricas	0.005	-	-	70 %
	E.8 Perturbación no intencionado de la información	0.011	-	60 %	-
	E.9 Eliminación no intencional de la información	0.033	-	-	60 %
	E.10 Fugas de información	1	30 %	-	-
	A.5 Uso de los recursos de los activos para fines no previstos	1	50 %	50 %	50 %

		A.8 Accesos no autorizados	0.033	50 %	50 %	-
		A.12 Alteración deliberada de la información	1	-	60 %	-
		A.13 Eliminación de la información	1	-	-	50 %
		A.14 Divulgación de la información	1	50 %	-	-
		A.18 Ataque destructivo del hardware o soportes	0.011	-	-	80 %
		A.19 Ocupación enemiga	0.005	60 %	-	60 %
[P.1]	Usuarios Externos		1	40 %	50 %	40 %
		E.5 Deficiencias de la organización	0.011	-	-	40 %
		E.10 Fugas de información	1	40 %	-	-
		E.15 Personal no disponible	1	-	-	40 %
		A.20 Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc)	0.033	-	-	40 %
		A.21 Extorsión	0.005	40 %	50 %	40 %

		A.22 Ingeniería Social	0.033	30 %	40 %	30 %
[P.2]	Usuarios internos		1	60 %	50 %	80 %
		E.5 Deficiencias de la organización	0.011	-	-	60 %
		E.10 Fugas de información	1	60 %	-	-
		E.15 Personal no disponible	1	-	-	40 %
		A.20				
		Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc)	0.033	-	-	80 %
		A.21 Extorsión	0.005	40 %	50 %	40 %
		A.22 Ingeniería Social	0.033	30 %	40 %	30 %
[P.3]	Proveedores		1	40 %	50 %	80 %
		E.5 Deficiencias de la organización	0.011	-	-	40 %
		E.10 Fugas de información	1	40 %	-	-
		E.15 Personal no disponible	1	-	-	40 %
		A.20				
		Indisponibilidad del personal (huelgas, bloqueo de	0.033	-	-	80 %

			accesos, absentismo laboral, etc)			
		A.21 Extorsión	0.005	40 %	50 %	40 %
		A.22 Ingeniería Social	0.033	30 %	40 %	30 %
[P.4]	Sub Contratistas		1	40 %	50 %	70 %
		E.5 Deficiencias de la organización	0.011	-	-	50 %
		E.10 Fugas de información	1	40 %	-	-
		E.15 Personal no disponible	1	-	-	40 %
		A.20 Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc)	0.033	-	-	70 %
		A.21 Extorsión	0.005	40 %	50 %	40 %
		A.22 Ingeniería Social	0.033	30 %	40 %	30 %
[P.5]	Clientes		1	40 %	40 %	50 %
		E.5 Deficiencias de la organización	0.011	-	-	50 %
		E.10 Fugas de información	1	40 %	-	-

	E.15 Personal no disponible	1	-	-	40 %
	A.20				
	Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc)	0.033	-	-	40 %
	A.21 Extorsión	0.005	40 %	40 %	40 %
	A.22 Ingeniería Social	0.033	20 %	20 %	20 %
	<hr/>				
[P.6]	Administrador es de los Sistemas de información	1	50 %	40 %	70 %
	E.5 Deficiencias de la organización	0.011	-	-	70 %
	E.10 Fugas de información	1	50 %	-	-
	E.15 Personal no disponible	1	-	-	50 %
	A.20				
	Indisponibilidad del personal (huelgas, bloqueo de accesos, absentismo laboral, etc.)	0.033	-	-	50 %
	A.21 Extorsión	0.005	40 %	40 %	40 %

A.22 Ingeniería	0.033	20	20	20
Social		%	%	%

*Nota:* Evaluación del nivel de probabilidad de las amenazas identificadas en la organización por activo según sus tres dimensiones básicas. Fuente: Elaboración Propia.

#### 3.3.4.4. Análisis de impacto potencial.

Una vez realizada la valoración de criticidad y la probabilidad de materialización de cada amenaza y por cada dimensión, se procede a definir el impacto el cual viene a ser el tanto por ciento del valor del activo que se disipa en caso la amenaza se materialice, según los criterios de la siguiente tabla:

Tabla 38.

*Escala de valoración del impacto de los activos.*

Valor en %	Convección	Descripción
valor > 80%	Muy Alto (MA)	Cuando la amenaza llegara a ocurrir, ocasionaría muy altas consecuencias en la Organización.
60% < valor < 80%	Alto (A)	Si la amenaza llegara a ocurrir, esta ocasionaría consecuencias altas en la Organización.
40% < valor < 60%	Medio (M)	Si la amenaza ocurriera, esta ocasionaría consecuencias medianas en la Organización.
20% < valor < 40%	Bajo (B)	Si la amenaza ocurriera, ocasionaría un bajo impacto en la Organización.
valor < 20%	Muy Bajo (MB)	Si la amenaza ocurriera, ocasionaría consecuencias mínimas en la Organización.

*Nota:* Se valoriza el impacto de las amenazas en caso la amenaza se materialice. Fuente: Elaboración Propia.

La siguiente tabla realizaremos el análisis de riesgos de los activos, los cuales se encuentran determinados por el impacto potencial por cada activo según el análisis realizado por cada una de las amenazas. Este análisis nos consentirá priorizar el plan de acción y la selección de las medidas de control.

Como valor final para los activos, se toma el valor más alto de los tres dominios y el de la frecuencia, para referenciar al activo y conocer su impacto potencial dentro de la organización.

$$\text{Impacto Potencial} = \text{Criticidad} \times \% \text{Impacto}$$

Tabla 39:

*Impacto Potencial.*

Ámbito	Activo	Criticidad			% Impacto			Impacto Potencial		
		C	I	D	C	I	D	C	I	D
[D.1]	Registros de actividades de software	3	4	3	60%	60%	70%	1.8	2.4	2.1
[D.2]	Información de Desarrollo Humano	7	7	6	40%	40%	50%	2.8	2.8	3
[D.3]	Información de Administración y Finanzas	8	8	7	60%	70%	70%	4.8	5.6	4.9
[D.4]	Información de Control de Proyectos Constructivos	10	10	8	60%	80%	70%	6	8	5.6
[D.5]	Información de Control de Calidad	8	8	7	70%	90%	70%	5.6	7.2	4.9



[D.6]	Información de Equipos	7	7	6	50 %	60 %	60 %	3.5	4.2	3.6
[D.7]	Información de Desarrollo Sostenible	8	8	8	60 %	60 %	80 %	4.8	4.8	6.4
[D.8]	Copias de Respaldo	10	10	10	60 %	90 %	90 %	6	9	9
[D.9]	Archivos de Datos de Configuración	6	6	6	30 %	40 %	40 %	1.8	2.4	2.4
[D.10]	Archivos de Contraseñas	8	6	8	40 %	30 %	40 %	3.2	1.8	3.2
[K.1]	Resguardo de la Información	8	8	8	50 %	50 %	50 %	4	4	4
[K.2]	Resguardo de las comunicaciones	8	8	6	40 %	40 %	40 %	3.2	3.2	2.4
[K.3]	Cifrado de soportes de la información	10	10	8	50 %	50 %	60 %	5	5	4.8
[S.1]	Canal de internet	10	10	9	50 %	60 %	70 %	5	6	6.3
[S.2]	Correo electrónico	10	10	10	30 %	30 %	40 %	3	3	4
[S.3]	Acceso remoto a usuario local	8	8	8	20 %	30 %	30 %	1.6	2.4	2.4
[SW.1]	Navegadores WEB	8	8	7	50 %	40 %	50 %	4	3.2	3.5
[SW.2]	Sistemas Operativos	8	9	8	40 %	60 %	60 %	3.2	5.4	4.8
[SW.3]	Aplicativos de ofimática	6	6	4	30 %	30 %	30 %	1.8	1.8	1.2

[SW.4]	Cientes de correo electrónico	10	8	8	40 %	60 %	60 %	4	4.8	4.8
[SW.5]	Gestor de máquinas virtuales	8	8	6	30 %	40 %	40 %	2.4	3.2	2.4
[SW.6]	Sistema de BD	10	10	8	40 %	80 %	80 %	4	8	6.4
[SW.7]	Sistema de gestión de backups	9	9	9	50 %	70 %	80 %	4.5	6.3	7.2
[SW.7]	Sistema de referenciación geográfica	5	5	5	50 %	60 %	70 %	2.5	3	3.5
[SW.8]	Sistema de pagos asociados	9	9	9	60 %	70 %	80 %	5.4	6.3	7.2
[SW.9]	Aplicativo para el diseño de arquitectura, mecánico y la cartografía	3	3	3	30 %	40 %	40 %	0.9	1.2	1.2
[SW.10]	Antivirus	9	9	9	40 %	50 %	50 %	3.6	4.5	4.5
[SW.11]	Desarrollo de Software a medida subcontratado	9	9	9	50 %	70 %	80 %	4.5	6.3	7.2
[HD.1]	Servidor	10	10	10	70 %	60 %	80 %	7	6	8
[HD.2]	Computador de escritorio	6	6	6	60 %	40 %	60 %	3.6	2.4	3.6

[HD.3]	Computador portátil (laptop)	6	6	6	60 %	40 %	60 %	3.6	2.4	3.6
[HD.4]	Móviles / Radios de comunicación	6	6	6	20 %	40 %	50 %	1.2	2.4	3
[HD.5]	DRONES	8	8	8	30 %	30 %	70 %	2.4	2.4	5.6
[HD.6]	Periféricos (Impresoras, escáneres, proyectores, etc.)	3	3	3	20 %	20 %	40 %	0.6	0.6	1.2
[HD.7]	Servidores de respaldo (backup)	10	10	9	60 %	50 %	70 %	6	5	6.3
[HD.8]	Router	8	8	8	50 %	50 %	50 %	4	4	4
[HD.9]	Switch	8	8	8	50 %	50 %	50 %	4	4	4
[HD.10]	Módems	6	6	6	30 %	40 %	40 %	1.8	2.4	2.4
[HD.11]	Puntos de acceso inalámbrico	6	6	6	20 %	20 %	20 %	1.2	1.2	1.2
[HD.12]	Antenas de comunicación	6	6	6	10 %	20 %	20 %	0.6	1.2	1.2
[SINF.1]	Discos virtuales	6	6	6	40 %	30 %	40 %	2.4	1.8	2.4
[SINF.2]	Memorias USB	3	3	3	10 %	10 %	10 %	0.3	0.3	0.3
[SINF.3]	Discos duros externos	6	5	5	20 %	20 %	20 %	1.2	1	1

[EAUX.1 ]	Equipos de alimentación eléctrica	3	1	3	10%	10%	20%	0.3	0.1	0.6
[EAUX.2 ]	UPS	3	1	3	0%	0%	20%	0	0	0.6
[EAUX.3 ]	Equipo de aire acondicionado	3	1	3	0%	0%	20%	0	0	0.6
[EAUX.4 ]	Cableado eléctrico	3	1	3	0%	0%	20%	0	0	0.6
[EAUX.5 ]	Cableado de comunicaciones (UTP)	3	1	3	0%	0%	20%	0	0	0.6
[COM.1]	Comunicaciones de Radio	4	4	4	40%	60%	60%	1.6	2.4	2.4
[COM.2]	Redes inalámbricas	7	7	7	50%	50%	50%	3.5	3.5	3.5
[COM.3]	Telefonía móvil	7	7	7	40%	30%	50%	2.8	2.1	3.5
[COM.4]	Redes LAN	7	7	7	50%	50%	50%	3.5	3.5	3.5
[COM.5]	Internet	8	8	8	40%	60%	60%	3.2	4.8	4.8
[L.1]	Oficinas - Moquegua	4	4	4	50%	40%	80%	2	1.6	3.2
[L.2]	Oficinas - Campamento Minero	4	4	4	50%	50%	80%	2	2	3.2
[L.3]	Conteiner	4	4	4	60%	50%	80%	2.4	2	3.2
[L.4]	Equipos móviles terrestres (camionetas, volquetes,	4	4	4	60%	50%	80%	2.4	2	3.2

	equipos de línea amarilla)									
	Plantas operativas (concreto, asfalto, etc.)									
[L.5]		7	7	7	60 %	60 %	80 %	4.2	4.2	5.6
[P.1]	Usuarios Externos	5	5	5	40 %	50 %	40 %	2	2.5	2
[P.2]	Usuarios internos	8	8	8	60 %	50 %	80 %	4.8	4	6.4
[P.4]	Proveedores	8	8	8	40 %	50 %	80 %	3.2	4	6.4
[P.5]	Sub Contratistas	5	5	5	40 %	50 %	70 %	2	2.5	3.5
[P.6]	Clientes	8	8	8	40 %	40 %	50 %	3.2	3.2	4
[P.7]	Administradores de los Sistemas de información	8	8	8	50 %	40 %	70 %	4	3.2	5.6

*Nota:* Evaluación del impacto potencial de los activos. Fuente: Elaboración Propia.

### 3.3.4.5. Análisis de riesgos.

Para la estimación del riesgo potencial, se realizó una combinación entre el impacto y la frecuencia, detallada en la tabla número 40:

Tabla 40.

*Cálculo de estimación del riesgo.*

Riesgo		Impacto					
		Muy alto 100	Alto 80	Medio 60	Bajo 40	Muy bajo 10	
FRECUENCIA	Muy Alta (MA)	1	100.0	80.0	60.0	40.0	10.0
	Alta (A)	0.033	3.30	2.64	1.98	1.32	0.33

Media (M)	0.011	1.10	0.88	0.66	0.44	0.11
Baja (B)	0.005	0.50	0.40	0.30	0.20	0.05
Muy Baja (MB)	0.003	0.30	0.24	0.18	0.12	0.03

*Nota:* Se determina los valores para la evaluación del riesgo. Fuente: Elaboración Propia.

En la tabla 41 se observa las zonas de riesgo obtenidas en relación entre el impacto y frecuencia:

Tabla 41.

*Zona de Riesgo.*

<b>Descripción</b>	<b>Escala</b>
Muy Alta (MA)	valor > 1.98
Alta (A)	0.66 < valor < 1.98
Media (M)	0.24 < valor < 0.66
Baja (B)	0.12 < valor < 0.24
Muy Baja (MB)	0 < valor < 0.12

*Nota:* Se establece las zonas de riesgo según escala de valorizada.

Fuente: Elaboración Propia.

Teniendo ya deducido el impacto potencial se podrá calcular el riesgo potencial relacionado, para ello se debe tener en cuenta la periodicidad con la que se puede ocasionar, haciendo uso de los rangos definidos en la tabla 41.

$$Riesgo = Frecuencia \times Impacto$$

En la siguiente tabla 42, describiremos los procesos de Colvias SAC, involucrados en la evaluación del riesgo.

Tabla 42.

*Descripción de procesos de Colvias SAC.*

	<b>Proceso</b>	<b>Sub proceso</b>
<b>PROCESOS ESTRATÉGICOS</b>	Gestión de Direcciónamiento Estratégico (GDE)	-
		Seguridad
		Salud Ocupacional
	Gestión de Desarrollo Sostenible (GDS)	Medio Ambiente
		Anti-Soborno
	RSE	
<b>PROCESOS MISIONALES</b>	Gestión Comercial (GC)	-
		Ejecución de Proyectos
	Gestión Técnica (GT)	Administración y Alquiler de Equipos
		Control de Calidad
<b>PROCESOS DE SOPORTE</b>	Gestión de Desarrollo Humano (GDH)	Administración de Personal Desarrollo de Calidad de Vida y Bienestar
	Gestión de Control de Proyectos (GCP)	-
	Gestión Legal (GL)	-
	Gestión Contable y Tributaria (GCT)	-
	Gestión Administrativa y Financiera (GAF)	Tecnología de la Información
		Compras

## Inventarios

---

Fuente: Colvias S.A.C.



Tabla 43.

*Evaluación del Riesgo Potencial de los activos.*

Ámbito	Proceso asociado	Activo	Responsable del activo	Frecuencia	Impacto Potencial			Riesgo Potencial		
					C	I	D	C	I	D
[D.1]	GDE, GDS, GC, GT, GDH, GCP, GCT y GAF	Registros de actividades de software	Coordinador de TI	1	1.8	2.4	2.1	1.80	2.40	2.10
[D.2]	GDH y GL	Información de Desarrollo Humano	Coordinador de RR.HH	1	2.8	2.8	3	2.80	2.80	3.00
[D.3]	GDE, GAF, GDS, GC, GL y GT	Información de Administración y Finanzas	Jefe Administrativo de Obra	1	4.8	5.6	4.9	4.80	5.60	4.90
[D.4]	GCP, GC, GAF y GT	Información de Control de Proyectos Constructivos	Jefe de Control de Proyectos	1	6	8	5.6	6.00	8.00	5.60

[D.5]	GT, GDE	Información de Control de Calidad	Jefe de Control de Calidad	1	5.6	7.2	4.9	5.60	7.20	4.90
[D.6]	GT, GDS, GDE y GAF	Información de Equipos	Coordinador de Equipos	1	3.5	4.2	3.6	3.50	4.20	3.60
[D.7]	GDE, GDS, GDH, GT, GL y GAF	Información de Desarrollo Sostenible	Director de Desarrollo Sostenible	1	4.8	4.8	6.4	4.80	4.80	6.40
[D.8]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Copias de Respaldo	Coordinador de TI	1	6	9	9	6.00	9.00	9.00
[D.9]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Archivos de Datos de Configuración	Coordinador de TI	1	1.8	2.4	2.4	1.80	2.40	2.40
[D.10]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Archivos de Contraseñas	Coordinador de TI	1	3.2	1.8	3.2	3.20	1.80	3.20

[K.1]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Resguardo de la Información	Coordinador de TI	1	4	4	4	4.00	4.00	4.00
[K.2]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Resguardo de las comunicaciones	Coordinador de TI	1	3.2	3.2	2.4	3.20	3.20	2.40
[K.3]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Cifrado de soportes de la información	Coordinador de TI	1	5	5	4.8	5.00	5.00	4.80
[S.1]	GAF	Canal de internet	Coordinador de TI	1	5	6	6.3	5.00	6.00	6.30
[S.2]	GAF	Correo electrónico	Coordinador de TI	1	3	3	4	3.00	3.00	4.00
[S.3]	GDE, GDS, GC, GT, GDH,	Acceso remoto a usuario local	Coordinador de TI	1	1.6	2.4	2.4	1.60	2.40	2.40

	GL, GCP, GCT y GAF										
[SW.1]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Navegadores WEB	Coordinador de TI	1	4	3.2	3.5	4.00	3.20	3.50	
[SW.2]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Sistemas Operativos	Coordinador de TI	1	3.2	5.4	4.8	3.20	5.40	4.80	
[SW.3]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Aplicativos de ofimática	Coordinador de TI	1	1.8	1.8	1.2	1.80	1.80	1.20	
[SW.4]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Clientes de correo electrónico	Coordinador de TI	1	4	4.8	4.8	4.00	4.80	4.80	
[SW.5]	GAF	Gestor de máquinas virtuales	Coordinador de TI	1	2.4	3.2	2.4	2.40	3.20	2.40	

[SW.6]	GAF	Sistema de BD	Coordinador de TI	1	4	8	6.4	4.00	8.00	6.40
[SW.7]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Sistema de gestión de backups	Coordinador de TI	1	4.5	6.3	7.2	4.50	6.30	7.20
[SW.8]	GDS, GT, GAF y GCP	Sistema de referenciación geográfica	Coordinador de Oficina Técnica	1	2.5	3	3.5	2.50	3.00	3.50
[SW.9]	GAF, GCT, GDE y GC	Sistema de pagos asociados	Jefe Administrativo de Obra	1	5.4	6.3	7.2	5.40	6.30	7.20
[SW.10]	GDS, GT, GAF y GCP	Aplicativo para el diseño de arquitectura, mecánico y la cartografía	Coordinador de Oficina Técnica	1	0.9	1.2	1.2	0.90	1.20	1.20
[SW.11]	GAF	Antivirus	Coordinador de TI	1	3.6	4.5	4.5	3.60	4.50	4.50

[SW.12]	GC y GAF	Desarrollo de Software a medida subcontratado	Coordinador de TI	1	4.5	6.3	7.2	4.50	6.30	7.20
[HD.1]	GAF	Servidor	Coordinador de TI	1	7	6	8	7.00	6.00	8.00
[HD.2]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Computador de escritorio	Jefe Administrativo de Obra	1	3.6	2.4	3.6	3.60	2.40	3.60
[HD.3]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Computador portátil (laptop)	Jefe Administrativo de Obra	1	3.6	2.4	3.6	3.60	2.40	3.60
[HD.4]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Móviles / Radios de comunicación	Jefe Administrativo de Obra	1	1.2	2.4	3	1.20	2.40	3.00
[HD.5]	GDS, GT, GAF y GCP	DRONES	Ingeniero de Topografía	1	2.4	2.4	5.6	2.40	2.40	5.60

[HD.6]	GDS, GC, GT, GDH, GCP, GCT y GAF	Periféricos (Impresoras, escáneres, proyectores, etc.)	Coordinador de TI	1	0.6	0.6	1.2	0.60	0.60	1.20
[HD.7]	GAF	Servidores de respaldo (backup)	Coordinador de TI	1	6	5	6.3	6.00	5.00	6.30
[HD.8]	GAF	Router	Coordinador de TI	1	4	4	4	4.00	4.00	4.00
[HD.9]	GAF	Switch	Coordinador de TI	1	4	4	4	4.00	4.00	4.00
[HD.10]	GAF	Módems	Coordinador de TI	1	1.8	2.4	2.4	1.80	2.40	2.40
[HD.11]	GAF	Puntos de acceso inalámbrico	Coordinador de TI	1	1.2	1.2	1.2	1.20	1.20	1.20
[HD.12]	GAF	Antenas de comunicación	Coordinador de TI	1	0.6	1.2	1.2	0.60	1.20	1.20
[SINF.1]	GAF	Discos virtuales	Coordinador de TI	1	2.4	1.8	2.4	2.40	1.80	2.40

[SINF.2]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Memorias USB	Coordinador Administrativo e inventarios	1	0.3	0.3	0.3	0.30	0.30	0.30
[SINF.3]	GAF	Discos duros externos	Coordinador de TI	1	1.2	1	1	1.20	1.00	1.00
[EAUX.1]	GAF	Equipos de alimentación eléctrica	Coordinador Administrativo e inventarios	1	0.3	0.1	0.6	0.30	0.10	0.60
[EAUX.2]	GAF	UPS	Coordinador de TI	1	0	0	0.6	0.00	0.00	0.60
[EAUX.3]	GAF	Equipo de aire acondicionado	Coordinador Administrativo e inventarios	1	0	0	0.6	0.00	0.00	0.60
[EAUX.4]	GAF	Cableado eléctrico	Coordinador Administrativo e inventarios	1	0	0	0.6	0.00	0.00	0.60
[EAUX.5]	GAF	Cableado de comunicaciones (UTP)	Coordinador de TI	1	0	0	0.6	0.00	0.00	0.60



[COM.1]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Comunicaciones de Radio	Coordinador de TI	1	1.6	2.4	2.4	1.60	2.40	2.40
[COM.2]	GAF	Redes inalámbricas	Coordinador de TI	1	3.5	3.5	3.5	3.50	3.50	3.50
[COM.3]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Telefonía móvil	Jefe Administrativo de Obra	1	2.8	2.1	3.5	2.80	2.10	3.50
[COM.4]	GAF	Redes LAN	Coordinador de TI	1	3.5	3.5	3.5	3.50	3.50	3.50
[COM.5]	GAF	Internet	Coordinador de TI	1	3.2	4.8	4.8	3.20	4.80	4.80
[L.1]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Oficinas - Moquegua	Jefe Administrativo de Obra	1	2	1.6	3.2	2.00	1.60	3.20

[L.2]	GDE, GDS, GC, GT, GDH, GL, GCP, GCT y GAF	Oficinas - Campamento Minero	Jefe Administrativo de Obra	1	2	2	3.2	2.00	2.00	3.20
[L.3]	GDS, GC, GT, GDH, GCP, GCT y GAF	Container	Jefe Administrativo de Obra	1	2.4	2	3.2	2.40	2.00	3.20
[L.4]	GDS, GC, GT, GDH, GCP, GCT y GAF	Equipos móviles terrestres (camionetas, volquetes, equipos de línea amarilla)	Coordinador de Equipos	1	2.4	2	3.2	2.40	2.00	3.20
[L.5]	GDS, GC, GT, GDH, GCP, GCT y GAF	Plantas operativas (concreto, asfalto, etc.)	Jefe de Planta	1	4.2	4.2	5.6	4.20	4.20	5.60
[P.1]	GDS, GC, GT, GDH, GCP, GCT y GAF	Usuarios Externos	Jefe Administrativo de Obra	1	2	2.5	2	2.00	2.50	2.00

[P.2]	GDH y GL	Usuarios internos	Jefe Administrativo de Obra	1	4.8	4	6.4	4.80	4.00	6.40
[P.3]	GDH, GL, GAF y GC	Proveedores	Jefe Administrativo de Obra	1	3.2	4	6.4	3.20	4.00	6.40
[P.4]	GDH, GL, GAF y GC	Sub Contratistas	Jefe de Control de Proyectos	1	2	2.5	3.5	2.00	2.50	3.50
[P.5]	GDE, GDH, GL, GAF y GC	Clientes	Director de proyecto	1	3.2	3.2	4	3.20	3.20	4.00
[P.6]	GAF	Administradores de los Sistemas de información	Jefe Administrativo de Obra	1	4	3.2	5.6	4.00	3.20	5.60

---

*Nota:* Evaluación del riesgo potencial de los activos asociados a los procesos de la organización, identificando al responsable de los activos. Fuente: Elaboración Propia.

### 3.3.5. Fase V: Definición de Planes de Acción para mitigar los riesgos.

Habiendo realizado el análisis de dominios de la ISO / IEC 27001:2013 y su análisis de riesgo de Colvias SAC, donde se identificó los activos de la organización, posibles amenazas y el nivel de riesgo asociado a cada activo, se propone un enfoque más amplio, en donde se proyectará diferentes planes de acción que ayudara a reducir el nivel de riesgo actual identificado en las zonas Alta (A) y Muy Alta (MA) de Colvias SAC enfocados en los dominios de la ISO/IEC 27001:2013 (Anexo A) y con ello mejorar los procesos de la gestión de riesgo y sus procesos asociados a TI de la organización.

Para los riesgos ubicados en las zonas Muy Baja (MB), Baja (B) y Media (M), se recomienda aceptarlos bajo una constante monitorización continua de los mismos y una revisión periódica de los niveles de impacto y probabilidad ante algún cambio en la organización en la cual se puedan ver afectos.

En la tabla 44 se detalla los planes de acción con los que se espera mejorar el estado de seguridad de la información enfocado en el análisis de riesgos de la ISO / IEC 27001:2013 (Anexo A):

Tabla 44.

*Planes de acción propuestos enfocados en los dominios de la ISO / IEC 27001:2013.*

<b>Plan de acción</b>	<b>Ítem Dominio</b>	<b>Descripción</b>
Plan de Acción 01.	A.5	Mejora de la Política de Seguridad de la información.
Plan de Acción 02.	A.7	Entrenamiento continuo para formar a los trabajadores en materia de seguridad de la información.

Plan de Acción 03.	A.7 / A.8	Mejorar los procedimientos de RR.HH.
Plan de Acción 04.	A.8 / A.11	Mejora en la gestión de los activos.
Plan de Acción 05.	A.9 / A.12	Monitorización de los programas informáticos. Protección de la información
Plan de Acción 06.	A.10	mediante mecanismos Criptográficos.
Plan de Acción 07.	A.12 / A.14	Instalación y mantenimiento del Software.
Plan de Acción 08.	A.14	Mejora en el Desarrollo y/o mantenimiento de sistemas informáticos.
Plan de Acción 09.	A.14 / A.13 / A.6	Mejora en los requerimientos de Seguridad y comunicación.
Plan de Acción 10.	A.15	Mejora de la seguridad en relación con los proveedores.
Plan de Acción 11.	A.16	Mejora en la gestión de incidentes de Seguridad de la Información.
Plan de Acción 12.	A.17	Plan de continuidad del negocio.
Plan de Acción 13.	A.18	Revisión de la Seguridad de la información.

*Nota:* Descripción breve de los planes de acción según dominio del Anexo “A” – ISO/IEC 27001:2013. Fuente: Elaboración Propia.

En las siguientes tablas se describen los planes de acción con los cuales se mejorará el estado de seguridad de la información enfocado en la ISO / IEC 27001:2013 (Anexo A):

Tabla 45.

*Plan de Acción 01 - Mejora de la Política de Seguridad de la información.*

<b>PLAN DE ACCIÓN 01</b>	<b>Mejora de la Política de Seguridad de la información</b>
Objetivo	Implementar una política de seguridad de la información para Colvias SAC.
Descripción	<p>Colvias SAC, deberá de desarrollar una política de seguridad de la información, la cual debe permitir mejorar a un mayor nivel la seguridad de la información dentro de la organización.</p> <p>Esta política deberá ser aprobada por la Alta Dirección de la organización, asimismo deberá de ser difundida a todos los empleados de Colvias SAC.</p> <p>Toda política será revisada como mínimo una vez por año en la vida de la organización para asegurar una mejora continua de la misma.</p>
Ámbito y Activos afectados a reducción del riesgo	<p>[D] Datos: Todos los activos</p> <p>[S] Servicios: Todos los activos</p> <p>[SW] Software: Todos los activos</p> <p>[HD] Hardware: Todos los activos</p> <p>[SINF] Soportes de información: Todos los activos</p> <p>[EAUX] Equipos auxiliares: Todos los activos</p> <p>[COM] Redes de comunicación: Todos los activos</p> <p>[L] infraestructura Física: Todos los activos</p> <p>[P] Recurso Humano: Todos los activos</p>
Dimensiones de seguridad de los activos afectados a reducción del riesgo	<p>Confidencialidad [C]</p> <p>Integridad [I]</p> <p>Disponibilidad [D]</p>

Responsables	Coordinador de TI Alta Gerencia
Controles ISO/IEC 27001:2013	A.5.1.1 A.5.1.2
Coste	Horas Hombre de dedicación del coordinador de TI Horas Hombre del equipo de la alta dirección Publicación y Difusión S/ 400
Duración	2 semanas

---

Fuente: Elaboración Propia.

Tabla 46.

*Plan de Acción 02 - Entrenamiento continuo para formar a los trabajadores en materia de seguridad de la información.*

---

<b>PLAN DE ACCIÓN 02</b>	<b>Entrenamiento continuo para formar a los trabajadores en materia de seguridad de la información</b>
Objetivo	Formar a los empleados de Colvias SAC en materia de Seguridad de la Información.
Descripción	Colvias SAC, deberá concretar un programa de formación en materia de seguridad de la información a todos sus trabajadores. Esta formación tiene como finalidad brindar conocimientos respecto a las normas y principios básicos de seguridad de la información, aplicables en Colvias SAC, mejorando el uso de los activos de información. Como responsable de la formación será el encargado de TI, a través de plataformas virtuales y/o en oficinas de la ciudad de Moquegua. Cada año se actualizará el programa de capacitación

---

---

	<p>en materia de Seguridad de la información, asimismo el responsable de TI sensibilizara a los empleados mediante artículos informativos vía correo electrónico corporativo en temas respecto a seguridad de la información.</p> <p>[D] Datos: Todos los activos</p> <p>[S] Servicios: Todos los activos</p> <p>[SW] Software: Todos los activos</p> <p>[HD] Hardware: Todos los activos</p> <p>[SINF] Soportes de información: Todos los activos</p> <p>[EAUX] Equipos auxiliares: Todos los activos</p> <p>[COM] Redes de comunicación: Todos los activos</p> <p>[L] infraestructura Física: Todos los activos</p> <p>[P] Recurso Humano: Todos los activos</p>
<p>Ámbito y Activos afectos a reducción del riesgo</p>	
<p>Dimensiones de seguridad de los activos afectos a reducción del riesgo</p>	<p>Confidencialidad [C]</p> <p>Integridad [I]</p> <p>Disponibilidad [D]</p>
<p>Responsables</p>	<p>Coordinador de TI</p> <p>Coordinador de RR.HH</p>
<p>Controles ISO/IEC 27001:2013</p>	<p>A.7.2.2</p>
<p>Coste</p>	<p>Horas Hombre de dedicación del coordinador de Tecnología de la Información en entrenamiento a los empleados</p> <p>Horas Hombre de entrenamiento de los empleados quienes no estén en operaciones</p> <p>Afiches de sensibilización / Plataforma TEAM / Plataforma Zoom S/. 450</p>

---



Duración	4 semanas, en el que se impartirá dos cursos de 2 horas cada uno.
----------	---

Fuente: Elaboración Propia.

Tabla 47.

*Plan de Acción 03 - Mejora de los procedimientos de RR.HH.*

<b>PLAN DE ACCIÓN 03</b>	<b>Mejora los procedimientos de RR.HH</b>
Objetivo	<p>Colvias SAC deberá de mejorar los procedimientos de RR.HH, proceso de selección, contratación y hasta su culminación del vínculo laboral.</p> <p>Colvias SAC, deberá de mejorar sus lineamientos de los procedimientos a cargo de RR.HH, debiendo tener en cuenta lo siguiente:</p> <ul style="list-style-type: none"> <li>- Mejorar el proceso de reclutamiento de empleados.</li> <li>- Definir los perfiles de cargo de la organización.</li> <li>- Al momento de la vinculación de personal se definirá en el contrato las responsabilidades y condiciones en materia de seguridad de la información de los trabajadores</li> </ul>
Descripción	<ul style="list-style-type: none"> <li>- En el RIT se deberá establecer las sanciones disciplinarias a seguir en caso de que algún empleado incumpla con la política o normas de seguridad de información de la organización.</li> <li>- El procedimiento se deberá de mejorar teniendo en cuenta las acciones a seguir, cuando un trabajador abandone la organización por voluntad propia, por despido y/o culminación del vínculo laboral. En este documento se describirá tanto el proceso de devolución y/o revocación de los activos informáticos de la organización que haya estado usando el trabajador.</li> </ul>

Ámbito y	[D] Datos: Todos los activos
Activos afectos a reducción del riesgo	[HD] Hardware: [HD.2] [HD.3] [HD.5] [HD.8] [SINF] Soportes de información: [SINF.1] [L] infraestructura Física: Todos los activos [P] Recurso Humano: [P.2] y [P.3]
Dimensiones de seguridad de los activos afectos a reducción del riesgo	Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsables	Coordinador de TI Coordinador Administrativo e inventarios A.7.1.1
Controles	A.7.1.2
ISO/IEC	A.7.2.1
27001:2013	A.7.2.3 A.7.3.1
Coste	Horas Hombre del coordinador de TI Horas Hombre del personal de administración.
Duración	4 semanas

---

Fuente: Elaboración Propia.

Tabla 48.

Plan de acción 04 - Mejora en la gestión de los activos.

---

<b>PLAN DE ACCIÓN 04</b>	<b>Mejora en la gestión de los activos</b>
Objetivo	Colvias SAC, deberá mejorar la gestión de los activos, definiendo las nociones precisas de todos los activos que posee Colvias SAC, así como también

	definir las responsabilidades de protección adecuadas.
Descripción	<p>Colvias SAC realizó la identificación de los activos en la fase 3; por lo que se deberá de asignar a cada activo un propietario, asimismo deberán de estar codificados.</p> <p>Colvias SAC debe establecer un procedimiento en el que se expliquen las reglas para un correcto uso de los activos, también el proceso a seguir si un empleado necesita manipular un activo o retirarlo fuera de las instalaciones de la organización. Este procedimiento debe ser difundido dentro de la organización.</p>
Ámbito y Activos afectos a reducción del riesgo	<p>[D] Datos: Todos los activos</p> <p>[S] Servicios: Todos los activos</p> <p>[SW] Software: Todos los activos</p> <p>[HD] Hardware: Todos los activos</p> <p>[SINF] Soportes de información: Todos los activos</p> <p>[EAUX] Equipos auxiliares: Todos los activos</p> <p>[COM] Redes de comunicación: Todos los activos</p> <p>[L] Infraestructura Física: Todos los activos</p>
Dimensiones de seguridad de los activos afectos a reducción del riesgo	<p>Confidencialidad [C]</p> <p>Integridad [I]</p> <p>Disponibilidad [D]</p>
Responsables	Coordinador de TI
Controles ISO/IEC 27001:2013	<p>A.8</p> <p>A.11.2.1</p>

	A.11.2.5
	A.11.2.6
Coste	Horas Hombre del coordinador de TI
Duración	3 Semanas

---

Fuente: Elaboración Propia.

Tabla 49.

*Plan de Acción 05 - Monitorización de los programas informáticos.*

<b>PLAN DE ACCIÓN 05</b>	<b>Monitorización de los programas informáticos</b>
Objetivo	Colvias SAC, deberá de controlar todos los programas informáticos con el fin de materialización de las potenciales amenazas.
Descripción	Colvias SAC debe de mejorar las reglas de seguridad para un mejor seguimiento de los programas de información de la organización. Implementar nuevas soluciones (procedimientos - documentados) para proteger los registros obtenidos de la monitorización de accesos no autorizados o alteraciones.
Ámbito y Activos afectados a reducción del riesgo	[D] Datos: Todos los activos [S] Servicios: Todos los activos [SW] Software: Todos los activos [COM] Redes de comunicación: Todos los activos [L] Infraestructura Física: Todos los activos
Dimensiones de seguridad de los activos afectados a reducción del riesgo	Confidencialidad [C] Integridad [I] Disponibilidad [D]

Responsables	Coordinador de TI
	A.6
Controles	A.12.4
ISO/IEC	A.9.4.2
27001:2013	A.9.4.5
	A.17
Coste	Horas Hombre del coordinador de TI
Duración	2 semanas

---

Fuente: Elaboración Propia.

Tabla 50:

*Plan de Acción 06 - Protección de la información mediante mecanismos Criptográficos.*

<b>PLAN DE ACCIÓN 06</b>	<b>Protección de la información mediante mecanismos Criptográficos</b>
Objetivo	Colvias SAC debe asegurar el uso adecuado de la criptografía de los sistemas de la organización protegiendo la autenticidad y/o integridad de la información.
Descripción	Colvias SAC, Implementará procedimientos que ayude a mejorar los controles criptográficos para los servidores de la organización que alojen información vital, además para los discos duros de los equipos y/o externos también se deberá de implementar controles criptográficos asegurando la autenticidad, confidencialidad e integridad de la información.
Ámbito y Activos afectados a	[D] Datos: Todos los activos

reducción del  
riesgo

Dimensiones de  
seguridad de los  
activos afectos a  
reducción del  
riesgo

Confidencialidad [C]  
Integridad [I]

Responsables      Coordinador de TI

Controles  
ISO/IEC  
27001:2013

A.10.1.1  
A.10.1.2

Coste                      Horas Hombre del coordinador de TI

Duración                3 semanas

---

Fuente: Elaboración Propia.

Tabla 51.

*Plan de Acción 07 – Instalación y mantenimiento de Software.*

---

<b>PLAN DE ACCIÓN 07</b>	<b>Instalación y mantenimiento de Software</b>
Objetivo	Colvias SAC debe, mantener actualizado los equipos informáticos en sus últimas versiones del SW, asimismo se debe evitar las posibles amenazas a consecuencia de programas maliciosos.

Descripción	<p>Colvias SAC, debe mejorar los mecanismos de control que impidan la manipulación del SW deliberadamente por parte de los usuarios.</p> <p>Colvias SAC, debe implementar un programa de revisiones periódicas de los programas instalados en los activos informáticos de los trabajadores.</p> <p>Definir los controles necesarios que permitan comprobar la existencia de nuevas actualizaciones de los programas, así se puedan instalar de manera automática en los equipos informáticos de los empleados.</p>
Ámbito y Activos afectos a reducción del riesgo	<p>Datos [D]: [D.1] y [D.6]</p> <p>[SW]: Todos los Activos</p>
Dimensiones de seguridad de los activos afectos a reducción del riesgo	<p>Confidencialidad [C]</p> <p>Integridad [I]</p> <p>Disponibilidad [D]</p>
Responsables	Coordinador de TI
Controles ISO/IEC 27001:2013	<p>A.12.2.1</p> <p>A.12.5.1</p> <p>A.12.6.1</p> <p>A.12.6.2</p>
Coste	<p>Horas Hombre del coordinador de TI</p> <p>Licencias de Software \$. 600.00</p>
Duración	5 semanas

---

Fuente: Elaboración Propia.

Tabla 52.

*Plan de Acción 08 – Mejora en el Desarrollo y/o mantenimiento de sistemas informáticos.*

<b>PLAN DE ACCIÓN 08</b>	<b>Mejora en el Desarrollo y/o mantenimiento de sistemas informáticos</b>
Objetivo	Colvias SAC deberá definir mecanismos de seguridad para el desarrollo de SW a realizarse en la organización
Descripción	<p>Actualmente Colvias SAC no desarrolla software propio, sin embargo, es necesario establecer un procedimiento para el desarrollo de software en la organización que puedan darse posteriormente.</p> <p>Asimismo, los cambios del SW deberán de ser controlados.</p> <p>Todo trabajador deberá de conocer los principios para el desarrollo de SW seguro, asegurando su seguridad.</p>
Ámbito y Activos afectos a reducción del riesgo	Software [SW]: [SW.1]
Dimensiones de seguridad de los activos afectos a reducción del riesgo	Confidencialidad [C] Integridad [I]
Responsables	Coordinador de TI
Controles ISO/IEC 27001:2013	A.14.2
Coste	Horas Hombre del coordinador de TI



Duración 3 semanas

Fuente: Elaboración Propia.

Tabla 53.

*Plan de Acción 09 – Mejora en los requerimientos de Seguridad y comunicación.*

<b>PLAN DE ACCIÓN 09</b>	<b>Mejora en los requerimientos de Seguridad y comunicación</b>
Objetivo	Colvias SAC deberá de identificar los requerimientos de seguridad de la información pertinentes para los proyectos que se ejecuten dentro de la organización y también deberá de resguardar la información que se trasmite por la red de comunicación de la organización.
Descripción	Colvias SAC deberá de analizar los requisitos de seguridad de la información para los programas existentes en la organización y también para los nuevos programas que se puedan necesitar. Definir controles que permitan resguardar las comunicaciones y transacciones que se realicen por las redes internas como en las publicas
Ámbito y Activos afectos a reducción del riesgo	Redes de comunicación [COM] : Todos los activos Servicios [S] : Todos los activos Datos [D] : Todos los activos
Dimensiones de seguridad de los activos afectos a reducción del riesgo	Confidencialidad [C] Integridad [I] Disponibilidad [D]

Responsables	Coordinador de TI
Controles ISO/IEC 27001:2013	A.13.1
	A.13.2
	A.14.1
Coste	Horas Hombre del coordinador de TI
Duración	3 semanas

Fuente: Elaboración Propia.

Tabla 54.

*Plan de Acción 10 – Mejora de la seguridad en las relaciones con los proveedores.*

<b>PLAN DE ACCIÓN 10</b>	<b>Mejora de la seguridad en relación con los proveedores</b>
Objetivo	Colvias SAC, debe comprobar que los proveedores dispongan un nivel de seguridad aceptable en sus servicios que ofrecen a la organización, así como también la organización debe garantizar el resguardo de los activos que sean accesibles por los proveedores
Descripción	Colvias S.A.C debe realizar la comprobación de implementación de los convenios con los proveedores. Verificar que el servicio ofrecido por el proveedor es el pactado.
Ámbito y Activos afectos a reducción del riesgo	Redes de comunicación [COM] : Todos los activos Servicios [S] : Todos los activos Datos [D] : Todos los activos
Dimensiones de seguridad de los activos afectos a	Confidencialidad [C] Integridad [I] Disponibilidad [D]

reducción del  
riesgo

Responsables	Coordinador de TI
Controles ISO/IEC 27001:2013	A.15
Coste	Horas Hombre del coordinador de TI
Duración	2 semanas

---

Fuente: Elaboración Propia.

Tabla 55.

*Plan de Acción 11 - Mejora en la gestión de incidentes de Seguridad de la Información.*

<b>PLAN DE ACCIÓN 11</b>	<b>Mejora en la gestión de incidentes de Seguridad de la Información</b>
Objetivo	Colvias SAC debe implementar un procedimiento de notificación y actuación de incidentes de seguridad de la información, dentro de él se debe establecer el flujo de comunicación de los eventos de seguridad y sus puntos débiles.
Descripción	Colvias SAC deberá de implementar un procedimiento de notificación de incidentes de seguridad de la información. Definir responsabilidades de los empleados respecto a los incidentes de seguridad de la información. Definir el flujo de comunicación para los casos de notificación de los incidentes. Tener una BD sobre la información conocida de los incidentes de seguridad de la información para estudiarlas y posteriormente generar las lecciones

	aprendidas las cuales deben ser comunicadas a toda la organización.
	[D] Datos: Todos los activos
	[S] Servicios: Todos los activos
	[SW] Software: Todos los activos
	[HD] Hardware: Todos los activos
Ámbito y Activos afectos a reducción del riesgo	[SINF] Soportes de información: Todos los activos
	[EAUX] Equipos auxiliares: Todos los activos
	[COM] Redes de comunicación: Todos los activos
	[L] infraestructura Física: Todos los activos
	[P] Recurso Humano: Todos los activos
Dimensiones de seguridad de los activos afectos a reducción del riesgo	Confidencialidad [C]
	Integridad [I]
	Disponibilidad [D]
Responsables	Coordinador de TI
Controles ISO/IEC 27001:2013	A.16
Coste	Horas Hombre del coordinador de TI
Duración	3 semanas

Fuente: Elaboración Propia.

Tabla 56.

*Plan de Acción 12 - Plan de continuidad del negocio.*

<b>PLAN DE ACCIÓN 12</b>	<b>Plan de continuidad del negocio</b>
Objetivo	Colvias SAC debe definir un plan de contingencia para asegurar el resguardo de los procesos y actividades críticas de la organización, que se puedan ver afectos por algún evento no deseado,

---

	garantizando la continuidad del funcionamiento de la organización en un plazo aceptable.
Descripción	<p>Colvias SAC deberá desarrollar un plan de emergencia que permita la continuidad del negocio ante cualquier interrupción de las actividades de la organización.</p> <p>Para realizar este plan se debe tener en cuenta los procesos más críticos del negocio.</p>
Ámbito y Activos afectos a reducción del riesgo	<p>[D] Datos: Todos los activos</p> <p>[S] Servicios: Todos los activos</p> <p>[SW] Software: Todos los activos</p> <p>[HD] Hardware: Todos los activos</p> <p>[SINF] Soportes de información: Todos los activos</p> <p>[EAUX] Equipos auxiliares: Todos los activos</p> <p>[COM] Redes de comunicación: Todos los activos</p> <p>[L] infraestructura Física: Todos los activos</p> <p>[P] Recurso Humano: Todos los activos</p>
Dimensiones de seguridad de los activos afectos a reducción del riesgo	<p>Integridad [I]</p> <p>Disponibilidad [D]</p>
Responsables	<p>Coordinador de TI</p> <p>Dueños de los procesos</p>
Controles ISO/IEC 27001:2013	A.17.1
Coste	<p>Horas Hombre del coordinador de TI</p> <p>Horas Hombre de los dueños de procesos</p>
Duración	2 semanas

---

Fuente: Elaboración Propia.

Tabla 57.

*Plan de Acción 13 – Revisión de la Seguridad de la información.*

<b>PLAN DE ACCIÓN 13</b>	<b>Revisión de la Seguridad de la información</b>
<b>Objetivo</b>	<p>Colvias SAC debe revisar los cumplimientos de las políticas, procedimientos, normas, requisitos legales de aplicables y obligaciones contractuales relacionadas con la seguridad de la información.</p> <p>Colvias SAC debe establecer un programa de auditoria aplicable a seguridad de la información que permita tener una visión independiente del estado de la seguridad de la información en la organización.</p>
<b>Descripción</b>	<p>La frecuencia de las auditorías internas deberá de ser como mínima una vez cada año.</p> <p>El coordinador de TI y la alta dirección deben verificar el cumplimiento de los procedimientos de seguridad de la información establecidos por la organización.</p>
<b>Ámbito y Activos afectos a reducción del riesgo</b>	<p>[D] Datos: Todos los activos</p> <p>[S] Servicios: Todos los activos</p> <p>[SW] Software: Todos los activos</p> <p>[HD] Hardware: Todos los activos</p> <p>[SINF] Soportes de información: Todos los activos</p> <p>[EAUX] Equipos auxiliares: Todos los activos</p> <p>[COM] Redes de comunicación: Todos los activos</p> <p>[L] infraestructura Física: Todos los activos</p> <p>[P] Recurso Humano: Todos los activos</p>
<b>Dimensiones de seguridad de los activos afectos a reducción del riesgo</b>	<p>Integridad [I]</p> <p>Disponibilidad [D]</p> <p>Confidencialidad [C]</p>

	Coordinador de TI
<b>Responsables</b>	Auditor Interno / Externo Alta Dirección
<b>Controles</b>	
<b>ISO/IEC 27001:2013</b>	A.18
	Horas Hombre del coordinador de TI Horas Hombre de la alta dirección
<b>Coste</b>	Horas Hombre del Auditor Interno y/o externo Costos por auditoría externa \$1200.00 Costos por auditoría interna S/. 1200
<b>Duración</b>	2 semanas

---

Fuente: Elaboración Propia.

### **3.3.5.1. Planificación de los planes de acción propuestos.**

Una vez conciliados los planes de acción con la organización se procede a realizar la planificación de ejecución de los mismos, con el fin de minimizar el nivel de riesgo identificado en Colvias SAC.

Como se observa, se logrará la realización completa de todos los planes de acción en 16 semanas, teniendo como fecha de inicio 01 de abril del 2020 y finaliza el 17 de julio del 2020. Además, ha de indicar que se debe tener en cuenta que, de estas 16 semanas, las últimas 02 semanas se va a dedicar al plan de acción número 13 que es la revisión de la seguridad de la información, plan de acción en el cual se realizara una nueva revisión de los dominios de la ISO IEC 27001:2013.

En el anexo 03, se detalla el plan de ejecución de los planes de acción.

### 3.3.5.2. Análisis de resultados esperados tras la ejecución de los planes de acción.

Que teniendo como objetivo la mejora de los procesos de la gestión de riesgo disminuyendo el nivel de riesgo de los activos evaluados en la fase III, se planteó planes de acción que con la ejecución de los mismo ayudara en la mitigación de los riesgos identificados, así como también una mejora del estado de los dominios de la ISO / IEC 27001:2013, la cual le ayudara como base principal a la organización para una implementación futura de la norma.

En la siguiente tabla, mostraremos la comparación entre la situación inicial identificada en la Fase III y lo que obtuvimos tras la simulación de la ejecución de los planes de acción que se espera que logren reducir el nivel de riesgo de los activos de la organización, dentro de los procesos de gestión de riesgo.

Tabla 58.

*Situación inicial vs situación que se espera obtener tras la ejecución de los planes de acción propuestos.*

<b>Id. Domi nio</b>	<b>Ídem Proceso</b>	<b>Dominio</b>	<b>% Obtenido Fase III</b>	<b>% Obtenido Fase V (deseado)</b>
A.5	P.1, P.4, P.5	Políticas de seguridad de la información	10%	90%
A.6	P.1, P.2	Organización de seguridad de la información	27%	77%
A.7	P.5, P.2	Seguridad de recursos humanos	23%	90%



A.8	P.2, P.3	Gestión de activos	29%	82%
A.9	P.4, P.3	Control de acceso	41%	84%
A.10	P.1, P.2	Criptografía	0%	90%
A.11	P.1	Seguridad física y ambiental	29%	84%
A.12	P3, P.4	Seguridad de las operaciones	34%	87%
A.13	P.1, P.2	Seguridad en las Comunicaciones	47%	90%
A.14	P.1, P.2, P.3	Adquisición, desarrollo y mantenimiento del sistema.	23%	81%
A.15	P.1, P.2	Relaciones con los proveedores	24%	90%
A.16	P.3, P.4, P.5	Gestión de incidencias de seguridad de la información	4%	73%
A.17	P.3, P.5	Aspectos de la gestión de continuidad del negocio en seguridad de la información	0%	70%
A.18	P.4, P.1, P.5	Cumplimiento	38%	80%

*Nota:* Se muestra el porcentaje obtenido de los dominios del anexo A de la norma ISO/IEC 27001:2013 de la organización. Fuente: Elaboración Propia.

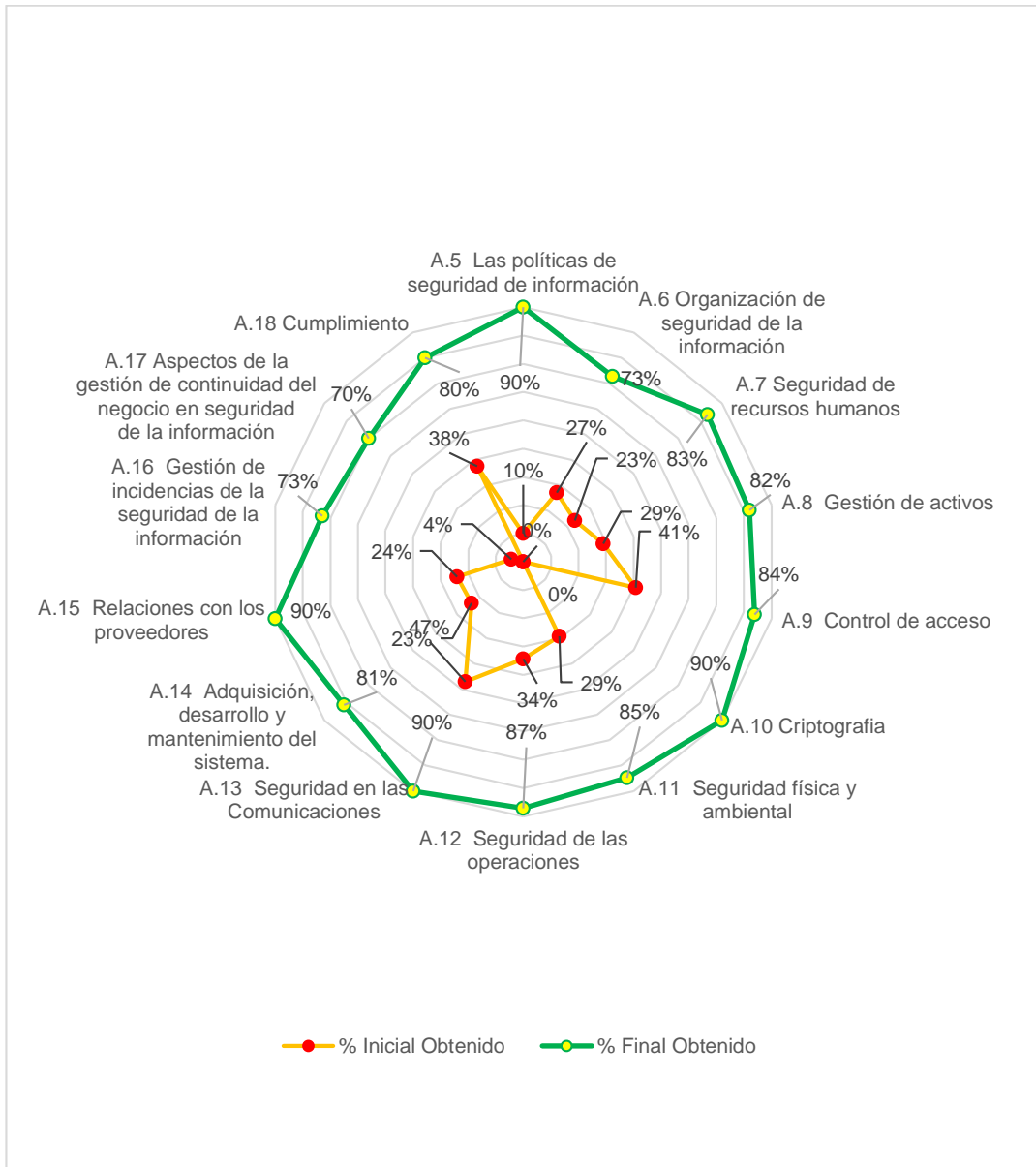


Figura 18. Análisis GAP ISO/IEC 27001:2013 Situación inicial vs situación tras la ejecución de los planes de acción propuestos. Fuente: Elaboración Propia.

Observamos que tras ejecutar los planes de acción propuesto en la organización hemos alcanzado un estado muy cercano a un nivel “Gestionado y Medible” según metodología CMM, lo cual ayudo a minimizar los niveles de riesgos identificados.

### **3.4. Conclusiones y recomendaciones.**

#### **3.4.1. Conclusiones.**

- a) Cumpliendo con el objetivo general, se puede afirmar que, habiendo concluido con las fases dispuestas en la investigación, se puede afirmar que se ha cumplido con la mejora de los procesos de gestión de riesgo de tecnología de la información.
  
- b) Según la cláusula 6.1.3 de la ISO/IEC 27001:2013, en la cual refiere que el proceso de evaluación y tratamiento de los riesgos de seguridad de la información debe alinearse con los principios previstos en la norma ISO 31000; por lo que, haciendo referencia a la norma ISO 31000, se logró cumplir con el objetivo específico “a”, con el cual se estableció los 05 procesos de la gestión de riesgo, mencionados en la Fase I.
  
- c) Se estableció el Anexo 02 – Declaración de aplicabilidad de los controles mencionados en el Anexo “A” de la norma ISO/IEC 27001:2013 y haciendo uso de la metodología CMM se estableció un análisis de madurez inicial de los controles asociados a los procesos de gestión de riesgo, determinando que el 76% de los controles estipulados en el Anexo “A” no se encuentran implementados en la organización y el otro 24% restante se encuentran gestionados o defectuosos; por lo que, se puede afirmar que se logró el objetivo específico “b”.
  
- d) Haciendo uso de la metodología MagerIT, se identificaron los activos y se realizó la evaluación de los riesgos asignándoles responsable a cada uno de los activos, bajo los criterios de integridad, disponibilidad y confidencialidad. Asimismo, se identificó que los procesos de Soporte son los que proporcionan el sustento a la gestión de riesgo de COLVIAS SAC y su buen manejo es fundamental para un óptimo desempeño de los procesos asociados

a TI; por lo que, se puede afirmar que se logró cumplir el objetivo específico “d”.

- e) Teniendo en cuenta el análisis de riesgo obtenido, se elaboró planes de acción aceptados por la Gerencia de Colvias SAC, los cuales ayudaron a mejorar la seguridad de la información dentro de la organización, logrando un nivel cercano a “Gestionable y Medible – CMM”.
- f) Se puede afirmar que en el desarrollo del presente trabajo se logró cumplir los objetivos, toda vez que se define una herramienta que permite gestionar los riesgos y poder hacer un seguimiento y control, alineada a la estructura de la metodología aplicada, la cual fue aceptada por la alta gerencia de Colvias SAC.

### **3.4.2. Recomendaciones.**

- a) Se debe tener en cuenta el uso de la metodología enfocada en ciclo de Deming a través de los parámetros de la norma ISO / IEC 27001: 2013, lo cual ayudara a la implantación futura de un SGSI en la organización.
- b) Crea una “Cultura de seguridad de la información” en Colvias SAC, para que los colaboradores tomen mayor conocimiento sobre la necesidad de salvaguardar los activos de la información de la organización.
- c) Implementar las mejoras de los planes de acción propuestos tras evaluación de los dominios de la ISO / IEC 27001:2013 en la Fase V.
- d) Implantar y documentar un programa de auditorías para verificar el cumplimiento de las propuestas implementadas.
- e) Desarrollar indicadores que nos permitan medir la eficacia de los controles y procedimientos implementados.
- f) Una vez implantadas las mejoras alcanzando un nivel de madurez “Gestionable Medible - CMM” se deberá conseguir la certificación ISO 27001:2013.

## REFERENCIAS

- Alcántara Flores, J. C. (2015). *Guía de implementación de la seguridad basado en la Norma ISO/IEC 27001, para apoyar la seguridad en los Sistemas Informáticos de la Comisaría del Norte P.N.P. en la ciudad de Chiclayo*. Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo, Chiclayo.
- Alcántara Rojas, P. V. (2013). *Metodología para minimizar las deficiencias de diseño basada en la construcción virtual usando tecnologías BIM*. Tesis de pregrado, Universidad Nacional de Ingeniería, Lima.
- Amutio, Candau, & Mañas. (2012). *Magerit metodología de análisis y gestión de riesgos de los sistemas de información* (3 ed.). Madrid, España: Ministerio de Hacienda y Administraciones Públicas.
- Anilema Guamán, Á. (2014). *Análisis de Factibilidad y propuesta para la implementación de la tecnología Cloud Computing para la empresa constructora Moncayo & Roggiero*. Tesis de pregrado, Universidad Politécnica Nacional, Quito.
- Arévalo-Ascanio, J., Bayona-Trillos, R., & Rico-Bautista, D. (2015). Responsabilidad social empresarial e innovación: una mirada desde las tecnologías de la información y comunicación en organizaciones. *Clío América*, 180–189.
- Atehortúa, I., Bustamante, M., & Valencia, M. (2008). *Sistema de Gestión Integral una sola Gestión, un solo Equipo*. Universidad de Antioquia.
- Baca Flores, V. M. (20 de Mayo de 2016). Diseño de un Sistema de Gestión de la Seguridad de la Información para la unidad de Gestión Educativa Local Chiclayo. *Revista de Ingeniería: Ciencia, Tecnología e Innovación*, 1(1), 42.
- Baca Urbina, G., Solares Soto, P. F., & Acosta Gonzaga, E. (2014). *Administración Informática I: Análisis y Evaluación de tecnologías de información*. México: Grupo Patria Cultural .

- Barrera, H., & Rodríguez, C. (2014). Metodologías Para el Análisis de Riesgos en los SGSI.
- Benavides Sepúlveda, A., & Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Scientia et Technica año XXII*, 23(1).
- Berrios Mesía, C. A., & Rocha Cam, M. A. (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.
- Calder, A. (2017). *Nueve pasos para el éxito: Una visión de conjunto para la aplicación de la ISO 27001:2013*. Reino Unido: IT Governance Publishing.
- Campos Merchan, L. N. (2015). *Proyecto de diseño e implementación de una estructura administrativa por procesos para la mediana empresa de obras civiles Construx S.A.*". Tesis de Pregrado, Universidad de Guayaquil, Guayaquil.
- Cardona Madariaga, D. F. (2009). *Las tecnologías de la información y las comunicaciones - TIC*. Colombia: Editorial Universidad del Rosario. Obtenido de <https://books.google.com.pe/books?id=6Qc4Gkw6ZMcC&pg=PA58&dq=tecnolog%C3%ADas+de+la+informaci%C3%B3n&hl=es-419&sa=X&ved=0ahUKEwj15Mj17vrgAhVI2FkKHmMnDSYQ6AEIKDAA#v=onepage&q&f=true>
- Carpentier, J. F. (2016). *La seguridad informática en la PYME: situación actual y mejores prácticas*. Barcelona: Ediciones ENI.
- Chambergó Anacleto, D. (2016). *Plan estratégico para la gestión administrativa de la empresa constructora ALTUM SAC*. Tesis de pregrado, Universidad Cesar Vallejo, Chiclayo.

- Chero López, M. Y. (2017). *Capacitación empresarial y la gestión administrativa de la empresa Constructora e Inversiones Santa Fe SAC*. Tesis de pregrado, Universidad Cesar Vallejo, Chimbote.
- Diario Gestión. (03 de Julio de 2014). Construcción puede potenciar su crecimiento con el estándar BIM. *Gestión*, pág. 17. Obtenido de <https://gestion.pe/tecnologia/construccion-potenciar-crecimiento-estandar-bim-64650>
- El Informe Delmont. (18 de Abril de 1979). *Principios y guías éticos para la protección de los sujetos*. Obtenido de Bioetica y derecho: <http://www.bioeticayderecho.ub.edu/archivos/norm/InformeBelmont.pdf>
- Esquema nacional de seguridad. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Hacienda y Administraciones Públicas.
- Fernández Fernández, D. (2015). *Modelo de Gestión de Riesgos de TI de acuerdo con las exigencias de la SBS, basados en las ISO/EC 27001, ISO/IEC 17799, Magerit para la Caja de Ahorro y Créditos Sipán SA*. Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo, Chiclayo.
- Fernández, V. (2006). *Desarrollo de sistemas de información : una metodología basada en el modelado*. Barcelona: Barcelona UPC. Obtenido de [https://books.google.com.pe/books?id=Sqm7jNzs\\_L0C&pg=PA49&dq=planificaci%C3%B3n+de+la+informaci%C3%B3n&hl=es-419&sa=X&ved=0ahUKEwj\\_5JtT9KHeAhXlwVkkHRBqBA0Q6AEILjAB#v=onepage&q=planificaci%C3%B3n%20de%20la%20informaci%C3%B3n&f=false](https://books.google.com.pe/books?id=Sqm7jNzs_L0C&pg=PA49&dq=planificaci%C3%B3n+de+la+informaci%C3%B3n&hl=es-419&sa=X&ved=0ahUKEwj_5JtT9KHeAhXlwVkkHRBqBA0Q6AEILjAB#v=onepage&q=planificaci%C3%B3n%20de%20la%20informaci%C3%B3n&f=false)
- Flores Cano, C. (29 de Agosto de 2018). Razones por las que las empresas de construcción pierden dinero. *Arq.com*. Obtenido de <http://noticias.arq.com.mx/Detalles/18449.html#.W9cspUxFzIX>



Giraldo, L. (21 de Diciembre de 2016). Tecnología para constructoras pyme. *En obra*, pág. 16. Obtenido de <https://en-obra.com/noticias/tecnologia-para-constructoras-pyme/>

Gómez Ruedas, J. (1999). *Dirección y Gestión de Proyectos de Tecnologías de la Información en la Empresa*. Madrid: Editorial Fundación Confemetal.

Hernández Sanpieri, R. (2014). *Metodología de la Investigación* (Sexta ed.). México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. Obtenido de <https://josedominguezblog.files.wordpress.com/2015/06/metodologia-de-la-investigacion-hernandez-sampieri.pdf>

Hurtado, M. (2018). Gestión de riesgo metodologías octave y magerit.

Isaca.org. (15 de Agosto de 2019). <https://www.isaca.org/>. Obtenido de <https://www.isaca.org/>: <https://www.isaca.org/>

ISO 27001. (2013). *ISO 27001:2013*. USA: International Organization of Standarization.

Jhuéz, J. (25 de Enero de 2018). *Capacitación CGR*. Obtenido de Metodologías para la gestión de Riesgo: <https://capacitacioncgr.jovenclub.cu/wp-content/uploads/2018/05/Metodologia-para-la-Gestion-del-Riesgo.pdf>

Lahuerta Amat, J. (2015). *Modelo de tecnologías de la información y la comunicación en una empresa constructora*. Tesis doctoral, Universidad Politécnica de Valencia, Lima. Obtenido de <https://riunet.upv.es/bitstream/handle/10251/57343/Modelo%20de%20tecnolog%C3%ADas%20de%20la%20informaci%C3%B3n%20y%20la%20comunicaci%C3%B3n%20en%20una%20empresa%20constructora.%20Jorge%20Lahuerta%20amat.pdf?sequence=1>

López Ramos, L. A. (2 de Diciembre de 2015). *Estructura organizacional y sus herramientas*. Obtenido de Gestipolis: <https://www.gestipolis.com/estructura-organizacional-herramientas/>

- López Ramos, L. A. (Diciembre 2 de 2015). *Estructura organizacional y sus herramientas*. Obtenido de Gestipolis: <https://www.gestipolis.com/estructura-organizacional-herramientas/>
- Maceli Simon, A. P. (2017). *Innovación Tecnológica en el sector de la construcción del Perú: Estado actual y diagnóstico*. Tesis doctoral, Universidad Politécnica de Valencia., Lima.
- Maristany Ruiz, F., & García Ibarrolla, D. B. (2008). *Colección EOI Tecnología e Innovación*. Fundación EOI. Obtenido de <https://books.google.com.pe/books?id=zVTVJeG4BGYC&pg=PA157&dq=tecnolog%C3%ADas+de+la+informaci%C3%B3n&hl=es-419&sa=X&ved=0ahUKEwjI5Mj17vrgAhVI2FkKHAMnDSYQ6AEIOjAD#v=onepage&q=tecnolog%C3%ADas%20de%20la%20informaci%C3%B3n&f=true>
- Mendoza , M. (2 de Julio de 2015). *La idea central de aplicar ISO 27001*. Obtenido de Welivesecurity: <https://www.welivesecurity.com/las/2015/07/02/idea-central-aplicar-iso-27001/>
- Montiel Acosta, H. L. (2015). *Sistemas de Seguridad de la Información de la Facultad de Ciencias Matemáticas y Físicas de la carrera de Ingeniería de Sistemas y Networking de la Universidad de Guayaquil siguiendo la Norma INEN ISO/IEC - 2013*. Tesis de pregrado, Universidad de Guayaquil, Guayaquil.
- Moreira Delgado, M. (20 de Marzo de 2012). *La organización de la información para la gestión del conocimiento en las empresas*. Obtenido de Gestipolis: <https://www.gestipolis.com/organizacion-informacion-para-gestion-conocimiento-empresas/>
- Ortiz, S. (12 de Noviembre de 2014). Las constructoras pymes, lejos de las nuevas tecnologías. *Obras web*. Obtenido de Obras web: <http://obrasweb.mx/construccion/2012/11/12/las-constructoras-pymes-lejos-de-las-nuevas-tecnologias>

Parot, C. (15 de Setiembre de 2014). Las TI en la construcción: Obras con tecnologías de punta. *EMB Construcción*. Obtenido de EMB CONSTRUCCIÓN:

<http://www.emb.cl/construccion/articulo.mvc?xid=1904&tip=1&xit=las-ti-en-la-construccion-obras-con-tecnologia-de-punta>

Parra Iglesias, E. (1998). *Tecnologías de la información en el control de gestión*. Madrid: Díaz de Santos, D.L. Obtenido de [https://books.google.com.pe/books?id=YuzRghoK00QC&printsec=frontcover&dq=control+de+la+informaci%C3%B3n&hl=es-419&sa=X&ved=0ahUKEwj3rfiQ\\_6HeAhUro1kKH2vCrcQ6AEIKDAA#v=onepage&q=control%20de%20la%20informaci%C3%B3n&f=false](https://books.google.com.pe/books?id=YuzRghoK00QC&printsec=frontcover&dq=control+de+la+informaci%C3%B3n&hl=es-419&sa=X&ved=0ahUKEwj3rfiQ_6HeAhUro1kKH2vCrcQ6AEIKDAA#v=onepage&q=control%20de%20la%20informaci%C3%B3n&f=false)

Peña Calvo, N. (2015). *Gestión y control de los Sistemas de Información* (Quinta ed.). España: Editorial Elearning S.L.

Prince2. (sf). *Prince2*. Obtenido de Wiki: <https://prince2.wiki/es/tematicas/riesgo/>

Puerta Gálvez, A. (2016). *Business Intelligence y las Tecnologías de la Información* (Segunda ed.). México: IT Campus Academy. Obtenido de <https://books.google.com.pe/books?id=3oEEDQAAQBAJ&pg=PA20&dq=tecnolog%C3%ADas+de+la+informaci%C3%B3n+TI+organizar&hl=es-419&sa=X&ved=0ahUKEwjWgl6LjfvAhUMX60KHxvCD4oQ6AEIMTAC#v=onepage&q=tecnolog%C3%ADas%20de%20la%20informaci%C3%B3n%20TI%20organizar&f=tru>

Quezada, V. (21 de Febrero de 2018). *El rol de los CISOs evoluciona en las organizaciones*. Obtenido de Search Data Center: <https://searchdatacenter.techtarget.com/es/cronica/El-rol-de-los-CISOs-evolucionan-en-las-organizaciones>

Rodríguez Bermúdez, J. R. (2015). *Planificación y dirección estratégica de sistemas de información*. Barcelona: Editorial UOC. Obtenido de <https://books.google.com.pe/books?id=vJDLDAQAQBAJ&pg=PT7&dq=directi%C3%B3n+de+la+informaci%C3%B3n&hl=es->

419&sa=X&ved=0ahUKEwjUjYqg-  
6HeAhXQo1kKHW03CtQQ6AEILjAB#v=onepage&q=direcci%C3%B3n  
%20de%20la%20informaci%C3%B3n&f=false

Santos Llanos, D. E. (2016). *Establecimiento, Implementación, Mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/iec 27001:2013, para una empresa de consultoría de Software*. Tesis de pregrado, Pontificia Universidad Católica del Perú, Lima.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (Diciembre de 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.

Superintendencia de Bancos. (8 de Julio de 2017). *Riesgo tecnológico*. Obtenido de Superintendencia de Bancos: <file:///C:/Users/Maryorie/Downloads/Riesgo%20Tecnol%C3%B3gico.pdf>

Talavera Álvarez, V. R. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de Salud de acuerdo a la ISO/IEC 27001:2013*. Tesis de pregrado, Pontificia Universidad Católica del Perú, Lima.

Turkley, F. (2010). *The Prince 2 Process Model*. London: Bizness Academy.

Valencia-Duque, F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 73-88.

Venegas Devia, G. A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs. *Sistemas & Telemática*, 12(30), 35-48. Obtenido de <https://www.redalyc.org/pdf/4115/411534000003.pdf>

Widhi Candra, J., Candra Briloyant, O., & Rebeca Tamba, S. (01 de Febrero de 2017). Planificación de SGSI basada en ISO / IEC 27001: 2013 mediante

el proceso de jerarquía analítica en la fase de análisis de brechas (Estudio de caso: Instituto XYZ). *IEEE Xplore*. Obtenido de <https://ieeexplore.ieee.org/document/8272916>

## ANEXOS

### ANEXO 1 – Resolución de Aprobación de Trabajo de Investigación.

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO  
RESOLUCIÓN N° 1472-2019/FIAU-USS  
Pimentel, 3 de agosto de 2020

**VISTO:**

El Acta de reunión N°1207-2020, de fecha 12 de julio de 2020 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS, para la ejecución de la Tesis: "MEJORA DE PROCESO DE GESTIÓN DE RIESGO DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA", presentado por RODRIGUEZ JUAREZ JOSE ANTONIO, del Programa de estudios INGENIERÍA DE SISTEMAS, y;

**CONSIDERANDO:**

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48º que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21º señala: "Los temas de trabajo de investigación, trabajo académico y tesis son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24º señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25º señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C."

Que, en el Acta de reunión N°1207-2020 de fecha 12 de julio de 2020, del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS, se indica entre los acuerdos la aprobación del tema de la Tesis denominado "MEJORA DE PROCESO DE GESTIÓN DE RIESGO DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA" de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de RODRIGUEZ JUAREZ JOSE ANTONIO en condición de egresado, del Programa de estudios INGENIERÍA DE SISTEMAS.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

**SE RESUELVE:**

**ARTÍCULO 1º:** APROBAR, el tema del Tesis denominado "MEJORA DE PROCESO DE GESTIÓN DE RIESGO DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA", perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de RODRIGUEZ JUAREZ JOSE ANTONIO, del Programa de estudios INGENIERÍA DE SISTEMAS.

**ARTÍCULO 2º:** ESTABLECER, que la inscripción del Título del Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

**ARTÍCULO 3º:** DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

**REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE**



Dr. Mario Fernando Ranco Moscol  
Decano - Facultad de Ingeniería,  
Arquitectura y Urbanismo  
UNIVERSIDAD SEÑOR DE SIPÁN SAC.



MBA. María Noelia Sialer Rivora  
Secretaria Académica / Facultad de Ingeniería,  
Arquitectura y Urbanismo  
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesado, Archivo

## ANEXO 2 – Carta de aceptación para la recolección de datos.



### CARTA DE ACEPTACIÓN

Moquegua, 10 de febrero de 2020

Señor:

Mg. Víctor Alexci Tuesta Monteza

DIRECTOR DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

A través de la presente saludarle y comunicarle que como Gerente de Proyecto de la Constructora Colvias S.A.C, del Departamento de Moquegua, acepto que el bachiller José Antonio Rodríguez Juárez de la escuela profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán, realice la recolección de datos de nuestra representada a través de su trabajo de investigación MEJORA DE PROCESO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001/IEC:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA.

Así mismo se establece la confidencialidad de la información requerida para el desarrollo de la actividad de recolección de datos del trabajo de investigación: "MEJORA DE PROCESO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001/IEC:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA", elaborado por el bachiller de la Escuela profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán.

En consecuencia, la Entidad Colaboradora dará acceso al bachiller a toda la información que sea necesaria y relativa al proyecto en el que participen para alcanzar los objetivos previstos. El bachiller se compromete a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, comprometiéndose a:

- a) No divulgar ni comunicar la información técnica que la Entidad Colaboradora les facilite, ya que esta será utilizada solo para la elaboración del trabajo de investigación que beneficiará a la gestión de riesgos de tecnología de la información de Colvias S.A.C.
- b) Impedir la copia o revelación de la información a terceros, salvo que éstos dispongan de una aprobación expresa y realizada por escrito por parte de la Entidad Colaboradora.
- c) No utilizar la información facilitada, o partes de la misma, para fines distintos a la ejecución del trabajo de investigación.

Sin otro particular, aprovecho en manifestarle los sentimientos de mi consideración y estima personal.

Atentamente, Manuel Castro Muñante

### ANEXO 3 – Instrumentos de recolección de datos.

#### CUESTIONARIO UTILIZADO

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?.	
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?.	
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	



n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	No
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realice un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Director de RRHH

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	No
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Coordinador de RRHH*

## Instrucciones:

- Colocar correctamente los datos solicitados
- Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	SI
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	SI
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: Generalista de RRHH

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	No
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Asistente de RRHH*

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	No
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	No
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	No
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO:

Asistente Social

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	No
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	No
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	No
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	No
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	No
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Auxiliar de RRHH

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI/NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?.	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?.	No
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Director Administrativo Financiero del Proyecto*

## Instrucciones:

- Colocar correctamente los datos solicitados
- Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Jefe Administrativo de Obra.



## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Coordinador Administrativo e Inventario

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporte al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Coordinador de tecnología de la Información

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Depositar Administrativo*

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	NO
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	NO
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Asistente de Compras

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	no
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	no
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	no
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: *Almacenero*

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	SI
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	NO
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	NO
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: AUXILIAR CONTABLE

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Coordinador de oficina técnica*

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	No
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Ingeniero de Oficina Técnica*



## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	No
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO:

Ingeniero de Planeamiento y Control.

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: Ingeniero de Topografía

## Instrucciones:

- Colocar correctamente los datos solicitados
- Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	SI
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso sucede algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	NO
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: ESPECIALISTA EN GESTIÓN DOCUMENTARIA Y SEGUIMIENTO DE CONTRATOS.

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	SI
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	NO
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	NO
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO CADISTA

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	NO
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	SI
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	NO
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: Jefe de Control de Proyectos

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO:

Ingeniero de Control de Proyectos

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	Si
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	NO
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	NO
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	NO
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	NO
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Supervisor de rendimientos de maquinaria

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que estén en desuso?	SI
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	NO
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: Asistente de oficina Técnica



## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	SI
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	NO
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: JEFE DE CONTROL DE CALIDAD

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que estén en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	No
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	No
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: Asistente de Control de Calidad.

## Instrucciones:

- Colocar correctamente los datos solicitados
- Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	SI
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	SI
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: DIRECTOR DE CONSTRUCCION GENERAL.

## Instrucciones:

1. Colocar correctamente los datos solicitados  
 2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	no
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: Director de Proyecto

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: GERENTE de construcción

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI/NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	SI
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: Residente de Obra.

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	no
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	no
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	no
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	no
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: Secretaria de Obra.

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	no
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que puede ocurrir con sus equipos de cómputo asignados?	si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO *Abogada de Ibra.*



Instrucciones:

1. Colocar correctamente los datos solicitados

2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: JEFE DE CAMPO.

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI/NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	no
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO. JEFE DE PLANTA.

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	no
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	no
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	no
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: *Ingeniero de Campo*

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	No
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Ingeniero de Perforación y voladura

Instrucciones:

1. Colocar correctamente los datos solicitados

2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	No
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO *Supervisor de Campo*

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que estén en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos Informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Ingeniero De Equipos

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realice un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	No
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	No
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Auxiliar de Equipos

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	Si
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Director de Desarrollo Sostenible



## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI/NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseñas para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Jefe de Gestión de SSO

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporte al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	Si
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	Si
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Jefe de Desarrollo Sostenible

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO. Jefe de SSO

## Instrucciones:

- Colocar correctamente los datos solicitados
- Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	No
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Jefe Ambiental

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	SI
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: COORDINADOR COACH MOTIVACIONAL.

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: Médico Ocupacional.

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	Si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	Si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO:

Medico Asistencial

Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI/NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	NO
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	SI
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	NO
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	NO
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	NO
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	NO
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	SI
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: SUPERVISOR SEO



## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI/NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	no
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	no
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	si
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	no
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	no
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	si
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	no
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	si

CARGO: *Asistente S60*

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	Si
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	Si
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	No
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	Si
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	No
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	No
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	No
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	Si
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	No
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	Si
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	No
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	Si
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	Si
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	Si

CARGO: *Supervisor Ambiental*

## Instrucciones:

1. Colocar correctamente los datos solicitados
2. Marcar con un "SI" o "NO", según corresponda.

COLVIAS

CUESTIONARIO	SI / NO
a) Dada la naturaleza de su trabajo, ¿Cuenta usted con 01 o más activos a su cargo?	SI
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	NO
c) ¿Usted reporta al área de TI sobre equipos a su cargo que estén en desuso?	NO
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	SI
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	SI
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	SI
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	SI
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	SI
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	SI
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que puede ocurrir con sus equipos de cómputo asignados?	SI
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	NO
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	SI
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	NO
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	SI

CARGO: *asistente de gestión integral*

**ANEXO 4 – Declaración de Aplicabilidad ISO/IEC 27001:2013.**

OBJETIVO DE CONTROL	DETALLE DEL ESTADO DEL CONTROL	APLICABILIDAD (SI/NO)	REQUERIMIENTO (RL, CC, CN y RAR)	JUSTIFICACIÓN DE LA INCLUSIÓN Y/O EXCLUSIÓN
<b>A.5. Políticas de seguridad de la información</b>				
<b>A.5.1 Dirección de gerencia para la seguridad de la información</b>				
A.5.1.1 Políticas para la seguridad de la información	Se ha evidenciado que la organización tiene una política de Seguridad de la Información, sin embargo, esta no está difundida al total de su personal; por lo que se puede decir que CUMPLE PARCIALMENTE.	SI	CN, RAR	La política de seguridad de la información debe estar firmado por la alta gerencia de la organización, deberá de ser difundida a todo el personal de la organización y deberá de estar visible en la organización.

<p>A.5.1.2 Revisión de las políticas de seguridad de la Información</p>	<p>La Política de seguridad de la información no se encuentra actualizada CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CN</p>	<p>La política de seguridad de la información deberá de actualizarse cuando se requiera y/o una vez al año.</p>
<p><b>A.6. Organización de seguridad de la información</b></p>				
<p><b>A.6.1 Organización interna</b></p>				
<p>A.6.1.1 Roles y responsabilidades de seguridad de la información</p>	<p>NO CUMPLE La organización no tiene establecido claramente los Roles y Responsabilidades asociadas a TI</p>	<p>SI</p>	<p>CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>

A.6.1.2 La segregación de funciones	En la organización se ha identificado que se tiene definido perfiles concretos que tienen responsabilidades y accesos sobre activos de TI. Sin embargo, no se tiene la documentación (procedimiento) que gestione la segregación de funciones. CUMPLE PARCIALMENTE	SI	CN	Existe una segregación de funciones según los privilegios de Administrador/usuario/invitado
A.6.1.3 Contacto con las autoridades	En la organización los contactos con las autoridades se realizan cuando se evidencia la necesidad en un momento específico, CUMPLE PARCIALMENTE.	SI	RL, CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
A.6.1.4 Contacto con los grupos de interés especial	En vista al rubro de la organización este punto aún no se encuentra plenamente implementado, NO CUMPLE	SI	CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013

<p>A.6.1.5 Seguridad de la información en gestión de proyectos</p>	<p>CUMPLE PARCIALMENTE La organización tiene a un coordinador de TI quien administra la seguridad de la información sin embargo no se tiene definida una Gestión de Proyectos</p>	<p>SI</p>	<p>CC, CN y RAR</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>
<p><b>A.6.2 Dispositivos móviles y trabajo a distancia</b></p>				
<p>A.6.2.1 Política de dispositivos móviles</p>	<p>La política de dispositivos móviles se encuentra dentro de la Política de Seguridad de la información. CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>
<p>A.6.2.2 Trabajo a distancia</p>	<p>Actualmente la organización viene aplicando el trabajo remoto, sin embargo no se tiene definida una política y procedimiento que gestione el Trabajo</p>	<p>SI</p>	<p>CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>

		Remoto CUMPLE PARCIALMENTE			
<b>A.7. Seguridad de recursos humanos</b>					
<b>A.7.1. Previo al empleo</b>					
	A.7.1.1 Investigación de antecedentes	<p>El departamento de RR.HH. dentro de la Organización es el encargado de todas las funciones de gestión de personal (Selección, contratación, seguimiento del personal, y Baja). Sin embargo tiene las siguientes falencias:</p> <ul style="list-style-type: none"> <li>- Control y seguimiento de las necesidades en cuanto a la formación del personal (aspectos competenciales, funcionales y de seguridad).</li> <li>- No se tiene acuerdos de Confidencialidad, protección de Datos</li> </ul>	SI	RL,CC, CN y RAR	Se realiza procesos de selección de personal, en los que según el curriculum /aptitudes de los postulantes son evaluados y así determinar si se encuentran aptos para el cargo a desempeñar.



		<p>personales, registro de entregas de equipamiento, políticas de Seguridad, etc.</p> <p>CUMPLE PARCIALMENTE</p>			
	<p>A.7.1.2 Términos y condiciones de empleo</p>	<p>El departamento de RR.HH. dentro de la Organización es el encargado de todas las funciones de gestión de personal (Selección, contratación, seguimiento del personal, y Baja). Sin embargo tiene las siguientes falencias:</p> <ul style="list-style-type: none"> <li>- Control y seguimiento de las necesidades en cuanto a la formación del personal (aspectos competenciales, funcionales y de seguridad).</li> <li>- No se tiene acuerdos de Confidencialidad, protección de Datos</li> </ul>	<p>SI</p>	<p>RL,CC, CN y RAR</p>	<p>Es necesario definir las condiciones de la relación laboral antes de realizar la contratación.</p>

		personales, registro de entregas de equipamiento, políticas de Seguridad, etc. CUMPLE PARCIALMENTE			
<b>A.7.2</b> Durante el empleo					
A.7.2.1 Responsabilidades de gestión	La organización tiene definido un procedimiento para los empleados en el cual define sus roles y responsabilidades, sin embargo, no ha sido difundido a todo el personal.	SI	RL,CC, CN y RAR	Todos los empleados propios y/o sub contratados deben cumplir con todos los roles y responsabilidades de seguridad de la información y ante cualquier infracción de dicha seguridad (Política, Procedimientos, etc) puede ser motivo para la terminación del vínculo laboral. Los usuarios de terceros son tratados como visitantes y sólo tienen acceso de	

					acompañamiento y las infracciones pueden ser causa de eliminación de los privilegios de acceso, así como también según la gravedad la separación laboral.
A.7.2.2	Concientización, educación y entrenamiento en seguridad de la información	La Organización no tiene definido un programa de capacitación y/o entrenamiento respecto a la Seguridad de la Información, CUMPLE PARCIALMENTE.	SI	RL,CC, CN y RAR	Se Considera de gran importancia la capacitación respecto a Seguridad de la Información, se debe crear una cultura de seguridad de la información.
A.7.2.3	Proceso disciplinario	La Organización tiene un proceso disciplinario formal, sin embargo, éste no ha sido comunicado a todo su personal. CUMPLE PARCIALMENTE	SI	RL, CN	Es necesario establecer un proceso disciplinario, con la finalidad de que se obligue a cumplir las normas por parte de los usuarios internos y externos.

<b>A.7.</b>					
<b>3 Finalización o cambio laboral</b>					
	A.7.3.1 Terminación o cambio de responsabilidades laborales	La organización tiene un procedimiento define las responsabilidades y deberes de seguridad de la información vigentes después de la terminación o cambio de empleo, sin embargo, en la mayoría de los casos no son comunicados a los empleados y/o sub-contratista. CUMPLE PARCIALMENTE	SI	CN	Es necesario fijar las condiciones de terminación del vínculo laboral o de cambio de puesto antes de realizar la contratación.
<b>A. Gestión de 8 activos</b>					
<b>A.8.</b>					
<b>1 Responsabilidad de los activos</b>					
	A.8.1.1 Inventario de activos	En la organización existe un inventario de activos de TI, sin embargo, no se encuentra actualizado y no existe un	SI	CC, CN y RAR	Los activos de TI deben de estar etiquetados y deben de estar actualizados en un inventario. Requisito ISO/IEC 27001:2013

		procedimiento para su gestión. CUMPLE PARCIALMENTE			
A.8.1.2 La propiedad de los activos	Los activos no se encuentran con la declaración de su responsable y/o propietario de manera generalizada. NO CUMPLE	SI	CN	Todos los activos tienen asignado un propietario /Responsable Requisito ISO/IEC 27001:2013	
A.8.1.3 Uso aceptable de los activos	La organización tiene un mínimo de prácticas establecidas de los activos de información, las cuales no se encuentran documentadas ni difundidas. NO CUMPLE	SI	RL,CC, CN y RAR	Es necesario garantizar que el uso de los activos de la organización sea el adecuado por parte de los trabajadores.	
A.8.1.4 Devolución de los activos	Los empleados de la Organización por temor a descuentos saben que al término de su vínculo laboral tienen que devolver todos los activos en su poder, sin embargo, no existe un procedimiento documentado para la gestión de los activos que el departamento de TI haya	SI	CN, RAR	Es necesario establecer un proceso que garantice la devolución de los activos que se entregan a los usuarios.	

		implementado. CUMPLE PARCIALMENTE			
<b>A.8.2 Clasificación de la información</b>					
A.8.2.1 Clasificación de la información	En la organización se tiene establecido los criterios de Clasificación de los activos de información; así como las políticas de seguridad a aplicar en su almacenamiento, tránsito y soporte; sin embargo no se evidencia su ejecución. CUMPLE PARCIALMENTE	SI	RL, CC y CN	La información se clasifica en términos requeridos según las políticas y directrices de la Organización.	
A.8.2.2 Etiquetado de información	La organización no tiene definido los procedimientos para el etiquetado de información de conformidad con el esquema de clasificación de información adoptado por la organización. El personal lo viene realizando por	SI	CN, RAR	La información debe estar clasificada y marcada en todo momento para facilitar su archivado y búsqueda.	

		conocimientos empíricos NO CUMPLE			
A.8.2.3 Manejo de activos		La organización carece de procedimientos de manipulación de los activos, sin embargo el personal ha venido realizando por su propia experiencia y/o conocimientos empíricos CUMPLE PARCIALMENTE	SI	CN, RAR	Es necesario garantizar que el uso de los activos de la organización sea adecuado por parte de los trabajadores.
<b>A.8. 3 Manejo Medios</b>					
A.8.3.1 Gestión de medios extraíbles		La organización no tiene definida una política de gestión de soportes extraíbles NO CUMPLE	SI	RL, CC, CN	Se dispone de un disco duro externo que se considera dentro de la categoría de soportes extraíbles, por lo que se debe implementar una correcta gestión de este tipo de soportes.

A.8.3.2 Eliminación de los medios de comunicación	En la organización existe un proceso para la eliminación de soportes. CUMPLE PARCIALMENTE	SI	RL, CC, CN	Política global de eliminación de la organización para la eliminación segura de los medios de información.
A.8.3.3 Transferencia de medios Físicos	La organización viene cumpliendo con la parte operativa de este control, sin embargo, no está documentada. CUMPLE PARCIALMENTE	SI	RL, CC, CN	Requisito ISO/IEC 27001:2013
<b>A.9 Control de acceso</b>				
<b>A.9.1 Requisitos del negocio del control de acceso</b>				
A.9.1.1 Política de control de acceso	En la organización no existe una política de control de acceso a los recursos compartidos en la red, solo se ha evidenciado que existe restricción de	SI	CN, RAR	Los accesos de usuario de la organización deben de cumplir con un conjunto estándar de privilegios de acceso de acuerdo con la Política de



	acceso a la información, pero no se encuentra documentado. NO CUMPLE			Autorización de Acceso a Datos y Protección de la Organización.
A.9.1.2 Acceso a redes y servicios de red	Se observa que en la organización los usuarios disponen de acceso a la red y a los servicios de red que hayan sido específicamente autorizados a utilizar. CUMPLE PARCIALMENTE	SI	CN, RAR	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
<b>A.9.2 Gestión de acceso a usuarios</b>				
A.9.2.1 Registro de usuarios y cancelación de registro	En la organización se viene realizando un proceso formal de registro y baja de usuarios para permitir la asignación de derechos de acceso. Sin embargo, este proceso no se encuentra documentado. CUMPLE PARCIALMENTE	SI	CC, CN y RAR	Los usuarios deben estar registrados en la DATA de la organización para poder acceder al mismo, se debe tener en cuenta los privilegios específicos que se otorguen

<p>A.9.2.2 Aprovisiona miento de acceso de usuario</p>	<p>Los accesos a los recursos, aplicaciones, herramientas son solicitados por el responsable de los distintos departamentos de la organización, no se tiene un procedimiento documentado. CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CN, RAR</p>	<p>Establecer una Gestión de Privilegios para todos los Sistemas incluidos en el alcance.</p>
<p>A.9.2.3 Gestión de derechos de acceso privilegiados</p>	<p>La organización no tiene gestionado la asignación y el uso de los derechos de acceso privilegiados, estos controles están implementados pero no se encuentran gestionados CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CN, RAR</p>	<p>Los dueños de los procesos de la organización gestionan los derechos de acceso, el coordinador de TI administra y controla su asignación, uso y revocación.</p>
<p>A.9.2.4 Gestión de información de autenticació</p>	<p>En la organización existen herramientas de Gestión de Credenciales para garantizar la aplicación de este control. NO está documentado. CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CN</p>	<p>La información de autenticación de usuarios se considera secreta, y deberá protegerse adecuadamente.</p>

	n secreta de usuario				
A.9.2.5	Revisión de los derechos de acceso de usuario	La organización no tiene definido un programa para la revisión de los derechos de accesos de los usuarios a intervalos regulares. NO CUMPLE	SI	CN	Los dueños de sistemas de la organización revisan el uso y acceso a sus sistemas.
A.9.2.6	Retiro o ajuste de los derechos de acceso	En la organización los derechos de acceso de todos los empleados a la información se eliminarán al terminar su vínculo laboral o acuerdo, o ajustarse al cambio. Sin embargo este control no está documentado CUMPLE PARCIALMENTE	SI	CC, CN	La eliminación y cambio de derechos debe realizarse de una forma ordenada y definida formalmente en la organización.
<b>A.9.3</b>	<b>Responsabilidades del usuario</b>				

	A.9.3.1 Uso de información de autenticación secreta	Los empleados de la organización no tienen buenas prácticas para el uso de la información de autenticación secreta. NO CUMPLE	SI	CN	Los usuarios deben hacer un correcto uso de sus contraseñas.
<b>A.9.4</b> Control de acceso de aplicación y sistema					
	A.9.4.1 Restricción de acceso a la Información	La organización tiene control para el acceso a la información y las funciones del sistema de aplicación CUMPLE PARCIALMENTE	SI	CC, CN	En la organización se debe establecer restricciones de acceso a la información, en función de los privilegios o perfiles que se otorgan.
	A.9.4.2 Procedimientos de conexión segura	Cuando la política de control de acceso lo exija, en la organización se evidencia que no existe un procedimiento que controle una conexión segura. NO CUMPLE	SI	CN	Se debe asegurar que las conexiones a los sistemas son seguras.

A.9.4.3 Sistema de gestión de contraseña	La organización tiene implementado una política de Contraseñas que está extendida a todas las Aplicaciones que requieren control de Acceso. CUMPLE PARCIALMENTE	SI	CN	Todos los sistemas disponen de mecanismos de gestión de contraseñas
A.9.4.4 Uso de programas de utilidad privilegiados	La organización no tiene definido un inventario de utilidades que puedan anular los controles del sistema. NO CUMPLE	SI	CN	Acceso limitado a los administradores de sistemas autorizados.
A.9.4.5 Control de acceso a código fuente del programa	NO APLICA	NO	-	La organización no desarrolla software.
<b>A.10 Criptografía</b>				

<b>A.10</b>					
<b>.1 Controles criptográficos</b>					
	A.10.1.1 Política sobre el uso de controles criptográficos	La organización no tiene una política sobre el uso de los controles criptográficos para la protección de la información. NO CUMPLE	SI	RL,CC, CN y RAR	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
	A.10.1.2 Gestión de claves	La organización deberá de desarrollar y aplicar una política sobre el uso, la protección y la duración de las claves criptográficas durante todo su ciclo de vida. NO CUMPLE	SI	RL,CC, CN y RAR	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
<b>A.11 Seguridad física y ambiental</b>					
<b>.1 Áreas seguras</b>					

<p>A.11.1.1 Perímetro de protección física</p>	<p>En la organización se identifica la existencia de 2 Perímetros de seguridad dentro de las instalaciones:  - Control de Acceso Físico a oficinas Moquegua (Nivel 3).  - Control de Acceso Físico a las Instalaciones ubicadas en campamento minero - (Campamento Minero).  Sin embargo estos perímetros de seguridad no se encuentran debidamente protegidos. ( NO existe una restricción de acceso por cualquier empleado)  NO CUMPLE</p>	<p>SI</p>	<p>CC, CN y RAR</p>	<p>Existen áreas seguras ( Sala de servidores, sala de archivo), correctamente delimitadas que deben estar recogidas dentro de los procedimientos del SGSI</p>
<p>A.11.1.2 Controles de entrada físicas</p>	<p>La organización no tiene definido los controles necesarios para la protección para asegurar que sólo el personal autorizado tenga acceso NO CUMPLE</p>	<p>SI</p>	<p>CC, CN y RAR</p>	<p>Debe de existir controles físicos de entrada en todas las áreas seguras que se han definido dentro del alcance del sistema.</p>

A.11.1.3 Protección de oficinas, habitaciones e instalaciones	NO CUMPLE	SI	CC, CN y RAR	La organización debe utilizar medidas de seguridad física de acuerdo con la política correspondiente
A.11.1.4 Protección contra amenazas externas y ambientales	NO CUMPLE	SI	CC, CN y RAR	Todos los sitios están sujetos a evaluación de riesgos antes y durante la ocupación
A.11.1.5 Trabajo en zonas seguras	La organización tiene un diseño y aplica procedimientos para trabajar en áreas seguras.CUMPLE PARCIALMENTE	SI	CC, CN y RAR	Es necesario definir un procedimiento de trabajo en áreas seguras, enfocado a mantener el nivel de Seguridad establecido en dichas áreas.



A.11.1.6 Áreas de entrega y carga	NO APLICA	NO	-	En la organización no existe una zona específica para la carga y descarga. Cualquier recepción de material, recepción de documentos, etc. se realiza por la puerta principal, y siempre cuando existe personal en la oficina.
<b>A.11</b> <b>.2</b> <b>Equipo</b>				
A.11.2.1 Emplazamiento y protección del equipo	Los equipos asociados a Comunicaciones (REDES) se encuentran ubicados en una sala la que no cuenta con medida de protección (control de acceso), tiene un control de temperatura, control anti-incendios, etc. El resto de los equipos Servidores está alojada en por proveedores externos <b>CUMPLE PARCIALMENTE</b>	SI	CC, CN y RAR	Los equipos son considerados como un activo de gran importancia para, por lo que se considera importante definir su instalación, así como la forma de protegerlos contra amenazas.

A.11.2.2 Servicios básicos	La organización protege los equipos contra fallas de alimentación y otras interrupciones CUMPLE PARCIALMENTE	SI	CC, CN y RAR	Los equipos críticos están protegidos por UPS y un grupo electrógeno diésel.
A.11.2.3 Seguridad de Cableado	En la organización se ha identificado que los cables de alimentación y telecomunicaciones no están protegidos en su totalidad contra interceptaciones, interferencias o daños. CUMPLE PARCIALMENTE	SI	CC, CN	Las conexiones de los puestos de trabajo se utilizan cableado de red, considerándose importante que el mismo cumpla siempre que sea posible con las normas de cableado estructurado.
A.11.2.4 Mantenimiento del equipo	La organización no tiene implementado un programa de mantenimiento de los equipos de TI; estos entran a mantenimiento cuando el coordinador de TI detecta fallas. NO CUMPLE	SI	CN, RAR	La operación correcta de los equipos de TI se considera de gran importancia, por lo que, se debe tener implementado un procedimiento que permita gestionar el mantenimiento de los mismos.

<p>A.11.2.5 Eliminación de activos</p>	<p>CUMPLE PARCIALMENTE La organización no tiene definido un procedimiento que permita gestionar la salida de equipos de la organización.</p>	<p>SI</p>	<p>RL, CC, CN y RAR</p>	<p>Estos son aprobados por el Director o Gerente de la Organización. Se debe establecer procedimientos que permitan a los usuarios que los portátiles y/o otros equipos sean sacados de la instalación bajo previa autorización.</p>
<p>A.11.2.6 Seguridad de equipo y activos fuera de las instalaciones</p>	<p>Se ha identificado que en la organización no se ha aplicado una seguridad correspondiente que permita sacar los equipos fuera de la organización NO CUMPLE</p>	<p>SI</p>	<p>CC, CN</p>	<p>Requisito ISO/IEC 27001:2013</p>
<p>A.11.2.7 Eliminación segura o la reutilización de los equipos</p>	<p>No se gestiona correctamente la eliminación de los activos cuando estos entran en desuso</p>	<p>SI</p>	<p>CC, CN</p>	<p>Se debe considerar como de gran importancia medidas de seguridad que permitan la eliminación o reutilización de los activos, ya que estas tareas son realizadas por el responsable de almacén y/o coordinador de TI</p>

A.11.2.8 Equipos de usuario desatendida	En la organización los usuarios no están conscientes de la importancia que sus equipos cuenten con la protección adecuada, mayormente cuando los empleados dejan sus ordenadores estos no se bloquean.	SI	RL, CC, CN y RAR	Es necesario bloquear la pantalla de los ordenadores por el usuario al dejar desatendido el ordenador.
A.11.2.9 Políticas de escritorio y pantallas limpias	NO CUMPLE, no se tiene una Política declarada, difundida y en uso dentro de la Organización.	SI	CC, CN y RAR	Es necesario mantener el bloqueo de pantalla y la política de escritorio limpio
<b>A.1 2 Seguridad de las operaciones</b>				
<b>A.12 .1 Responsabilidades y procesamientos operacionales</b>				
A.12.1.1 Procedimientos	La organización no tiene definido procedimientos operativos dentro del	SI	CN	Se debe disponer procedimientos operativos documentados que se han incluido dentro del Sistema de Gestión

operacional es documentad os	SGSI. NO CUMPLE			
A.12.1.2 Gestión del cambio	En la organización no se tiene definido procedimientos de Gestión de Cambios implementados; debido que no se usa de manera habitual. NO CUMPLE	SI	CC, CN y RAR	Es necesario definir un proceso de gestión del cambio.
A.12.1.3 Gestión de la capacidad	La organización no monitorea el uso de los recursos. NO CUMPLE	SI	CN	Se deben planificar las capacidades en base a las informaciones sobre disponibilidad de los recursos.
A.12.1.4 Separación de desarrollo, pruebas y	Los entornos de pruebas esta segregado reduciendo el riesgo de acceso no autorizado. CUMPLE PARCIALMENTE	SI	CN	Todos los entornos de Prueba y Producción se separan físicamente o lógicamente usando switches y firewalls

	entornos operativos				
<b>A.12 .2 Protección del malware o programas maliciosos</b>					
	A.12.2.1 Controles contra el malware	En la organización se tiene implementado controles de detección, prevención y recuperación como protección contra el malware, combinados con una correcta concienciación del usuario. CUMPLE PARCIALMENTE	SI	CN, RAR	Los equipos de TI usados en la organización utilizan el Sistema Operativo Windows los cuales necesitan ser protegidos mediante herramientas antimalware, que ofrezcan una barrera de seguridad contra el código malicioso y el código móvil
<b>A.12 .3 Backup o código de seguridad</b>					
	A.12.3.1 Copias de seguridad de la información	En la organización se realizan copias de Seguridad de la información, sin embargo, no se tiene un programa que permita gestionar por fechas las copias	SI	CN, RAR	Es necesario considerar de manera primordial la formalización y realización periódica de Copias de Seguridad de la información que garanticen la

		de seguridad de la información. CUMPLE PARCIALMENTE			recuperación de los datos, en caso de fallo.
<b>A.12</b> <b>.4 Registro y supervisión</b>					
	A.12.4.1 Registro del Evento	La organización no tiene implementado un registro de los eventos de los Servidores y de la Red, estos no son analizados regularmente salvo que ocurra una incidencia mayor NO CUMPLE	SI	CC, CN	Es necesario guardar registros del Firewall y del Directorio Activo
	A.12.4.2 Protección de la información de registro	Las instalaciones de la organización y la información no se encuentran en su totalidad protegidas contra la manipulación indebida y el acceso no autorizado. CUMPLE PARCIALMENTE	SI	CN	Los registros de logs que se generen en los sistemas deben estar protegidos, de forma que solo el personal de TI pueda acceder.

<p>A.12.4.3 Registros de administrador y operador</p>	<p>La organización no tiene en su totalidad un registro de las actividades del administrador del sistema CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CC, CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>
<p>A.12.4.4 Sincronización del reloj</p>	<p>En la organización se ha identificado que los relojes de todos los sistemas de procesamiento de información relevantes se sincronizarán con una única fuente de tiempo de referencia. SI CUMPLE</p>	<p>SI</p>	<p>CN</p>	<p>Todos los sistemas se sincronizarán con un reloj identificado y se mostrarán en GMT.</p>
<p><b>A.12.5 Control de software operacional</b></p>				
<p>A.12.5.1 Instalación de software</p>	<p>En la organización no se tiene implementado un procedimiento que permita controlar la instalación de</p>	<p>SI</p>	<p>RL, CC, CN y RAR</p>	<p>Aplicable a los programas y aplicativos que forman parte del alcance dentro de la organización</p>



	en sistemas operativos	software en sistemas operativos. NO CUMPLE			
<b>A.12 .6 Gestión vulnerabilidad Técnica</b>					
	A.12.6.1 Gestión de vulnerabilidades técnicas	No se tiene identificado las vulnerabilidades de los sistemas de información, la organización deberá de evaluar la exposición a dichas vulnerabilidades y se tomarán las medidas apropiadas para abordar el riesgo asociado. NO CUMPLE	SI	CN	Se realiza un control de vulnerabilidades de todos los sistemas del alcance.
	A.12.6.2 Restricciones en la instalación de software	La organización debe implementar reglas que controlen la instalación de software por parte de los usuarios. NO SE CUMPLE	SI	CN	Se restringe la instalación de software a los empleados.

<b>A.12</b>					
<b>.7 Consideraciones sobre la auditoría de sistemas de información</b>					
	A.12.7.1 Controles de auditoría de sistemas de la información	La organización no realiza periódicamente prácticas de auditorías donde se pueda identificar vulnerabilidades a los Sistemas. <b>NO SE CUMPLE</b>	SI	CN	Se debe analizar los sistemas de información, comprobando que los niveles de seguridad son adecuados, y las políticas de seguridad se cumplen de forma adecuada, como mínimo una vez al año.
<b>A.13</b>					
<b>Seguridad en las Comunicaciones</b>					
<b>A.13</b>					
<b>.1 Gestión de la seguridad Red</b>					
	A.13.1.1 Controles red	Se ha identificado que en la organización su arquitectura y diseño de red contempla la segmentación de acceso y el control de los mecanismos de acceso entre las distintas redes. Sin	SI	CC, CN	La red de datos, y de los servidores está sometida a Controles de Seguridad de red, gestionados por el personal de TI

		embargo esto no está documentado CUMPLE PARCIALMENTE			
A.13.1.2	Seguridad de los servicios de red	La organización no tiene en su totalidad los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red identificados, donde se incluya los acuerdos de servicios de red, ya se trate de servicios internos. CUMPLE PARCIALMENTE	SI	CN	La red de datos, y de los servidores están sometidos a Controles de Seguridad de red, gestionados por el personal de TI
A.13.1.3	Segregación en las redes	En la organización los grupos de servicios de información, usuarios y sistemas de información están segregados en las redes de datos. SI CUMPLE	SI	CC, CN	Arquitectura de red

**A.13**  
**.2 Intercambio de información**

<p>A.13.2.1 Las políticas y los procedimientos para el intercambio de la información</p>	<p>En la organización se identifican prácticas en este sentido, sin embargo estas no están inventariadas y documentadas CUMPLE PARCIALMENTE</p>	<p>SI</p>	<p>CN, RAR</p>	<p>Aplica, porque existen supuestos en los que se intercambia información</p>
<p>A.13.2.2 Acuerdos de intercambio de información</p>	<p>No existen acuerdos para la transferencia segura de información comercial entre la organización y las partes externas NO CUMPLE</p>	<p>SI</p>	<p>CC, CN</p>	<p>Política de conectividad de terceros de la organización</p>

A.13.2.3 La mensajería electrónica	La organización tiene contratado el servicio de mensajería por Microsoft, por lo que, la información involucrada en la mensajería electrónica se encuentra protegida.	SI	CC, CN	Se intercambia información por correo electrónico
A.13.2.4 Acuerdos de confidencialidad y divulgación	En la organización se ha identificado la existencia de acuerdos de confidencialidad tanto para el personal interno como el externo; así como en los contratos existentes con los proveedores y/o sub-contratistas vinculados con la Organización; Sin embargo no existe una constancia de la existencia de procedimientos para asegurar el cumplimiento.  CUMPLE PARCIALMENTE	SI	RL, CC, CN y RAR	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
<b>A.14 Adquisición, desarrollo y mantenimiento del sistema.</b>				

**A.14**  
**.1** **Requisitos de seguridad de los sistemas de información**

<p>A.14.1.1 Análisis y especificación de los requisitos de seguridad</p>	<p>En la Organización se ha establecido requisitos de Seguridad ad-hoc en los procesos de contratación de algunos proveedores; sin embargo no están tipificados y documentados los requisitos de seguridad de la organización hacia los proveedores de servicios. <b>NO CUMPLE</b></p>	<p>SI</p>	<p>CC, CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>
<p>A.14.1.2 Protección de los servicios de aplicación en redes públicas</p>	<p>La información asociada con los servicios de aplicación que se transporten por las redes públicas está protegida contra actividades fraudulentas, conflictos contractuales y divulgación y modificación no autorizadas. Sin embargo no está documentado <b>CUMPLE PARCIALMENTE</b></p>	<p>SI</p>	<p>RL, CC y CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>

A.14.1.3 Protección de las transacciones de servicios de aplicación	La información involucrada en las transacciones del servicio de aplicación se encuentra protegida para evitar la transmisión incompleta, el enrutamiento erróneo, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación no autorizada de mensajes o la repetición.	SI	CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
<b>A.14.2 Seguridad en los procesos de desarrollo y de apoyo</b>				
A.14.2.1 Política segura de desarrollo	No se considera en las actividades actuales de la organización	NO	-	La organización no considera el desarrollo de software en sus actividades actuales.
A.14.2.2 Procedimientos de control de	Está practica lo realiza los proveedores contratados en el desarrollo del software de la organización CUMPLE PARCIALMENTE	SI	CC, CN y RAR	El alcance incluye sistemas de información desarrollados por los proveedores sub contratados.

cambios del sistema				
A.143.2.3 Revisión técnica de aplicaciones después de la plataforma de funcionamiento	Está practica lo realiza los proveedores contratados en el desarrollo del software de la organización, no se tiene un procedimiento documentado. CUMPLE PARCIALMENTE	SI	CN	Aplicable a los programas y aplicativos que forman parte del alcance de la organización.
A.14.2.4 Restricciones sobre los cambios en los paquetes de software	No se considera en las actividades actuales de la organización	NO	-	La organización no considera el desarrollo de software en sus actividades actuales.



A.14.2.5 Principios de ingeniería sistema seguro	La organización establece sus principios para la ingeniería de sistemas seguros, sin embargo estos no están documentados. SI CUMPLE	SI	CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
A.14.2.6 Entorno de desarrollo seguro	No se considera en las actividades actuales de la organización	NO	-	La organización no considera el desarrollo de software en sus actividades actuales.
A.14.2.7 Desarrollo Outsourced	No se considera en las actividades actuales de la organización	NO	-	La organización no considera el desarrollo de software en sus actividades actuales.
A.14.2.8 Pruebas de seguridad del sistema	Esta práctica no se realiza y no se tiene un procedimiento documentado NO CUMPLE	SI	CC, CN	Se deben realizar pruebas seguridad de los sistemas

	A.14.2.9 Pruebas de aceptación del sistema	Esta práctica no se realiza y no se tiene un procedimiento documentado <b>NO CUMPLE</b>	SI	CN	Se deben realizar pruebas de aceptación de los sistemas
<b>A.14.3 Datos de prueba</b>					
	A.14.3.1 Protección de datos de prueba	La organización no tiene implementado un programa que permita seleccionar los datos de prueba, se protegerán y se controlarán.	SI	CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
<b>A.1.5 Relaciones con los proveedores</b>					
<b>A.15.1 Seguridad de la información en relaciones con los proveedores</b>					
	A.15.1.1 La política de seguridad de la	La organización realiza prácticas referido a este control, sin embargo, estas no se	SI	CC, CN y RAR	Es de gran importancia dejar clara la forma de tratar la seguridad en el contrato de los servicios con terceros.

	información para relaciones con los proveedores	encuentran documentadas. NO CUMPLE			
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	La organización no tiene implementado requisitos de seguridad de la información acordadas con cada proveedor, que les permita acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización. NO CUMPLE	SI	CC	Existen relaciones con proveedores que deben tratar la seguridad de la información
A.15.1.3	Cadena de suministro de tecnología de	La organización no tiene categorizados ni documentados, se ha verificado la existencia de requisitos de seguridad para los proveedores más críticos, pero no se han analizado correctamente. NO CUMPLE	SI	CC	Existen suministros por parte de proveedores

	comunicación e información				
<b>A.15.2 Gestión de la prestación de servicios Proveedor</b>					
	A.15.2.1 Supervisor y revisar los servicios de proveedores	La organización viene realizando prácticas de supervisión periódicamente la prestación de servicios de los proveedores. Sin embargo no se tiene documentado CUMPLE PARCIALMENTE	SI	CC	No se revisan y evalúan proveedores
	A.15.2.2 Gestión de cambios en los servicios de proveedores	La organización realiza prácticas en los cambios en la prestación de servicios, mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de la información existentes, Sin embargo, no se tiene la documentación. CUMPLE PARCIALMENTE	SI	CC, CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013

A.1 6 Gestión de incidencias de la seguridad de la información					
A.16 .1 Gestión de incidentes de seguridad de la información y mejoras					
A.16.1.1	Responsabilidades y procedimientos	La organización no tiene implementado un procedimiento de gestión de Incidentes de TI NO CUMPLE	SI	CC, CN y RAR	Es necesario considerar, un procedimiento de gestión de los incidentes de TI
A.16.1.2	Reporte de eventos de seguridad de la información	La organización no tiene un flujo de comunicación en relación a las notificaciones de incidentes de seguridad dentro y fuera de la organización. NO CUMPLE	SI	CC, CN y RAR	Se necesita un procedimiento que permita gestionar los incidentes de TI
A.16.1.3	Reporte de debilidades	La organización no tiene mecanismos que permitan asegurar contratos con los	SI	CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013

de seguridad de información	proveedores. NO CUMPLE			
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	La organización no evalúa los eventos de seguridad de la información NO CUMPLE	SI	CN	Incidentes dentro del alcance del SGSI
A.16.1.5 Respuesta a incidentes de seguridad de información	La organización no tiene procedimientos documentados que permita que los incidentes sean respondido NO CUMPLE	SI	CC, CN	Incidentes dentro del alcance del SGSI

<p>A.16.1.6 Lecciones aprendidas de los incidentes de seguridad de la información</p>	<p>La organización no tiene un procedimiento para la gestión de incidentes que permitan obtener lecciones aprendidas de los mismos NO CUMPLE</p>	<p>SI</p>	<p>CN</p>	<p>Es necesario mantener un registro de los incidentes</p>
<p>A.16.1.7 Recolección de evidencias</p>	<p>La organización no tiene un procedimiento para la gestión de incidentes que permitan obtener lecciones aprendidas de los mismos NO CUMPLE</p>	<p>SI</p>	<p>CN</p>	<p>Es necesario definir en el procedimiento de Gestión de Incidentes los pasos para el tratamiento de los mismos.</p>
<p><b>A.17 Aspectos de la gestión de continuidad del negocio en seguridad de la información</b></p>				
<p><b>A.17.1 Continuidad en la seguridad de la información</b></p>				

<p>A.17.1.1 Planificación de la continuidad de la seguridad de la información</p>	<p>En la organización se ha identificado que la información crítica es conocida; pero no se ha realizado de manera procedimientos documentados que permita determinar el alcance y las necesidades. NO CUMPLE</p>	<p>SI</p>	<p>CN, RAR</p>	<p>Es necesario considerar un plan que planifique poner en marcha la continuidad del negocio ante eventos inesperados.</p>
<p>A.17.1.2 Implementación de la continuidad en la seguridad de la información</p>	<p>La organización no tiene documentado los procedimientos y controles que permita asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa. NO CUMPLE</p>	<p>SI</p>	<p>CN</p>	<p>Se implanta la Continuidad del Negocio dentro del ámbito de implantación de la norma ISO:IEC 27001:2013 de Seguridad de la Información</p>
<p>A.17.1.3 Verificar, revisar y</p>	<p>NO CUMPLE</p>	<p>SI</p>	<p>CN</p>	<p>Cumplir con los requisitos del negocio. Tratamiento de Riesgos</p>



	evaluar la continuidad de seguridad de la información				
<b>A.17</b>					
<b>.2 Redundancias</b>					
	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	En la organización existen redundancias en la infraestructura que soportan la información desde el punto de vista del Almacenamiento, tratamiento y transferencia de la información. Sin embargo para ciertas informaciones críticas desde el punto de vista de la operativa no está garantizada esta redundancia <b>NO CUMPLE</b>	SI	CC, CN	Se debe establecer redundancias de elementos críticos

<b>A.18 Cumplimiento</b>					
<b>A.18.1 Cumplimiento con los requisitos legales y contractuales</b>					
	A.18.1.1 Identificación de la legislación aplicable y requisitos contractuales	Todos los requisitos legislativos, reglamentarios y contractuales pertinentes de la organización deberán identificarse explícitamente, documentarse y mantenerse al día para cada sistema de información y la organización. CUMPLE PARCIALMENTE	SI	CC, CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013
	A.18.1.2 Derechos de propiedad intelectual	Se tiene procedimientos, pero no se han generado nuevas revisiones CUMPLE PARCIALMENTE	SI	CN	Política de Seguridad de la información Requisito ISO/IEC 27001:2013

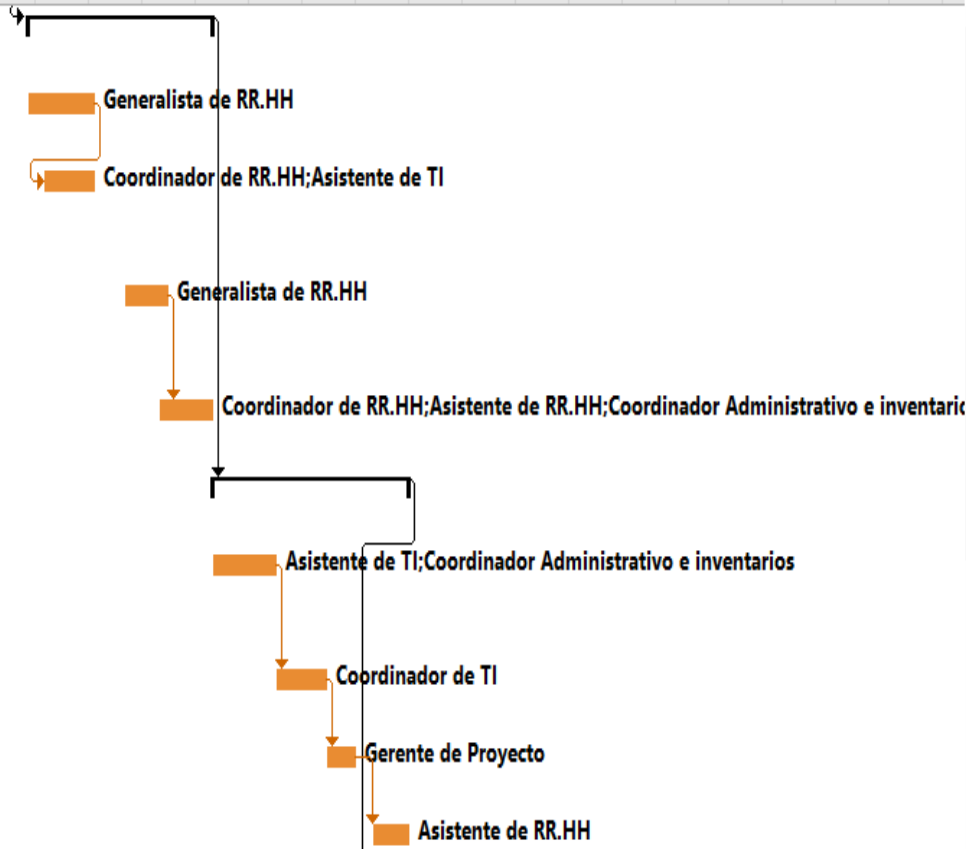
<p>A.18.1.3 Protección de los registros de la organización</p>	<p>La organización no protege en su totalidad sus registros contra la pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de conformidad con los requisitos legislativos, reglamentarios, contractuales y comerciales <b>SE CUMPLE PARCIALMENTE</b></p>	<p>SI</p>	<p>CN</p>	<p>Política de Seguridad de la información Requisito ISO/IEC 27001:2013</p>
<p>A.18.1.4 Privacidad y protección de datos personales</p>	<p>Dentro de la organización el responsable de TI y los dueños de los procesos gestionan la privacidad y la protección de la información de identificación personal se garantizará según se requiera en la legislación y la reglamentación pertinentes cuando proceda</p>	<p>SI</p>	<p>RL, CC, CN</p>	<p>Requisito ISO/IEC 27001:2013</p>
<p>A.18.1.5 Regulación de los</p>	<p><b>NO CUMPLE</b></p>	<p>SI</p>	<p>RL, CC, CN y RAR</p>	<p>Requisito ISO/IEC 27001:2013</p>

	controles criptográficos				
<b>A.18</b> <b>.2 Información revisiones de seguridad</b>					
A.18.2.1 Revisión independiente de seguridad de la información	La organización no tiene implantado un sistema de Gestión de la Seguridad de la Información  Se tienen algunos procedimientos para el control y seguimiento de Auditorías en la organización  CUMPLE PARCIALMENTE	SI	CN	Se realizan auditorías internas en materia de Seguridad de la Información	
A.18.2.2 Cumplimiento con las políticas y estándares	El responsable de TI no revisa periódicamente el cumplimiento del proceso de información y los procedimientos dentro de su área de responsabilidad.  NO CUMPLE	SI	CN	Se realizan auditorías internas en materia de Seguridad de la Información	

de seguridad				
A.18.2.3 Revisión de cumplimiento o técnico	La organización no revisa periódicamente los sistemas de información <b>NO CUMPLE</b>	SI	CN, RAR	Requisito ISO/IEC 27001:2013



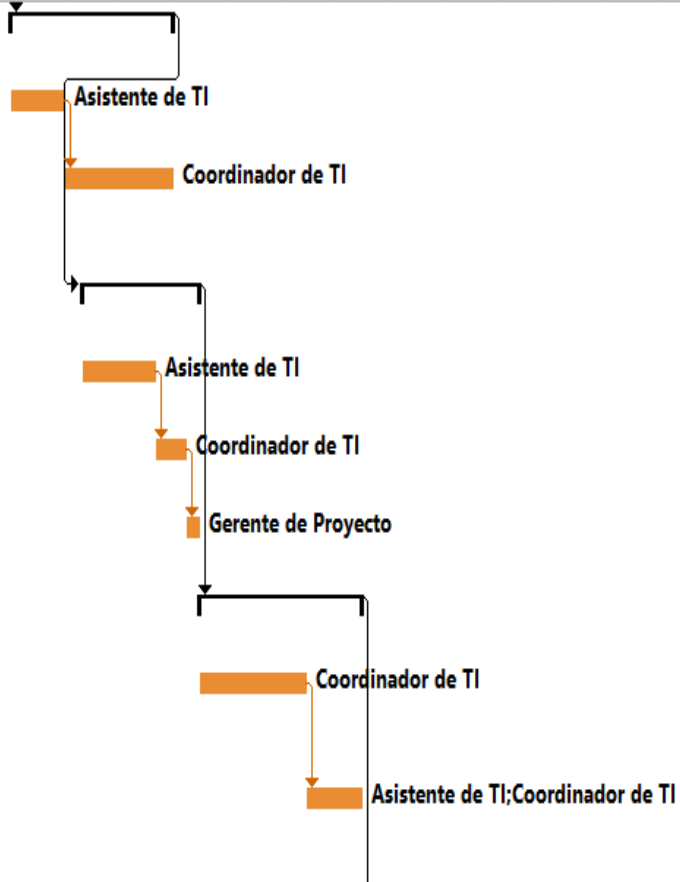
Mc de tan	Planes de Acción	Duració	Comienzo	Fin	12 abr '20	19 abr '20	26 abr '20	3 may '20	10 may '20	17 may '20	24 may '20	31 may '20			
					D	X	S	M	V	L	J	D	X	S	M
	<b>Plan de Acción 03 - Mejora los procedimientos de RR.HH</b>	<b>10.13 días?</b>	<b>mar 14/04/20</b>	<b>vie 24/04/20</b>											
	Revisión y Actualización de los procedimientos de selección de personal del área de RR.HH	4 días?	mar 14/04/20	sáb 18/04/20											
	Revisión de las responsabilidades y condiciones en materia de seguridad de la información en los contratos laborales.	4.88 días?	mié 15/04/20	sáb 18/04/20											
	Revisión del reglamento interno de trabajo "proceso disciplinario" en materia de seguridad de la información.	2.63 días?	lun 20/04/20	mié 22/04/20											
	Revisión del proceso de devolución de los activos de la organización.	5.25 días?	mié 22/04/20	vie 24/04/20											
	<b>Plan de Acción 04 - Mejora en la gestión de los activos</b>	<b>9.13 días?</b>	<b>vie 24/04/20</b>	<b>mar 5/05/20</b>											
	Actualizar y codificar el inventario de activos, asignando cada activo a un propietario o responsable de éste.	11.19 días?	vie 24/04/20	mar 28/04/20											
	Implementar procedimiento de la gestión de activos dentro de la organización	3 días?	mar 28/04/20	vie 1/05/20											
	Aprobar el Procedimiento de la Gestión de Activos	4.38 días?	vie 1/05/20	sáb 2/05/20											
	Difundir el procedimientos de Gestión de Activos	2.25 días	lun 4/05/20	mar 5/05/20											



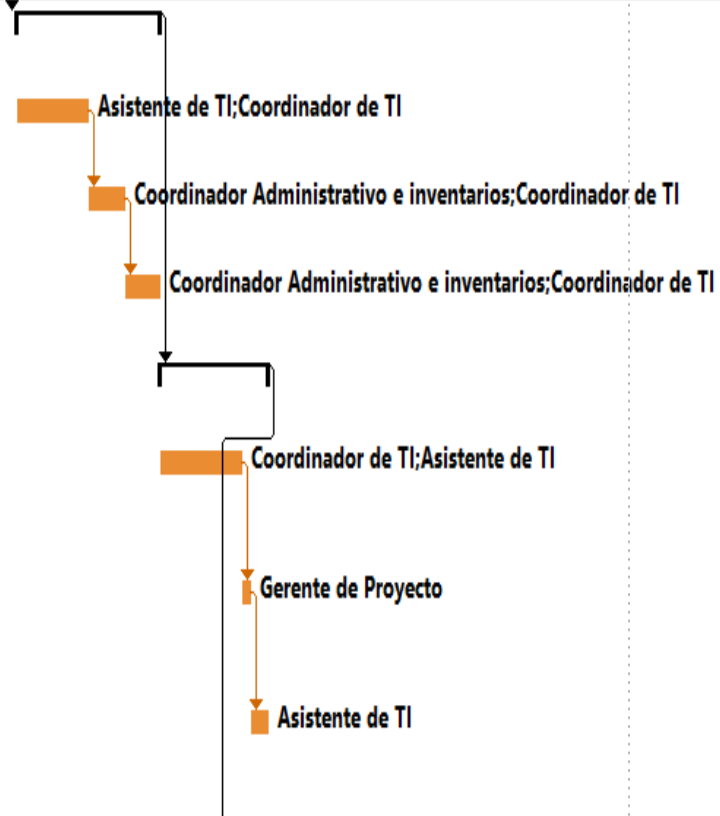
Mc de tar	Planes de Acción	Duració	Comienzo	Fin	3 may '20							10 may '20							17 may '20							24 may '20							31 may '20							7 jun '20							14 jun '20							21 jun '20						
					D	X	S	M	V	L	J	D	X	S	M	V	L	J	D	X	S	M	V	L	J	D	X	S	M	V	L	J	D	X	S	M	V	L	J	D	X	S	M	V	L	J	D	X	S	M	V	L	J							
	<b>Plan de Acción 05 - Monitorización de los programas informáticos</b>	<b>9.38 días?</b>	<b>lun 4/05/20</b>	<b>jue 14/05/20</b>																																																								
	Implementar procedimiento que mejore las medidas de monitorización de los sistemas de la organización	4.63 días?	lun 4/05/20	vie 8/05/20																																																								
	Implementar controles para proteger los registros obtenidos de la monitorización de accesos no autorizados o alteraciones.	5.88 días?	vie 8/05/20	mar 12/05/20																																																								
	Aprobar procedimiento de monitorización de los sistemas de la organización	4.38 días?	mar 12/05/20	jue 14/05/20																																																								
	<b>Plan de Acción 06 - Protección de la información mediante mecanismos Criptográficos</b>	<b>10.13 días?</b>	<b>mié 13/05/20</b>	<b>sáb 23/05/20</b>																																																								
	Implementar procedimiento que mejore los controles criptográficos en todos los servidores, discos duros de los equipos y/o externos de la organización que contengan información confidencial.	4 días?	mié 13/05/20	lun 18/05/20																																																								
	Ejecución del procedimiento Controles Criptográficos	16.38 días	lun 18/05/20	sáb 23/05/20																																																								



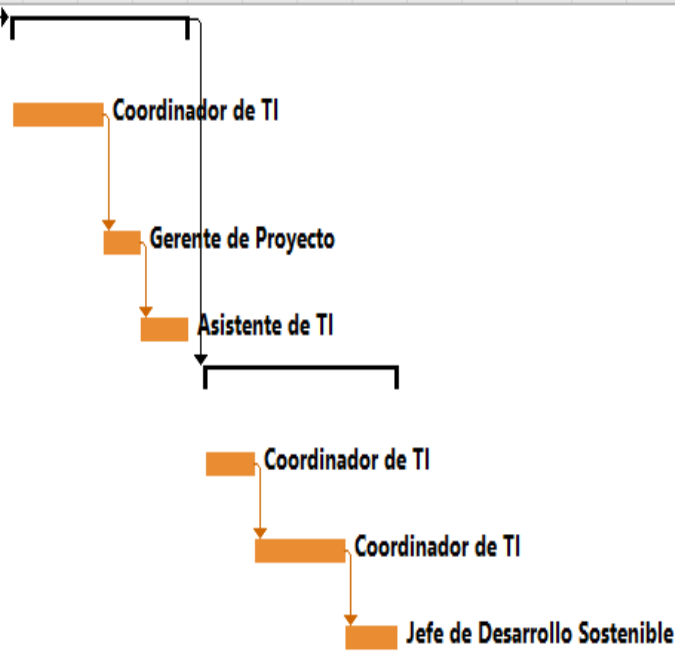
Mc de tar	Planes de Acción	Duració	Comienzo	Fin	20	24 may '20	31 may '20	7 jun '20	14 jun '20	21 jun '20	28 jun '20	5 jul '20	12 ju									
					J	D	X	S	M	V	L	J	D	X	S	M	V	L	J	D	X	S
	<b>Plan de Acción 07 - Instalación y mantenimiento de Software</b>	7.38 días?	sáb 23/05/20	lun 1/06/20																		
	Implementar un procedimiento para la gestión de perfil de los usuarios	10.38 días	sáb 23/05/20	mié 27/05/20																		
	Realizar un programa de revisiones periodicas del software instalado en los equipos de los empleados.	5.13 días?	mié 27/05/20	lun 1/06/20																		
	<b>Plan de Acción 08 - Mejora en el Desarrollo y/o mantenimiento de sistemas informáticos</b>	5.44 días?	jue 28/05/20	mié 3/06/20																		
	Implementar un procedimiento para el desarrollo de software dentro de la organización	10.38 días?	jue 28/05/20	dom 31/05/20																		
	Revisión de procedimiento de desarrollo de software	2.25 días	lun 1/06/20	mar 2/06/20																		
	Aprobar Procedimiento para el desarrollo de Software	2 días	mar 2/06/20	mié 3/06/20																		
	<b>Plan de Acción 09 - Mejora en los requerimientos de Seguridad y comunicación</b>	8.63 días?	mié 3/06/20	vie 12/06/20																		
	Implementar un procedimiento para la administración y gestión de las redes de comunicación dentro de la organización	5 días?	mié 3/06/20	mar 9/06/20																		
	Realizar la gestión y control de las redes para proteger la información en los sistemas y aplicaciones.	5.69 días?	mar 9/06/20	vie 12/06/20																		



Mc de tar	Planes de Acción	Duració	Comienzo	Fin	jun '20		14 jun '20		21 jun '20		28 jun '20		5 jul '20		12 jul '20		19 jul '20		26 jul '20	
					L	J	D	X	S	M	V	L	J	D	X	S	M	V	L	J
	<b>Plan de Acción 10 - Mejora de la seguridad en relación con los proveedores</b>	6.88 días?	sáb 13/06/20	sáb 20/06/20																
	Realizar la comprobación de la implementación de los acuerdos con los proveedores	5.88 días?	sáb 13/06/20	mar 16/06/20																
	Implementar Procedimiento de control de proveedores	4.13 días?	mié 17/06/20	jue 18/06/20																
	Revisión del servicio ofrecido por el proveedor sea el acordado.	6 días	jue 18/06/20	sáb 20/06/20																
	<b>Plan de Acción 11 - Mejora en la gestión de incidentes de Seguridad de la Información</b>	5.63 días?	sáb 20/06/20	vie 26/06/20																
	Desarrollar el procedimiento para la notificación de los incidentes de seguridad de la información y sus lecciones aprendidas.	8 días?	sáb 20/06/20	jue 25/06/20																
	Revisión y Aprobación del Procedimiento de Notificación de Incidentes de Seguridad de la información	1 día?	jue 25/06/20	jue 25/06/20																
	Difundir el procedimiento de notificación de incidentes de seguridad de la información y lecciones aprendidas	3 días?	jue 25/06/20	vie 26/06/20																



Mc de tar	Planes de Acción	Duraci	Comienzo	Fin	Calendar
	Plan de Acción 12 - Plan de continuidad del negocio	8.88 días?	jue 25/06/20	sáb 4/07/20	Calendar grid from Jun '20 to Ago '20
	Establecer un plan para la continuidad de negocio ante cualquier interrupción de las actividades de la organización.	4 días?	jue 25/06/20	mar 30/06/20	
	Revisión y aprobación del plan de continuidad de negocio	6 días?	mar 30/06/20	jue 2/07/20	
	Difusión del plan de continuidad de negocio	7.13 días?	jue 2/07/20	sáb 4/07/20	
	Plan de Acción 13 - Revisión de la Seguridad de la información	10 días?	lun 6/07/20	jue 16/07/20	
	Definir programa de revisión interna de los controles del Anexo A - ISO 27001:2013	3 días?	lun 6/07/20	mié 8/07/20	
	Ejecutar Programa de revisión interna del Anexo A - ISO 27001.2013	4 días?	mié 8/07/20	lun 13/07/20	
	Definir programa de auditoria interna en materia de Seguridad de la Información	3 días?	lun 13/07/20	jue 16/07/20	



## ANEXO 6 – Validación por Juicios de Expertos



### FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS - JUEZ-1

#### 1. INFORMACIÓN DEL EXPERTO:

- 1.1 Nombre y Apellido : Luis Chavarria Aragón
- 1.2 Profesión : Ingeniero de Computación y Sistemas
- 1.3 Institución donde trabaja : Colvias SAC
- 1.4 Cargo que desempeña : Coordinador de TI
- 1.5 Teléfono : 986685420
- 1.6 Nombre del instrumento evaluado : Encuesta
- 1.7 Correo Electrónico : [luis.chavarria@colvias.com](mailto:luis.chavarria@colvias.com)

#### 2. NOMBRE:

#### 3. SOBRE LA INVESTIGACIÓN

##### 3.1. Título de la Investigación:

MEJORA DE PROCESOS DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA

##### 3.2. Objetivo del Estudio:

Determinar la capacidad de las encuestas para medir las cualidades para lo cual se aplicaron en el personal de Colvias SAC.

#### 4. ASPECTOS DE VALIDACIÓN

Para la construcción y validación de instrumentos: Se elaboró la siguiente escala:

INDICADORES	CRITERIO
Objetividad	Permite medir los hechos observados
Claridad	Está compuesto con un lenguaje apropiado
Coherencia	Los items planteados guardan relación
Organización	Presentación ordenada
Pertinencia	Permite conseguir datos de acuerdo a los objetivos planteados, siendo relevante para la investigación

Donde:

Valor	Criterio
1	Totalmente desacuerdo
3	Medianamente de acuerdo
5	Totalmente de acuerdo

Calculo del Coeficiente de Validez por cuestión (pregunta):

$$C_p = \sum_{i=1}^n J_{ip}$$

Dónde:  $J_{ip}$  es el rango asociado a la evaluación del juez experto "i" de la pregunta "p".

Calculo del Coeficiente de Validez:

$$CV = \frac{Jz}{K}$$

Dónde:

Jz: es la media aritmética del puntaje obtenido por pregunta de los jueces expertos.

K: es la constante (puntaje deseado = 25).

**Escala de Validez:**

Rango	Criterio de Validez
0.01 - 0.20	Muy bajo
0.21 - 0.60	Bajo
0.61 - 0.80	Moderado
0.81 - 0.90	Alto
0.91 - 1	Muy Alto

**5. APRECIACIONES:**

CUESTIONARIO EVALUADO	Objetividad	Claridad	Coherencia	Organización	Pertinencia	PUNTAJE DESEADO	PUNTAJE OBTENIDO	VALIDEZ x CUESTIÓN
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	5	5	5	5	5	25	25	1.00
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	5	3	5	5	5	25	23	0.92
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	5	5	5	5	5	25	25	1.00
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	5	5	5	5	5	25	25	1.00
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	5	5	5	5	5	25	25	1.00
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	5	5	5	5	5	25	25	1.00
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	5	3	5	5	5	25	23	0.92
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	5	5	5	5	5	25	25	1.00
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	5	3	5	5	5	25	23	0.92

j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	5	3	5	5	5	25	23	0.92
k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	5	3	5	5	5	25	23	0.92
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	5	5	5	3	5	25	23	0.92
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	5	5	5	5	5	25	25	1.00
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	5	5	5	5	5	25	25	1.00

**6. OBSERVACIONES:**

---



---



---



---



---



---

Moquegua, Martes 12 de Mayo del 2020




---

Ing. Luis Chavarria Aragón  
CIP 166401

**FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS - JUEZ-2**

**1. INFORMACIÓN DEL EXPERTO:**

- 1.1 Nombre y Apellido : Hilda Milagros Santa Cruz Quiroz
- 1.2 Profesión : Ingeniero de Sistemas
- 1.3 Institución donde trabaja : Hospital Regional Lambayeque
- 1.4 Cargo que desempeña : Operador Logístico
- 1.5 Teléfono : 979394071
- 1.6 Nombre del instrumento evaluado : Encuesta
- 1.7 Correo Electrónico : [hsantacruz@hrlamb.gob.pe](mailto:hsantacruz@hrlamb.gob.pe)

**2. NOMBRE:**

**3. SOBRE LA INVESTIGACIÓN**

**3.1. Título de la Investigación:**

MEJORA DE PROCESOS DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA

**3.2. Objetivo del Estudio:**

Determinar la capacidad de las encuestas para medir las cualidades para lo cual se aplicaron en el personal de Colvias SAC.

**4. ASPECTOS DE VALIDACIÓN**

Para la construcción y validación de instrumentos: Se elaboró la siguiente escala:



INDICADORES	CRITERIO
Objetividad	Permite medir los hechos observados
Claridad	Está compuesto con un lenguaje apropiado
Coherencia	Los Items planteados guardan relación
Organización	Presentación ordenada
Pertinencia	Permite conseguir datos de acuerdo a los objetivos planteados, siendo relevante para la investigación

Donde:

Valor	Criterio
1	Totalmente desacuerdo
3	Medianamente de acuerdo
5	Totalmente De acuerdo

Calculo del Coeficiente de Validez por cuestión (pregunta):

$$C_p = \sum_{i=1}^n J_{ip}$$

Dónde:  $J_{ip}$  es el rango asociado a la evaluación del juez experto "i" de la pregunta "p".

Calculo del Coeficiente de Validez:

$$C_v = \frac{J_z}{K}$$

Dónde:

$J_z$ : es la media aritmética del puntaje obtenido por pregunta de los jueces expertos.  
 $K$ : es la constante (puntaje deseado = 25).

Escala de Validez:

Rango	Criterio de Validez
0.01 - 0.20	Muy bajo
0.21 - 0.60	Bajo
0.61 - 0.80	Moderado

0.81 - 0.90	Alto
0.91 - 1	Muy Alto

##### 5. APRECIACIONES:

CUESTIONARIO EVALUADO	Objetividad	Claridad	Coherencia	Organización	Pertinencia	PUNTAJE DESEADO	PUNTAJE OBTENIDO	VALIDEZ
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	5	5	5	5	5	25	25	1.00
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	5	3	5	3	5	25	21	0.84
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	5	3	5	5	5	25	23	0.92
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	5	5	5	5	5	25	25	1.00
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	5	5	5	3	5	25	23	0.92
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	5	5	5	5	5	25	25	1.00
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	5	3	5	5	5	25	23	0.92
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	5	3	5	5	5	25	23	0.92
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	5	5	5	5	5	25	25	1.00
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con	5	3	5	3	5	25	21	0.84

sus equipos de cómputo asignados?

k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	5	3	5	5	5	25	23	0.92
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	5	3	5	3	5	25	21	0.84
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	5	5	5	3	5	25	23	0.92
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	5	5	5	5	5	25	25	1.00

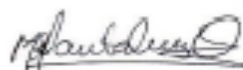
#### 6. OBSERVACIONES:

Mediante el presente suscribo que el presente modelo se encuentra validado, debido que el presente instrumento cumple en cada etapa para el desarrollo de la investigación.

\_\_\_\_\_

\_\_\_\_\_

Moquegua, 22 de mayo del 2020



Ing. Hilda Milagros Santa Cruz Quiroz  
C.P. 2023109

**FICHA DE VALIDACIÓN POR JUICIO DE EXPERTOS - JUEZ-3**

**1. INFORMACIÓN DEL EXPERTO:**

- 1.1 Nombre y Apellido : Carlos Alberto Sánchez Acosta
- 1.2 Profesión : Ingeniero de Sistemas
- 1.3 Institución donde trabaja : Ingenova Group SAC
- 1.4 Cargo que desempeña : Responsable de Proyectos de TI
- 1.5 Teléfono : 970011177
- 1.6 Nombre del instrumento evaluado : Encuesta
- 1.7 Correo Electrónico : [carlos.sanchez@ingenova.com.pe](mailto:carlos.sanchez@ingenova.com.pe)

**2. NOMBRE:**

**3. SOBRE LA INVESTIGACIÓN**

**3.1. Título de la Investigación:**

MEJORA DE PROCESOS DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO / IEC 27001:2013 PARA UNA EMPRESA CONSTRUCTORA PERUANA

**3.2. Objetivo del Estudio:**

Determinar la capacidad de las encuestas para medir las cualidades para lo cual se aplicaron en el personal de Colvias SAC.

**4. ASPECTOS DE VALIDACIÓN**

Para la construcción y validación de instrumentos: Se elaboró la siguiente escala:

INDICADORES	CRITERIO
Objetividad	Permite medir los hechos observados
Claridad	Está compuesto con un lenguaje apropiado
Coherencia	Los Items planteados guardan relación
Organización	Presentación ordenada
Pertinencia	Permite conseguir datos de acuerdo a los objetivos planteados, siendo relevante para la investigación

Donde:

Valor	Criterio
1	Totalmente desacuerdo
3	Medianamente de acuerdo
5	Totalmente De acuerdo

Calculo del Coeficiente de Validez por cuestión (pregunta):

$$C_p = \sum_{i=1}^n J_{ip}$$

Dónde:  $J_{ip}$  es el rango asociado a la evaluación del juez experto "i" de la pregunta "p".

Calculo del Coeficiente de Validez:

$$C_v = \frac{\bar{J}_z}{K}$$

Dónde:

$\bar{J}_z$ : es la media aritmética del puntaje obtenido por pregunta de los jueces expertos.  
 K: es la constante (puntaje deseado = 25).

Escala de Validez:

Rango	Criterio de Validez
0.01 - 0.20	Muy bajo
0.21 - 0.60	Bajo

0.61 - 0.80	Moderado
0.81 - 0.90	Alto
0.91 - 1	Muy Alto

##### 5. APRECIACIONES:

CUESTIONARIO EVALUADO	Objetividad	Claridad	Coherencia	Organización	Pertinencia	PUNTAJE DESEADO	PUNTAJE OBTENIDO	VALIDEZ
a) Dada la naturaleza de su trabajo. ¿Cuenta usted con 01 o más activos a su cargo?	5	5	5	5	5	25	25	1.00
b) ¿Tiene conocimiento de la cantidad de softwares que usted tiene asignado en su activo informático?	5	5	5	5	5	25	25	1.00
c) ¿Usted reporta al área de TI sobre equipos a su cargo que están en desuso?	5	3	5	5	5	25	23	0.92
d) ¿Usted necesita el uso de contraseña para acceder a información segura?	5	3	5	3	5	25	21	0.84
e) ¿Considera importante realizar el cambio de contraseñas con cierta frecuencia?	5	5	5	3	5	25	23	0.92
f) ¿En caso suceda algún incidente informático usted conoce a quien se debe reportar?	5	3	5	5	5	25	23	0.92
g) ¿Usted cree que realiza un correcto uso de los servicios que brinda el área de TI?	5	5	5	5	5	25	25	1.00
h) ¿Es usted consciente en la importancia de tomar las medidas de seguridad necesarias para un buen funcionamiento de los equipos informáticos asignados?	5	1	5	5	5	25	21	0.84
i) ¿Considera la importancia de realizar la actualización de los programas antivirus de sus equipos de cómputo asignados?	5	3	5	3	5	25	21	0.84
j) ¿Sabe usted lo importante que es realizar periódicamente copias de seguridad de la información ante algún siniestro que pueda ocurrir con sus equipos de cómputo asignados?	5	3	5	5	5	25	23	0.92

k) ¿Sabe usted si la empresa tiene un sistema de gestión de seguridad de la información en los procesos de TI?	5	3	5	3	5	25	21	0.84
l) ¿Cree usted que el diseño de un SGSI permitirá mejorar la seguridad de la información de su área de trabajo?	5	1	5	3	5	25	19	0.76
m) ¿Aprobaría usted el desarrollo de un SGSI en su área de trabajo?	5	5	5	3	5	25	23	0.92
n) ¿Aprobaría usted que se implementen actividades dirigidas a todos los colaboradores que ayude a sensibilizar sobre la importancia de la seguridad de la información?	5	5	5	5	5	25	25	1.00

#### 6. OBSERVACIONES:


Seria de mucha ayuda el desarrollo de un SGSI en la empresa donde laboro bajo la norma ISO / IEC 27001:2013, con el propósito de poder generar un sentido de pertenencia y apropiación en temas de seguridad en cada uno del personal que labora en la empresa, y concientizar sobre los riesgos que pueden afectar la seguridad de la información.

Moquegua, del 2020



GABRIELA HERPIO SAAVEDRA ACOSTA  
INGENIERO DE SISTEMAS  
REG. CIP. N° 193176

**ANEXO 7 – Registro de consentimiento para la aplicación de encuesta en Colvias SAC.**

<b>PROYECTO QUELLAVECO</b>		
<b>REGISTRO DE INDUCCIÓN, CAPACITACIÓN, ENTRENAMIENTO Y SIMULACROS DE EMERGENCIA</b>		
Razón Social: COLVIAS S.A.C RUC: 20603730837 Dirección: Av. Juan Arona Nro. 755 Piso 10 Oficina 113 - Urb. Santa Cruz - San Isidro - Lima Actividad Económica: Construcción		N° Trabajadores en el centro laboral Aprox: <u>    </u>
		N° Registro <u>01</u>

Tema:	Aplicación de Encuesta de Mejora de Proceso de Gestión de Riesgo de Tecnología ...				
Facilitador/Lugar:	José Antonio Rodríguez Juárez	OP: Colvias	Inducción	Simulacro de Emergencia	
Firma:	<i>José</i>	N° Asistentes: 20	Capacitación	Toolbox	
Fecha: 26/05/2020	Hora Inicio: 17:00	Hora Fin: 17:30	N° de Horas: 30'	Entrenamiento	Otro <input checked="" type="checkbox"/>

N°	APELLIDOS Y NOMBRES	EMPRESA - CONTRATO	PUESTO DE TRABAJO	DNI	FIRMA	NOTA
1	Castro Munante Manuel	Colvias	Gerente de Const	06658994	<i>[Signature]</i>	
2	ROMERO CARRERA CARLOS	COLVIAS	JEFE AMBIENTAL	42244251	<i>[Signature]</i>	
3	Julita Mamani Gonzales	Colvias	Sup. Ambiental	47551858	<i>[Signature]</i>	
4	Sánchez Farro Isaac	Colvias	Sup. SSO	41788596	<i>[Signature]</i>	
5	José Antonio Rodríguez Juárez	Colvias	Asist. SSO	41807389	<i>[Signature]</i>	
6	Leonildo Leon Ramos	Colvias	Jefe Acta Obra	41892537	<i>[Signature]</i>	
7	RAMIREZ TORRES JONATHAN	COLVIAS	ING. PERUCL	40619571	<i>[Signature]</i>	
8	Julita Saindy Jefferson	Colvias	Ing. Campo	0945650	<i>[Signature]</i>	
9	Walter Diaz Jose	Colvias	Almacenero	40174763	<i>[Signature]</i>	
10	Rocha Guy Mamani Michael	Colvias	Aux. RRHH	46044413	<i>[Signature]</i>	
11	Niño Diaz Alexis	Colvias	JEFE de Campo	42177790	<i>[Signature]</i>	
12	Caicedo Santoval Juan P.	Colvias	Jefe Equipos	000619658	<i>[Signature]</i>	
13	Chambi Laura Jorge	Colvias	Asist. Of. Tec.	46294806	<i>[Signature]</i>	
14	JENNIFER RODRIGUEZ	COLVIAS	MEDICO ASISTENCIAL	001798187	<i>[Signature]</i>	
15	Brazado Poma Leon	Colvias	Jefa SSO	45535332	<i>[Signature]</i>	
16	Fernandez Rayner Anon	Colvias	Sup. Campo	40765940	<i>[Signature]</i>	
17	Linares Lorna Olimar	Colvias	Ing. Control Proj.	46527000	<i>[Signature]</i>	
18	Hoyos Josán Karo C	Colvias	Jefe de DS	40503795	<i>[Signature]</i>	
19	BAZAN ESTRADA JOSE	COLVIAS	COORDINADOR O.T.	44987059	<i>[Signature]</i>	
20	Sosa Amezu Henry	Colvias	Sup. Topografía	42060886	<i>[Signature]</i>	

Observaciones:

.....

.....

.....

.....

.....

.....



<b>PROYECTO QUELLAVECO</b>		<b>REGISTRO DE INDUCCIÓN, CAPACITACIÓN, ENTRENAMIENTO Y SIMULACROS DE EMERGENCIA</b>		<b>COLVIAS</b>
Razón Social: COLVIAS S.A.C RUC: 20603730637 Dirección: Av. Juan Arona Nro. 755 Piso 10 Oficina 113 - Urb. Santa Cruz - San Isidro - Lima Actividad Económica: Construcción			N° Trabajadores en el centro laboral Aprox: <u>    </u>	N° Registro <u>02</u>

Tema:	Aplicación de Encuesta de Mejora de Procesos de Gestión de Riesgo de Tecnología ...			
Facilitador/Lugar:	José Antonio Rodríguez Lueroz	Op. Colvias	Inducción	Simulacro de Emergencia
Firma:	<i>[Firma]</i>	N° Asistentes: 20	Capacitación	Toolbox
Fecha: 26/05/2020	Hora Inicio: 17:00	Hora Fin: 17:30	N° de Horas: 30'	Entrenamiento
				Otro <input checked="" type="checkbox"/>

N°	APELLIDOS Y NOMBRES	EMPRESA - CONTRATO	PUESTO DE TRABAJO	DNI	FIRMA	NOTA
1	Martinez Moron Alexandra	Colvias	AUX Equipos	44425391	<i>[Firma]</i>	
2	Alejandro Andrade Ch.	Colvias	Medico Ocupacional	40971891	<i>[Firma]</i>	
3	Estefanía Larra Piña	Colvias	Abogada	43417492	<i>[Firma]</i>	
4	VALDIVIEZO MARIQUE PAHELA	COLVIAS	Coord. Coach Mot.	40669796	<i>[Firma]</i>	
5	Alvarado Manami Danny	Colvias	Asist. Personal	44748607	<i>[Firma]</i>	
6	Elvis Lopez Gomez	Colvias	Cadista	46472457	<i>[Firma]</i>	
7	Julio Julca Garcia	Colvias	Sup. Adm	25775665	<i>[Firma]</i>	
8	ROEDA VICENTO CHRISTIAN	COLVIAS	CA-J	40612579	<i>[Firma]</i>	
9	Alvaro Cochon Ceaman	Colvias	Exp. Gest. Doc. y Seg	29842658	<i>[Firma]</i>	
10	Zamora Huacña Alfredo	Colvias	Coord. RR.HH.	44631581	<i>[Firma]</i>	
11	Estada Quiso Elizabeth	Colvias	Asist. Social	29666854	<i>[Firma]</i>	
12	Pengifo Grandes Karla	COLVIAS	Generalista RR.HH	45453843	<i>[Firma]</i>	
13	GRONERA JITO CAROLINA	COLVIAS	ASIST. RR.HH.	72612717	<i>[Firma]</i>	
14	Gonzales Gamboa Norman	Colvias	Director Adm. y F.	09304806	<i>[Firma]</i>	
15	Jessenia Perille Baltian	Colvias	Secretaria de Obra	04440103	<i>[Firma]</i>	
16	Jorge Sabas Castro	colvias	Asist. Compras	09564351	<i>[Firma]</i>	
17	Jimenez Lema Jessica	Colvias	Asist. Gestion Ind	77094549	<i>[Firma]</i>	
18	Basanova Luis	Colvias	Residente de Obra	4372542	<i>[Firma]</i>	
19	Navarria Tragon Luis	Colvias	Coord. F.I	44899873	<i>[Firma]</i>	
20	ARBOLEDA GOENAGA FRANCISCA	COLVIAS	DIRECTOR DE CONST	00248897	<i>[Firma]</i>	

Observaciones:

.....


.....

.....

.....

.....

.....

<b>PROYECTO QUELLAVECO</b>		
<b>REGISTRO DE INDUCCIÓN, CAPACITACIÓN, ENTRENAMIENTO Y SIMULACROS DE EMERGENCIA</b>		
Razón Social: COLVIAS S.A.C RUC: 20603730837 Dirección: Av. Juan Arona Nro. 755 Piso 10 Oficina 113 - Urb. Santa Cruz - San Isidro - Lima Actividad Económica: Construcción		N° Trabajadores en el centro laboral Aprox: <u>    </u>
		N° Registro <b>03</b>

Tema:	Aplicación de Encuesta de Mejora de Procesos de Gestión de Riesgo de Tecnología...				
Facilitador/Lugar:	José Antonio Rodríguez Acevedo	Op. Colvias	Inducción	Simulacro de Emergencia	
Firma:	<i>[Signature]</i>	N° Asistentes:	11	Capacitación	Toolbox
Fecha: 26/05/2020	Hora Inicio: 13:00	Hora Fin: 13:30	N° de Horas: 30'	Entrenamiento	Otro <input checked="" type="checkbox"/>

N°	APELLIDOS Y NOMBRES	EMPRESA - CONTRATO	PUESTO DE TRABAJO	DNI	FIRMA	NOTA
1	Centeno Velazquez Mariel	COLVIAS	Ing. Of. Técnica	71821192	<i>[Signature]</i>	
2	Echevarria Retuer Felix	Colvias	Jefe de Gestión SSO	25802258	<i>[Signature]</i>	
3	Fustamante Resquejo Christian	Colvias	Ing. Planeamiento y C	44170738	<i>[Signature]</i>	
4	Gonzalo Del Campo José L.	Colvias	Sup. Rend. de Mesa	10494731	<i>[Signature]</i>	
5	Losa Farfan Manuel A.	Colvias	Jefe de Calidad	46390539	<i>[Signature]</i>	
6	Martinez Pulido Oscar	Colvias	Jefe control Proy.	000606319	<i>[Signature]</i>	
7	Torres Ortiz Manuel	COLVIAS	Director de Proy.	06624220	<i>[Signature]</i>	
8	Requero Chavez Marco	COLVIAS	Jefe de Planta	44863502	<i>[Signature]</i>	
9	Joselyn Bustos Vega	Colvias	Director de RRHH	08694034	<i>[Signature]</i>	
10	Johana Ortiz	Colvias	Director D.S.	00176796	<i>[Signature]</i>	
11	Alberto Yunga Salinas	Colvias	Aux. Contable	44421378	<i>[Signature]</i>	
12						
13						
14						
15						
16						
17						
18						
19						
20						

Observaciones:

.....

.....

.....

.....

.....

.....