UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSGRADO

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN PARA MINIMIZAR LOS RIESGOS DE LOS PROCESOS QUE SOPORTA EL ÁREA DE TI EN INSTITUCIONES DE EDUCACIÓN BÁSICA REGULAR DE LA REGIÓN DE LAMBAYEQUE

TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR
BRAYAN YERAK HUAMAN VILLANUEVA

ASESOR
RICARDO DAVID IMAN ESPINOZA
https://orcid.org/0000-0003-0409-8773

Chiclayo, 2021

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN PARA MINIMIZAR LOS RIESGOS DE LOS PROCESOS QUE SOPORTA EL ÁREA DE TI EN INSTITUCIONES DE EDUCACIÓN BÁSICA REGULAR DE LA REGIÓN DE LAMBAYEQUE

PRESENTADA POR:

BRAYAN YERAK HUAMAN VILLANUEVA

A la Escuela de Posgrado de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR:

María Ysabel Arangurí García

PRESIDENTE

León Tenorio Gregorio Manuel

SECRETARIO

Ricardo David Iman Espinoza

VOCAL

Agradecimientos

Esta tesis es dedicada a Dios quién supo guiarme por el buen camino y darme las fuerzas necesarias para poder continuar sin desfallecer.

A mi familia, quienes con sus palabras de aliento no me dejaron decaer para seguir adelante. Por quienes soy una persona con valores y principios, lo que me ha permitido lograr con perseverancia mis objetivos.

Gracias también a mi asesor quien con su paciencia y dedicación me pudo orientar en este proceso, apoyando a que este sueño pueda hacerse realidad.

Índice

Lista de figuras

Resumen

Esta investigación se centra en establecer a las instituciones educativas un modelo de gestión de riesgos de tecnología de información que les permita minimizar los diferentes riesgos de los procesos que son soportados por el área de TI, para ello se realizó un análisis a 5 instituciones de educación básica regular para conocer la situación actual, donde se demostró que las áreas de TI no tienen identificado los diferentes servicios que brinda a las instituciones, ni mucho menos a los activos que dan soporte a estos servicios, generando un aumento de probabilidades a posibles riesgos que pueden originar las interrupciones en los servicios ofrecidos, paralizando diferentes actividades dentro de la organización.

Para el desarrollo del modelo se realizó una armonización de estándares, metodologías o marco de trabajo que hagan énfasis en la gestión de riesgo, las cuales sirvieron como base para el modelo propuesto que tiene como objetivo minimizar los riesgos que puedan afectar a los servicios que dan soporte a los procesos de las instituciones educativas. Este modelo fue validado por expertos para medir su confiabilidad usando el alfa de Cronbach y la concordancia del contenido usando Kendall.

Por último, el modelo fue aplicado en un caso de estudio, en donde se identificó 23 activos críticos que dan soporte a los diferentes procesos de la institución educativa, de las cuales se identificó un total de 38 escenarios de riesgos, siendo 15 riesgos con niveles altos. Lográndose proponer diferentes proyectos para minimizar o mitigar los diferentes riesgos identificados.

Palabras claves: Instituciones educativas, básica regular, gestión de riesgo, activos de información, metodologías.

Abstract

This research focuses on establishing an information technology risk management model for educational institutions that allows them to minimize the different risks of the processes that are supported by the IT area. To this end, an analysis was carried out on 5 educational institutions Regular basic to know the current situation, where it was shown that the IT areas have not identified the different services that they provide to the institutions, much less to the assets that support these services, on the other hand, being able to generate interruptions in the services offered paralyzing different activities within the organization.

For the development of the model, a harmonization of standards, methodologies or frameworks that emphasize risk management was carried out, which served as the basis for the proposed model that aims to minimize the risks that may affect the services they provide. support to the processes of educational institutions. This model was validated by experts to measure its reliability using Cronbach's alpha and content concordance using Kendall.

Lastly, the model was applied in a case study at a regular basic education institution in the Lambayeque region, where 23 critical assets that support the different processes of the institution were identified, of which a total of 38 risk scenarios, with 15 risks with high levels. Being able to propose different projects to minimize or mitigate the different risks identified.

Keywords: educational institutions, regular basic, risk management, information assets, methodologies.

I. Introducción

El presente trabajo de investigación, se evaluó uno de los desafíos que las áreas de TI de afrontan en las instituciones de educación básica regular, que es convertirse en un aliado de valor para el negocio, para ello deben estar alineados con la organización. Según Pastor [1], indica que las TI presentan dificultades para alinearse con el negocio, debido a la falta de un gobierno de TI o por la falta de un modelo que ayude a demostrar el valor que estas aportan a las organizaciones.

Teniendo en cuenta que todos los recursos de una organización siempre están expuestos a diferentes tipos de amenazas, las cuales pueden generar pérdidas económicas o interrupción en sus servicios, si estas no cuentan con un plan de respaldo ante posibles fallas o ataques a los servicios de TI. [2] [3]. Es por ello que algunas organizaciones toman como prioridad la evaluación y gestión de riesgos, porque, consideran a la información como un recurso estratégico vital para la productividad y competitividad organizacional permitiendo que puedan lograr el éxito, tengan una continuidad y una ventaja competitiva en el mercado [4].

En el contexto internacional, el estudio realizado por IBM Security y Ponemon Institute (USA) acerca de la violación y pérdida de información, la cual fue realizado en 11 países y 2 regiones, donde participaron un total de 419 organizaciones obtuvieron que la pérdida de información va desde los 2.600 hasta los 100.00 registros comprometidos, generando una pérdida de $3.62 millones de dólares. También identificaron las causas de violación de datos, las cuales eran por ataques maliciosos (47%), fallas del sistema (28%) y por factor humano (25%), de las cuales el costo por cada registro perdido va desde los $156, $128 y $126 respectivamente, teniendo un aumento del (1.8%) respecto a años anteriores. [5].

El informe sobre los riesgos de TI, que las instituciones educativas enfrentan, realizado por Brooks, Ryan [6], muestran que las organizaciones educativas no siempre toman las decisiones correctas acerca de la de la seguridad de sus activos, por lo tanto, no pueden identificar qué y quién representa una amenaza real para sus diferentes activos. Por ello realizaron una encuesta a 125 organizaciones, donde identificaron los riesgos más comunes de TI, estos riesgos lo podemos clasificar en: riesgos críticos, medios y bajos.

Las instituciones educativas consideran como un riesgo crítico, la pérdida de datos, donde las causas más comunes son los errores que comenten los usuarios, el equipo de TI en la manipulación de datos, las cuales representan el (78%), otros de los motivos son los ataques por hackers que representan el (37%). Otro de los riesgos críticos, es la violación de datos, las razones principales por lo que este riesgo se materializa son por los errores de los miembros del equipo de TI (33%), por errores de usuario con el (29%), ataques por phishing (27%) o por el uso de contraseñas compartidas entre los diferentes usuarios con el (23%). Las consecuencias que se ocasionan cuando estos riesgos se manifiestan, son daños en su reputación, y los enormes costos para restaurar los datos.

Entre los riesgos medios que las instituciones educativas consideran son, la interrupción de sistema, entre los principales motivos de que los sistemas que ofrece el área de TI fallen tenemos el corte de energía eléctrica con un (39%), errores de usuarios (27%). El daño físico de hardware es otros de los riesgos que las instituciones educativas enfrentan, debido a que no son conscientes de la repercusión que pueden tener los daños en los activos de hardware, entre los incidentes que se detectaron están las fallas de energía (69%), las fallas propias del hardware (62%). Estos riesgos no conducen a consecuencias catastróficas, pero de igual forma generan pérdidas financieras, daños en la reputación e interrupción de los diferentes servicios que ofrece el área de TI a la institución.

El robo de propiedad intelectual, puede generar daños en la reputación, pérdida en la ventaja competitiva y gastos financieros, pero para las instituciones educativas este riesgo es de nivel bajo. Las causas que generan estos tipos de incidentes son los despidos con un (39%), errores de usuarios (24%), el abuso de privilegios en los usuarios (17%) y por hackers (58%).

Panchal [7], expresa que las instituciones educativas dependen cada vez más de los servicios TI para llevar a cabo sus procesos, aumentando la probabilidad de fallas operativas, debido a que, estas instituciones no toman en cuenta realizar una evaluación de riesgos de TI, debido a que estas instituciones tienen una visión limitada de exposición a los riesgos que están expuestos sus diferentes recursos, por lo tanto desconocen las diferentes amenazas que estos riesgos representan para el negocio [6].

En el contexto nacional, las instituciones educativas han comenzado automatizar sus procesos haciendo uso de los servicios de TI, generando que la información este expuesta a diferentes amenazas, la cual puede ocasionar pérdidas financieras, desventaja competitiva, debido a que no identifican las vulnerabilidades que sus activos están expuestos [8]. A pesar que existe diferentes marcos y estándares para la gestión de riesgos, los gerentes de los proyectos de TI no cuentan con una metodología adecuada, porque no tratan directamente al contexto de educación básica regular [9] [10]. Y las organizaciones que implementaron una gestión de riesgos, no lo hacen de una manera experimental, porque, desconocen cuál es el procedimiento para una evaluación de riesgos, afrontándose a situaciones adversas que pueden afectar a la organización, generando pérdidas financieras, interrupción en sus servicios [10].

Las instituciones educativas básicas regular de la región de Lambayeque, no es indiferente a la problemática que pueda tener el área de TI, con respecto a la gestión de riesgos, donde la evaluación realizada a cada institución fue aplicada a cada uno de los miembros del área de TI, donde se obtuvieron los siguientes resultados.

El (73.3%) de las personas encuestadas revelaron que no cuentan con un inventario de los activos de TI, además de no contar con controles, medidas, procedimientos para resguardar y preservar sus activos de información, tales como documentos físicos, software y dispositivos físicos. Por otro lado, el (86.7%) manifestaron que no tienen identificados los diferentes servicios que soporta el área de TI, siendo esto una de las actividades claves que se debería de tener para brindar un mejor soporte a los servicios que el área de TI ofrece a la organización.

Solo el (26.7%) de los encuestados expresaron que evalúan las diferentes amenazas a las que están expuestas sus activos del área de TI, identificando así sus riesgos internos y externos de cada uno de ellos, siendo esto, una da las funciones principales que toda organización debería de realizar, para establecer medidas de seguridad o planes de contingencia, en caso de que algún riesgo se logre materializar, de las cuales pueden afectar a los diferentes procesos que son soportado por el área de TI. A demás, tan solo el (13,3%) revelaron que dan seguimiento a los diferentes riesgos que se han presentado dentro de la institución, por lo tanto, el (86,7%) expresan que no cuentan con un manual de procedimiento ante posibles fallas de los diferentes servicios que

brindan a la institución y ni muchos menos tienen un registro histórico de los riesgos que se han manifestado anteriormente.

Debido a lo expuesto anteriormente, las áreas de TI deben de proteger sus activos, debido a que son el soporte de las organizaciones para mejorar sus procesos [11], por eso se plantea la siguiente interrogante: ¿Cómo implementar un modelo de gestión de riesgos para minimizar los riesgos que están expuestos los diferentes procesos que soporta el área de TI es instituciones de educación básica regular de la región de Lambayeque?, por lo cual esta investigación propone que la implementación de un modelo de gestión de riesgos, se pude minimizar los diferentes riesgos a que están expuestos los procesos que son soportados por el área de TI. Con este propósito, se planteó:

- Determinar el marco de trabajo más adecuado a utilizar en la investigación, mediante una evaluación comparativa entre los diferentes de marcos de trabajo existentes.
- Elaborar la propuesta de un modelo de gestión de riesgos para minimizar los riesgos de los procesos que soporta el área de TI en las instituciones educativas básicas regular de la región de Lambayeque.
- Validar el modelo de gestión de riesgos de tecnología de información, mediante juicio de expertos.
- Implementación parcial de modelo de gestión de riesgos de tecnología de información para minimizar los riesgos de los procesos que soporta el área de TI en las instituciones educativas básica regular de la región de Lambayeque.

La propuesta del modelo de gestión de riesgos de TI en instituciones educativas básica regular, permite hacer uso de manera eficiente de la infraestructura y delos servicios de TI que pude tener las instituciones educativas, mejorando sus procesos de negocio, debido a la planificación y gestión de riesgos, la cual impacta positivamente en el clima organizacional y genera una ventaja competitiva.

El modelo de gestión de riegos de TI en las instituciones educativas básica regular, permite evaluar las diferentes amenazas que están expuestos sus activos, permitiendo así realizar planes de contingencia y asignar recursos financieros para hacer frente a estos riesgos, logrando así reducir costo, esfuerzo y tiempo por la finalización tardía de un proceso o la interrupción de algún servicio que el área de TI ofrece a la institución educativa.

La gestión de riesgos de información en el área de TI, sirve para la mejora de tomas de decisiones en las instituciones educativas privadas, además de generar el mejor uso de sus diferentes recursos a través de las buenas prácticas y así poder obtener una ventaja competitiva sobre la demanda del mercado.

Considerando el aporte de investigación desde el punto de vista metodológico, en la propuesta de un modelo de gestión construido siguiendo los criterios y métodos utilizados en reconocidas metodologías de gestión de riesgos de TI.

II. Marco teórico

1.1 Antecedentes:

Según Vanegas [4], en su investigación tuvieron como objetivo realizar un análisis de riesgos para evitar que los proyectos de software fracasen, y así eludir las fallas frecuentes que existen a la hora de desarrollar un nuevo sistema, debido a que los diferentes procesos de las organizaciones dependen de los servicios que ofrecen el área de TI o de terceros. Para ello realizaron una comparación de diferentes modelos de riesgos de TI como: CRAMM , RISK IT, EBIOS ,MAGERIT, OCTAVE, COBIT, e ITIL V3, además de normas como: ISO/IEC 31010, ISO/IEC 27000, BS 7799-3:2006, UNE 71504:2008 y AS/NZS 4360, donde compararon sus diferentes actividades y características con respecto a la gestión de riesgos, donde plantearon un modelo "MOGRIT", donde aumentaron la confiabilidad de las organizaciones con los servicios de TI logrando minimizar el impacto de los diferentes riesgos.

Se toma en cuenta la presente investigación, debido a las diferentes comparaciones que realizan con respecto a la gestión de riesgos, tomándose como referencia para tener una visión más amplia de normas y estándares ISO, que puedan ser utilizadas en la presente propuesta de investigación a la hora de establecer el modelo adaptado en las instituciones educativas.

Según Moncayo [12], el problema que plantearon en su investigación, menciona que las MYPES no identifican sus activos, por lo tanto, desconocen los diferentes riesgos a los que están expuestos cada uno de ellos. Por otro lado, menciona que los diferentes modelos que existen para la evaluación de riesgos de TI no se adaptan a las necesidades de las medianas y pequeñas empresas, porque son muy complejas y requieren mucho tiempo para su implementación, la cual genera costos elevados que las instituciones no están dispuestas asumir. Para ello realizaron una comparación de diversas metodologías, como son: Norma internacional de información financiera, Magerit y Octave, donde se analizarán las diferentes fases de cada una de ellas, para adaptarlos a las necesidades de las MYPES y así aportar una metodología más factible para que puedan evaluar y analizar los diferentes riesgos que están expuestos sus activos y así poder tener prevenciones oportunas y adecuadas. Los resultados que se

lograron con la implementación del modelo propuesto fue disminuir el impacto de los riesgos identificados, a través de planes de acción.

Considerando que las instituciones educativas básica regular, puede ser considerada una MYPE, se toma como referencia esta investigación, porque permite identificar y determinar las vulnerabilidades de los activos de información, facilitando los parámetros de medición que podría ser utilizado en el modelo propuesto, además de proporcionar diferentes metodologías que pueden ser utilizadas en esta investigación.

Según Crespo [13], hace énfasis que las organizaciones utilizan cada vez más los sistemas informáticos, lo cual se convirtió en una de las mayores preocupaciones, porque buscan proteger su infraestructura y su información que es su activo más valioso. Por eso realizaron la comparación de estándares y metodologías: AS/NZS ISO 31000:2009, UNE 71504:2008, OCTAVE, ISO/IEC 27005:2011, MEHARI, CRAMM y MAGERIT, para llevar a cabo la auditoría en base al análisis de los riesgos logrando identificar las diferentes vulnerabilidades y amenazan que están expuestas los activos de la organización.

Esta investigación sirve como referencia ya que realiza una comparación de distintas metodologías donde resalta las técnicas y métodos que utilizan para el análisis de riesgos, la cual servirá para tener un enfoque más amplio a la hora de plantear técnicas e instrumentos en el análisis de riesgos dentro de las instituciones educativas.

Según Asencio [14], la información es considerada como uno de los activos más importante para las organizaciones, ya que a través de ella pueden tener una ventaja competitiva. Es por ello que debe ser protegida de las diferentes amenazas y vulnerabilidades a las que están expuesta, la cual pueden afectar a las instituciones. Por estas razones formuló una guía para la gestión de seguridad de la información basada en la NTP ISO/IEC 17799, ISO 27001 y COBIT 5 para minimizar los riesgos de gestión de la información asociados a confidencialidad, integridad, disponibilidad. Luego de llevarlo a cabo en un caso de estudio, se logró minimizar los diferentes riesgos que estaban expuestos sus activos referentes a la confidencialidad, integridad y disponibilidad.

Se toma como referencia a este antecedente, debido a que indica cómo detectar la situación actual de la organización, para luego poder definir de una manera más

certera un modelo que permita minimizar los riesgos, la cual facilita a la presente investigación porque facilita parámetros que podrían ayudar a detectar la situación actual de las instituciones educativas y así poder plantear una propuesta que mejor se adapte para poder lograr la minimización de los posibles riesgos.

Según Mercado [15], hace mención que las entidades del sector público están automatizando sus servicios a través de sistemas sofisticados, pero no tienen un modelo de seguridad para resguardar todos sus procesos, siendo esto una parte critica las entidades del sector público, por ello compararon 11 modelos de seguridad de la información, con el objetivo de armonizar un modelo que se adapte a las necesidades de este tipo de instituciones, la cual se propusieron 114 métricas e indicadores, la cual les permite a las instituciones medir el desempeño de sus controles e identificar en nivel de seguridad que cuentan sus servicios y así poder establecer las precauciones necesarias.

Esta investigación sirve como referencia, ya que realiza una comparación de diferentes modelos para poder establecer métricas e indicador para el control y seguridad e los procesos, ayudando a esta investigación a tener una visión general de los modelos que podrían ayudar a las instituciones educativas a la supervisión y control de sus procesos.

Según Guzmán [16], menciona que las organizaciones se apoyan en los servicios de TI para automatizar sus procesos, pero a su vez indica que estas organizaciones solo establecen controles de seguridad de manera aislada solamente cuando detectan que sus activos están expuestos amenazas, es por ello que se debe velar por la eficacia, eficiencia y la calidad de estos servicios con el fin de lograr la continuidad de cada uno de los procesos del negocio que las áreas de TI soportan. Si bien es cierto que existen diferentes estándares que tratan sobre la seguridad de información, pero no afrontan directamente a los grupos empresariales, la cual requiere consideraciones adicionales para que puedan identificar los diferentes servicios que las organizaciones dependen para su supervivencia. Es por ello que se basaron en ISO/IEC 27000 y en el estándar ISM3 para la seguridad de la información, donde evaluaron las metodologías desde diferentes enfoques, donde propusieron un modelo la cual se adaptaba a sus necesidades. Con la implementación de dicho modelo en un caso de estudio se detectó las diferentes amenazas que eran sometidos sus activos, logrando

implementar controles de seguridad, además de alcanzar un uso eficiente y eficaz de sus recursos de TI para dar soporte a sus procesos.

Con respecto a este antecedente, resalta que se debe tener registros de los activos de una organización para poder realizar una evaluación de amenazas de manera efectiva, la cual sirve como referencia a la presente investigación ya que uno de sus objetivos es identificar los diferentes activos de las áreas de TI que contribuyen a través de sus servicios a los procesos del negocio, permitiendo así identificar las diferentes amenazas para minimizar los riesgos a los que están expuestos.

Según Moscoso, Peña y Soto [17], en su investigación resalta que las empresas de saneamiento están altamente vinculadas con las herramientas que ofrece el área de TI como apoyo a sus procesos de negocio, donde resaltan que no se implementa adecuadamente la gestión de riesgos, por tanto, desconocen los diferentes riesgos que están expuestos sus diferentes activos y el impacto que podría traer si algún riesgo se materializa, además de los costos que implicaría la reposición de los activos involucrados. Estos tipos de empresas son supervisadas por el estado, cualquier alteración o perdidas de información conllevaría hasta 200 unidades impositivas tributarias (UIT). Por estas razones tuvieron que analizar diversos estándares y normas, como son la ISO 31000:20111, MARGERIT, OCTAVE, NIST y COBIT5, donde evaluaron las diferentes fases y etapas donde desarrollaron un modelo de gestión de riesgos para contribuir a la operación de sus procesos. La aplicación de este modelo logró formular 16 proyectos que trataban a 52 riesgos de alta prioridad, disminuyendo las pérdidas financieras y asegurando la continuidad de sus diferentes actividades del negocio.

Este antecedente se toma como referencia, por lo que desarrolla un modelo para poder identificar los activos y así definir los posibles riesgos a los que están expuestos, para poder elaborar un plan de acción con el fin de poder minimizar los riesgos, la cual se tomara en cuenta las diferentes metodologías que utilizaron y así poder orientarlo en las instituciones educativas.

Según Vásquez y Alva [18], menciona que las deficiencias de una gestión de riesgo dentro de una micro financiera puede ocasionar daños irremediables como el desprestigio institucional, pérdidas financieras, pérdidas en su cartera de clientes,

hasta la continuidad del negocio. Para ello se realizó una comparación de diferentes estándares y metodologías como son: la ISO/IEC31:2009,27005:208,2201:2012, OCTAVE, MARGERIT y COBIT 5, donde realizaron un análisis en cada una de las actividades de cada etapa, de las metodologías mencionadas anteriormente, con el objetivo de establecer un modelo que se adapte a las necesidades de las micro financieras. En su modelo propuesto indican que deben de establecer cuáles son sus procesos críticos para poder evaluar los riesgos a los que se encuentra expuestos. Con la implementación del modelo propuesto lograron identificar que el (44%) de sus macro procesos eran críticos, que el (22%) de sus macro procesos eran vitales para la organización.

Este antecedente se toma como referencia debido a que emplea ciertas técnicas para detectar situación actual de la empresa la cual puede servir en las instituciones educativas, además se rescatara el análisis que hicieron de las diferentes metodologías con respecto a las diferentes actividades que se deben de realizar en una implementación de gestión de riesgos.

Según Arangurí, Imán y León [10], en su investigación hacen referencia que en las diferentes universidades de la región de Lambayeque no se lleva a cabo de manera efectiva la gestión de riesgos, generando pérdidas de productividad debido a la interrupción de sus servicios , ya que no existe una guía estructurada que se adapte al contexto de este tipo de instituciones que ayude a la identificación de los diferentes riesgos a los que están expuestos sus recursos; además de que estas instituciones desconocen cuáles son los procesos soportados por el área de TI que les puede afectar si un riesgo se materializa. Para ello realizaron un análisis comparativo de las diferentes estándares y metodologías para identificar las fases coincidentes y plasmar un modelo que se adapte a las necesidades de las universidades. Con la implementación del modelo propuesto se logró identificar un total de 73 riesgos, de las cuales 11 eran de alta prioridad, para el cual establecieron 5 proyectos para tratar estos riesgos.

Se toma en cuenta este antecedente, porque, el modelo que propusieron es aplicada en las universidades privadas, la cual tiene una relación con la presente investigación ya que está orientada en las instituciones educativas privadas básica regulares, la cual

puede servir como referencia para la identificación de fases, la cual se podría utilizar los diferentes criterios para plasmar el modelo que se desea desarrollar.

1.2 Base Teórico Conceptual:

En este apartado se proporción los diferentes conceptos a cerca de la gestión de riesgos e instituciones básica regular, las cual han servido a la presente investigación como un sustento teórico para la propuesta, desarrollo implementación del modelo propuesto [19].

1.2.1 Instituciones educativas:

Las instituciones educativas tienen como objetivo lograr el aprendizaje de sus alumnos, estableciendo vínculos con su entorno y brindando las herramientas necesarias para el desarrollo personal [20]. Existen los siguientes tipos de instituciones educativas en el Perú según su tipo de gestión:

i. Públicas: Son gestionadas por autoridades nombradas por el estado peruano.

ii. Privada: Son gestionadas por personas jurídicas con el objetivo de brindar el servicio educativo utilizando sus propios recursos

iii. Públicas de gestión privada: Son dirigidas por entidades a través de un convenio, las cuales deben de prestar los servicios educativos de manera gratuita.

En el Perú, la educación básica es obligatoria, porque aquí se forma al educando de manera física, afectiva y cognitiva, logrando así desarrollando sus diferentes capacidades. Pera esta investigación nos centraremos en el sistema educativo básica regular.

1.2.1.1 Instituciones educativas Básica regular:

La educación básica regular esta dirigidos para niños y adolescentes, la cual está conformada por 3 niveles según el artículo 36 (de la ley 28044). Estas instituciones trabajan con un currículo nacional la cual es establecido y diseñado por el ministerio de educación del Perú (MINEDU):

i. Educación inicial: Este nivel está conformado por 2 ciclos, el primero ciclo I para niños menores a 3 años y el ciclo 2 que lo comprenden niños que están en la edad de 3 a 5 años. Para pasar este nivel es obligatorio al menos llevar el último año.

ii. Educación primaria: Comprendida desde los 6 años hasta los 12 años, uno de los requisitos primordiales en este nivel es aprobar por lo menos uno de los cursos básicos que es lenguaje o matemática. Está conformado por 3 ciclos, el ciclo III que lo comprende alumnos de primer y segundo grado, el ciclo IV conformado por alumnos de tercer y cuarto grado y el ciclo V agrupados por alumnos que están en los últimos grados que son quinto y sexto grado de primaria.

iii. Educación secundaria: Este es el último nivel, el cual está dirigido a jóvenes de 12 a 17 años. Este nivel se encuentra organizado por 2 ciclos, el ciclo VI conformado por alumnos que se encuentran cursando los primeros años del nivel secundario que son los del primer y segundo año y el ciclo VII conformados por alumnos de tercer hasta el quinto año de secundaria.

Todos los ciclos de los diferentes niveles son obligatorios, según lo establecido por el MINEDU

1.2.1.2 Reporte de instituciones educativas básica regular

Según el reporte que brinda el ministerio de educación son un total de 1802 instituciones educativas básica regular que existen en la región de Lambayeque, las cuales comprenden los niveles inicial, primaria o secundaria, de las cuales 1191 son de gestión pública y 611 son de gestión privada.

1.2.2 Gestión de Riesgos de TI:

1.2.2.1 Gestión

La gestión es un conjunto de actividades que se tienen que realizar para cumplir los objetivos propuestos, por lo tanto, las instituciones educativas deben de establecer sus objetivos, para ello deben de planificar cada una de las estrategias

que utilizarán, los recursos que serán necesarios y los controles que se tendrán en cuenta con el fin de implementar cada uno de los planes y alcanzar los objetivos propuestos [21, p. 140].

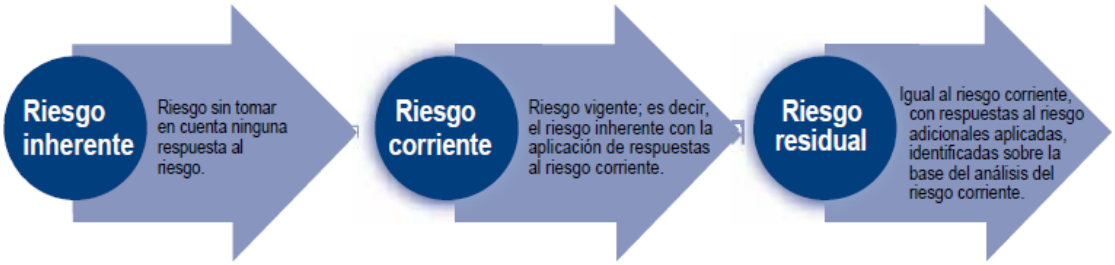
1.2.2.2 Riesgo

Cuando hablamos de riesgos, hacemos referencia a eventos cuyos resultados pueden generar daños inesperados sino tenemos las precauciones adecuadas. Existen varios tipos de riesgos, pero en esta investigación hacemos referencia a los riesgos operativos, que según la Real Academia Española (RAE) define como: "…riesgo que sufre una empresa derivada de la posibilidad de fallos en su propio funcionamiento" [22].

Según COBIT [23], los riesgos se pueden clasificar de 3 formas:

- Riesgos inherentes, son aquellos riesgos que están presentes pero las instituciones no realizan ningún tipo de acción para cambiar su probabilidad o cambiar su impacto.
- Riesgo corriente: Es aquel riesgo inherente, a pesar de establecer algún tipo de respuesta.
- Riesgo residual: Son aquellos riesgos a las cuales se han establecido acciones y se encuentra en los niveles establecidos por las instituciones.

Figura 1: Tipos de riesgos



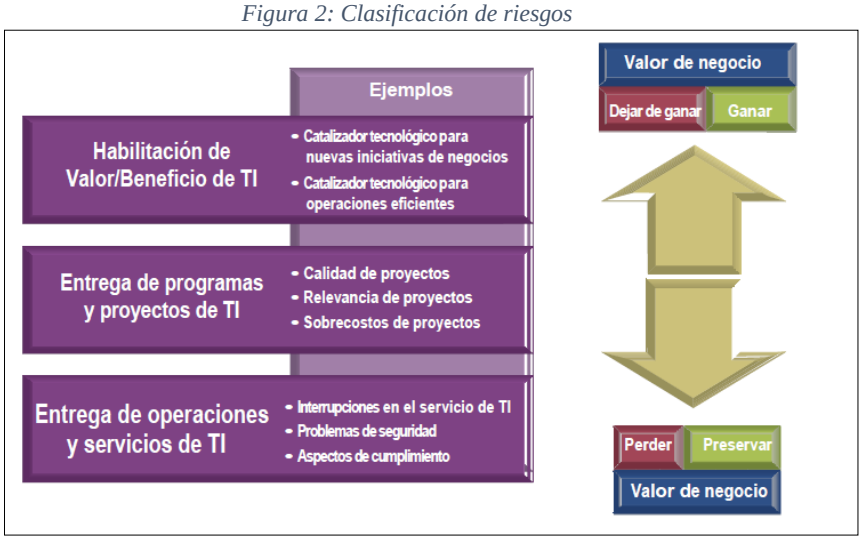
Fuente 1: COBIT FOR RISK

1.2.2.3 Riesgos de TI

El riesgo de TI son los posibles sucesos que pueden afectar a las organizaciones para alcancen sus objetivos, las cuales pueden presentarse con cierta frecuencia sino son gestionados correctamente por las organizaciones. Los riesgos pueden

están presentes en diferentes niveles dentro del área de TI, pueden existir riesgos en los servicios que área de TI brinda hacia la organización como por ejemplo la interrupción de algún servicio necesario para la institución pueda realizar sus actividades sin ningún problemas o problemas de seguridad la cual puede ocasionar perdida de información o alteración de esta, otro tipo de riesgo a los que están expuesto el área de TI son en la entrega de proyectos que se van elaborando como puede ser que el proyecto no cumple las expectativas del personal de la institución o por problemas internos no se puede entregar, como se puede apreciar en la siguiente imagen 1.

Figura 2: Clasificación de riesgos



Fuente: 2 Extraído de [23]

Los riesgos de TI siempre van a estar presente como se muestra en la imagen 1, independientemente si son reconocidos o no por las instituciones, por eso [23], recomienda realizar una buena gestión de riesgos de TI, para así evitar incertidumbres dentro de la organización y poder cumplir con los objetivos planteados.

1.2.2.4 Gestión de riesgos de TI

Según la norma AS/NZS [24, p. 16] “La gestión de riesgos puede ser aplicada a muchos niveles en una organización.”. Considerando que las instituciones educativas están expuestas a diversas variedades de riesgos que pueden afectar en diversos aspectos haciendo un incierto el alcance de sus objetivos, por eso, que la gestión de riesgos es importante porque ayuda a establecer estrategias con el fin de identificar los posibles riesgos para evaluar su impacto y probabilidad antes de

que estos riesgos lleguen a materializarse con el fin de establecer medidas preventivas que ayuden a reducir su efecto negativo en la organización.

Se toman en cuenta las fases principales que se debe de tomar en cuenta para realizar una implementación de gestión de riesgos, las cuales fueron tomadas según la ISO 31000 [25]:

a) Establecer el contexto y criterios: Sirve para establecer los diferentes factores tanto dentro como fuera de la organización que podrían repercutir en el alcance de los objetivos establecidos por las instituciones. Otra de las actividades importantes dentro de la gestión de riesgos es establecer los criterios de aceptación y evaluación, ya que les permite saber desde un principio de que niveles de probabilidad e impacto las instituciones están dispuestas asumir.

b) Evaluación del riesgo: Es el proceso principal dentro de toda la gestión de riesgos, para ello se debe realizar de una manera sistemática y utilizar los conocimientos de las partes interesadas ya que ellos conocen la realidad actual de las organizaciones. Lo primero que se debe de realizar en esta actividad es la identificación de los riesgos, para luego proceder analizar y evaluar estos riesgos con los criterios definidos en la etapa anterior y así poder identificar los riesgos que podrían afectar a las instituciones.

c) Tratamiento de los riesgos: Una de las actividades principales en esta etapa es decidir que tratamiento se debe para abordar los diferentes riesgos que se han detectado y que pueden ser críticos para las organizaciones.

d) Seguimiento y revisión: Uno de los objetivos principales que abarca esta fase es de dar seguimiento a cada una de las etapas establecidas dentro de la gestión de riesgos, con el fin de comunicar los hallazgos que se van encontrando y así dar una mejora continua en cada implementación.

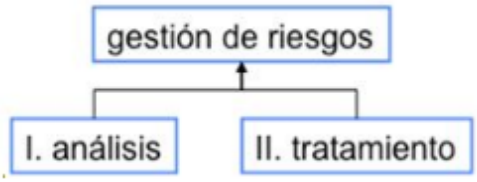
1.2.2.5 Metodologías para la gestión de Riesgos:

En este apartado haremos referencia a las diferentes metodologías que en sus procedimientos permitan identificar y tratar los diferentes riesgos que hoy en día están expuesto los diferentes activos tecnológicos, para luego poder ser enfocados desde el contexto de las instituciones educativas con el fin de minimizar los diferentes riesgos a los que están expuesto y así asegurar el desarrollo de sus actividades.

1.2.2.5.1 Magerit:

Esta metodología fue elaborada por el Consejo Superior de Administración Electrónica, la cual está enfocada directamente para el uso de las TI, donde se tiene como objetivo minimizar los riesgos de los diferentes recursos que son utilizados para brindar los diferentes tipos de servicios que puede ofrecer una organización. Magerit es una metodología que permite identificar el valor que tiene cada recurso y por lo tanto saber que se debe de proteger, para ello establece 2 requisitos mínimos para una protección adecuada de la información, que es el análisis y el tratamiento de los riesgos [26].

Figura 3: Gestión de riesgos

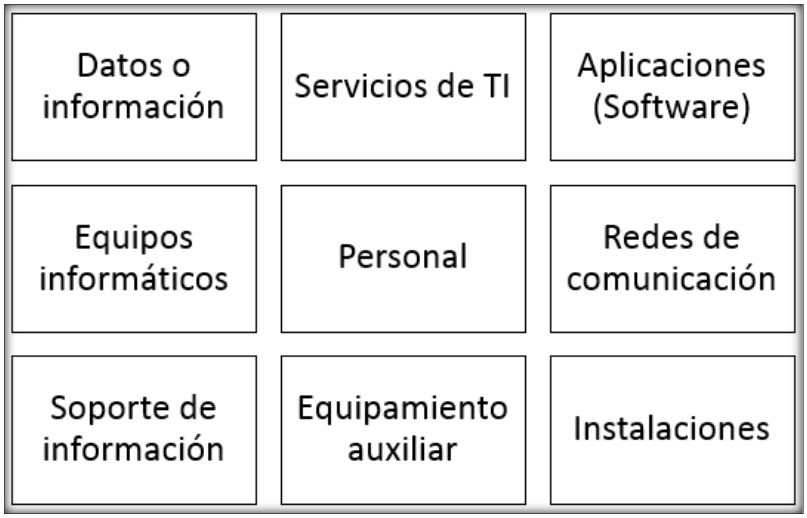


Fuente: 3 MAGERIT [26]

En el proceso de análisis y gestión de riesgos establecido por Magerit, la actividad principal es la identificación de activo para poder analizar las diferentes amenazas a las que se encuentra. Una vez identificado los riesgos hacen uso de un mapa de riesgos, con el objetivo de poder identificar de manera más practica los diferentes niveles de riesgos que presenta la institución, también presenta un conjunto de salvaguardas que las instituciones pueden utilizar como referencia para dar respuestas a los riesgos ya identificados y así poder establecer un conjunto de programas de seguridad.

Por lo mencionado en el párrafo Magerit [26, p. 23], estable diferentes tipos de activos como se muestra en la figura 3, sobre las cuales, las organizaciones deben de identificar que activo cuentan en cada uno de los perfiles establecidos con el objetivo de poder identificar las amenazas potenciales y a la vez poder establecer salvaguardas por cada uno de ellos

Figura 4: Catalogo de activos



Fuente 4: Magerit [26, p. 23]

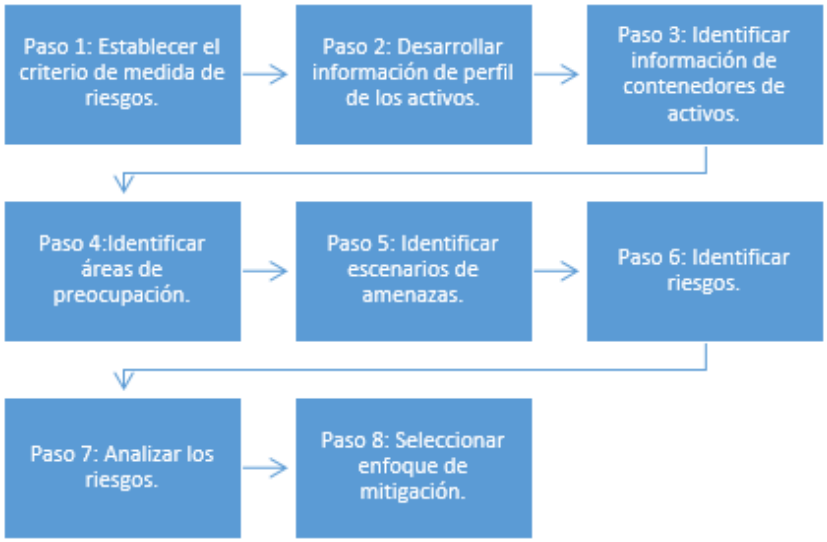
Los objetivos que toma en cuenta Margerit [26], menciona lo importante que es, que las organizaciones tengan en cuenta dentro de sus actividades la implementación de una gestión de riesgos, la cual debe ser realizada de manera sistemática para tener una mejor planificación y control sobre los riesgos identificados. Por ello las instituciones educativas básica regular, deben de tomar en consideración estas recomendaciones, con el objetivo de identificar los diferentes riesgos a los que están expuestos los activos que soportan los diferentes procesos del área de TI, que pueden afectar de manera parcial o completa los diferentes procesos de las instituciones de educación básica regular, por eso es recomendable que este tipo de instituciones realicen una implementación de gestión de riesgos para evitar diferentes tipos de consecuencias que podrían afectar a estas instituciones.

1.2.2.5.2 OCTAVE ALLEGRO

Esta metodología es adecuada para la evaluación de los riesgos, para organización que no cuentan con alguna experiencia suficiente en la gestión de los riesgos. Se

enfoca en el riesgo organizacional y en su estrategia. Tiene como objetivo anticiparse a la materialización de las amenazas.

Figura 5: Fases de OCTAVE Allegro



Fuente: 5 Octave Allegro [27]

Según la imagen 4 [27], esta metodología cuenta con 8 pasos, las cuales son:

1. Establecer criterios de medición del riesgo: Aquí se establecen los criterios que las instituciones deben utilizar para medir el riesgo y como este afectaría en la organización. Este modelo establece un conjunto de criterios para evaluar las diferentes consecuencias que se tendrían, la cuales las clasifica en las siguientes categorías (Reputación o confianza del cliente, financiera, productividad, seguridad y problemas legales).

2. Desarrollar perfil de los activos de información: Aquí se establece los perfiles de cada uno de los diferentes activos de la organización. En el perfil de cada activo se deben describir características únicas. Se enfoca en los activos de información que tienen valor para la organización.

3. Identificar los contenedores de activos de información: Se identifica los lugares donde los activos se almacenan, y procesan. Estos contenedores pueden ser de tipo técnico, físico o humano.

4. Identificar las áreas de preocupación: Aquí se detalla las situaciones que podrían afectar a los activos de la organización.

5. Identificar escenarios de amenazas: Se debe establecer varios escenarios de riesgos por cada activo, para así identificar las amenazas y los medios por el cual se pude llevar a cabo logrando afectar a los activos. Un escenario de riesgo debe establecer los siguientes factores: Actor ya sea interno o externo, el motivo de la amenaza y la consecuencia que esta tendría.

6. Identificar el riesgo: Aquí se identificar las consecuencias que se tendría en la organización si una amenaza se materializa. En este paso se determina el impacto de cada riesgo identificado, la cual se calcula con la siguiente ecuación "… Riesgo= Amenaza(condición) + Impacto (consecuencia) [27]."

7. Analizar el riesgo: En este paso se clasifica los riesgos de acuerdo a su impacto y probabilidad y como estos afectarían a las áreas de preocupación.

8. Seleccionar un enfoque de mitigación: Una vez que los riesgos identificados hayan sido clasificados por su impacto y probabilidad, se establece estrategias para la mitigación de estos.

1.2.2.5.3 NIST

La National Institute of Standards and Technology NIST [28], ve a la evaluación de riesgos como un elemento clave que abarca a toda la organización, la cual lo divide en 4 componentes que son necesarios para una buena gestión de riesgos:

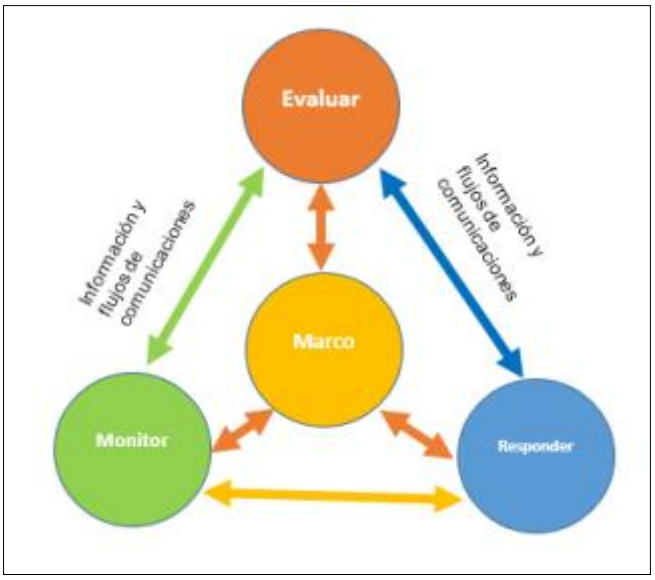
1. El primer componente tiene como propósito establecer una estrategia base para la gestión de riesgos que vayan acorde a las necesidades de la organización y que facilite la toma de decisiones a la hora de responder y monitorear los riesgos.

2. El segundo componente, su función principal es detectar diferentes amenazas y vulnerabilidades internas o externas que puedan ser explotadas y causar daños considerables a la organización.

3. En el tercer componente, tiene como objetivo establecer planes de acción como respuesta a los diferentes riesgos detectados, de acuerdo a la tolerancia al riego que la organización se haya establecido.

4. El cuarto componente, encargado de evaluar que tan efectiva fue la respuesta a los riesgos, además de verificar la implementación de las respuestas a los riesgos que han sido planteadas anteriormente.

Figura 6: Componentes claves de la NIST 800-30



Fuente: 6 NIST 800-30 [28]

En general, NIST SP 800-30 proporciona una guía para la evaluación de los riesgos, la cual está compuesta por los siguientes 9 pasos:

1. Caracterización del sistema: Aquí se establece el alcance y los límites operacionales para la evaluación de riesgos.

2. Identificación de amenazas: Se identifican las fuentes de motivación para las amenazas.

3. Identificación de vulnerabilidades: Se enumera las debilidades de cada uno de los activos, las cuales podrían ser explotadas por las amenazas.

4. Control de análisis: Se verifica la existencia de controles actuales sobre los activos.

5. Determinación de probabilidades: Se evalúa la probabilidad de que las vulnerabilidades de los activos sean explotadas y se conviertan en amenaza para la organización.

6. Análisis de impacto: Se analiza en cuanto impactaría a la organización, si los riesgos identificados llegarán a ocurrir.

7. Determinación del riesgo: Ayuda evaluar el riesgo en los sistemas de información.

8. Recomendación de controles: Aquí se establece estrategias para reducir el nivel de impacto hasta un nivel aceptable para la organización.

9. Documentación de resultados: Informe de la descripción de las amenazas y vulnerabilidades, la cuales sirve para tener como referencias en evaluaciones futuras.

Figura 7: Evaluación de riesgos según NIST 800-30

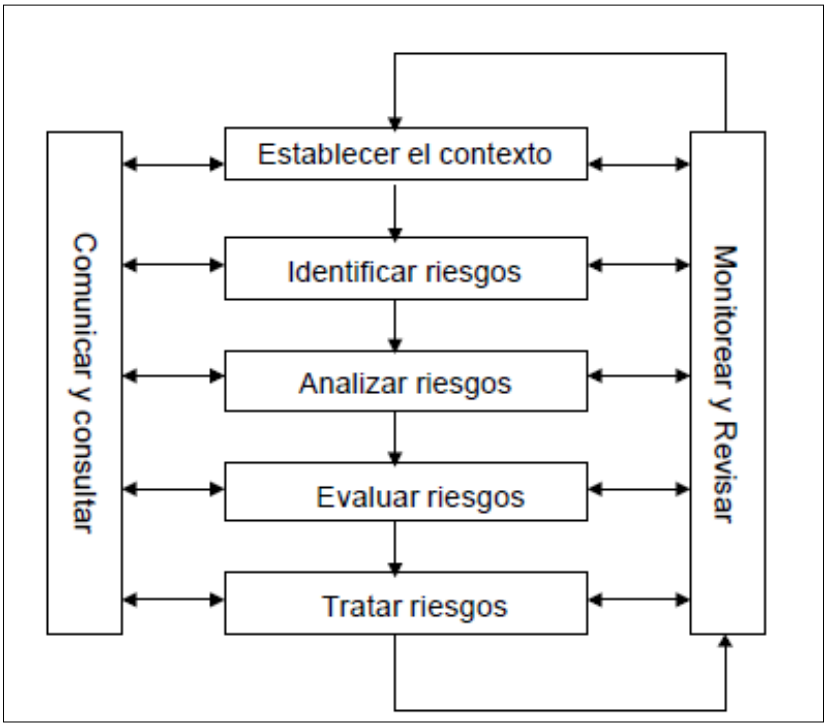
Fuente: 7 NIST 800-30 [28]

La utilización de la NIST 800:30, puede aportar a las instituciones educativas básica regular con la protección de sus diferentes sistemas de información, que estas utilizan para procesar y almacenar información valiosa y crucial para las organizaciones. Es por ello que la NIST recomienda a las organizaciones gestionar sus riesgos debe ser una actividad esencial, con el fin de proteger sus elementos claves para que puedan alcanzar sus objetivos.

1.2.2.5.4 AS/NZ 4360:204

Este estándar provee una guía para para la administración de los riesgos, la cual puede ser aplicado a todas las etapas de una actividad, función, proyecto, producto o activo. El diseño y la implementación de esta norma puede ser adaptado de acuerdo a las diferentes necesidades que presenten las organizaciones. Las fases que se tiene en cuenta en esta norma es el establecimiento del contexto, la identificación, análisis, evaluación y tratamiento de los riesgos identificados [24].

Figura 8: Fases de gestión de riesgos según AS/NZ



Fuente: 8 Obtenido de AS/NZ 4360:204 [24]

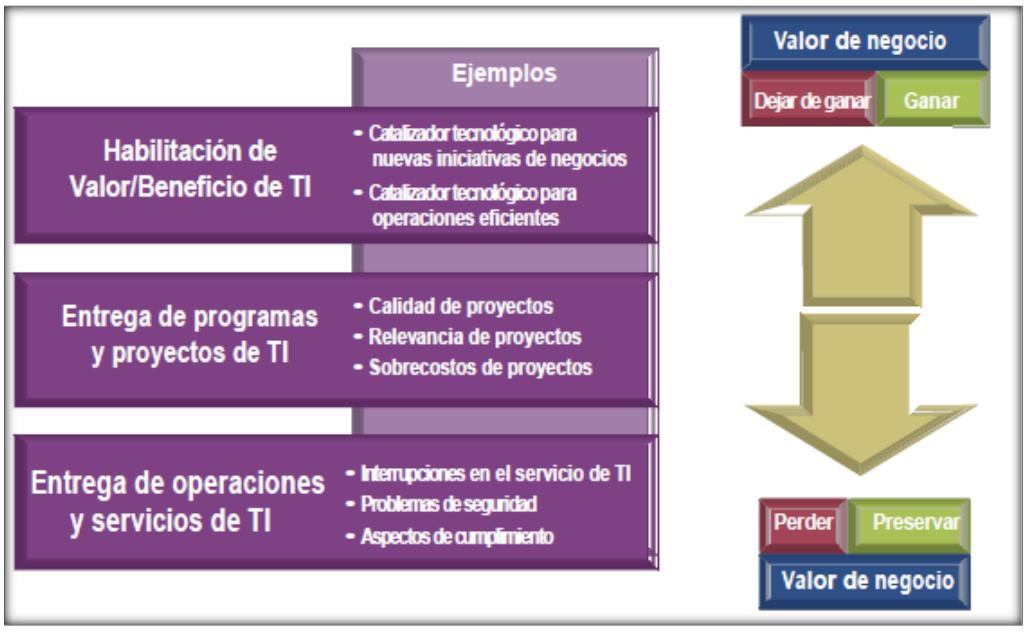
Esta norma puede contribuir a la identificación de oportunidades y amenazas de las instituciones educativas, permitiendo así mejorar su gestión de incidentes, la cual tienen como objetivo la reducción de las pérdidas, que se pueden generar cuando un riesgo se materializa. Es por ello que a las instituciones educativas básicas regular se debe de persuadir para que tengan una gestión proactiva y no reactiva a la hora de gestionar los diferentes riesgos a los que están expuestos sus activos, las cuales pueden ocasionar diferentes interrupciones en sus procesos.

1.2.2.5.5 COBIT FOR RISK

COBIT para riesgos considera a la información como un recurso importante para las organizaciones, sobre cual la tecnología juega un papel muy importante, porque, a través de ella se obtiene, se analiza y se distribuye a las diferentes áreas de las instituciones, poro COBIT se centra en los procesos básicos de la gestión de riesgos que va desde el análisis de la situación actual en las que se encuentra las instituciones, el establecimiento de criterios, la establecimiento de escenarios de riesgos hasta la generación de una cultura del riesgo [23].

Este marco de trabajo [23], puede ser utilizado para organizaciones del sector público y privado, para crear valor en la obtención de beneficios a un costo óptimo de los recursos mientras se optimiza los riesgos. Los beneficios pueden ser financiero, en sus servicios, etc., por ello establece ciertas categorías para poder identificar los diferentes riesgos de TI, como se muestra en la Figura 7:

Figura 9: Categorías de riesgo de TI



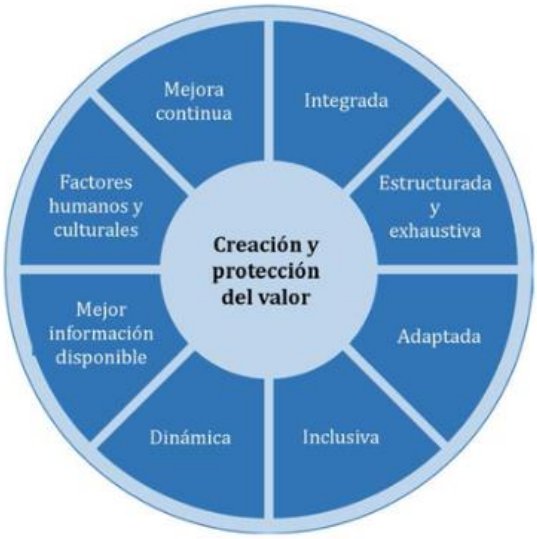
De las categorías establecidas por COBIT [23], resaltan riesgos asociados a las pérdidas de utilización de tecnología, riesgos al utilizar nuevas tecnologías para mejorar procesos, riesgos en la entrega de los servicios ofrecidos por TI. También menciona que se debe tener en cuenta que no siempre se puede evitar el riesgo, por lo tanto, se debe establecer el apetito del riesgo con el fin de poder definir lo que las instituciones están dispuestas asumir.

1.2.2.6 Estándares ISO para la gestión de riesgos:

1.2.2.6.1 ISO 31000:

Este estándar tiene como propósito asistir a las organizaciones durante la integración de la gestión de riesgo con el fin de crear y proteger todo aquello que tenga valor para ellos, por ello, establece una serie de principios como se muestra en la Figura 8, que las organizaciones deben de tener en cuenta durante el proceso de gestión de riesgos [25]. .

Figura 10: Principios de la ISO 31000



Fuente 9: ISO 31000 [25]

Para la implementación de gestión de riesgos, según la ISO 31000, se debe de considerar lo siguiente [25]:

- Las organizaciones deben de establecer lo que desean lograr en cada una de las actividades de la gestión de riesgos alineándolo a sus objetivos y estrategias.

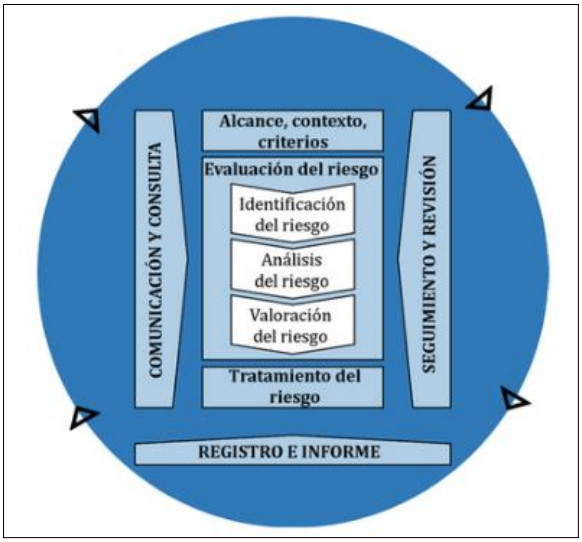
- Establecer las diferentes responsabilidades que deben de tomar en cuenta en el proceso de gestión de riesgos, y así poder facilitar la comunicación entre las diferentes partes interesadas.

- Establecer una serie de criterios, las cuales deben ser tomadas en cuenta para valorar los riesgos e identificar al tipo de riesgo que se están enfrentando y así poder establecer las medidas adecuadas.

- Establecer las diferentes actividades que se van a realizar durante todo el proceso de gestión de riesgos, teniendo en cuenta el tiempo y los recursos necesarios durante la implementación.

A pesar de no ser un estándar certificado, puede ser utilizada por cualquier tipo de organización con el objetivo de identificar y tratar los diferentes riesgos a los que se encuentran expuestas, fomentando una reacción proactiva dentro de ella [25]. Este estándar también puede ser orientado a las áreas de TI de las instituciones educativas y así establecer una manera concreta de como apoyas sus procesos y cumplir con los objetivos de la organización, en la figura 8 se muestra las etapas que la ISO 31000 tiene en cuenta:

Figura 11: Proceso de gestión de riesgos



Fuente: 10 Obtenido de la ISO 31000:2018 [25].

1.2.2.6.2 ISO 27000

Este estándar presenta un conjunto de políticas, directrices y actividades, con el objetivo de proteger los activos de información, porque son consideradas importantes para el logro de los objetivos de la organización. La ISO 27000 puede ser aplicada a cualquier tipo de organización sin importar el tipo o tamaño de esta, la cual tiene como objetivo reconocer los diferentes riesgos a los que están expuestos estos activos, ya que, siempre van a estar sujetos alguna amenaza, error, etc., por lo tanto, deben de tener una protección adecuada permitiendo así asegurar

la confidencialidad, disponibilidad e integridad de los datos desde la manera en cómo se recopilan, procesan y se almacena y así asegurar la seguridad de la información [29].

La ISO 27000 establece algunos principios fundamentales, para lograr una implementación exitosa, las cuales son:

- Generar una conciencia sobre la seguridad de la información dentro de la organización en la que se va implementar, para así lograr un compromiso durante la gestión por las diferentes partes interesadas ya sea internas o externas a la organización [29].

- Se debe establecer los controles apropiados para la evaluación de riesgos con el objetivo de tener una prevención activa y así poder detectar incidentes de seguridad, además de asignar responsabilidades para la seguridad de la información [29].

- Tener una mejora continua cada vez que se vaya a implementar con el fin de realizar modificaciones necesarias para mejorar en la detección en incidentes de seguridad [29].

La ISO 27000, te da un alcance general acerca de la seguridad de la información, aquí encontramos una familia de estándares, donde cada una hace énfasis en ciertos criterios como requisitos para la seguridad de información, directrices para realizar una auditoría, como realizar una gestión de seguridad, etc. En esta investigación se centrará en la ISO/IEC 27005 debido a que proporciona como realizar una gestión de riesgos orientado en los procesos, la cual es una de los objetivos que se tiene en esta investigación.

III. Metodología

2.1 Tipo y nivel de investigación:

Esta investigación es cuantitativa, debido a que trabaja aplicando el método deductivo y análisis estadístico, pero de tipo experimental porque a través de la base teórica, se pretende aplicar un modelo de gestión de riesgos que se adapte a las necesidades de las instituciones educativas y así poder minimizar los diferentes riesgos a los que se encuentras expuestos, y poder lograr el aseguramiento de la información y mejorando el desempeño organizacional.

Y a su vez, esta investigación es descriptivo porque se detallan situaciones o eventos, teniendo como resultado el impacto de las personas que lo rodea sin cambiar su entorno.

2.2 Diseño de Investigación:

El diseño de la presente investigación será Cuasi experimental, debido a que se manipula deliberadamente al menos una variable independiente, **modelo de gestión de riesgos**, para ver su efecto con una o más variables dependientes, **minimizar los riesgos de los procesos que soporta el área de TI,** podemos considerar el esquema cuasi experimental, cuya forma es la siguiente:

G O1 X O2

Dónde:

- G: Caso del estudio seleccionado.
- O1: Minimizar los riesgos en los procesos que soporta el área de TI en las instituciones educativas de la región, antes de la aplicación del modelo de gestión de riesgos.
- X: Modelo de gestión de riesgos de TI.
- O2: Minimizar los riesgos en los procesos que soporta el área de TI en las instituciones educativas de la región, después de la aplicación del modelo de gestión de riesgos.

2.3 Población, muestra y muestreo:

2.3.1 Población:

La población que se considerará para la presente investigación serán las instituciones educativas básicas regular privadas de la región Lambayeque con más de 500 alumnos, donde se encontraron 16 instituciones, sobre las cuales se aplicarán los cálculos de la muestra para la aplicación de los instrumentos diseñados.

2.3.2 Muestra.

Para la siguiente investigación se aplicará la fórmula de muestra finita:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + (Z^2 * P * Q)}$$

Dónde:

- N= Universo
- e = 0.1 (Máximo de error permisible)
- Z= 1.65 (Valor tabla) (90%)
- P = 0.5 (Proporción de la población)
- Q= 0.5 (1-P)

Calculando:

$$n = \frac{1.65^2 * 0.5 * 0.5 * 16}{(16-1) * 0.1^2 + (1.65^2 * 0.5 * 0.5)}$$

$$n = \frac{2.72 * 0.5 * 0.5 * 16}{15 * 0.01 + (2.72 * 0.5 * 0.5)}$$

$$n = 13.1$$

Luego de realizar la fórmula con los datos relevantes de la investigación se obtuvo como muestra 13 instituciones básicas regular privadas de la región Lambayeque con más de 500 alumnos.

2.3.3 Muestreo:

Para la presente investigación se empleará el muestreo no probabilístico por conveniencia, debido a que las instituciones educativas serán seleccionadas según a la accesibilidad que se tenga en cada una de ellas.

2.4 Técnica e instrumentos de recolección de datos

2.4.1 Técnicas de recolección de datos:

Juicio de expertos:

Este método es útil para verificar la viabilidad que se tienen en la investigación, porque, el experto a cargo tendrá que evaluar, según su experiencia en el campo laborar, con el fin de validar que la información propuesta es viable en la investigación.

Método de observación.

Será uso de la observación para describir los diferentes acontecimientos y por así explicar el porqué, de dichos sucesos, obteniendo así datos fiables a la hora de demostrar ciertas conductas, eventos o situaciones que se desean analizar.

2.4.2 Instrumentos de recolección de datos:

Planilla de Juicio de Expertos.

La plantilla de juicio de experto estará conformada por un conjunto de criterios, donde el experto tendrá que valorar cada ítem de acuerdo al criterio y as su experiencia, brindando un puntaje al indicador que se está poniendo en juicio para luego sacar un promedio al sumar todos los puntajes.

Ficha de observación.

Es un formato que permite conocer la manera como se desarrollan las actividades y los resultados que se tienen de ellas.

2.5 Procedimientos:

Después de haber establecido las diferentes técnicas e instrumentos de recolección de datos, se debe de proceder a la recopilación de la información utilizando estas herramientas, la cual es importante para la revisión de documentación estratégica. Esta actividad se puede llevar a cabo a través de entrevistas, cuestionarios y observación.

Entrevistas:

Se debe acordar las fechas donde se llevará a cabo esta actividad con los directores de tecnología de información, para poder recolectar información acerca de los diferentes procesos que ellos soportan como área para las instituciones educativas.

a) Elaborar las preguntas claves según el tipo de usuario a entrevistar.

b) Llevar un orden a la hora de realizar las preguntas, para evitar obtener las mismas respuestas por el usuario.

c) Una vez culminada la entrevista, la información recopilada será procesada según el tipo de pregunta.

d) Por último, se debe obtener una matriz de las respuestas de los usuarios encentados por cada una de las preguntas realizadas.

Cuestionarios:

Los cuestionarios deberán se desarrollados por el personal de cada área de las instituciones educativas, con el objetivo de poder recopilar la información necesaria para poder establecer una buena gestión de riesgos. Aquí se planteará una lista de preguntas que será dirigidas a los directores y jefes del área de TI de los centros educativos con el fin de analizar el estado actual en el que se encuentra la institución.

a. Establecer a que tipos de usuarios va estar dirigido la encuesta.

b. Realizar preguntas concisas para que el usuario pueda responder de una manera eficiente.

c. Después de haber culminado las encuestas, la información recolectada debe ser procesada por las herramientas establecidas anteriormente.

2.6 Técnicas de procesamiento:

Luego de haber recolectado la información de las diversas áreas entrevistadas, se procedió a utilizar herramientas informáticas como es el SPSS o Excel, la cual sirvió para procesamiento de los datos, de los resultados finales de la actividad anterior. Asimismo, los resultados obtenidos de dicho procesamiento, fueron detallados

gráficamente a través de cuadros estadísticos para la mejor compresión de los resultados.

2.7 Consideraciones éticas

En esta investigación se tomará en cuenta los siguientes criterios éticos, las cual se basó en el código deontológico que el Colegio del Perú(CIP) hace mención en sus diferentes artículos, la cual se

Tabla 1: Criterios éticos según el CIP

CRITERIOS ÉTICOS	
PRINCIPIOS GENERALES	Los ingenieros deben ser responsables, leales y honestos debido a que están al servicio de la sociedad. Siempre deben de actuar con respeto e integridad haciendo honor a su profesión.
DE LA RELACIÓN CON EL PUBLICO	Los ingenieros deben estar en la capacidad de brindar un asesoramiento oportuno en las consultas que ellos tengan y a su vez mantener la discreción con la información recopilada durante el desarrollo de su trabajo.
	Los ingenieros, una vez aceptado el cargo, deberá actuar como asesor y defensor de los intereses del cliente siempre y cuando haya una parcialidad en el ejercicio de sus actividades.
DE LA COMPETENCIA PROFECIONAL	Los ingenieros podrán ofrecer sus servicios a través de publicaciones, la cual la información que publiquen debe será verdadera.
	Debe de haber un respeto por los otros ingenieros, sin hablar mal del trabajo realizado por otro colega.

Fuente: 11 Elaboración propia

IV. Resultados

3.1 Diagnóstico del sector:

De las instituciones educativas encuestadas que se analizaron para el análisis diagnóstico del sector, se identificó que el (100%) contaban con un área de tecnología de información, la cual dependían directamente de gerencia general. La encuesta fue aplicada al personal de las áreas de TI de cada una de las instituciones educativas básica regular; donde se obtuvieron los siguientes resultados:

El (86,7%) del personal encuestado, mencionaron que conocen cuales son los servicios que son ofrecidos por el área de TI, y a su vez mencionan que no existe una documentación adecuada para brindar soporte ante una manifestación de un riesgo o un cambio que se quisiera realizar, debido a que solo el 26,7% cuentan con un inventario de TI, siendo esto uno de los factores claves para la toma de decisiones a la hora de querer mejorar los procesos de las instituciones educativas. Por otro lado, el (73.3%) señalaron que tienen definidos sus roles y funciones y a su vez el mismo porcentaje de encuestados revelaron que dependen mucho de este personal para brindar soporte a los servicios que se ofrece a las diferentes áreas de las instituciones.

A pesar que cuentan con el apoyo de la alta dirección, en su mayoría con un (93,3%),para ofrecer seguridad o mejoras de dichos procesos, solo el (26,7%) de los encuestados expresaron que han evaluado sus riesgos internos y externos de sus activos del área de TI, siendo una da las funciones principales que se debería de realizar, ya que a través de esta actividad se pueden identificar las diferentes amenazas y vulnerabilidades que están expuestos estos activos, de las cuales afectan a los diferentes procesos que son soportado por el área de TI. A demás, tan solo el (13,3%) revelaron que dan seguimiento a los diferentes riesgos que se han presentado dentro de la institución, por lo tanto, el (86,7%) expresan que no cuentan con un manual de procedimiento ante posibles fallas de los diferentes servicios que brindan a la institución y ni muchos menos tienen un registro histórico de los riesgos que se han manifestado anteriormente.

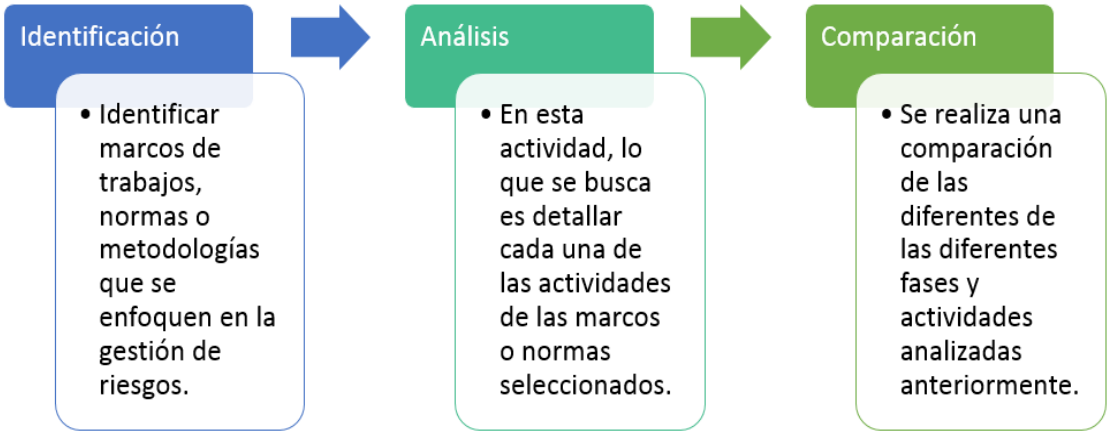
Con lo referente al uso de una metodología o marco de referencia para la gestión de riesgos de los diferentes activos del área de TI, según los encuestados se tiene que el (100%) no cuenta con el uso de una metodología debido a que desconocen o no lo

creen necesario, a pesar que el (100%) afirmaron que han tenido problemas con algún servicio que ofrecen y muchos de esos inconvenientes se han presentado reiteradas veces. Solo el (46.7%) aludieron que verifican que sus servicios estén operando correctamente, debido a que el (100%) de encuestados revelaron que deben de informar los inconvenientes que presentan a la alta dirección.

3.2 Análisis de estándares:

Para el desarrollo de la armonización del modelo propuesto, se tuvo que realizar una serie de pasos como se muestra en la siguiente imagen 8:

Figura 12: Pasos para la armonización de metodologías, normas de gestión de riesgos



Fuente: 12 Elaboración propia

a) Identificación: Para llevar a cabo esta actividad se tuvo como base el análisis realizado en los antecedentes de esta investigación, la cual sirvió para identificar las diferentes normas, metodologías o marcos de trabajos que pudieran servir para la propuesta del modelo.

   Logrando identificar un total de 12 entre normas, marcos y metodologías de las cuales se pueden clasificar de la siguiente manera:

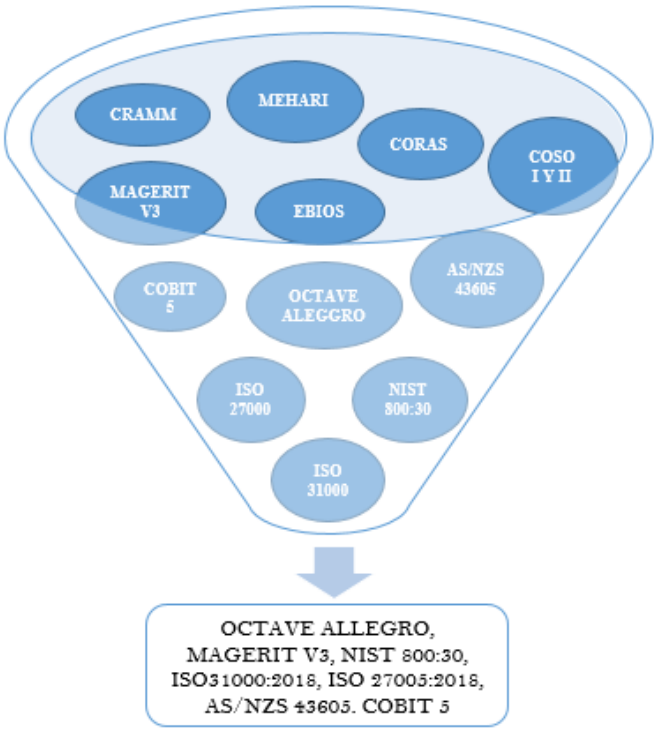
   - 7 metodologías que hacen énfasis en la gestión de riesgos, las cuales tenemos: COSO, CRAMM, EBIOS, MAGERIT V3, MEHARI, NIST 800:30 y OCTAVE

   - 3 normas o estándares, entre ellas son: La norma ISO 31000:2018, ISO 27005:2018 y la norma australiana AS/NZS 43605.

- 2 marcos de trabajos: CORAS y COBIT For Risk

Una vez identificado las normas y marcos se procedieron a realizar un análisis general de cada una de ellas con el fin de poder determinar si hace énfasis en la gestión de riesgos, adicionalmente verificar si la información es accesible para el análisis comparativo. Además, se realizó un detalle general de cada una de ella para determinar su enfoque y ver la factibilidad de su uso como se muestra en el anexo II**,** teniendo como resultado lo siguiente, tal como se muestra en la siguiente imagen 9:

Figura 13: Identificación de normas y metodologías de gestión de riesgos



Fuente: 13 Elaboración propia

- De las 3 normas identificadas, fueron seleccionadas para realizar el análisis y comparación de cada una de ellas, porque hacen énfasis en las diferentes etapas de la gestión de riesgos desde el establecimiento del contexto de las instituciones hasta el seguimiento o monitoreo de los riesgos.

- Las metodologías como OCTAVE, MAGERIT, NIST, son utilizadas en esta investigación debido a que todas ellas hacen énfasis en todas

las etapas de la gestión de riesgos resaltando una que otra en diferentes actividades, la cual es útil para esta investigación.

- COBIT For Risk, establece un marco de trabajo donde se describe los procesos básicos para una gestión de riesgos con el fin de generar valor a las organizaciones mientras se optimizan los riesgos. Se basa en el APO12 que trata sobre la gestión de riesgos.

- COSO, esta metodología quedo descarta en esta investigación debido a que está orientada para fines contables y de auditoría, la cual la es utilizada para el control interno, para la evaluación de fraudes y presentación de informes financieros. Otra metodología descartada es CRAMM, debido a que se requiere de un personal experto para la utilización, además del uso de su propia herramienta para el análisis de riesgos, otros de los motivos es que solo centrarse en ataques que están expuesta la organización para asegurar la continuidad del negocio.

- CORAS, a pesar de que es un marco de trabajo que se basa en el análisis de los riesgos de seguridad, se prefirió no utilizarla debido a la poca disponibilidad de información.

- MEHARI, se utiliza para medir la eficiencia de las políticas de seguridad establecidas por las organizaciones, además de que puede ser usada como apoyo a otros modelos de gestión de riesgos, además de ser complemento de la norma ISO 27000. Es por ello que esta metodología quedo descartada en la presente investigación.

- EBIOS, es considerada más una herramienta de apoyo compatible con normas internacionales como la ISO 31000 y 27000, la cual es utilizada para estudiar el diseño de nuevos sistemas, como sistemas existentes. Esta metodología responde a una autoridad ya sea el jefe del proyecto, diseñador del proyecto, etc., basándose más en seguridad durante en los requerimientos y desarrollo de software, siendo descartada por que tiene un enfoque diferente al objetivo principal de esta investigación.

b) Análisis: Luego de haber seleccionado las metodologías a utilizar en esta investigación, se procedió a realizar un análisis detallado de cada uno de ellos tal como se muestra en el **anexo III**. Se llevó a cabo esta actividad para detallar cada una de las actividades de las fases que cuenta cada una de ellas, además de identificar técnicas y criterios que utilizan, las cuales pueden ser utilizadas a la hora de llevar a cabo la propuesta del modelo.

c) Comparación: Una vez realizada el análisis de los diferentes normas, marcos y estándares identificados para la gestión de riesgos, se procedió a realizar una comparación de las diferentes fases o procesos de cada una de ellas con el objetivo de evaluar como estos estándares y metodologías se pueden complementar para analizar los diferentes riesgos en los servicios ofrecidos por el área de TI que soporta los procesos en las instituciones educativas básica regular.

   Durante el análisis de la comparación de estos estándares, normas y marcos de trabajo se logró establecer fases o etapas en que concordaba ciertas actividades de cada una de ellas, estas etapas son las siguientes:

   - Establecer el contexto externo, interno y criterios de riesgos.
   - Identificación de activos.
   - Identificación de riesgos.
   - Análisis del riesgo.
   - Evaluación de riesgos.
   - Tratamiento de riesgos
   - Seguimiento y monitoreo
   - Comunicación y consulta

   Luego de establecer estas etapas se procedió a determinar las actividades de cada norma o cada metodología según los ítems ya establecidos, como se muestra en las siguientes imágenes.

Figura 14: Comparación de estándares y metodologías

FASES	ISO 31000:2018	NTP -ISO 27005:2018	OCTAVE	Norma AS/NZS 43605	NIST 800:30	MAGERIT v3	COBIT
ESTABLECER CONTEXTO INTERNO, EXTERNO Y CRITERIOS	**Establecer contexto**	**Establecer contexto**		**F1. Establecer el contexto**	-	**Fase 1: Establecer los criterios de riesgo de Medición**	-
	Definir el alcance	Alcance y limites	-	Establecer el contexto estratégico	-	Roles y funciones	-
	Establecer contexto externo	Establecer el contexto	-	Establecer el contexto organizacional	-	Contexto interno	Establecer contexto externo
	Establecer contexto interno	Organización para la gestión de riesgo de seguridad	-	Establecer el contexto de administración de los riesgos	-	Contexto interno	Establecer contexto interno
	Establecer el contexto del proceso de gestión de riesgos.	Criterios básicos ➢ Criterios de valoración de riesgo. ➢ Criterios de impacto. ➢ Criterios de aceptación del riesgo	**F1: Establecer los criterios de riesgo de Medición** ➢ Criterios de medida de riesgo. ➢ Priorización de las Areas de Impacto	Desarrollar criterios de evaluación de riesgos	-	Establecer criterios	-
	-	-	-	Definir la estructura	-	-	-
IDENTIFICACION DE ACTIVOS		**Identificación de riesgo:** ➢ Identificación de activos	**F2: Desarrollar un perfil de activos de información** ➢ Identificar activo ➢ Valorar el activo ➢ Evaluar el activo ➢ Perfil del activo	-	**P1: Caracterización del sistema** ➢ Hardware ➢ Software ➢ Acoplamiento del sistema ➢ Datos e información ➢ Sistema y criticidad de datos ➢ Sistema y los datos de sensibilidad	**F2: Análisis de riesgos** Paso 1: Activos ➢ Identificación de activo ➢ Dependencia de activos ➢ Valorar el activo ➢ Equipo de valoración y tratamiento	BAI09 Gestionar los Activos.
			F3 - Identificar contenedores de activos de información ➢ Identificación de contenedor técnico. ➢ Identificación de contenedor físico. ➢ Identificación de contenedor personas	-			

Fuente: 14 Elaboración propia

Figura 15: Comparación de estándares y metodologías

FASES	ISO 31000:2018	NTP -ISO 27005:2018	OCTAVE	Norma AS/NZS 43605	NIST 800:30	MAGERIT v3	COBIT
IDENTIFICACIÓN DE RISGOS	**Identificación del riesgo** ➢ Identificación fuente de riesgo ➢ Identificación de causa y los eventos ➢ Identificar amenazas y oportunidades ➢ Identificar vulnerabilidades y capacidades ➢ Ver cambios internos y externos	**Identificación de riesgo:** ➢ Identificación de activos ➢ Identificación de amenazas ➢ Identificación de controles existentes ➢ Identificación de vulnerabilidades ➢ Identificación de consecuencias.	**F4: Identificación de las Areas de Preocupación** ➢ Establecer las áreas de preocupación. ➢ Documentar las áreas de preocupación. **F5: Identificación de Escenarios de Amenaza** ➢ Identificar escenarios de amenazas. ➢ Selección de respuesta a los escenarios. **F6: Identificación de riesgos** ➢ Registrar las consecuencias.	**Fase 2: Identificación de Riesgos** ➢ Lista de eventos que pueden afectar a los activos ➢ Identificar las causas y escenarios ➢ Establecer el contexto de administración de riesgos ➢ Desarrollar criterios de evaluación de riesgos	**P2: Identificación de amenazas** ➢ Historial de ataques del sistema. ➢ Información de agencia de inteligencia **P3: Identificación de vulnerabilidades** ➢ Reporte de los riesgos más importantes ➢ Comentarios de auditoria. ➢ Requerimiento de seguridad ➢ Resultados de pruebas de seguridad	**Paso 2: Amenazas** ➢ Identificación de amenazas. ➢ Valoración de amenazas.	APO12.03 Mantener un perfil de riesgo.
ANÁLISIS DEL RIESGO	**Análisis del riesgo** ➢ Probabilidad de los eventos y consecuencias ➢ Magnitud de consecuencias	**Análisis de riesgo:** ➢ Análisis de riesgo ➢ Evaluación de consecuencia. ➢ Evaluación de probabilidad. ➢ Determinar el nivel del riesgo	**F7: Análisis de Riesgos** ➢ Revisar los criterios de medida de riesgos y las consecuencias. ➢ Calcular el puntaje de riesgo relativo.	**F3: Análisis de riesgos** ➢ Determinar los controles existentes. ➢ Consecuencia y probabilidades	**P4: Determinación de la probabilidad** ➢ Reporte de riesgos más importantes ➢ Comentarios de auditoria ➢ Requerimiento de seguridad ➢ Resultado de prueba de seguridad **P5: Análisis de impacto** ➢ Análisis del impacto ➢ Valoración de los activos críticos ➢ Datos críticos ➢ Datos sensibles	**Paso 3: Determinación del impacto potencial** **Paso 4: Determinación del riesgo potencial** **Paso 5: Salvaguardas**	APO12.02 Analizar el riesgo.

Fuente: 15 Elaboración propia

Figura 16: Comparación de estándares y metodologías

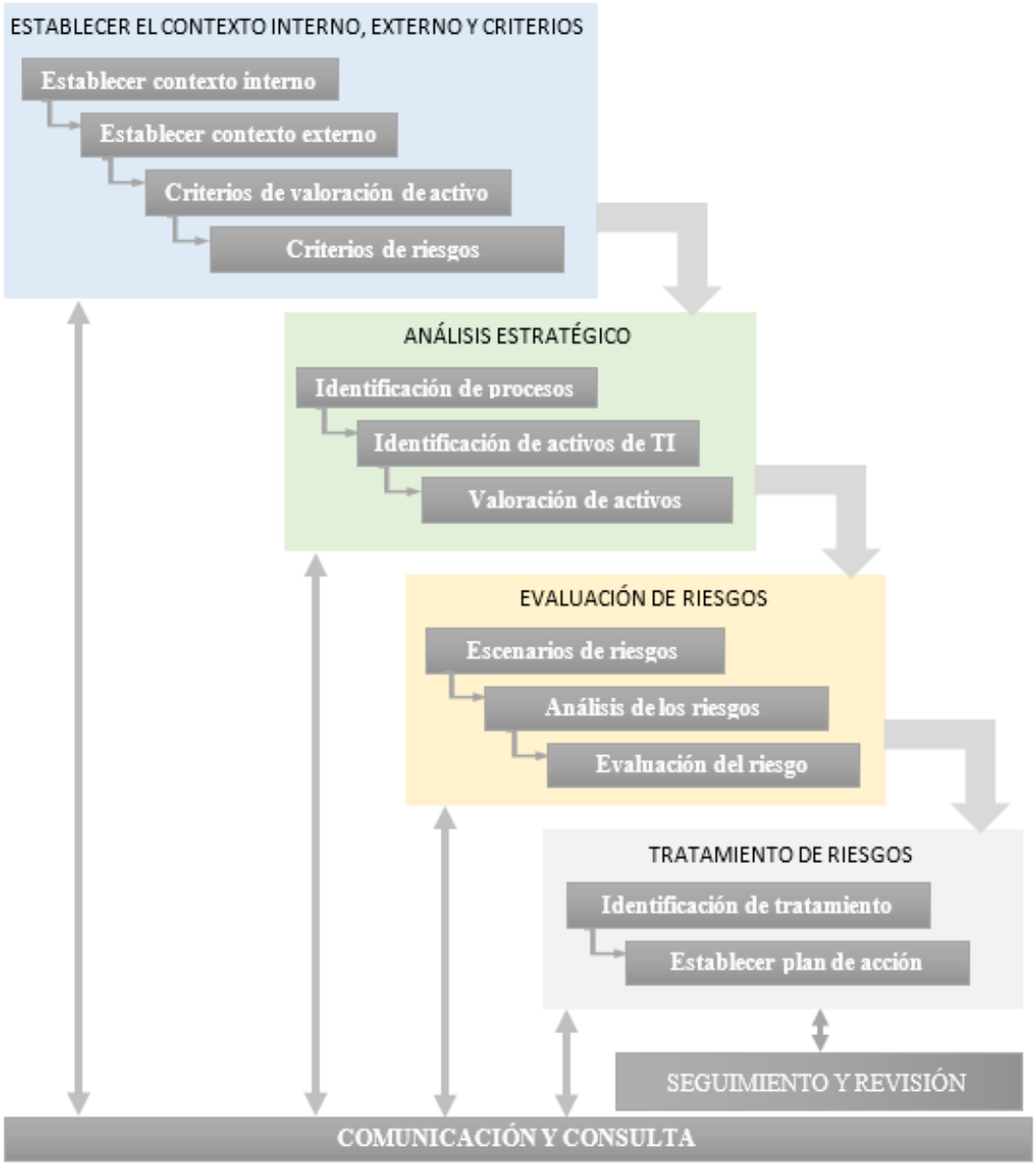
FASES	ISO 31000:2018	NTP -ISO 27005:2018	OCTAVE	Norma AS/NZS 43605	NIST 800:30	MAGERIT v3	COBIT
EVALUACIÓN DE RIESGOS	**Valoración del riesgo** ➢ Comparación del nivel de riesgo identificado durante el proceso de análisis con criterios de riesgo establecidos.	Valorar el riesgo	**F 8: Evaluación de Riesgos** ➢ Estrategia y desarrollo del plan	**F4: Valoración del riesgo** ➢ comparar el nivel de riesgo detectado durante el proceso de análisis con los criterios de riesgo establecidos previamente.	**P6: Determinación del riesgo** ➢ Probabilidad de explotación de amenaza ➢ Magnitud del impacto ➢ Adecuación de controles actuales y planeados	**Paso 6: Evaluación del riesgo** ➢ Interpretación de los valores de impacto y riesgo residuales **Paso 7: Aceptación del riesgo**	APO12.04 Expresar el riesgo. ADM03.01 Evaluar la gestión del riesgo
TRATAMIENTO DE RIESGO	**Tratamiento del riesgo** ➢ Selección de opción de tratamiento.	Tratamiento del riesgo.	**F9: Desarrollo de estrategia y planes de seguridad** ➢ Estrategia de protección	**F5: Tratamiento del riesgo** ➢ Identificar y evaluar y seleccionar las opciones de tratamiento de riesgos	-	**Paso 8: Tratamiento del riesgo** ➢ Análisis de costo y beneficio	APO12.05 Definir un portafolio de acciones para la gestión de riesgos.
	➢ Implementación del plan de acción	Aceptación del riesgo de seguridad	➢ Planes de mitigación	➢ Preparar e implementar planes de tratamiento	➢ Recomendaciones de control	➢ Opciones de tratamiento de riesgos	APO12.06 Responder al riesgo.
SEGUIMIENTO Y MONITOREO	Seguir y revisar los controles.		-	**F6: Monitorear y revisar**	➢ Monitorear los factores de riesgos y actualizar la evaluación del riesgo.		EDM03.03 Supervisar la gestión de riesgos.
COMUNICACION Y CONSULTA	Comunicación y consulta	-	-	-	-	-	-
REGISTROS	Registro del proceso de gestión de riesgos	-	-	-	-	-	-

Fuente: 16: Elaboración propia

3.3 Propuesta:

Para el desarrollo de esta propuesta de investigación se realizó una comparación de diferentes estándares, normas o marcos de trabajo que hagan énfasis en la gestión de riesgos, dicha comparación se puede visualizar en el anexo V, dicha compasión sirvió para adaptarla a las necesidades de las instituciones educativas básica regular, para que puedan identificar los diferentes procesos que son soportados por el área de TI a través de sus servicios y a la vez evaluar los diferentes riesgos a los que están expuestos estos activos.

Figura 17: Modelo de gestión de riesgo para instituciones educativas



FASE I: ESTABLECER EL CONTEXTO

Las instituciones educativas en esta fase deberán de establecer el contexto interno y externo, adicionalmente se deberá de establecer los diferentes criterios, la cual servirá para la evaluación de los riesgos.

Proceso 1: Establecer el contexto externo:

En este apartado las instituciones educativas deberán establecer su situación actual referente a las condiciones locales y nacionales, para ello se debe de establecer lo siguiente:

a) **Socio-Cultural:** Sirve para identificar el estilo de vida que tienen los padres de familia y alumnos de acuerdo a su ubicación geográfica.
   Fuente: Datos censales, información del INEI.
b) **Entes regulatorios:** Son las instituciones reguladoras encargadas de controlar a las diferentes instituciones educativas para que cumplan las exigencias legales y reglamentarias y así puedan cumplir con los servicios básicos.
   Obtener de: MINEDU, SUNAT, INDECOPI, INDECI
c) **Competitivo:** Sirve para identificar a las diferentes instituciones educativas básica regular y analizar cómo podría afectar a la institución además de identificar a la competencia directa.
   Obtener de: Análisis FODA
d) **Proveedores:** Hace referencia a los diferentes proveedores que contribuye al desarrollo de las diferentes actividades que las instituciones educativas realizan en el día a día.
   Obtener de: Lista de proveedores.
e) **Tecnológico:** Son los diferentes usos de la tecnología ya se hardware o software que se puede utilizar para mejorar el soporte a los diferentes servicios que son utilizados por las instituciones educativas.
   Obtener de: Revista o foros de tecnología.

Para llevar a cabo esta actividad se tendrá en cuenta la siguiente plantilla con código **GR001**. Para llevar a cabo esta actividad, se debe reunir los diferentes directivos de las instituciones educativas y el encargado del área de TI.

LOGO	ESTABLECER EL CONTEXTO EXTERNO					
	Fase:	1	**Proceso**	1	**Actividad**	-
	Código:	**GR001**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: Se establece los siguientes criterios para identificar contextos externos que las instituciones educativas deben establecer para conocer su entorno externo, adicionalmente a estos, se pueden agregar otros criterios para conocer el entorno de las instituciones educativa.

N°	CONTEXTO	FUENTE	DETALLE
1	**Socio-Cultural**	Datos censales	*Personas que se encuentre en los niveles socioeconómicos A, B, C*
2	**Entes regulatorios**	MINEDU, SUNAT, INDECOPI, INDECI	*Son las normar o reglas que la institución educativa debe cumplir correctamente, la cual no generé algún problema por el incumplimiento de alguna de estas.*
3	**Competitivo**	Análisis FODA	*Lista de las instituciones que podrían afectar directamente. Ejemplo: Institución A, Institución B, Institución C, etc.*
4	**Proveedores**	Lista de proveedores	*Lista de proveedores que contribuye a los procesos de las instituciones educativas como: proveedor de internet, dominio, etc.*
5	**Tecnológico**	Revista o foros de tecnología.	*Lista de la tecnología que podría ayudar en los diferentes procesos de la institución.*
N	**Criterio N**	Fuente N	Detalle N
…	**…**	…	…

CREADO POR **APROBADO POR**

Proceso 2: Establecer el contexto interno:

En este proceso las instituciones educativas deben de establecer los siguientes parámetros para analizar cómo se encuentra actualmente, para ello se establecen los siguientes parámetros.

a) **Estructura organizacional:** Se utiliza para poder comprender como está conformada jerárquicamente y así poder identificar las diferentes áreas que cuentan las instituciones educativas.
   Obtener de: Organigrama de la institución educativa.

b) **Objetivos organizacionales:** Sirve para identificar cuáles son los objetivos que se han planteado en las instituciones educativas.
   Obtener de: Plan estratégico.

c) **Cultura organizacional:** Permite identificar los hábitos, actitudes y valores que se comparte los trabajadores de las instituciones educativas, la cual pueden facilitar o dificultar el desarrollo de cualquier estrategia.
   Obtener de: Misión, Visión, Valores, Plan estratégico.

d) **Partes interesadas:** Se hace referencia a las personas que podrían verse afectada por el desempeño de las instituciones educativas.
   Obtener de: Plan estratégico, Misión, Visión.

e) **Recursos:** Son los diferentes recursos que las instituciones educativas utilizan para el cumplimiento de sus diferentes actividades, las cuales dan soporte a sus procesos.
   Obtener de: Inventario de activos.

Para llevar a cabo esta actividad se tendrá en cuenta la siguiente plantilla con código **GR002**. Para llevar a cabo esta actividad, se debe reunir los diferentes directivos de las instituciones educativas y el encargado del área de TI.

LOGO	ESTABLECER EL CONTEXTO INTERNO					
	Fase:	1	**Proceso**	2	**Actividad**	-
	Código:	**GR002**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: Se establece los siguientes criterios para identificar contextos externos que las instituciones educativas deben establecer para conocer su entorno externo, adicionalmente a estos, se pueden agregar otros criterios para conocer el entorno de las instituciones educativas.

N°	CONTEXTO	FUENTE	DETALLE
1	**Estructura organizacional:**	Organigrama institucional.	*Se plasma el organigrama de la institución, para identificar la jerarquía de la institución, la cual sirve para la toma de decisiones.*
2	**Objetivos organizacionales**	Plan estratégico.	*Se listan los objetivos de las instituciones educativas.*
3	**Cultura organizacional**	Misión, Visión, Valores, Plan estratégico.	*Se obtiene la visón, misión y valores que tiene la organización.*
4	**Partes interesadas:**	Plan estratégico, Misión, Visión.	*Los actores principales en la institución: el personal docente, los alumnos, padres de familia, etc.*
5	**Recursos:**	Inventario de activos.	*Lista de la tecnología que podría ayudar en los diferentes procesos de la institución: servidores, computadoras, software, etc.*
N	**Criterio N**	Fuente N	Detalle N
…	**…**	…	…

CREADO POR **APROBADO POR**

Proceso 3: Criterios de valoración de activo

Las instituciones educativas deben establecer los diferentes criterios para evaluar sus activos y así identificar el nivel de criticidad de cada uno de ellos, con el fin de identificar cuáles son los activos que podrían afectar a la organización si un riesgo se materializa. Para ello se establece los siguientes criterios para evaluar un activo y son confidencialidad, disponibilidad e integridad.

VALOR	CONFIDENCIALIDAD
1 (Muy bajo)	De acuerdo al valor, describir el nivel de confidencialidad que se tendría en este rango, con respecto a los activos.
2 (Bajo)	…
3 (Medio)	…
4 (Alto)	…
5 (Muy alto)	…

Tabla 2: Nivel de confidencialidad

VALOR	DISPONIBILIDAD
1 (Muy bajo)	De acuerdo al valor, describir el nivel de disponibilidad que se tendría en este rango, con respecto a los activos.
2 (Bajo)	…
3 (Medio)	…
4 (Alto)	…
5 (Muy alto)	…

Tabla 3: Nivel de disponibilidad

VALOR	INTEGRIDAD
1 (Muy bajo)	De acuerdo al valor, describir el nivel de integridad que se tendría en este rango, con respecto a los activos.
2 (Bajo)	…
3 (Medio)	…
4 (Alto)	…
5 (Muy alto)	…

Tabla 4: Nivel de integridad

Para que las instituciones educativas puedan establecer los diferentes criterios de valoración de sus activos, se hará uso de la plantilla **GR003**.

LOGO	ESTABLECER CRITERIO DE VALORACIÓN DE ACTIVOS					
	Fase:	1	**Proceso**	2	**Actividad**	-
	Código:	**GR003**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: A continuación, se presenta un modelo que las instituciones educativas pueden tener en consideración para la valoración de sus activos, caso contrario, pueden cambiar los criterios de valoración, teniendo en cuenta en cuenta que el valor va (1 al 5) siendo el 1 el valor más bajo y 5 el valor más crítico.

VALOR	CONFIDENCIALIDAD
1 (Muy bajo)	La información es pública .
2 (Bajo)	La información es de uso interno de la institución.
3 (Medio)	La información es confidencial y solo el personal de algunas área pueden acceder a ella
4 (Alto)	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5 (Muy alto)	La información es solo accedida por el personal de alto rango o con permisos a ella

VALOR	DISPONIBILIDAD
1 (Muy bajo)	El funcionamiento es normal en las actividades
2 (Bajo)	Los servicios de TI deben estar disponible al 10% del tiempo.
3 (Medio)	Los servicios de TI deben estar disponible al 30% del tiempo.
4 (Alto)	Los servicios de TI deben estar disponible al 60% del tiempo.
5 (Muy alto)	Los servicios de TI deben estar disponible al 90% del tiempo.

VALOR	INTEGRIDAD
1 (Muy bajo)	Se tolera pérdida o alteración de sus componentes en un 80% - 100%
2 (Bajo)	Se tolera pérdida o alteración de sus componentes en un 60% - 79%
3 (Medio)	Se tolera pérdida o alteración de sus componentes en un 40% - 59%
4 (Alto)	Se tolera pérdida o alteración de sus componentes en un 20% - 39%
5 (Muy alto)	Se tolera pérdida o alteración de sus componentes en un 0% - 19%

CREADO POR **APROBADO POR**

Proceso 4: Criterios de riesgos

En este proceso las instituciones educativas deben de establecer el nivel de riesgos que están dispuestas asumir. Además, se debe establecer los criterios para evaluar la probabilidad y el impacto que las organizaciones están dispuesto aceptar. Por eso se consideran las siguientes actividades.

Actividad 1: Criterios de evaluación de Riesgo

Definir probabilidad: Representa la posibilidad que algún tipo de riesgo se pueda presentar en las instituciones educativas.

- **Escala**: Contendrá los 5 niveles recomendados en la escala de Likert
- **Probabilidad**: El jede de TI de la institución educativa deberá establecer los diferentes niveles, la cual corresponderá a cada uno de los 5 valores, de acuerdo a su experiencia.
- **Descripción**: El jefe de TI, deberá de describir cada una de las diferentes clasificaciones que estableció, para que se pueda entender el rango de dicho nivel de probabilidad.

Para llevar a cabo esta actividad se tendrá en cuenta la siguiente tabla 4:

PROBABILIDAD		
ESCALA	**CATEGORÍA**	**PROBABILIDAD(P)**
1	Muy bajo	*Descripción de la frecuencia de que el evento ocurra. Ejemplo: El evento puede ocurrir cada 2 años.*
2	Bajo	…
3	Moderado	…
4	Alto	…
5	Muy alto	…

Tabla 5: Probabilidad de ocurrencia

Definir el Impacto: Representa el grado del daño que puede causar en las instituciones educativas, con respecto a perdida financieras, en la interrupción de servicio o la disminución del rendimiento del personal.

- **Valor**: Contendrá los 5 niveles recomendados en la escala de Likert
- **Clasificación**: El jede de TI, el gerente y el contador de la institución educativa deberá establecer los diferentes niveles de impacto que puede tener.
- **Descripción**: El jefe de TI, deberá de describir cada una de las diferentes clasificaciones que estableció, para que se pueda entender el rango de dicho nivel de impacto.

Para llevar a cabo esta actividad se tendrá en cuenta la siguiente plantilla:

IMPACTO		
ESCALA	**CATEGORÍA**	**IMPACTO (I)**
1	Muy bajo	*Descripción de como impactaría la ocurrencia de un evento dentro de la organización. Se puede tomar los siguientes criterios (Pérdidas financieras, interrupción de servicios o en el rendimiento de los colaboradores).*
2	Bajo	…
3	Moderado	…
4	Alto	…
5	Muy alto	…

Tabla 6: Impacto en la organización

Nivel de aceptabilidad: Aquí se establecen los diferentes niveles de aceptabilidad del riesgo, que las instituciones educativas deben te tener en cuenta cuando comparen los resultados obtenido en el análisis de riesgos con los niveles de aceptabilidad.

- **Nivel del riesgo**: Se considera 5 niveles que las instituciones educativas deben utilizar para ubicar el riesgo según su probabilidad e impacto (PXI).
- **PXI**: Se establecieron los siguientes rangos que las instituciones educativas deben de utilizar a la hora de evaluar un riesgo.
- **Categoría**: Son las medidas cualitativas, que representa a cada rango que ha sido establecido. La cual servirá para evaluar el efecto que tiene el riesgo identificado con respecto al activo que cuenta la institución.

NIVEL	PXI	CATEGORÍA
1	[1-2]	Bajo
2	[3-4]	Muy bajo
3	[5-10]	Moderado
4	[10-15]	Alto
5	[15-25]	Muy alto

Tabla 7: Niveles de aceptabilidad del riesgo

Para el desarrollo de esta actividad se hará uso de la plantilla **GR004,** donde se establece un ejemplo de como las instituciones educativas deben de establecer la probabilidad y el impacto para evaluar los diferentes riesgos que se han detectados, con el objetivo de poder identificar el nivel del riesgo que representa para la institución. Para el llenado de esta plantilla pueden utilizar el juicio de experto basado en experiencias anteriores.

LOGO	ESTABLECER CRITERIÓS DE EVALAUCIÓN DE RIESGOS					
	Fase:	1	**Proceso**	4	**Actividad**	1
	Código:	**GR004**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: A continuación, se presenta un ejemplo de cómo podemos llenar los siguientes criterios de evaluación de riesgos. Se debe tomar en cuenta que el valor va (1 al 5) siendo el 1 el valor más bajo y 5 el valor más crítico.

PROBABILIDAD		
CATEGORIA	**ESCALA**	**PROBABILIDAD**
MUY ALTO	**5**	Ocurre al menos 2 veces a la semana .
ALTO	**4**	…
MODERADO	**3**	…
BAJO	**2**	…
MUY BAJO	**1**	Puede ocurrir una vez cada dos años.

IMPACTO		
CATEGORIA	**ESCALA**	**IMPACTO**
MUY ALTO	**5**	Paralizar todos los procesos de la organización por más de una semana.
ALTO	**4**	…
MODERADO	**3**	…
BAJO	**2**	…
MUY BAJO	**1**	La organización puede continuar con sus laborares, sin ningún inconveniente.

Después de haber analizado la probabilidad y el impacto, se debe comparar con los siguientes criterios, para así determinar el nivel del riesgo:

NIVEL	PXI	CATEGORÍA
1	[1-2]	Bajo
2	[3-4]	Muy bajo
3	[5-10]	Moderado
4	[10-15]	Alto
5	[15-25]	Muy alto

CREADO POR **APROBADO POR**

Actividad 2: Criterios de aceptación de riesgos:

Aquí se establece los diferentes niveles de riesgos, la cual servirá para la evaluación de los riesgos, donde permitirá a las instituciones educativas decidir hasta que nivel de riego están dispuestos aceptar para alcanzar sus objetivos, caso contrario establecer las medidas necesarias. Es por ello que se debe establecer el apetito y la tolerancia, para que las instituciones educativas tomen en cuenta a la hora de evaluar los riesgos.

- Apetito de riesgo: Se estable el nivel del riesgo que las instituciones educativas están dispuestas asumir para cumplir con sus objetivos.
- Tolerancia al riesgo: Es el nivel máximo que la institución puede soportar para un determinado riesgo.

Las instituciones educativas después de analizar los diferentes riesgos, haciendo uso de la tabla 6, tendrán que compararlo con los criterios establecidos en la tabla 7, para determinar la categoría a la que pertenece el riesgo identificado.

NIVEL	PXI	CATEGORÍA
1	[1-4]	Aceptable
2	[5-10]	Tolerable
3	[11-25]	Intolerable

Tabla 8: Niveles de aceptación de riesgo

Para ello la persona encargada deberá de analizar los diferentes niveles de riesgos, haciendo uso de la plantilla **GR005**, donde se tendrá que comparar los resultados de la evaluación de la probabilidad por el impacto (PXI), con los criterios de aceptación del riesgo y así poder identificar los riesgos que son aceptables para la institución.

LOGO	ESTABLECER CRITERIÓS DE ACEPTACIÓN DE RIESGOS					
	Fase:	1	**Proceso**	3	**Actividad**	2
	Código:	**GR005**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: Esta plantilla sirve para que las instituciones educativas puedan establecer los diferentes niveles de aceptación de los riesgos, los niveles de tolerancia y los que no son tolerables. A su vez se establece los siguientes niveles de aceptación de riesgo que las instituciones pueden utilizar para su evaluación.

Matriz de probabilidad por impacto

IMPACTO						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		PROBABILIDAD				

A continuación, se presenta los siguientes niveles que las instituciones educativas pueden utilizar para la evaluación de los riesgos.

NIVEL	PXI	CATEGORÍA
1	[1-4]	Aceptable
2	[5-10]	Tolerable
3	[11-25]	Intolerable

CREADO POR **APROBADO POR**

Actividad 3: Criterios de seguimiento de riesgos:

Aquí se establece la frecuencia en que las instituciones educativas debe realizar seguimiento a los diferentes riesgos que se han detectado según su nivel de riesgo, con el fin de priorizar las diferentes medias y los planes de acción a estos. Se recomienda a las instituciones el siguiente cuadro de seguimiento de los riesgos.

- Seguimiento: Es el tiempo en que se debe de dar seguimiento a los riesgos según los niveles de riesgos obtenidos en la evaluación de probabilidad e impacto.
- Nivel de riesgo: Es la medida cualitativa obtenida de la evaluación del riesgo.

SEGUIMIENTO	NIVEL DEL RIESGO
Anual	Bajo
Semestral	Muy bajo
Trimestral	Moderado
Mensual	Alto
Semanal	Muy alto

Tabla 9 Tiempo de seguimiento de riesgos

Este criterio debe ser utilizado después de haberse realizado una evaluación de riesgos en las instituciones educativas, las cuales ayudaran a tener un mejor control sobre los riesgos y así poder poner más énfasis a los riesgos de mayor prioridad,

FASE 2: ANÁLISIS ESTRATÉGICO

Proceso 1: Identificar las áreas de la institución educativa.

En este proceso se tiene como objetivo identificar las diferentes áreas que existen dentro de una institución educativa y a la ves el responsable de estas. Para la identificación de estas podemos hacer uso de su organigrama de la institución para identificar estas áreas y a la ves realizar una encuesta al director a cargo.

IDENTIFICAR ÁREAS				
N°	LISTA DE ÁREAS	RPTA		Responsable
		SI	NO	
#N	*Área N*	*X*		*Responsable N*
…	…			…

Tabla 10 Identificación dela áreas de I.E

Para el desarrollo de esta actividad se tiene que tener en cuenta lo siguiente:

- **Responsable**: Nombre completo de la persona quien está llenando dicha plantilla.
- **ÁREA**: Se entregará un listado de posibles áreas que la institución educativa pueda contar

- **RPTA**: Se deberá marcar SI (X) en caso la institución cuente con dicha o NO(X) si desconocen o no lo toman en cuenta.
- **Procesos adicionales**: En caso la institución educativa encuestada cuente con otro proceso, deberá ser agregado en este apartado.

LOGO	**IDENTIFICACIÓN DE ÁREA DE LA I.E.P**					
	Fase:	II	**Proceso**	1	**Actividad**	-
	Código:	**GR006**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: El encargado tendrá que marcar (SI) si cuentan el proceso o (NO) si no cuentan con dichos procesos.

RESPONSABLE	*Nombre del entrevistado*		
N°	**LISTADO DE ÁREAS**	**RPTA**	**PERSONA A CARGO**
		SI / **NO**	
1	Área Académica	***x***	Se indica la persona encargada de dicha área
2	Área atención al cliente	***x***	
3	Área de contabilidad	***x***	
4	Área de logística	***x***	
5	Área de sistemas	***x***	
6	Área de marketing	***x***	
7	Área de psicología	***x***	
8	Área de enfermería o tópico	***x***	
Áreas adicionales			

CREADO POR **APROBADO POR**

Proceso 2: Identificar los procesos de la institución educativa.

En este proceso tiene como objetivo identificar los diferentes procesos que las instituciones educativas llevan a cabo, la cual en la siguiente tabla 10 se establecerá una serie de procesos establecidos por el ministerio de educación para mejorar la calidad de los servicios educativo, la cual servirá para identificar cuáles son los procesos que las instituciones educativas básica regular utilizan.

IDENTIFICAR PROCESOS				
N°	**TIPO DE PROCESO**	**RPTA**		**OBSERVACION**
		SI	**NO**	
#N	*TIPO N*	*X*		*OBSERVACIÓN N*
…	**…**			**…**

Tabla 11: Identificar procesos

Para el desarrollo de esta actividad se tiene que tener en cuenta lo siguiente:

- **Área**: Es el área donde pertenece la persona que se está entrevistando.
- **Responsable**: Nombre completo de la persona quien está llenando dicha plantilla.
- **Tipo de proceso**: Se entregará la plantilla con los procesos que MINEDU ha establecido para las instituciones educativas básica regular.
- **RPTA**: Se deberá marcar SI (X) en caso la institución cuente con dicho proceso o NO(X) si desconocen o no lo toman en cuenta.
- **Observación**: Se deberá de llenar si desea justificar el porqué de la respuesta en caso sea necesario o resaltar alguna información de dicho proceso.
- **Procesos adicionales**: En caso la institución educativa encuestada cuente con otro proceso, deberá ser agregado en este apartado.

La plantilla **GR006**, se establece los procesos que el ministerio de educación establece que puede tener una institución educativa básica regular, las cuales han sido tomadas en cuenta, con el fin de poder identificar cuáles de estos procesos, las instituciones educativas llevan a cabo. A continuación, se presenta como debe ser llenado la plantilla **GR006** por el usuario.

LOGO	IDENTIFICACIÓN DE PROCESOS DE LA I.E.P					
	Fase:	II	**Proceso**	2	**Actividad**	-
	Código:	**GR006**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: El encargado tendrá que marcar (SI) si cuentan el proceso o (NO) si no cuentan con dichos procesos.

ÁREA	*Área del entrevistado*	**RESPONSABLE**	*Nombre del entrevistado*

N°	TIPO DE PROCESO	RPTA SI	RPTA NO	OBSERVACION
1	**ESTRATÉGICOS (PE)**			
	PE01. Gestionar la planificación	*x*		
	PE02. Gestionar las relaciones interinstitucionales		*x*	*Se tiene pero de manera parcial.*
	PE03. Gestionar el sistema de control interno	*x*		
	PE04. Gestionar el desarrollo e innovación		*x*	*Se está planteando estrategias para llevar a cabo dicho proceso.*
	PE05. Marketing educativo	*x*		
	PE06. Análisis de las partes interesadas.	*x*		
2	**OPERATIVOS (PO)**			
	PO01. Gestionar el servicio educativo	*x*		
	PO02.Gestionar los recursos para los aprendizajes.	*x*		
	PO03. Gestionar el desarrollo del personal de servicio en las instituciones educativa	*x*		
	PO04. Gestionar la infraestructura educativa	*x*		
3	**SOPORTE (PS)**	*x*		
	PS01. Gestionar Recursos Humanos	*x*		
	PS02. Administrar los recursos financieros	*x*		
	PS03. Administrar sistema logístico.	*x*		
	PS03. Administrar los sistemas y TIC	*x*		
	PS03. Atender asuntos jurídicos legales		*x*	*Este proceso se encuentra tercerizado.*

Procesos adicionales

No se cuenta con otros procesos.

CREADO POR **APROBADO POR**

Proceso 2: Identificación de Activos de TI:

En este proceso se pretende identificar los diferentes activos que el área de TI cuenta, para brindar los diferentes servicios a las diferentes áreas de las instituciones educativas. Se hace énfasis en esta etapa debido a que los activos, son todo aquello que le da valor a la organización y por lo tanto requiere protección. Se establece los siguientes perfiles para la identificación de los activos.

a) **Servicios [SE]:** Medio para entregar valor a las diferentes áreas de las instituciones educativas, satisfaciendo las necesidades de sus usuarios para que logren sus objetivos.
   Obtener de: Se debe realizar entrevistas o encuestas a los encargados de cada área para identificar los servicios que son ofrecidos por el área de TI.
b) **Aplicaciones informáticas: [APW]:** Se hace referencia a las diferentes aplicaciones, ya sean propias o no del área de TI (programas o aplicativos, etc.). Las cuales son utilizadas por las diferentes áreas de la institución para lograr o mejorar el desarrollo de sus actividades.
   Obtener de: Reunión con él en cargado del área de TI.
c) **Soporte de TI [STI]:** Es la estructura tecnológica que brinda soporte a las diferentes aplicaciones propias o de terceros de las instituciones educativas.
   Obtener de: Inventario de TI.

<u>Actividad 1: Identificar activos:</u>

Para la identificación de activos de acuerdo a los perfiles ya mencionados anteriormente se debe utilizar la siguiente plantilla **GR006**, la cual tiene que ser realizada por cada miembro del área de TI, donde tendrán realizar lo siguiente.

- **Área**: Es el área en donde pertenece la persona que se está entrevistando.
- **Responsable**: Persona quien está llenando dicha plantilla.
- **Activos**: Es la identificación de los diferentes activos que cuenta el área de TI, para brindar soporte a los diferentes procesos que soporta de la institución educativa. Para la identificación de activos se debe tomar en cuenta los perfiles establecidos anteriormente (Servicios, Aplicaciones y Soporte de TI).
- **Propio**: Por cada activo que se identifique, se debe marcar SI(X) si el activo pertenece a la institución o NO(X) si el activo no le pertenece a la institución.

- **Observación**: Sirve para detallar el estado actual en que se encuentra cada uno de los activos que se está identificando.

A continuación, se muestra como el usuario deberá de llenar la plantilla **GR006** descrita anteriormente.

LOGO	**IDENTIFICACIÓN DE ACTIVOS DE TI**					
	Fase:	II	**Proceso**	3	**Actividad**	1
	Código:	**GR006**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ÁREA		**RESPONSABLE**		
N°	**ACTIVOS**	**PROPIO**		**OBSERVACION**
		SI	**NO**	
	SERVICIOS: *Medio para entregar valor a las diferentes áreas de las instituciones educativas, satisfaciendo las necesidades de sus usuarios para que logren sus objetivos*			
	Servicio de intranet.			
	Aplicaciones móviles			
	Servicio web			
	Servicio de correo electrónico			
	Servicio #n			
	. . .			
	APLICACIONES: *Se hace referencia a las diferentes aplicaciones que se brinda, ya sean propias o no del área de TI*			
	Sistema contable			
	Sistema de gestión académica			
	Sistema de pensiones			
	Aplicaciones #n			
	. . .			
	SOPORTE DE TI: *Es la estructura tecnológica que brinda soporte a las diferentes aplicaciones propias o de terceros de las instituciones educativas.*			
	Servidor web			
	Servidor de base de datos			
	Dispositivos de comunicación			
	Soporte de TI #n			
	. . .			

CREADO POR **APROBADO POR**

Actividad 2: Listado de los activos de Tecnología de información:

Una vez identificadas los diferentes activos que cuentan el área de TI, se aplicará el siguiente formato Tabla 9, para tener identificados de manera ordenada todos los activos que cuentan según su perfil. Se consideran las siguientes características que las instituciones educativas deben de tomar en cuenta:

- **Número de ítem**: Llevar un control de la cantidad total de activos.
- **Tipo de activo**: Para identificar a que perfil del activo pertenece.
- **Activo**: Nombre del activo el cual se ha identificado.
- **Código**: Código único para identificar el activo.

N°	Código	Perfil del activo	Activo	Responsable
# ítem	Código del activo	Tipo de activo	Nombre del activo	Área responsable

Tabla 12: Listado de activos

Proceso 3: Valoración de Activos de TI

Esta actividad tiene como objetivo identificar los diferentes servicios de TI utilizados por las diferentes áreas de las instituciones educativas, y a su vez identificar que tan importante son estos activos para estas áreas y así poder evaluar en como impactaría a la organización si algunos de activos de TI, tuvieran alguna interrupción. Para el desarrollo de esta actividad se debe tomar en cuenta lo siguiente:

- **Utilizaremos** Se hará uso de los siguientes criterios1: nivel de confidencialidad (**Tabla 1**), nivel de disponibilidad (**Tabla 2**), nivel de integridad (**Tabla 3**), las cuales fueron establecidas en el **proceso 3 de la fase 1**.
- **Área**: Se indica el área a la cual se está encuestando.
- **Responsable**: Es el encargado de cada área el responsable de llenar la plantilla.
- **Activos**: Se le presentará la lista de activos que han sido identificados en la **fase 2**, para que el usuario identifique cuales de estos activos son utilizados por su área.
- Uso: Aquí el usuario tendrá que marcar (X), si el activo mencionado es utilizado por su área.
- **Criterios**: Es este recuadro el usuario tendrá que valorar a los activos según los criterios de valoración que se han establecidos anteriormente.
- **Observación**: Se debe indicar como ayuda el activo en los procesos que tiene la institución educativa.
- **Otros activos**: Van los activos que no han sido identificados por el área de TI.

LOGO	VALORACIÓN DE ACTIVOS					
	Fase:	II	**Proceso**	3	**Actividad**	-
	Código:	**GR007**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CONFIDENCIALIDAD (C)	
1	La información es pública .
2	La información es de uso interno de la institución.
3	La información es uso para ciertas áreas de la institución
4	La información es accedida para ciertas personas
5	La información solo es accedida por personal de alto rango

DISPONIBILIDAD (D)	
1	El funcionamiento es normal en las actividades
2	Disponible al 10% del tiempo.
3	Disponible al 30% del tiempo.
4	Disponible al 60% del tiempo.
5	Disponible al 90% del tiempo.

INTEGRIDAD (I)	
1	Se tolera pérdida o alteración de sus componentes en un 100%
2	Se tolera pérdida o alteración de sus componentes en un 80%
3	Se tolera pérdida o alteración de sus componentes en un 50%
4	Se tolera pérdida o alteración de sus componentes en un 15%
5	Se tolera pérdida o alteración de sus componentes en un 0%

ÁREA			RESPONSABLE				
N°	ACTIVOS		USO	CRITERIOS			OBSERVACIÓN
	CÓDIGO	DESCRIPCION		C	D	I	TOTAL
1	S-AM	Aplicaciones móviles					Observación 1
2	S-SW	Servicio web	**x**	3	5	4	Observación 2
3	A-SC	Sistema contable					Observación 3
4	A-SGA	Sistema de gestión académica	**x**	4	5	5	Observación N
5	T-SW	Servidor web					…
…	…	...					…
…	…	...					…
…	…	…					…
#N	Código N	Activo #N					…
							..
OTROS ACTIVOS: ***sirve para poder identificar activos que utilizan las diferentes áreas, las cuales no han sido identificados por el área de TI.***							
#N	Código N	Activo #N					…
…	…	...					…
…	…	…					…

CREADO POR

APROBADO POR

FASE 3: EVALUACIÓN DEL RIESGO

Proceso 1: Identificación de riesgos:

Una vez identificados y ordenados por el valor los diferentes activos de las instituciones educativa, en esta fase se requiere analizar las diferentes amenazas y vulnerabilidades que puede tener cada uno de los activos. Para realizar esta actividad se puede utilizar los controles que actualmente existen en las instituciones educativas y además tomar de ayuda las diferentes amenazas que se proponen en la NTP 27000:2014 como ayuda para la identificación de las diferentes vulnerabilidades que pueden tener cada uno de los activos.

Se establecen los siguientes tipos de amenazas que las instituciones educativas básicas regular, pueden utilizar para la evaluación de escenarios, la cual les ayudará a identificar las diferentes amenazas a las que están expuestos sus activos.

- **Naturales**: Se refiere a diferentes fenómenos naturales, que la organización no puede controlar y que, al producirse, pueden afectar a sus procesos.
- **Servicios**: Hace referencia a los inconvenientes que pueden suceder por usos de servicios de tercero o propios.
- **Usuario no intencional**: Son acciones no intencionales, realizada por el personal interno de la organización, por problemas internos del mismo software, etc.
- **Usuario intencional**: Personas mal intencionadas tienen acceso o no, pueden causar ataques deliberados ya sea para beneficiarse o causar daños.
- **Información**: Son las posibles amenazas que pueden generar inconsistencia en los datos mostrados en los servicios prestados.
- **Software**: Son los softwares propios o de terceros que pueden traer interrupciones a los servicios ofrecidos ya sea por una actualización o por permisos no deseados.

Para identificar las vulnerabilidades de los diferentes activos que dan soporte a las instituciones educativas, se estableció la siguiente lista de amenazas en la **plantilla GR008.** Dicha plantilla se puede ir retroalimentando conforme vayan analizando las diferentes amenazan que puede tener las instituciones educativas en sus activos de TI.

LOGO	LISTADO DE AMENAZAS					
	Fase:	III	**Proceso**	1	**Actividad**	1
	Código:	**GR008**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

TIPO DE AMENAZA	AMENAZA
NATURALES	Polvo
	Corrección o Humedad
	Desastres naturales
	Corte de suministro eléctrico
	Amenaza N° …
SERVICIOS	Interrupción de servicios internos y externos.
	Fallo de servicio de comunicaciones
	Corte de suministro eléctrico
	Fallos eléctricos
	Espionaje
	Software dañado
	Amenaza N° …
USUARIO NO INTENCIONAL	Errores de usuarios
	Errores de configuración
	Escape de información
	Errores de mantenimiento
	Caídas del sistema
	Indisponibilidad del personal
	Perdidas de equipos
	Usuario mal entrenado
	Negligencia del usuario.
	Amenaza N° …
USUARIO INTENCIONAL	Usuario deshonesto
	Empleados despedidos
	Penetración del sistema
	Robo de información
	Acceso no autorizado
	Ingeniería social
	Amenaza N° …
INFORMACIÓN	Acceso no autorizado a la información
	Modificación no autorizada
	Eliminación no autorizada
	Robo de activo contenedores de información
	Corrupción de datos
	Ataques de hacking
	Fuga de información
	Alteración de información
	Amenaza N°…
SOFTWARE	Actualizaciones no controladas
	Instalaciones no autorizadas
	Saturación de operaciones en el software
	Virus informático
	Amenaza N° …

CREADO POR **APROBADO POR**

Actividad 1: Escenarios de riesgos

Esta actividad tiene el objetivo de simular diferentes escenarios de riesgos, la cual permite identificar las diferentes amenazas y vulnerabilidades que cuentas los activos de las instituciones educativas y así poder identificar los diferentes servicios que pueden ser afectados si estos escenarios llegaran a materializarse. Para desarrollar esta actividad se presenta la plantilla en donde las instituciones educativas podrían utilizar:

- **Código:** Identificador único por cada escenario de riesgo.
- **Tipo de amenaza:** Se encuentran mencionadas en la plantilla **GR008**.
- **Amenaza:** Agente interno o externo que puede poner en peligro los activos de las instituciones educativas al explotar una vulnerabilidad.
- **Vulnerabilidad:** Cualidad vulnerable de un activo, la cual puede ser aprovechada por una amenaza.
- **Riesgo:** Es la representación cuando una vulnerabilidad es aprovechada por una amenaza, la cual es la probabilidad de que una amenaza se convierta en un desastre aprovechando dicha vulnerabilidad.
- **Activos afectados:** Se hace referencia a los servicios, aplicaciones o soporte de TI que pueden ser afectados si un riesgo se llega a materializar.
- **Tiempo:** Es la duración del efecto una vez que el riesgo se manifieste.
- **Efectos:** Son las consecuencias que enfrentarían las instituciones educativas si algún escenario de riesgo se materializa.

  -Escenario negativo: Escenario negativo no deseado que podrían afectar a las instituciones educativas.

  Escenario positivo: La cual puede ser aprovechada las instituciones educativas para generar un beneficio.

LOGO	ESCENARIO DE RIESGOS					
	Fase:	III	**Proceso**	1	**Actividad**	1
	Código:	**GR009**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CÓDIGO: *#identificador*		**TIEMPO:** *Duración del riesgo*	
TIPO DE AMENAZA: *Ver plantilla **GR008***		**AMENAZA:** *Ver plantilla Ver plantilla **GR008***	
VULNERABILIDAD: *Cualidad vulnerable de un activo, aprovechada por una amenaza.*		**RIESGOS:** *Es la consecuencia que se tendría si la amenaza explora la vulnerabilidad del activo.*	
ACTIVOS AFECTADOS: *Se hace referencia a los servicios, aplicaciones o soporte de TI que pueden ser afectados si un riesgo se llega a materializar*.			

CREADO POR **APROBADO POR**

Actividad 2: Listar Amenazas y Vulnerabilidades identificadas

Una vez llevado a cabo los escenarios de riesgos, se deben de listar los diferentes riesgos identificados teniendo en cuenta las amenazas y vulnerabilidades que tiene cada uno de los activos de las instituciones educativas, para ello haremos uso de la plantilla **GR010**, donde se tendrá en cuenta los siguientes elementos.

- **Numero**: Numero del riesgo
- **Etiqueta del Activo**: Etiqueta del activo que se está evaluando sus amenazas y vulnerabilidades.
- **Activo**: Nombre del activo que se está evaluando sus amenazas y vulnerabilidades.
- **Código**: Es el identificador del escenario de riesgo. Lo podemos encontrar en las plantillas **GR009** utilizadas en la actividad anterior.
- **Amenaza**: La amenaza que ha sido identificado para el activo.
- **Vulnerabilidad**: La vulnerabilidad que tiene el activo, para que la amenaza sea un riesgo potencial.
- **Riesgo**: Impacto negativo que tendría la institución si el riesgo identificado se materializara.

LISTA DE AMENAZA Y VULNERABILIDAD						
	ACTIVO		ESCENARIO			
N°	Etiqueta	Nombre	Código	Amenaza	Vulnerabilidad	Riesgo
N	*Etiqueta N*	*Activo N*	*Código N*	*Amenaza N*	*Vulnerabilidad N*	*Riesgo N*
…	…	…	…	…	..	…

Tabla 13: Lista de amenaza y vulnerabilidades

En esta actividad se hará uso de la plantilla **GR010,** donde se tendrá que listar de manera ordenada las diferentes amenazas y vulnerabilidades, según el perfil del activo y la etiqueta del activo, con el fin de mantener un orden a la hora de pasar a la siguiente fase.

LOGO	LISTADO DE RIESGOS					
	Fase:	3	**Proceso**	1	**Actividad**	2
	Código:	**GR010**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ACTIVO			ESCENARIO DE RIESGO			
N°	**ETIQUETA**	**NOMBRE**	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**
#	*Etiqueta #*	*Nombre del activo*	*Identificador del escenario*	*Amenaza 1 del activo*	*Vulnerabilidad 1 del activo*	*Esc. Negativo 1*
..	..	…	…	…	…	…
..	..	…	…	…	…	…
..	..	…	…	…	…	…
..	..	…	…	…	…	…
N	*Etiqueta N*	*Nombre N*	*Código N*	*Amenaza N*	*Vulnerabilidad N*	*Esc. Negativo N*

CREADO POR **APROBADO POR**

Proceso 2: Análisis de riesgos

En el análisis de riesgos se debe de tener en cuenta la identificación de la naturaleza del riesgo (NR), por eso, las instituciones educativas deben de considerar la naturaleza de riesgo a los que se están enfrentando, las cuales son:

- Riesgo Estratégico (RE): Amenazas que pueden afectar a la capacidad de la institución educativa para cumplir sus metas y objetivos, por ejemplo: cambio de tipo de enseñanza o el impacto de la tecnología.
- Riesgo Financiero (RF): Perdida potencial de activos, tangibles inversiones o ingreso.
- Riesgo Operativos (RO): Riesgo de error, errores manuales, o del sistema, entre ellos tenemos la precisión de la información, accesibilidad y confidencialidad, integridad y seguridad de datos, confiabilidad y obsolescencia de hardware, capacidad de infraestructura, conectividad, respaldo y recuperación, capacidad de la infraestructura de comunicaciones, conectividad y compatibilidad del sistema.
- Riesgo Legales (RL): Riesgos que están relacionados con el cumplimiento de una institución como son las ordenanzas locales, políticas y procedimientos internos.
- Riesgo Reputación (RR): Percepción externa y sus efectos en la reputación y la marca de la institución.

Se tiene como objetivo de analizar los diferentes riesgos identificados en la etapa anterior, analizando su probabilidad y el impacto que se tendría si el riesgo se llegara a materializarse y a la vez establecer si es una amenaza o una oportunidad para la organización, para el desarrollo de esta fase se necesita:

- Lista de criterios de evaluación, se obtiene del **proceso 4 de la FASE 1**, la cual servirán para analizar cada uno de los riesgos identificados, además de establecer el nivel de riesgos que sería el resultado de la (probabilidad x el impacto)
- Lista de amenazas y vulnerabilidades, la podemos obtener de la plantilla **GR010,** la cual fue realizada en la fase anterior.

Para llevar a cabo esta actividad se hará uso de la siguiente tabla **11,** la cual contiene:

- **Número**: Numero del riesgo
- **Etiqueta del Activo**: Etiqueta del activo que se está evaluando sus amenazas y vulnerabilidades.
- **Activo**: Nombre del activo que se está evaluando sus amenazas y vulnerabilidades.

- **Código**: Es el identificador del escenario de riesgo. Lo podemos encontrar en las plantillas **GR009** utilizadas en la actividad anterior.
- **Amenaza**: La amenaza que ha sido identificado para el activo.
- **Vulnerabilidad**: La vulnerabilidad que tiene el activo, para que la amenaza sea un riesgo potencial.
- **Probabilidad (P):** Niveles de probabilidad establecidos en la plantilla **GR003.**
- **Impacto (I):** Niveles de impacto establecidos en la plantilla **GR003.**
- **(PXI):** Es el resultado final, después de haber analizar el impacto y la probabilidad de cada uno de los riesgos detectados.
- **Categoría (CAT):** Es el nivel del riesgo que tiene el escenario de riesgo identificados en la plantilla **GR010.**
- **Naturaleza del riego (NR):** Son 5 tipos de la naturaleza de riesgo, las cuales han sido mencionada anteriormente que las instituciones educativas básica regular deben de considera.

#	ACTIVO		RIESGO			ANALISIS				
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CÓDIGO	P	I	(PxI)	CAT	NR
1	*Etiqueta 1*	*Activo 1*	*Amenaza 1*	*Vulnerabilidad 1*	*Ident. 1*	*3*	*3*	*6*	*Moderado*	*RO*

Tabla 14: Análisis de riesgos

A continuación, se muestra la plantilla **GR011**, que se utiliza para el análisis de riesgo, la cual contiene los datos de entrada necesarios para la evaluación de los diferentes escenarios de riesgos identificados.

LOGO	ANÁLISIS DE RIESGOS					
	Fase:	III	**Proceso**	**2**	**Actividad**	3
	Código:	**GR011**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

PROBABILIDAD (P)		
NIVEL	**CATEGORIA**	**PROBABILIDAD**
1	Muy bajo	Puede ocurrir una vez cada dos años.
2	Bajo	Puede ocurrir 2 veces al año.
3	Moderado	Puede ocurrir 1 vez cada 3 meses.
4	Alto	Puede ocurrir 1 vez al mes.
5	Muy alto	Ocurre al menos 2 veces a la semana .

IMPACTO (I)		
NIVEL	**CATEGORIA**	**IMPACTO**
1	Muy bajo	El daño no contiene consecuencias relevantes para la organización.
2	Bajo	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la organización.
3	Moderado	El daño contiene consecuencias relevantes para la organización y su operación.
4	Alto	El daño tiene consecuencias muy graves para la organización.
5	Muy alto	El daño tiene consecuencias muy graves para la organización y podrían ser irreversibles.

EVALUACIÓN (PxI)		
NIVEL	**(PxI)**	**CATEGORIA**
1	[1-2]	Muy bajo
2	[3-4]	Bajo
3	[5-10]	Moderado
4	[10-15]	Alto
5	[15-25]	Muy alto

#	ACTIVO		RIESGO			ANALISIS				
	ETIQUETA	**ACTIVO**	**RIESGO**	**VULNERABILIDAD**	**CÓDIGO**	**P**	**I**	**(PxI)**	**CAT**	**NR**
1	*Etiqueta 1*	*Nombre del activo 1*	*Riesgo 1*	*Vulnerabilidad 1*	*Identificador 1*	*3*	*3*	*6*	*Moderado*	
2	*Etiqueta 2*	*Nombre del activo 1*	*Riesgo 2*	*Vulnerabilidad 1*	*Identificador 2*	*3*	*1*	*3*	*Bajo*	
…	…	…	…	…	…	…	…	…	…	
…	…	…	…	…	…	…	…	…	…	
…	…	…	…	…	…	…	…	…	…	
#	*Etiqueta N*	*Nombre del activo N*	*Riesgo N*	*Vulnerabilidad N*	*Identificador N*	*3*	*3*	*6*	*Moderado*	

CREADO POR **APROBADO POR**

Proceso 3: Evaluación de riesgos

En esta actividad se debe realizar la comparación de los resultados obtenidos en la etapa del análisis del riesgo, dicha comparación es realizada con los indicadores en la etapa de criterios de evaluación del riesgo. Para ello se tiene se tiene que realizar las siguientes actividades:

Actividad 1: Posicionar el riesgo:

Esta actividad tiene como finalidad posicionar el código del riesgo que ha sido identificado en la fase anterior según su probabilidad e impacto, para ello se hará uso de una matriz como se muestra en la tabla 12, la cual les permite a las instituciones educativas básica regular, poder identificar cuáles son los riesgos que debe de tratar primero, ya que al materializarse podría tener un gran impacto en la organización.

IMPACTO						
	5					R12,R13
	4	R3	R7	R11	R14	
	3		R8	R10		R15
	2		R6	R9		
	1	R1,R2			R4	R5
		1	2	3	4	5
		PROBABILIDAD				

Tabla 15: Matriz de probabilidad por impacto

La persona encargada de realizar la evaluación de riesgo deberá de posicionar los diferentes riesgos identificados según su probabilidad e impacto, haciendo uso de la tabla 12.

Actividad 2: Valoración de riesgos:

Se hará uso de la tabla 7, la cual ha sido establecido en la FASE I, permitiendo comparar los resultados obtenidos en la etapa anterior con el apetito y tolerancia que tiene la institución educativa. Para ello se usa la tabla 13 donde:

- **C:** Es el resultado obtenido en la etapa de análisis del riesgo (**PXI**)
- **A:** Apetito del riesgo. Obtener de los criterios de aceptación del riesgo ver (Tabla 7).

- **T**: Tolerancia al riesgo. Obtener de los criterios de aceptación del riesgo ver (Tabla 7).

CONDICIÓN	VALORACIÓN
C < A	Aceptable
C>=A Y <<T	Tolerable
C>T	Intolerable

Tabla 16: Comparación de apetito y tolerancia

Esta actividad se llevará acabo haciendo uso de la siguiente plantilla **GR012**, la cual contiene:

- **N°:** Es el número del riesgo que se va a evaluar
- **Activos:** Activo identificado que presenta de uno a más riesgos.
- **Amenaza:** Es la amenaza que se está presentando identificado es la etapa anterior.
- **Vulnerabilidad**: La causa por la cual se está presentando la amenaza identificada.
- **PXI**: Es producto de la evaluación obtenida en la fase anterior de la probabilidad y del impacto.
- **Apetito (A):** Apetito del riesgo, establecido en los criterios del riesgo. *(Ver tabla 7 –T7)*
- **Tolerancia (T):** Tolerancia del riesgo, establecido en los criterios del riesgo. *(Ver tabla 7 – T7)*
- **Valorización (V):** Es la comparación de "PXI" con "A y "T" para determinar el nivel de valoración según la tabla propuesta. *(Ver tabla 7 – T7)*
- **Tipo de riesgo (TR):** Indica si el riesgo identificado es una oportunidad (O) o una amenaza (A) - *(Ver tabla 11 – T11).*

#	ACTIVO		RIESGO			ANÁLISIS			EVALUACIÓN		
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CODIGO	PXI	CATEGORÍA	T.R	A	T	VALOR
#	Etiqueta1	Activo1	Amenaza1	Vulnerabilidad1	Codigo1	9	Moderado	o	T7	T7	T7

Tabla 17: Tabla de evaluación del riesgo

LOGO	EVALUACIÓN DEL RIESGO					
	Fase:	III	Proceso	**3**	**Actividad**	2
	Código:	**GR012**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

VALORAR	
Aceptable (A)	C<A
Tolerable (T)	C>=A Y <<T
Intolerable (I)	C>T

#	ACTIVO		RIESGO			ANÁLISIS		EVALUACIÓN		
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	CATEGORÍA	A	T	VALOR
#	Etiqueta 1	Activo 1	Riesgo 1	Vulnerabilidad 1	Código 1		Categoría 1	Tabla 7	Tabla 7	Tabla 7
…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…

CREADO POR

APROBADO POR

FASE 4: TRATAMIENTO DE RIESGOS:

Las instituciones educativas deben analizar los diferentes riesgos (amenazas u oportunidades) según su impacto y probabilidad, para establecer una estrategia de acuerdo al tipo de riesgo identificado.

Estrategias para Amenazas:

- **Escalar:** Cuando la amenaza se encuentra fuera del alcance y la propuesta excede la autoridad de gerencia.
- **Evitar:** Dejar de realizar las actividades que pueden hacer provocar el riesgo identificado, para disminuir la probabilidad de ocurrencia.
- **Transferir-Compartir:** Transferir el evento a un tercero para que no afecte a la organización.
- **Mitigar:** Minimizar el impacto y la probabilidad realizando planes de acción**.**
- **Aceptar:** Indica las pérdidas que se tendría si el riesgo se manifiesta, pero no se realiza ningún tipo de acción. Lo cual la institución estaría aceptando las consecuencias cuando este se presente.

Estrategias para oportunidades:

- **Escalar**: La persona encargada debe notificar de la oportunidad, cuando este exceda su autoridad.
- **Explotar:** Se utiliza para asegurarse de que la oportunidad suceda.
- **Mejorar:** Realizar actividades para mejorar las circunstancias y así la organización pueda verse beneficiada.
- **Aceptar:** Se reconoce la oportunidad, pero no se toman medidas proactivas.

Actividad 1: Identificación del tratamiento:

Para establecen un tratamiento, primero se debe identificar el tipo de riesgo que se está enfrentando (oportunidad o amenazas) y establecer el tratamiento correspondiente según el tipo, para luego ordénalos de manera descendente por tipo y por su impacto en las instituciones educativas.

#	ACTIVO		RIESGO			EVALUACIÓN			TRATAMIENTO
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CODIGO	PXI	CAT.	VALOR	
#	Etiqueta1	Activo1	Amenaza1	Vulnerabilidad1	Codigo1	9	Moderado	Tolerable	Mitigar

LOGO	TRATAMIENTO DE RIESGOS					
	Fase:	IV	**Proceso**	**1**	**Actividad :**	1
	Código:	**GR013**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

OPORTUNIDAD	AMENAZA
Escalar	Escalar
Explotar	Transferir-compartir
Compartir	Mitigar
Mejorar	Evitar
Aceptar	Aceptar

#	ACTIVO		RIESGO			EVALUACIÓN		TRATAMIENTO
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	VALOR	
#	Etiqueta 1	Activo 1	Amenaza 1	Vulnerabilidad 1	Código 1	9	Tolerable	Mitigar
…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…
N	Etiqueta #	Activo N	Amenaza N	Vulnerabilidad N	Código N	…	…	…

CREADO POR

APROBADO POR

Actividad 2: Establecer plan de acción:

Una vez identificado la estrategia que se va utilizar en cada uno de las amenazas detectadas, se debe implementar un plan de acción por cada una de ellas, para ello se propone la siguiente plantilla:

- **Nombre del proyecto**: Nombre para identificar el plan de acción
- **Código:** Identificador único del plan de acción.
- **Objetivo**: Especificar como se va a beneficiar la institución educativa aplicando el plan de acción propuesto.
- **Responsable:** Es el encargado de responder por el plan de acción.
- **Tiempo:** Es el tiempo en que se llevará a cabo el plan de acción.
- **Riesgos**: Se hace referencia a los diferentes riesgos que se serán tratados con el plan de acción propuesto.
- **Nivel del riesgo:** Se hace referencia al nivel máximo del riesgo por el cual se está llevando a cabo el plan de acción.
- **Recursos necesarios**: Recursos necesarios para poner en marcha el plan de acción.
- **Presupuesto:** Se debe indicar el número de personas que trabajaran el plan de acción, por la cantidad de horas trabajadas: Número de personas*tiempo*costo hora
- **Procesos del negocio:** Hace referencia a todos los procesos que se beneficiaran con la implementación de la propuesta.

LOGO	PROPUESTA DEL PLAN DE ACCIÓN					
	Fase:	I4	**Proceso**	**1**	**Actividad :**	2
	Código:	**GR014**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

"NOMBRE DEL PROYECTO"	
OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*	
RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*	
OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*	

CREADO POR **APROBADO POR**

FASE 5: SEGUIMIENTO Y REVISIÓN

Después de haber establecido los planes de acción y haberlos puesto en marcha, las instituciones educativas tienen que realizar un monitoreo continuo de los diferentes planes propuestos para identificar en qué estado se encuentra cada uno de ellos. Para que las instituciones puedan realizar un correcto seguimiento, se debe utilizar la siguiente tabla 15, para dar así poder establecer en qué estado se encuentra cada uno de los planes de acción propuesto.

VALOR	ESTADO	DESCRIPCIÓN
1	Concluido	Hace referencia a que la ejecución del plan de acción ha terminado.
2	En ejecución	Hace referencia a que el plan de acción se encuentra en etapa de ejecución.
3	Pendiente	Indica que el plan de acción aún no ha comenzado.
4	No concluido	Hace referencia cuando el proyecto no ha sido concluido en la fecha asignada.

Tabla 18: Estado del seguimiento de planes

Actividad 1 Listado de plan de acción:

Para el desarrollo de esta actividad haremos uso de los planes propuestos en la fase anterior, se tiene como objetivo revisar y controlar el estado actual e identificar los resultados que se van obteniendo de los planes de acción.

- **Plan de Acción:** Nombre del proyecto al que se le está dando seguimiento.
- **Estrategia:** La estrategia que se está utilizando para la implementación del plan de acción.
- **Responsable:** Encargado de llevar a cabo el plan de acción.
- **Tiempo:** Duración del proyecto una vez que haya iniciado.
- **Fecha de inicio (F.I):** Fecha en la que se dará inicio el plan de acción.
- **Fecha de Fin (F.F):** Fecha fin en la que debe culminar la implementación del plan de acción propuesto.
- **Presupuesto Asignado (PA):** Presupuesto total que ha sido asignado para llevar a cabo la implementación del plan de acción propuesto.
- **Presupuesto Utilizado (PU):** Es la cantidad del presupuesto que se está utilizando durante la implementación.
- **Estado:** Se debe utilizar los diferentes estados que se han establecido en la tabla anterior. (Ver tabla 15)

LOGO	LISTADO DE PLANES DE ACCIÓN					
	Fase:	V	**Proceso**	**1**	**Actividad :**	3
	Código:	**GR015**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Concluido
En ejecución
Pendiente
No concluido

PLAN DE ACCIÓN						SEGUIMIENTO			
#	**PROYECTO**	**ESTRATEGIA**	**RESPONSABLE**	**TIEMPO**	**P.A**	**F.INICIO**	**F.FIN**	**P. U**	**ESTADO**
	Nombre del proyecto.	*Estrategia que se aplicara para mitigar los riesgos correspondientes en el plan de acción*	*Encargado de llevar a cabo el proyecto.*	*Tiempo de duración del proyecto*	*Presupuesto asignado proyecto.*	*Fecha en que inicio el proyecto*	*Fecha donde debe terminar el proyecto*	*Presupuesto utilizado en el proyecto.*	*Ver tabla 15*

CREADO POR **APROBADO POR**

Actividad 2 Revisión del plan de acción:

Se tiene como objetivo de verificar el estado actual de cada uno de los planes de acción, para ello se hará uso de la siguiente plantilla la cual cuenta con los siguientes puntos a determinar:

- **Plan de acción**: Hace referencia al plan de acción que se está dando seguimiento.
- **Presupuesto Asignado**: Presupuesto asignado al inicio del proyecto.
- **Presupuesto utilizado**: Se indica el presupuesto que se va utilizando hasta la fecha de revisión del plan de acción.
- **Responsable**: Se hace referencia a la persona o área encargada de ejecutar el plan de acción propuesto.
- **Fecha de revisión**: Se debe de indicar la fecha en que se está realizando la revisión del plan de acción.
- **Actividades**: Lista de actividades que va realizando para cumplir el objetivo principal del plan de acción.
- **Observación**: Observaciones del personal quien está realizando el seguimiento.
- **Estado**: Estado en el que se encuentra el plan de acción después de la revisión que ha realizado el encargado.

LOGO	REVISIÓN DEL PLAN DE ACCIÓN			
	Fase:	1	**Proceso :**	1
	Código:	**GR016**	**Páginas:**	__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1	**Fecha de aplicación:**	__/__/__

"NOMBRE DEL PROYECTO"	
OBJETIVO: *Lo que la institución educativa desea lograr con el desarrollo del plan de acción que se está llevando a cabo.*	
RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
RIESGOS: *Los diferentes riesgos que se están tratando con el plan de acción que se está llevando a cabo.*	**NIVEL DEL RIESGO:** *Se debe de indicar el nivel del riesgo más alto del cual se están tratando.*
PRESUPUESTO: *Presupuesto total asignado al proyecto.*	**PRESUPUESTO UTILIZADO:** *Número de personas*tiempo*costo hora*
FECHA DE REVISIÓN: *Fecha en que se le da seguimiento al proyecto.*	**ESTADO:** *Estado actual en el que se encuentra el proyecto a la hora de finalizar la revisión.*
EVIDENCIAS: *Fotos o documentos que demuestren el estado actual del proyecto que se está llevando a cabo.*	

CREADO POR **APROBADO POR**

FASE 6: COMUNICACIÓN DEL RIESGO

Esta fase sirve para comunicar a las partes interesadas los hallazgos que se van realizando en cada una de las actividades de las fases de la gestión de riesgos. Esta fase tiene como objetivo lo siguientes puntos:

1. Uno de los objetivos que se pretende es promover la conciencia y compresión durante la gestión de riesgos dentro de la institución educativa básica regular.
2. Mejorar la toma de decisiones en cada una de las fases de gestión de riesgos.
3. Promover la participación de las diferentes partes interesadas con el objetivo de que la gestión de riesgo sea eficaz y eficiente durante su implementación.

Para ello se establece la plantilla, donde contiene los siguientes ítems:

- **Realizado por**: Es el encargado de reportar los diferentes avances o hallazgos durante la implementación de cada una de las actividades de la gestión de riesgos.
- **Enviado a**: Se debe de comunicar a las diferentes partes interesadas de la institución educativa básica regular sobre los avances o hallazgos encontrados durante la implementación.
- **Asunto**: Hace referencia el motivo por el cual se emitiendo el documento.
- **Evidencias**: Se describe los diferentes hallazgos o avances realizados a través de documentos, fotografías, donde se evidencie lo que se desea comunicar.

LOGO	COMUNICACIÓN			
	Fase:	6	**Proceso :**	1
	Código:	GR003	**Páginas:**	__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1	**Fecha de aplicación:**	__/__/__

REALIZADO: *Persona que envía el mensaje.*	**ENVIADO A:** *A quien va dirigido el documento*
ASUNTO: *Indica el motivo por el cual se emitiendo el documento.*	
EVIDENCIAS: *Se describe los diferentes hallazgos o avances realizados a través de documentos, fotografías, donde se evidencie lo que se desea comunicar*	

CREADO POR **APROBADO POR**

V. Discusión

El objetivo general planteado en esta investigación de minimizar los riesgos de los procesos que soporta el área de TI en instituciones educativas básica regular de la región de Lambayeque, se desarrolló el modelo de gestión de riesgos de tecnología de información. A continuación, se dará respuesta a cada uno de los objetivos que se establecieron en esta investigación, a través de la evaluación de los indicadores:

1. **Número de marcos para la gestión de riesgos**

   Según el análisis del sector que se realizó para identificar la problemática que existe en las instituciones educativas, se manifestó (Ver anexo 1, pregunta 21) que no se cuenta con alguna norma o estándar para llevar a cabo una gestión de riesgos en los activos de TI que dan soporte a los procesos de las instituciones, siendo una actividad clave para contribuir al logro de sus objetivos. Para ello se tuvo que realizar 3 pasos:

   El primero paso se tuvo que identificar las diferentes normas, metodologías o marcos de trabajo que hagan énfasis en la gestión de riesgos, teniendo como resultados una gran variedad de guías, metodologías que contribuyen de alguna manera en la gestión de riesgos. En esta investigación en una primera instancia se tomó en cuenta a 7 entre normas, marcos y metodologías.

   En el segundo paso se procedió a realizar un análisis de tallado de cada una de las normas, marcos y metodologías que fueron seleccionadas previamente, con el objetivo de conocer a detalle cada una de ellas.

   Por último, se realizó la comparación, en la cual se logró establecer etapas en que concordaba ciertas actividades de estas normas y estándares. Esta comparación sirvió para poder llevar a cabo la propuesta del modelo, con el objetivo de minimizar los riesgos soportados por el área de TI en las instituciones de educación básica regular.

2. **Validez del modelo propuesto de gestión de riesgos en instituciones de educación básica regular**

   Para llevar a cabo esta actividad, el modelo propuesto se sometió a una evaluación de 3 expertos con el fin de determinar el nivel de confiabilidad que existe en el modelo de gestión de riesgos de tecnología de información para minimizar los

riesgos de los procesos que soporta el área de TI en las instituciones educativas básica regular de la región de Lambayeque.

Después de procesar cada uno de los resultados de los expertos y aplicar el Alfa de Cronbach, se encuentra en el anexo IV, se obtuvo que existe un nivel de confiabilidad del 74%.

Tabla 19: Resultados del Alfa de Cronbach

CRITERIOS	VALOR
Número de ítems	15
Σ Varianza de los ítems	0.924
Varianza de los ítems	3.021
Coeficiente del Alfa de Cronbach	**0.743**

Fuente: Elaboración propia

Tabla 20: Niveles de confiabilidad

RANGO	VALOR
Valor < 0.50	Confiabilidad nula
0.50 < valor < 0.60	Confiabilidad baja
0.60 < valor < 0.70	Confiable
0.70 < valor < 0.80	Muy confiable
0.80 < valor < 0.90	Excelente confiabilidad
1.0	Confiabilidad perfecta

Comparando el resultado obtenido en la evaluación del Alfa de Cronbach con los niveles de confiabilidad, se puede observar que el modelo propuesto es **Muy confiable**, con un valor de **0.74.**

Como segundo paso se procedió a realizar la evaluación de contenido del modelo propuesto, con el objetivo para ver el nivel de concordancia que hay entre los expertos, para ello se utilizó la **W de Kendall**. Para ello se debe de tener en cuenta lo siguiente:

Primera hipótesis. *Cuando W > 0*, existe concordancia entre las evaluaciones que han realizado los expertos.

Segunda hipótesis. *Cuando W = 0*, no existe concordancia entre las evaluaciones que han realizado los expertos.

Los resultaron que se obtuvieron, luego de haber sido procesados por el SPSS, fueron los siguientes:

Figura 18: Análisis Kendall

COEFICIENTE DE KENDALL				
Donde: N = Cantidad de actividades. W = Coeficiente de concordancia. K = Cantidad de expertos. X^2 = Suma de los cuadrados de las desviaciones. P = Significación Asintótica.				
	SUFICIENCIA	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**
N	15	15	15	15
W	0,133	0,280	0,267	0,200
K	3	3	3	3
X^2	4,0	8,4	8,0	6,0
P	0,135	0,015	0,018	0, 050

Se concluye, que la hipótesis para la presente investigación es la primera, porque podemos corroborar que W es mayor a 0, entonces, si existe el coeficiente de concordancia entre los expertos en cada uno de los indicadores propuesto suficiencia, claridad, coherencia y relevancia.

3. Número de riesgos detectados en los activos del área de TI en las instituciones básica regular:

Teniendo en cuenta el análisis realizado para determinar la problemática que existe en las instituciones educativas básica regular, se manifestaron (Ver anexo, pregunta 3, 4, 7, 11) que el área de TI no cuenta con un inventario de sus activos, además de no tener mapeado todos los servicios que ofrecen a la institución siendo estas actividades factores claves para mejorar sus procesos y proteger a los activos que dan soporte a sus procesos críticos de la institución.

Los resultados obtenidos de la implementación del modelo en un caso de estudio, se obtuvo como resultado la identificación de 23 activos críticos del área de TI que dan soporte a los procesos de las instituciones, de las cuales se logró identificar un total de 38 escenarios de riesgos, de las cuales 3 son considerados

riesgos de muy alto nivel, 12 de nivel alto, 17 de nivel moderado, 4 de nivel bajo y 2 de nivel muy bajo.

4. **Número de proyectos propuesto para minimizar los riesgos en los activos del área de TI en las instituciones básica regular:**

   En el análisis llevado a cabo para establecer la problemática y el estado actual de las instituciones, se determinó que este tipo de instituciones no realizan un análisis de los diferentes riesgos a los que están expuesto sus activos y desconocen en qué manera pude impactar en la organización, otra de las cosas que se detectó en este análisis es que no dan seguimiento a los riesgos que se le han presentado y ni siquiera toman las medidas necesarias para prevenir en un futuro.

   Con la implementación del modelo del modelo se pudo identificar un total de 38 escenarios de riesgos a los que están expuestos sus activos del área de TI, siendo un total de 15 riesgos de nivel muy alto y alto que pueden perjudicar a la institución, las cuales se estableció planes de acción en 4 proyectos agrupados por diferentes riesgos con el objetivo mitigar estos riesgos o reducir el nivel de impacto.

VI. Conclusiones

1. Para el desarrollo del modelo propuesto, se basó en 3 etapas, la primera que fue la identificación de estándares y metodologías que hagan referencia a la gestión de riesgos, una vez identificado se pasó a la segunda etapa en donde se detalló cada una de sus actividades, técnicas o herramientas que utilizan para la gestión de los riesgos, las cuales sirvieron para la tercera etapa de la comparación de cada una de ellas, logrando armonizar cada uno de sus conceptos, las cuales sirvió para la propuesta realizada del modelo de gestión de riesgos de tecnología d información para minimizar los riesgos de los procesos que soporta el área de TI adaptándose a las necesidades de las instituciones de educación básica regular. Existe una gran variedad de modelos de gestión de riesgos, en la cuales también se ha realizado una armonización de normas o marcos de trabajo, las cuales han sido aplicados a diferentes tipos de sectores tanto en la región Lambayeque como a nivel nacional, sin embargo, no se encontró antecedentes de propuestas para que se puedan llevar a cabo en instituciones de educación básica regular.

2. Como producto acreditable de la presente tesis se propuso el modelo de gestión de riesgos de tecnología de información para minimizar los riesgos de los procesos que soporta el área de TI en instituciones educativas básica regular de la región de Lambayeque, la cual fue validado por 3 expertos con el fin de determinar el nivel de confiabilidad que existe en el modelo, como se explica en el análisis de resultados. (Ver el instrumento de validación en el Anexo N° 04).

3. Se valoró la implementación del modelo de gestión de riesgos de TI validado, aplicándolo en un caso de estudio en instituciones educativas básica regular de la región de Lambayeque, logrando identificar 15 procesos, de las cuales 23 activos que posee el área de TI son críticos para el cumplimiento de los objetivos de estos procesos que tienen en cuenta la institución educativa básica regular en la cual fue aplicado

4. Con la ejecución del modelo de gestión de riesgos propuesto se pudo identificar un total 15 riesgos de nivel alto y muy alto, los cuales serán tratados con un total de 6 proyectos.

VII. Recomendaciones

1. En la implementación parcial del modelo propuesto en un caso de estudio, se lograron proponer un total de 6 proyectos, que ayuda a la institución educativa minimizar los riesgos a los que están expuestos los servicios ofrecidos del área de TI a las diferentes áreas de la institución educativa, las cuales se recomienda llevar a cabo la implementación de estos proyectos con el objetivo de evitar las interrupciones en los servicios, la inconsistencia de los datos y resguardar la información como registros académicos, registros médicos y psicólogos de los alumnos y docentes.
2. Se recomienda a la institución educativa básica regular a seguir utilizando el modelo propuesto con el objetivo de poder identificar nuevos activos de información y poder tomar acciones correctivas frente a nuevas vulnerabilidades o amenazas a las que podrían estar expuestas y así lograr la reducción de los riesgos tomando acciones preventivas.
3. Se recomienda la implementación de un sistema, para llevar un mejor control de cada una de las fases propuestas, la cual le permita visualizar la matriz de los riesgos e identificar de una manera sencilla y rápida los riesgos que se deben de tener prioridad, adicionalmente el sistema debe de permitir el registro de nuevos riesgos y dar seguimiento a los planes de acciones.

VIII. Referencias

[1] C. A. Pastor Carrasco, «Impacto del riesgo en el gobierno de las tecnologías de información y comunicación en la gestión empresarial industrial del siglo XXI,» Lima, 2010.

[2] R. Gómez, D. H. Pérez, Y. Donoso y A. Herrera, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información,» *Revista de ingeniería,* nº 31, 2010.

[3] F. J. Valencia Duque, M. López Trujillo y C. E. Marluanda, «Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional,» *Reseachgrate,* 2016.

[4] G. A. Vanegas Devia y C. J. Pardo, «Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT,» *S&T,* 2014.

[5] «Cost of Data Breach Study,» Junio 2017. [En línea]. Available: https://www.ibm.com/downloads/cas/ZYKLN2E3. [Último acceso: 15 Junio 2019].

[6] R. Brooks, «Netwrix,» IT Risks in the Education Sector, 2019 Febrero 28. [En línea]. Available: https://blog.netwrix.com/2019/02/28/it-risks-in-the-education-sector-real-threats-vs-expectations/. [Último acceso: 2019 08 20].

[7] P. Panchal, «Information technology riks in higher education: strategy for assesment, planning and management,» New York, 2019.

[8] L. C. Aliaga Flores, «Diseño de un sistema de gestión de seguridad de información para un instituto educativo,» Lima, 2013.

[9] G. C. Llontop Díaz, «Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Network,» Lima, 2018.

[10] M. Y. Arangurí García, R. D. Iman Espinoza y L. T. Gregorio Manuel, «Modelo de gestión de riesgos de ti basados en estándares adaptados a las ti que soportan los procesos para contribuir a la generación de valor en las universidades privadas de la región Lambayeque,» Chiclayo, 2016.

[11] P. Caneo, «Gobierno de TI para obtener el mayor valor de las tecnologías de información,» *Gerencia,* 2013.

[12] D. E. Moncayo Racines, «Modelo de Evaluación de riesgos en activos TIC'S para pequeñas y medianas empresas del sector automotriz,,» Quito, 2014.

[13] M. D. C. Crespo Rin, «El Análisis de Riesgos dentro de una Auditoría Informática: pasos y posibles metodologías,» 2014.

[14] H. C. Asencios Carbajarl, «Guía metodológica de sistema de gestión de seguridad de la información basada en la NTP-ISO/IEC 17799, 27001 y COBIT 5 para minimizar los riesgos de gestión de la información en el poder judicial de Carhuaz,» Huaraz , 2017.

[15] J. C. Rojas Medina, «Modelo de gestión de seguridad de la información para el E-Gobierno,» Lima, 2016.

[16] G. F. Guzmán Pacheco, «Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega,» Huancayo, 2015.

[17] L. A. Moscoso Anaya , E. E. Peña Núñez y M. D. C. Soto Castrillón, «Modelo de gestión de riesgos de TI que contribuyen a la operación de los procesos de

gestion comercial de las empresas del sector de saneamiento del norte del Perú,» Chiclayo, 2018.

[18] F. B. Vasquez Velásquez y J. D. P. Alva Zapata, «Modelo de gestión de riesgos de TI para contribuir en la continuidad de las microfinancieras de la región Lambayeque,» Chiclayo, 2018.

[19] MINEDU, «Diseño curricular de educación básica regular,» 7 Noviembre 2005. [En línea]. Available: http://www.minedu.gob.pe/normatividad/reglamentos/DisenoCurricularNacional.pdf. [Último acceso: 2019 10 15].

[20] MINEDU, «Minedu.gob.pe,» [En línea]. Available: http://www.minedu.gob.pe/p/ley_general_de_educacion_28044.pdf. [Último acceso: 15 08 2019].

[21] J. A. Pérez Fernández de Velasco, Gestion Por Procesos, ESIC, 2009.

[22] AOSACIÓN DE ACADEMIAS DE LA LENGUA ESPAÑOLA, «https://dle.rae.es/riesgo,» [En línea]. Available: https://dle.rae.es/. [Último acceso: 2020 05 10].

[23] ISACA, COBIT 5 para riesgos, 2013.

[24] CD&A Consultores de Riesgos, «Estandar autraliano de administración de riesgos AS/NZS 4360:1999».

[25] ISO, «Gestión del riesgo - Directrices ISO 31000,» [En línea]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

[26] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, MARGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Madrid: Secretaría de Estado de Administraciones Públicas, 2012.

[27] M. Á. Mendoza, «welivesecurity,» 30 Septiembre 2014. [En línea]. Available: https://www.welivesecurity.com/la-es/2014/09/30/8-pasos-evaluacion-de-riesgos-2/. [Último acceso: 10 05 2020].

[28] Joint Task Force Transformation Initiative, «National Institute of Standards andTechnology (NIST) 800-30,» 2012.

[29] «NORMA ISO 27001,» [En línea]. Available: https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/. [Último acceso: 15 10 2019].

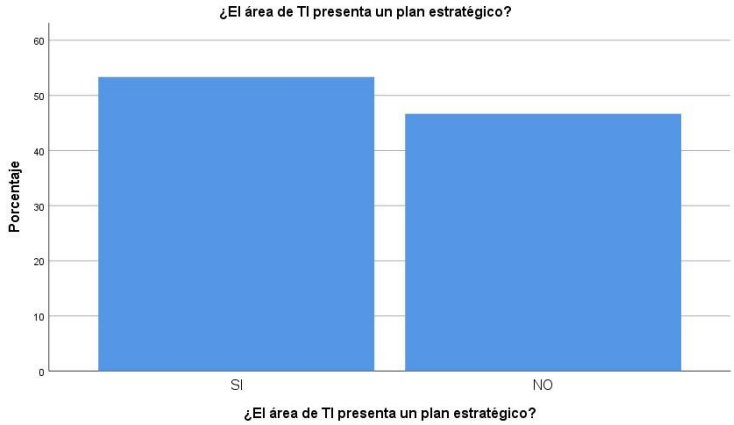
[30] 11 Julio 2014. [En línea]. Available: https://www.computing.es/infraestructuras/opinion/1075279001801/gobierno-cobit-5.1.html. [Último acceso: 08 08 2019].

IX. Lista de anexos

ANEXO I: RESULTADOS DE ENCUESTA

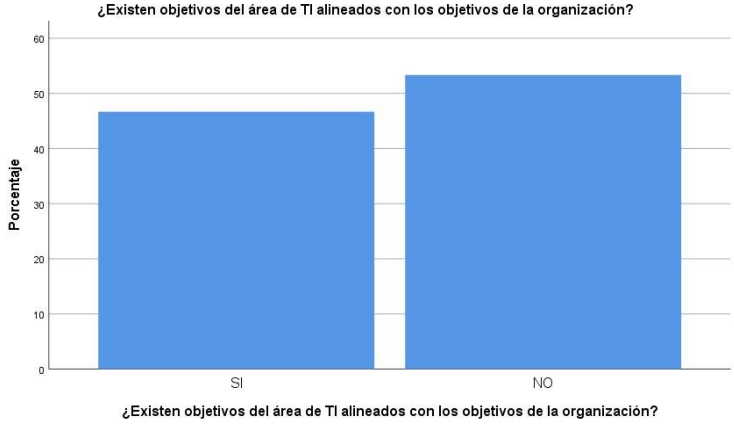
- **El área de TI presenta un plan estratégico**

		Frecuencia	Porcentaje
Válido	SI	8	53,3
	NO	7	46,7
	Total	15	100,0



- **Existen objetivos del área de TI alineados con los objetivos de la organización**

		Frecuencia	Porcentaje
Válido	SI	7	46,7
	NO	8	53,3
	Total	15	100,0

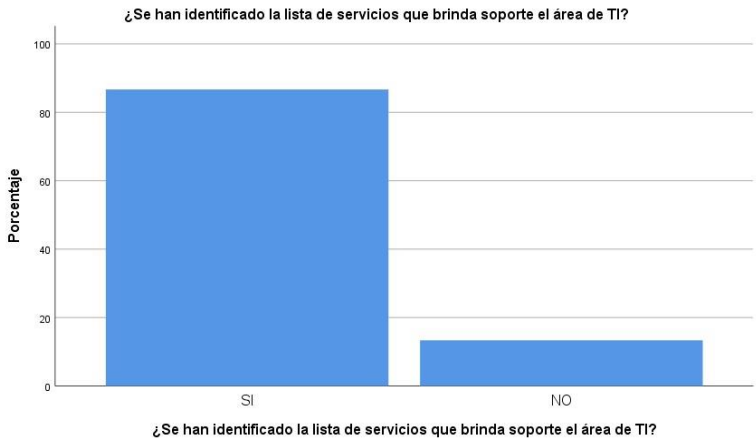


- **Se cuenta con un inventario de los activos que tiene el área de TI**

		Frecuencia	Porcentaje
Válido	SI	4	26,7
	NO	11	73,3
	Total	15	100,0

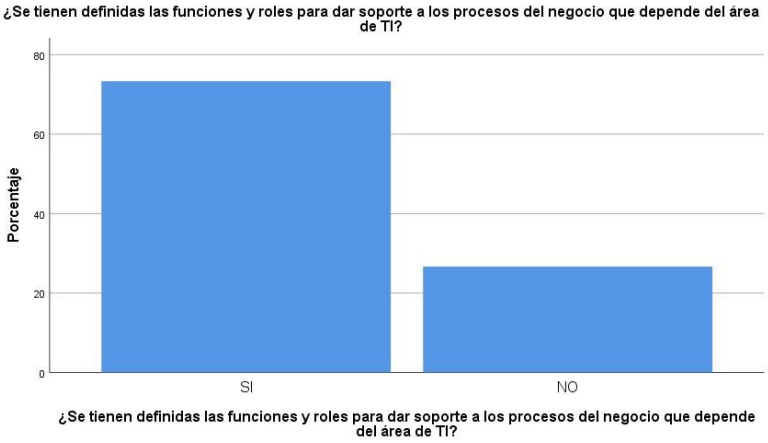
- **Se han identificado la lista de servicios que brinda soporte el área de TI**

		Frecuencia	Porcentaje
Válido	SI	13	86,7
	NO	2	13,3
	Total	15	100,0



- **Se tienen definidas las funciones y roles para dar soporte a los procesos del negocio que depende del área de TI**

		Frecuencia	Porcentaje
Válido	SI	11	73,3
	NO	4	26,7
	Total	15	100,0

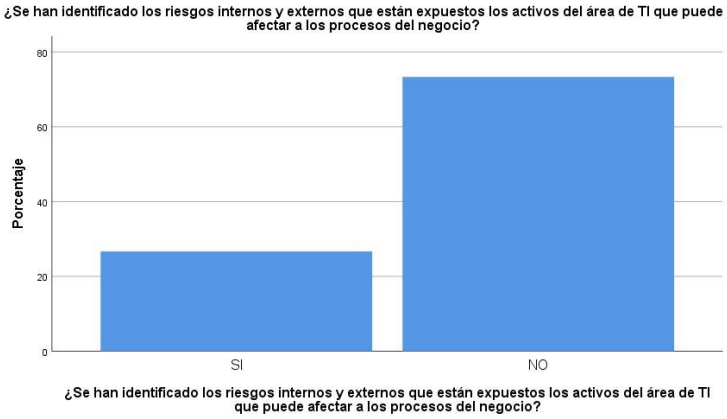


- **El área de TI cuenta con el apoyo de alta dirección para la mejora o seguridad de sus procesos**

		Frecuencia	Porcentaje
Válido	SI	14	93,3
	NO	1	6,7
	Total	15	100,0

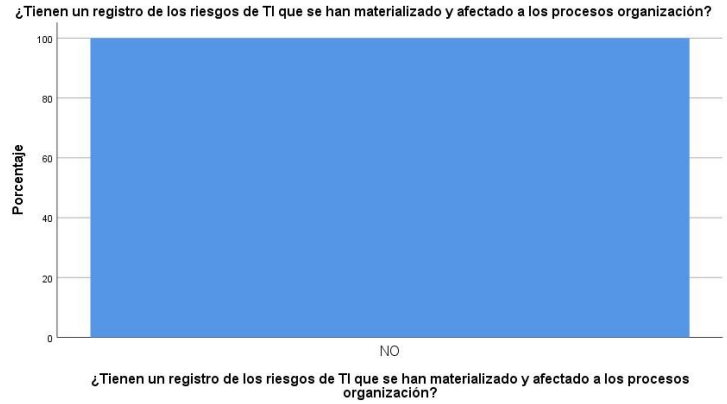
- **Se han identificado los riesgos internos y externos que están expuestos los activos del área de TI que puede afectar a los procesos del negocio**

		Frecuencia	Porcentaje
Válido	SI	4	26,7
	NO	11	73,3
	Total	15	100,0



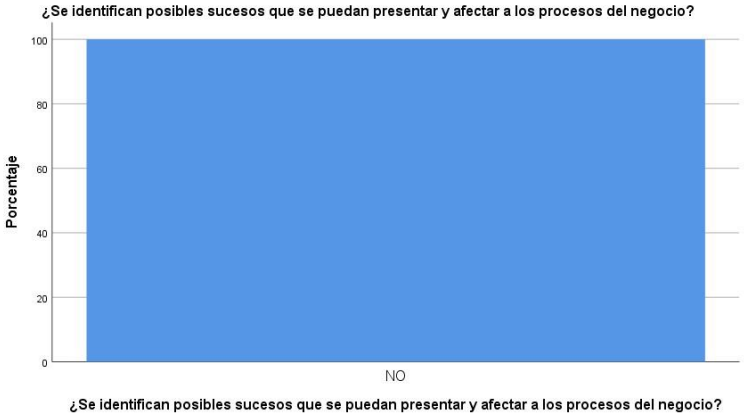
- **Tienen un registro de los riesgos de TI que se han materializado y afectado a los procesos organización**

		Frecuencia	Porcentaje
Válido	NO	15	100,0



- **Se identifican posibles sucesos que se puedan presentar y afectar a los procesos del negocio**

		Frecuencia	Porcentaje
Válido	NO	15	100,0

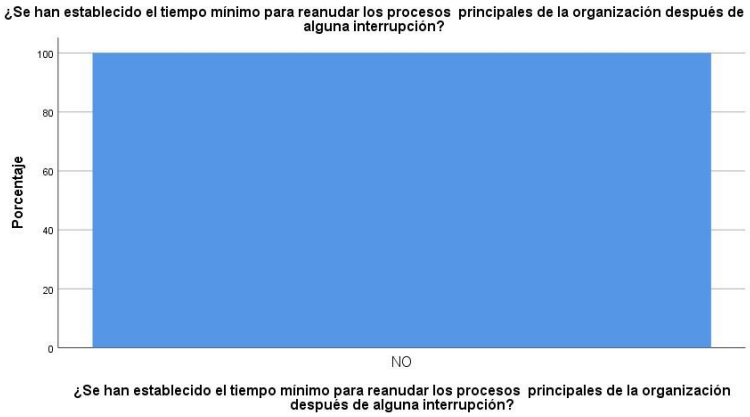


- **Se analizan los riesgos que la organización está dispuesta asumir**

		Frecuencia	Porcentaje
Válido	SI	2	13,3
	NO	13	86,7
	Total	15	100,0

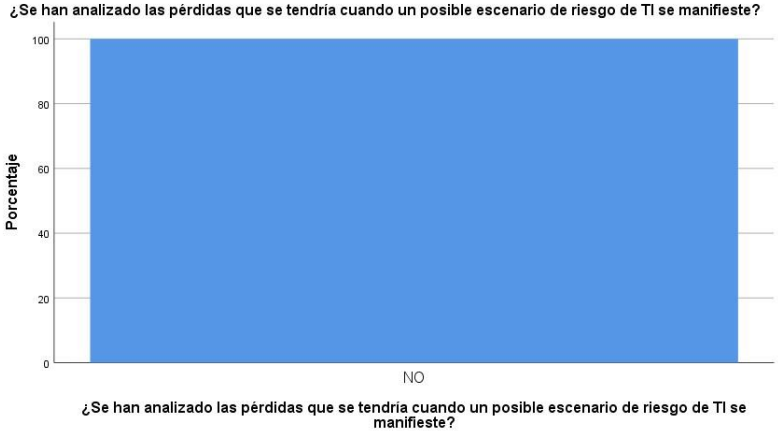
- **Se han establecido el tiempo mínimo para reanudar los procesos principales de la organización después de alguna interrupción**

		Frecuencia	Porcentaje
Válido	NO	15	100,0



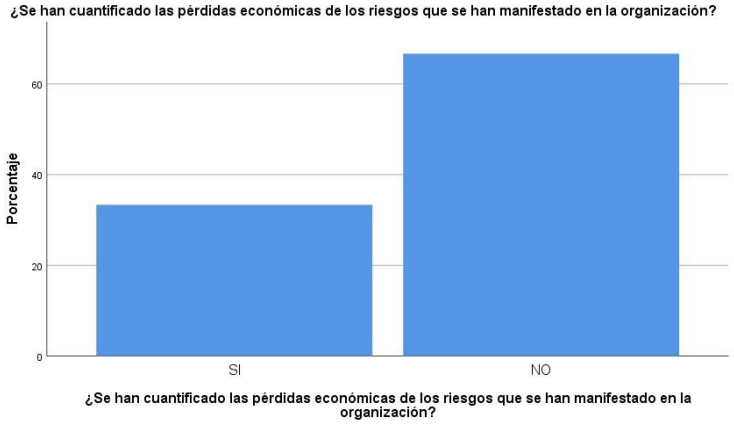
- **Se han analizado las pérdidas que se tendría cuando un posible escenario de riesgo de TI se manifieste**

		Frecuencia	Porcentaje
Válido	NO	15	100,0



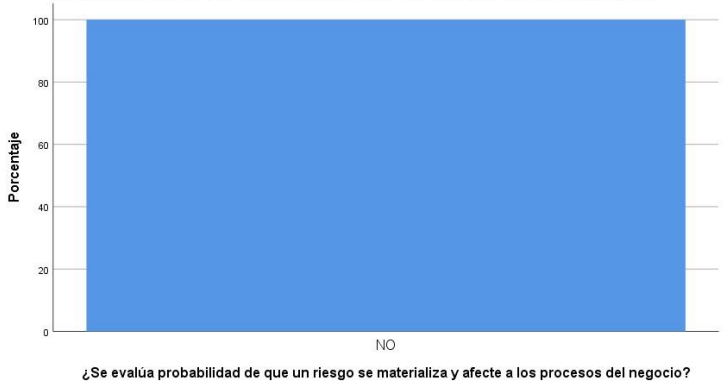
- **Se han cuantificado las pérdidas económicas de los riesgos que se han manifestado en la organización**

		Frecuencia	Porcentaje
Válido	SI	5	33,3
	NO	10	66,7
	Total	15	100,0



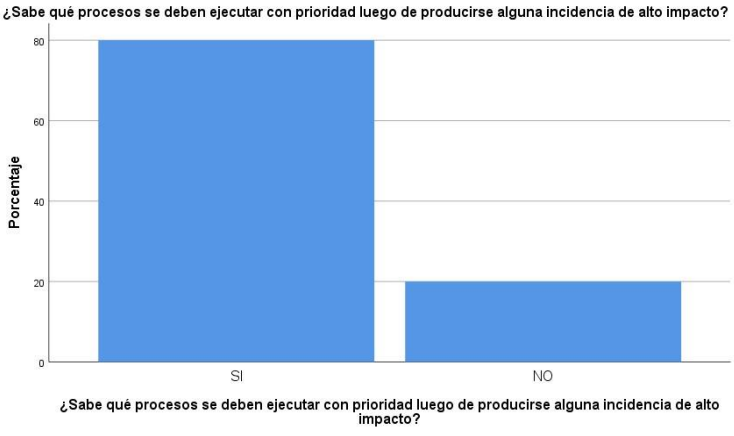
- **Se evalúa probabilidad de que un riesgo se materializa y afecte a los procesos del negocio**

		Frecuencia	Porcentaje
Válido	NO	15	100,0



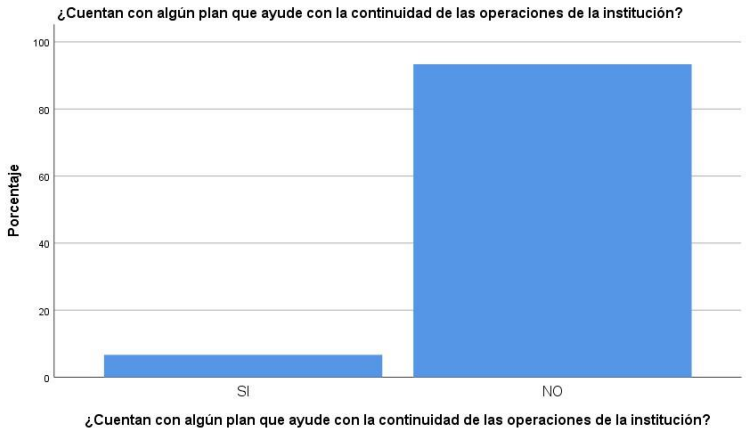
- **Sabe qué procesos se deben ejecutar con prioridad luego de producirse alguna incidencia de alto impacto**

		Frecuencia	Porcentaje
Válido	SI	12	80,0
	NO	3	20,0
	Total	15	100,0



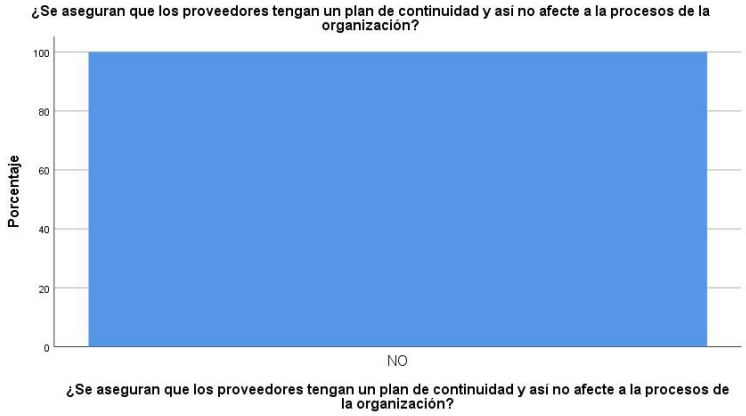
- **Cuentan con algún plan que ayude con la continuidad de las operaciones de la institución**

		Frecuencia	Porcentaje
Válido	SI	1	6,7
	NO	14	93,3
	Total	15	100,0



- **Se aseguran que los proveedores tengan un plan de continuidad y así no afecte a los procesos de la organización**

		Frecuencia	Porcentaje
Válido	NO	15	100,0

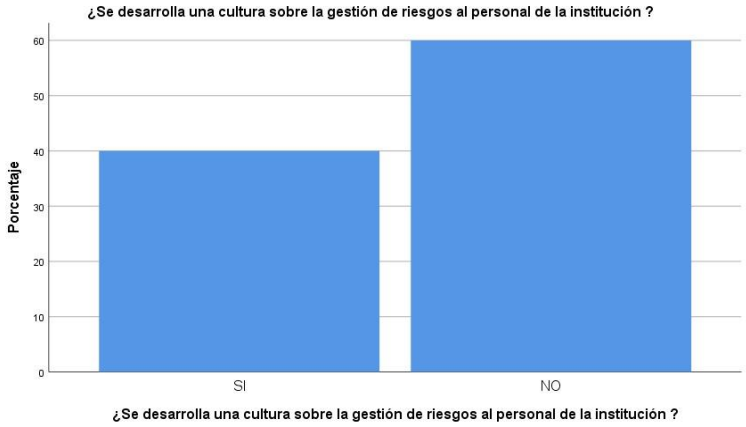


- **Tienen un inventario de las actividades de control que se realizan para la gestión de riesgos**

		Frecuencia	Porcentaje
Válido	NO	15	100,0

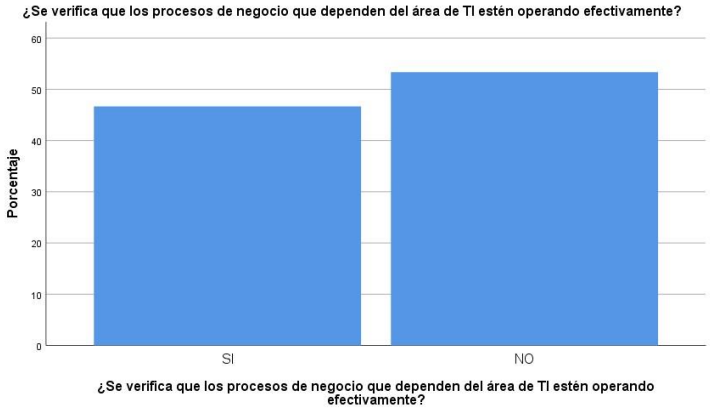
- **Se desarrolla una cultura sobre la gestión de riesgos al personal de la institución**

		Frecuencia	Porcentaje
Válido	SI	6	40,0
	NO	9	60,0
	Total	15	100,0



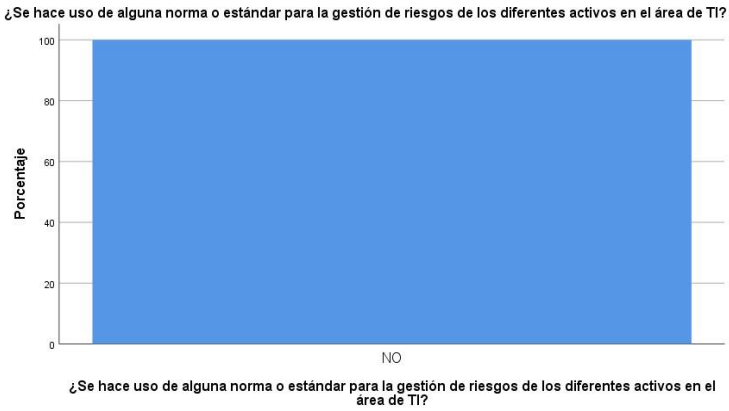
- **Se verifica que los procesos de negocio que dependen del área de TI estén operando efectivamente**

		Frecuencia	Porcentaje
Válido	SI	7	46,7
	NO	8	53,3
	Total	15	100,0



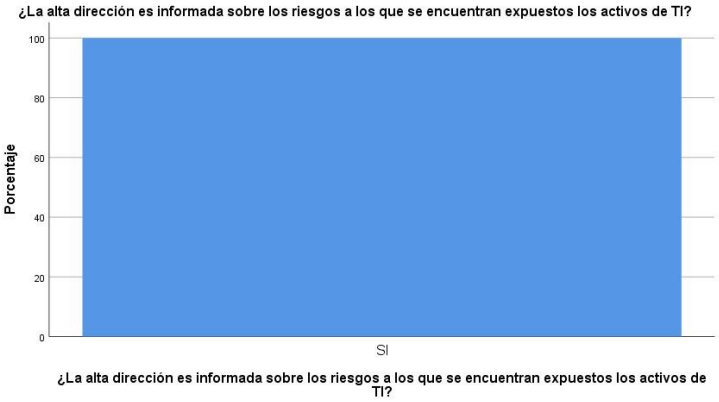
- **Se hace uso de alguna norma o estándar para la gestión de riesgos de los diferentes activos en el área de TI**

		Frecuencia	Porcentaje
Válido	NO	15	100,0



- **La alta dirección es informada sobre los riesgos a los que se encuentran expuestos los activos de TI**

		Frecuencia	Porcentaje
Válido	NO	15	100,0



ANEXO II: IDENTIFICACIÓN DE NORMAS, MARCOS Y GUÍAS DE GESTIÓN DE RIESGO

NOMBRE	ORGANIZACIÓN	TIPO	DOCUMENTACIÓN	DESCRIPCIÓN	ESTRUCTURA
COBIT RISK	Publicada el 2013 por ISACA	Marco de trabajo	Ofrecer una guía detallada sobre gobierno y gestión de riesgo en la industria de TI	Describe los procesos básicos para la gestión de riesgos, ayudados por los facilitadores de COBIT 5. Tiene el objetivo de crear valor a través de la obtención de beneficios mientras se optimizan los riesgos	APO12: (pg50 y 63) 1. Recolectar datos 2. Análisis de riesgos 3. Mantener un perfil de riesgo 4. Expresar el riesgo 5. Definir un portafolio de opciones para el riesgo 6. Responder al riesgo
CORAS	Publicada en el año 2001 por SINTEF (Grupo de investigación noruego)	Marco para el análisis de riesgos de los sistemas críticos de seguridad	Poca disponibilidad de la información.	Tiene como objetivo proporcionar un marco de trabajo para analizar los riesgos de seguridad, enfocado directamente a las amenazas. Hace uso de las lluvias de ideas de manera estructurada para realizar escenarios de amenazas y riesgos	7 pasos: 1. Presentación 2. Análisis de alto nivel 3. Aprobación 4. Identificación del riesgo 5. Estimación del riesgo 6. Evaluación del riesgo 7. Tratamiento del riesgo.
COSO	Actualizada el 2017	Metodología	Audiovisuales	Facilita a las organizaciones evaluar y mejorar su sistema de control interno. Este estándar está dirigido para fines contables y de auditoría con el objetivo de realizar un control interno para evaluar la ética profesional, gestión de riesgo empresarial e identificar fraudes y la presentación de informes financieros.	5 componentes 1. Ambiente de control 2. Evaluación de riesgos 3. Actividades de control 4. Información y comunicación 5. Supervisión

CRAMM	Desarrollada en 1992 por el Central Communication and Telecommunication Agency (CCTA)	Metodología	No hay mucha información acerca de esta metodología.	CRAMM se puede utilizar para todo tipo de organizaciones para justificar la seguridad, las inversiones relacionadas con contingencias para obtener información y demostrar la necesidad de acción en el nivel gerencial. Es necesario aplicar su herramienta para su utilización.	3 etapas: 1. Identificación y valoración de activos 2. Evaluación de amenazas y vulnerabilidades 3. Selección de contramedidas y recomendaciones
EBIOS	Publicada por la Agencia Nacional de Ciberseguridad de Francia (ANSSI)	Herramienta	Documentación no tan detallada.	Este método sirve para evaluar y tratar los riesgos digitales, además de identificar las medidas de seguridad que se deben tomar para validar nivel aceptable de riesgos. Genera recursos y argumentos útiles para la comunicación y toma de decisiones dentro de la organización.	5 pasos: 1. Alcance y línea de base de seguridad 2. Orígenes de riesgo 3. Strategic scenarios 4. Operational scenarios 5. Tratamiento de riesgos
ISO 31 000	Actualizada en el 2018 , Es una norma publicada por la Organización Internacional de Normalización [ISO] y la Comisión Electrotécnica Internacional [IEC]	Norma o estándar	Documentación detallada	El marco de gestión del riesgo de esta norma proporciona las políticas, los procedimientos y las disposiciones organizativas que integran la gestión de riesgos en toda la organización a todos los niveles. Su propósito es brindar información basada en pruebas y análisis para tomar decisiones sobre cómo seleccionar y determinar el tratamiento de los riesgos.	Fases: 1. Establecer contexto 2. Identificación del riesgo 3. Análisis del riesgo 4. Valoración del riesgo 5. Tratamiento del riesgo 6. Seguir y revisar los controles. 7. Comunicación y consulta 8. Registro del proceso de gestión de riesgos
Magerit	elaborada por el antiguo Consejo Superior de Administración Electrónica	Metodología	Se detalla a través de 3 libros en donde indican el paso a paso.	Tiene como objetivo de implementar un marco común para el análisis y la gestión de riesgos en los sistemas de información, sobre la base de la norma ISO/IEC 27000 MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para	Fase 1: Establecer los criterios de riesgo de Medición F2: Análisis de riesgos 1. Paso 1: Activos 2. Paso 2: Amenazas 3. Paso 3: Determinación del impacto potencial 4. Paso 4: Determinación del riesgo potencial

				tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos. MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información.	5. Paso 5: Salvaguardas 6. Paso 6: Evaluación del riesgo 7. Paso 7: Aceptación del riesgo 8. Paso 8: Tratamiento del riesgo
MEHARI	Desarrollada por las CLUSIF (club de la Securite de l'Information Francais) en el año 1995.	Metodología		Es una metodología utilizada para apoyar a los responsables de la seguridad informática, la cual es un completo de la norma ISO 27000. Tiene como objetivo principal de proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos ISO/IEC 27005:2008. Esta metodología puede ser usada con un método continuo de trabajo o como apoyo a otras prácticas de la gestión de la seguridad.	3 etapas: 1. Análisis o evaluación de riesgos. 2. Evaluación de seguridad 3. Análisis de amenazas
NIST :800:30	Publicada en julio del 2002, la cual fue desarrollada por el National Institute of Standards and Technology [NIST]	Guía	Documentación detallada	Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información, la cual necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito	1. Paso 1: caracterización del sistema 2. Paso 2: identificación de amenazas 3. Paso 3: identificación de vulnerabilidades 4. Paso 4: análisis de controles 5. Paso 5: determinación de la probabilidad 6. Paso 6: análisis del impacto 7. Paso 7: determinación de riesgos 8. Paso 8: recomendaciones de control

OCTAVE	desarrollada por la Universidad Carnegie Mellon en el año 2001	Metodología	Documentación en inglés.	Octave-allegro diseñado para permitir una amplia evaluación de los riesgos operacionales de la organización con el objetivo de entregar resultados más sólidos, esto sin la necesidad de tener un amplio conocimiento análisis de riesgo. Esta metodología se enfoca principalmente en los activos de información, en cómo se almacenan, transportan, procesan y como están expuestos a las amenazas y las vulnerabilidades	1. La primera contempla la evaluación de la organización 2. En la segunda se identifican las vulnerabilidades a nivel de infraestructura de TI. 3. En la última fase de desarrolla un plan y una estrategia de seguridad.
Norma AS/NZS 43605	Fue el primero en salir, ahora exite una tercera versión del 2004, aprobada como estándar (base para la iso 31000)	Norma	Si hay facilidad de documentación.	El objetivo de este estándar es proveer una guía que permita tanto a empresas públicas o privadas como a individuos, grupos o comunidades lograr: Una base más confiable y rigurosa para la toma de decisiones y planificación, mejor identificación de oportunidades y amenazas y generar valor desde la incertidumbre y variabilidad.	5 fases: 1. - Establecer el contexto 2. - Identificar riesgos: 3. - Analizar riesgos 4. - Evaluar riesgos 5. -Tratamiento de riesgos 6. Comunicación 7. Monitoreo

ANEXO III: ANALISIS DETALLADO DE CADA METODOLOGÍA

<table>
<tr><th colspan="3">ISO 31000:2018</th></tr>
<tr><td colspan="3">Definición: La norma establece un número de principios que es necesario cumplir para que la gestión del riesgo sea eficaz, y recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos globales de gobierno, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura de la organización.</td></tr>
<tr><td rowspan="11">Componentes del marco de referencia</td><td colspan="2">Dirección y compromiso</td></tr>
<tr><td rowspan="8">Diseño de marco de referencia para la gestión de riesgo</td><td>Entender a la organización y su contexto</td></tr>
<tr><td>Establecer la política para la gestión de riesgo</td></tr>
<tr><td>Rendición de cuentas</td></tr>
<tr><td>Rendición de cuentas</td></tr>
<tr><td>Integración de los procesos de la organización</td></tr>
<tr><td>Recursos</td></tr>
<tr><td>Establecer mecanismos para la comunicación interna y la presentación de informes</td></tr>
<tr><td>Establecer mecanismos para la comunicación externa y la presentación de informes</td></tr>
<tr><td colspan="2">Implementar la gestión del riesgo</td></tr>
<tr><td colspan="2">Monitorear y revisar el marco de referencia</td></tr>
<tr><td colspan="2">Mejora continua del marco de referencia</td></tr>
<tr><td colspan="3">Proceso de gestión de riesgos</td></tr>
<tr><td rowspan="16">Establecer el contexto</td><td rowspan="5">Definir el alcance: La gestión de riesgo puede aplicarse a niveles distintos (estratégico, operacional de un programa, proyecto u otras actividades).</td><td>Objetivos y las decisiones que se necesitan tomar.</td></tr>
<tr><td>Resultados esperados</td></tr>
<tr><td>Tiempo, ubicación las inclusiones y las exclusiones específicas.</td></tr>
<tr><td>Herramientas y técnicas apropiadas de evaluación de riesgos.</td></tr>
<tr><td>Recursos requeridos , responsabilidades.</td></tr>
<tr><td rowspan="3">Contexto externo: Entorno donde la organización busca conseguir sus objetivos. Se basa de acuerdo a cada tipo de organización (legales o reglamentarios).</td><td>Entorno social, cultural, legal , reglamentario, financiero, tecnológico, económico, natural y competitivo (local, regional, nacional o internacional).</td></tr>
<tr><td>Tendencias que tengan impacto con los objetivos de la organización.</td></tr>
<tr><td>Relaciones con las partes interesadas</td></tr>
<tr><td rowspan="5">Contexto interno: Aquí el proceso de gestión de riesgo se debe limitar a la cultura, procesos , estructura y estratégica de la organización.</td><td>Objetivos de la organización.</td></tr>
<tr><td>Análisis FODA.</td></tr>
<tr><td>Estructura de la organización, funciones y responsabilidades.</td></tr>
<tr><td>Políticas, los objetivos y estrategias.</td></tr>
<tr><td>Normas y directrices adoptados por la organización.</td></tr>
<tr><td rowspan="6">Criterios de riesgo: Se establecen los criterios que se deben aplicar para evaluar la importancia de un riesgo. Pueden estar impuestos de o derivarse de requisitos legales o reglamentarios. (la cantidad</td><td>La naturaleza , y los tipos de las causas y de las consecuencias.</td></tr>
<tr><td>Definición de la probabilidad.</td></tr>
<tr><td>Plazos de la probabilidad y o de las consecuencias.</td></tr>
<tr><td>Determinar el nivel de riesgo.</td></tr>
<tr><td>Opiniones de las partes interesadas.</td></tr>
<tr><td>Nivel de riesgo (aceptable o tolerable)</td></tr>
</table>

	de riesgo que puede o no puede tomar)	
Apreciación del riesgo o evaluación del riesgo	**Identificación del riesgo**: Se identifica el origen del riesgo, las áreas de impacto y los sucesos, causas y sus consecuencias potenciales. Lista de riesgos (crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos).	Origen del riesgo o fuente del riesgo tangible o intangible
		Las causas y los eventos.
		Las amenazas y oportunidades.
		Vulnerabilidades y las capacidades.
		Consecuencias y sus impactos en el objetivo.
		Sesgos y los supuestos y las creencias de las personas involucradas.
	Análisis del riesgo: Comprensión del riesgo, la cual proporciona entradas para su evaluación y así poder tomar decisiones sobre estos. EL análisis puede ser cualitativo, semi - cuantitativo o cuantitativo	Se analiza determinando las consecuencias y probabilidad.
		Se debe tener en cuenta los controles existentes, así como su eficacia y su eficiencia.
		La naturaleza y la magnitud de las consecuencias.
		EL nivel de riesgo se puede evaluar a través de diversos factores (disponibilidad, calidad, la cantidad y la validez de la pertinencia de la información)
	Evaluación del riesgo o valoración del riesgo: Implica comparar el nivel de riesgo obtenido en la etapa de análisis y compararlo con los criterios de riesgos que se han establecidos.	Aquí también se puede llevar la decisión de no tratar el riesgo.
		Las decisiones se deberían de tomar de acuerdo con los requisitos legales reglamentario y requisitos de otro tipo.
		Reconsiderar los objetivos.
		Mantener los controles existentes
Tratamiento de riesgo	**Selección de opciones de tratamiento del riesgo**: La organización debería tener en consideración los valores y las percepciones de las partes interesadas y los medios apropiados para comunicarse con ellas.	Se debe establecer un orden de prioridad en que se van a implementar e identificar con claridad el tratamiento a realizar.
		Para tener la seguridad de que las medidas son eficaces es necesario que se le dé seguimiento al plan de tratamiento del riesgo.
		Pueden surgir riesgos secundarios que se deben tratar en el mismo plan de tratamiento original y no tratarse como riesgos nuevos.
	Preparación e implementación del plan de acción: Se deben de discutir con las partes interesadas apropiadas. Otras de las consideraciones es que las partes interesadas deben estar al tanto del riesgo residual, por ello se debe de documentar. Se documenta de cómo se va a implementar el tratamiento seleccionado:	La razón por que se seleccionó dicho tratamiento.
		El responsable de la aprobación y el responsable de la implementación.
		Acciones propuestas.
		Recursos necesarios, incluye contingencias.
		Medidas del desempeño.
		Requisitos en materia de información y de seguimiento.
		Calendario y la programación
Seguimiento y revisión	Seguimiento de los planes de acciones, debe ser periódica o eventual. EL encargado de del	Asegurar los controles eficaces y eficientes. Analizar y sacar conclusiones de los sucesos (tendencias, éxitos y fallos.)
		Detectar cambios en el contexto interno y externo.

	seguimiento debe estar definido.	identificar riesgos emergentes.
Comunicación y consulta	Busca promover la toma de conciencia y la compresión del riesgo mientras que la consulta implica obtener la retroalimentación e información. Se debe realizar en todas las etapas de los procesos de gestión de riesgos, con las partes interesadas.	Planes de comunicación y consulta: Ayudar que se identifiquen correctamente los riesgos, conseguir la aprobación y el apoyo para un plan de tratamiento.
		Reunir las diferentes áreas de experiencia para cada etapa del proceso de la gestión de riesgos.
		Proporcionar suficiente información para facilitar la supervisión del riesgo.
Registro del proceso de gestión de riesgos	Proporciona la base para la mejora de los procesos de los métodos y de las herramientas, así como del proceso.	Aprendizaje continuo.
		Reutilizar la información.
		Costes y esfuerzos que suponen la creación y mantenimiento de los registros.
		Necesidades legales, reglamentarias y operacionales.
		Método de acceso
General		
Definición de las metas y objetivos de las actividades de gestión del riesgo.		
Definición de las responsabilidades del proceso para la gestión del riesgo y dentro de este.		
Definición del alcance, la profundidad y la extensión de las actividades de gestión del riesgo que se van a llevar a cabo, incluyendo las exclusiones e inclusiones específicas.		
Definición de la actividad, proceso, función, proyecto, producto, servicio o activo en términos de tiempo y ubicación.		
Definición de las relaciones entre el proyecto, el proceso o la actividad particulares y otros proyectos, procesos o actividades de la organización.		
Definición de las metodologías para la valorización del riesgo		
Identificación y especificación de las decisiones que se deben tomar.		
Identificación, establecimiento del alcance o marco de los estudios necesarios, su extensión y objetivos, y los recursos necesarios para tales estudios		

NTP -ISO 27005:2018		
Establecer el contexto Establecimiento del contexto	Se debe establecer el contexto interno y externo para la gestión de riesgo de la seguridad de la información, establecer los criterios básicos , definir el alcance y los límites y establecer una organización apropiada que opere la gestión de riesgos.	
	Alcance y límites: Es importante definir el alcance para asegurar que todos los activos relevantes son tomados en cuenta en la evaluación del riesgo.	Los objetivos estratégicos del negocio.
		Procesos del negocio.
		Las funciones y estructura de la organización.
		Políticas de seguridad de la información.
		Los activos de información.
		Ubicaciones físicas de la organización y sus características.
		Las expectativas de las partes interesadas.
		Entorno socio cultural
	Organización para la gestión de riesgos de seguridad de la información: Se define los roles y las responsabilidades	Desarrollo del proceso de GRS.
		Identificación y análisis de las partes interesadas.
		Definición de roles y responsabilidades de todas las partes.
		Definición de rutas de escalamiento.
		Especificación de los registros que se guardarán.

	principales de la organización:	
Establecer los criterios básicos	Aquí se enfoca en los criterios de valoración de los riesgos, criterios de evaluación del impacto y criterios de aceptación del riesgo. -Realizar la evaluación del riesgo y establecer un plan de tratamiento de riesgos. -Definir e implementar políticas y procedimientos, incluyendo la implementación de los controles.	
	Criterio de valoración del riesgo: es para evaluar el riesgo de seguridad en la organización.	Valor estratégico del proceso.
		Criticidad de los activos
		Importancia operacional (disponibilidad, confidencialidad y de integridad)
		Expectativas y percepciones de las partes interesadas.
	Criterios de impacto: Se determina el daño o costos para la organización causados por un evento de seguridad de la información.	Nivel de clasificación del activo.
		Brechas de seguridad.
		Operaciones deterioradas.
		Pérdida de negocios.
		Alteración de planes.
		Daños a la reputación
	Criterios de aceptación del riesgo: La organización debe definir sus propias escalas para los niveles de aceptación del riesgo:	Puede incluir múltiples umbrales.
		Pueden aplicarse a diferentes clases de riesgo.
		Pueden incluir requisitos para un tratamiento adicional futuro.
		Pueden variar en el tiempo (criterios del negocio, operaciones, tecnología, finanzas y factores sociales)
Identificación de riesgo	Aquí se determina qué podría suceder para causar pérdidas en la organización. Se conoce (cómo cuándo y por qué) la pérdida podría suceder.	
	Identificación de activos: Aquello que tiene valor para la organización y por lo tanto requiere protección (hardware y software).	Se debe identificar el propietario de cada activo, para ver quién es el responsable la cual tiene responsabilidad (producción, desarrollo, mantenimiento, uso y seguridad) además de ubicación, y función.
		Debe detener un nivel adecuado de detalle la cual provea información suficiente.
	Identificación de amenazas: Amenaza para dañar los activos (información, procesos y sistemas)	Las amenazas pueden suceder dentro o fuera de la organización.
		Se deben identificar por (acciones no autorizadas, daños físicos, fallos técnicos)
		Una amenaza puede afectar a varios activos, generando diferentes impactos.
	Identificación de controles existentes: Se requiere para evitar trabajo o costos innecesarios ejemplos (duplicar controles)	Un control existente o planificado puede ser inefectivo, insuficiente o no justificado.
		Se debe revisar documento, conteniendo información de los controles.
		Verificar con las personas responsables de la seguridad.
		Realizar una revisión de sitio.
		Revisar los resultados de auditorías.
	Identificación de vulnerabilidades: La presencia de una vulnerabilidad no causa daño en sí misma, ya que es necesario que haya una amenaza presente para explotarla. Se pueden identificar vulnerabilidades en: Organización, procesos y procedimientos, rutinas de gestión, personal, entorno físico, configuración de sistemas de información, hardware, software o equipos de comunicación.	
	Identificación de consecuencias: Se identifica los daños o consecuencias que podrían afectar a la organización pueden ser (pérdida de eficacia, condiciones adversas de funcionamiento, pérdida del negocio, reputación, daño , entre otro.)	

<table>
<tr><td rowspan="9">Análisis de riesgo</td><td colspan="2">El análisis del riesgo puede llevarse a cabo con diversos grados de detalle en función de la criticidad de los activos, el alcance de las vulnerabilidades conocidas, y los incidentes anteriores</td></tr>
<tr><td rowspan="2">Análisis del riesgo:</td><td>Cualitativo: describir magnitud de las consecuencias (baja, media, alta) y la probabilidad de que esa consecuencia puede ocurrir.</td></tr>
<tr><td>Cuantitativo: Utiliza escala numérica, tanto para la consecuencia como para la probabilidad.</td></tr>
<tr><td rowspan="3">Evaluación de consecuencias: El valor del impacto puede ser expresado en forma cualitativa y cuantitativa.</td><td>Las consecuencias en el negocio por la pérdida, así como las o compromiso del activo, potenciales consecuencias adversas al negocio y/o consecuencias legales o reglamentarias por la divulgación, modificación, indisponibilidad y/o destrucción de información, y otros activos de información</td></tr>
<tr><td>Las consecuencias pueden ser expresadas en términos monetarios, técnicos o criterios de impacto humano, u otros criterios.</td></tr>
<tr><td>Las consecuencias en el tiempo y las finanzas deberían ser medidas con el mismo enfoque utilizado en la probabilidad de amenazas y vulnerabilidades.</td></tr>
<tr><td rowspan="4">Evaluación de probabilidad de incidentes: Es necesario evaluar la probabilidad de ocurrencia de cada escenario y el impacto que produzca utilizando las técnicas de análisis cualitativo o cuantitativo.</td><td>fuentes deliberadas de amenaza: motivación y capacidades.</td></tr>
<tr><td>Fuentes accidentales de amenaza (factores geográficos).</td></tr>
<tr><td>Vulnerabilidades, tanto sumadas como individuales.</td></tr>
<tr><td>Controles existentes.</td></tr>
<tr><td colspan="2">Determinar el nivel del riesgo: Asigna valores de probabilidad y las consecuencias de un riesgo. Esos valores pueden ser cuantitativos o cualitativos.</td></tr>
<tr><td rowspan="2">Valorar el riesgo</td><td rowspan="2">Se utiliza los criterios de valoración de riesgos que van hacer utilizados para tomar decisiones.</td><td>Importancia del proceso de negocio o actividad soportada por un activo particular.</td></tr>
<tr><td>Propiedad de la seguridad de la información: Si un criterio no es relevante para la organización (ya se confidencialidad, integridad, etc.)</td></tr>
<tr><td rowspan="5">Tratamiento de riesgo</td><td colspan="2">Las opciones de tratamiento deberían ser seleccionadas basándose en el resultado de la evaluación de riesgo. Algunos tratamientos pueden apuntar a más de un riesgo.</td></tr>
<tr><td>Modificación del riesgo</td><td>Modificación del riesgo: (restricciones de tiempo financiero, técnicas y operacionales, culturales, éticas, del entorno)</td></tr>
<tr><td>Retención del riesgo</td><td>Esta dentro del criterio de aceptación de riesgos, no hay necesidad de implementar controles.</td></tr>
<tr><td>Evitar el riesgo</td><td>Los riesgos son muy altos, o los costos de implementar un tratamiento exceden a los beneficios.</td></tr>
<tr><td>Compartir el riesgo</td><td>Compartir ciertos riesgos con las partes externas. Esto puede crear nuevos riesgos o modificar los riesgos existentes, por lo tanto, requiere un tratamiento adicional</td></tr>
<tr><td>Aceptación de riesgo de seguridad de la información</td><td colspan="2">Los planes de tratamiento del riesgo deberían describir cómo se evaluaron los riesgos y se van a tratar de cumplir los criterios de aceptación del riesgo</td></tr>
<tr><td>Comunicación y consulta</td><td colspan="2">La comunicación eficaz entre los interesados es importante, ya que esto puede tener un impacto significativo sobre las decisiones que deben tomarse. La comunicación se asegurará que los responsables de la aplicación de gestión de riesgo</td></tr>
</table>

Seguimiento y revisión del riesgo de seguridad de la información	**Seguimiento y revisión de los factores de riesgos**: Los riesgos no son estáticos. Las amenazas, vulnerabilidades, probabilidades o consecuencias pueden cambiar bruscamente sin ningún tipo de indicación. Por lo tanto, el constante seguimiento	Nuevos activos.
		Modificaciones necesarias del valor de los activos.
		Nuevas amenazas.
		Posibilidad de nuevas vulnerabilidades o en aumento.
		Aumento de impacto o consecuencias.
		Información sobre incidentes de seguridad.
	Seguimiento, revisión y mejora de la gestión de riesgos: El seguimiento permanente y la revisión son necesarios para garantizar que el contexto, los resultados de la evaluación de los riesgos y tratamiento, así como los planes de gestión, siguen siendo relevantes y adecuados a las circunstancias.	

COBIT FOR RISK		
General	Partes interesadas	Pueden ser internas o externas a la empresa. Incluyen al consejo directivo, la gerencia ejecutiva, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores de servicios, clientes y reguladores
	Metas y métricas	Los principios, políticas y marcos de referencia son instrumentos para comunicar las reglas de la empresa, en apoyo de los objetivos de gobierno y los valores de la empresa
Flujo de trabajo en el desarrollo de escenarios de riesgo	Flujo de trabajo en el desarrollo de escenarios de riesgo	Utilizar la lista de ejemplos de escenarios de riesgo genéricos (ver figura 38 del capítulo 3) para definir un conjunto manejable de los escenarios de riesgo a la medida de la empresa.
		Afinar los escenarios seleccionados sobre la base de la validación anterior, detallándolos a un nivel acorde con la criticidad de la entidad.
Factores de riesgo	**Contexto externo:**	Factores económicos y de mercado
		Tasa de cambio del mercado
		Industria y competencia
		Situación geopolítica
		Ambiente regulatorio
		Estado de la tecnología y su evolución
		Panorama de amenazas
	Contexto interno:	Metas y objetivos de la empresa ¿Cuáles son las necesidades de las partes interesadas y cómo podrían verse impactadas por los riesgos?
		Importancia estratégica de TI para la empresa ¿TI es un diferenciador estratégico, un habilitador funcional o una función de soporte?
		Complejidad de TI ¿TI es altamente compleja (es decir, de arquitectura compleja, fusiones recientes) o TI es simple, estandarizada y efectivamente integrada?
		Modelo operativo El grado en que la empresa opera de manera independiente o está vinculada con sus

		clientes/proveedores, el grado de centralización/descentralización.
		Cultura de la empresa ¿La cultura existente en la empresa requiere cambiar para poder enfrentar de manera efectiva la gestión de riesgos?
		Capacidad financiera La capacidad de la empresa para proporcionar apoyo financiero para mejorar y mantener el ambiente de TI, en tanto optimiza el riesgo.
	Capacidades de gestión de riesgos	Gobierno del riesgo
		Gestión del riesgo
	Capacidades Relacionadas con TI	Evaluar, Dirigir Y Supervisar (EDM)
		Alinear, Planificar Y Organizar (APO)
		Construir, Adquirir E Implementar (BAI)
		Entregar, Dar Servicio Y Soporte (DSS)
		Supervisar, Evaluar Y Valorar (MEA)
Estructura de escenarios de riesgo	Actor	Interno (empleados, contratistas)
		Externo (competidores, desconocidos, socios, regulador, mercado)
	Tipo de amenazas	Maliciosa
		Accidental
		Error
		Falla
		Naturaleza
		Requerimiento externo
	Evento	Revelación
		Interrupción
		Modificación
		Robo
		Destrucción
		Diseño inefectivo
		Ejecución inefectiva
		Reglas y regulaciones
		Uso inapropiado
	Activo/Recurso	Personas y habilidades
		Estructuras organizativas
		Procesos
		Infraestructura
		Información
		Aplicaciones
	Tiempo	Duración
		Momento que ocurre el riesgo
		Detección
		Tiempo transcurrido

OCTAVE
Definición: El enfoque OCTAVE Allegro consta de ocho pasos que se organizan en cuatro fases, como se ilustra en la Figura 2. En la fase 1, la organización desarrolla criterios de medición del riesgo consistentes con los conductores de organización. Durante la segunda fase, los activos de información que están determinados a ser críticos están perfiladas. Este proceso de perfilado establece límites claros para el activo, identifica sus requisitos de seguridad, e identifica todos los lugares donde se almacena el activo, transportado producto. En la fase 3, las amenazas al activo de información se identifican en el contexto de los lugares donde se almacena el activo, transportarse, o producto. En la fase final, los riesgos

para se identifican y analizan los activos de información y el desarrollo de enfoques de mitigación se haya comenzado.		
Establecer los criterios de riesgo de Medición	**Criterios de medida de riesgo**	Confianza Reputación / cliente
		Financiera
		Productividad
		Seguridad y la salud
		Multas / sanciones legales
		Definido por el usuario área de impacto
	Priorización de las Áreas de Impacto	Dar prioridad a las áreas de impacto de más importante a menos importante.
Desarrollo de los Perfiles de Activo de Información	Su objetivo es ayudar a una organización: - identificar los activos que son importantes para la misión de la organización - identificar las vulnerabilidades y amenazas a esos activos	
	Identificar el activo: La primera actividad en esta etapa de la evaluación de riesgos implica la identificación de un conjunto de activos de información en la que podría llevarse a cabo una evaluación.	
	Valorar el activo: Se debe realizar la evaluación de riesgos estructurado únicamente en aquellos activos que son críticos para el logro de metas y el logro de la misión de la organización, así como aquellos que son importantes debido a factores tales como el cumplimiento de la normativa. (CONFIABILIDAD, DISPONIBILIDAD E INTEGRIDAD)	
	Evaluar el activo: Recopilar información acerca de su activo de información que es necesaria para iniciar el proceso de evaluación de riesgos estructurado. (para registrar esta información.)	
	Perfil del activo	Perfil crítica Información de recursos. (¿Por qué es este activo fundamental para la organización?, Es esta información de los activos sujetos a requisitos reglamentarios?)
		Registre una descripción para el activo crítico
		Identificar y documentar los propietarios de los activos de información crítica
		Registrar los requisitos de seguridad de la confidencialidad, integridad y disponibilidad
		Identifica el más importante requisito de seguridad
Identificación de los Contenedores de los Activos	Repositorio donde se almacena la información	Identificación de contenedor técnico
		Identificación de contenedor físico
		Identificación de contenedor personas
Identificación de las Áreas de Preocupación	Situaciones donde se puede afectar un activo de la información	Establecer las Áreas de Preocupación
		Documentar las Áreas de Preocupación
Identificación de Escenarios de Amenaza	Relacionado con los activos críticos que no han sido identificado en el área de preocupación.	Actividad 1: Identificar los escenarios de amenazas adicionales
		Actividad 2: Selección de las respuestas de los cuestionarios de escenario de amenaza
		Actividad 3: Probabilidad
Sexto Paso: Identificación de Riesgos	Se analiza el impacto a la organización de manera detallada.	Actividad 1: Registrar consecuencias de las amenazas Amenaza (condición) + Impacto (consecuencia) = Riesgo [Pasos 4 y 5] + [Paso 6] = Riesgo
Séptimo Paso: Análisis de Riesgos	Mide de forma cualitativa el grado en que afecta a la organización.	Actividad 1: Revisar criterios de medida de riesgo (valores) y las consecuencias
		Actividad 2: Calcular el puntaje de riesgo relativo
Octavo Paso: Selección de		Mitigar
		Mitigar o transferir

enfoque de mitigación	Opciones de tratamiento para los riesgos identificados.	Transferir o aceptar
		Aceptar

MAGERIT		
Definición: Es un método formal que sirve para investigar los riesgos que soportan los sistemas de información existentes en cada una de las organizaciones para recomendar las medidas apropiadas que deben de adoptar las organizaciones.		
Determinar el contexto	Determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos.	
ANALISIS DE RIESGOS	**Activos** (En un sistema de información hay 2 cosas esenciales:)	Datos que materializan la información.
		Servicios auxiliares que se necesitan para poder organizar el sistema.
		Las aplicaciones informáticas (software) que permiten manejar los datos.
		Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
		Los soportes de información que son dispositivos de almacenamiento de datos.
		El equipamiento auxiliar que complementa el material informático.
		Las redes de comunicaciones que permiten intercambiar datos.
		Las instalaciones que acogen equipos informáticos y de comunicaciones.
		Las personas que explotan u operan todos los elementos anteriormente citados.
	Dependencias (Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.)	Activos esenciales (información que se maneja, servicios prestados)
		Servicios internos (que estructuran ordenadamente el sistema de información)
		El equipamiento informático (aplicaciones (software) , equipos informáticos (hardware), comunicaciones, soportes de información: discos, cintas, etc.)
		El entorno: activos que se precisan para garantizar las siguientes capas (equipamiento y suministros: energía, climatización, etc., mobiliario
		Los servicios subcontratados a terceros
		Las instalaciones físicas
		El personal • usuarios
		Operadores y administradores
	Valoración ¿Por qué interesa un activo? Por lo que vale. No se está hablando de lo que cuestan las cosas, sino de lo que valen.	**confidencialidad**: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
		integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial-mente falsos o, incluso, faltar datos.
		d**isponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.
AMENZAS	**Identificación de las amenazas**	De origen natural Hay accidentes naturales (terremotos, inundaciones, ...).

		Del entorno (de origen industrial) Hay desastres industriales (contaminación, fallos eléctricos, ...)
		Defectos de las aplicaciones Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'13.
		Causadas por las personas de forma accidental Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
	Valoración de las amenazas (Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.)	degradación: cuán perjudicado resultaría el [valor del] activo
		probabilidad: cuán probable o improbable es que se materialice la amenaza
Determinación del impacto potencial	Impacto acumulado	El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.
		El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.
		El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.
		El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.
	Impacto repercutido	El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.
		El impacto es tanto mayor cuanto mayor es el valor propio de un activo.
		El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.
		El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.
Determinación del riesgo potencial	Riesgo acumulado	el impacto acumulado sobre un activo debido a una amenaza y la probabilidad de la amenaza
	Riesgo repercutido	el impacto repercutido sobre un activo debido a una amenaza y la probabilidad de la amenaza (Riesgo = valor del activo*vulnerabilidad * impacto)
Salvaguardas	Tipos	[PR] prevención
		[DR] disuasión
		[EL] eliminación
		[IM] minimización del impacto / limitación del impacto
		[CR] corrección
		[RC] recuperación
		[MN] monitorización
		[DC] detección
		[AW] concienciación

		[AD] administración

Norma AS/NZS 43605		
Definición: Esta norma es un estándar australiano-neozelandés que provee una guía genérica para el establecimiento e implementación del proceso de administración de los riesgos, involucrando la implementación de los contextos y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.		
Establecer el Contexto	Establecer el contexto estratégico	a) Definiendo la relación entre la organización y su entorno, identificando sus FODA. Este contexto incluye los aspectos financieros, operativos, competitivos, políticos, percepciones públicas/imagen–, sociales, de clientes, culturales y legales de las funciones de la organización
		b) Identificando los interesados internos y externos
	Establecer el contexto organizacional	a) La administración de los riesgos tiene lugar en el contexto de las amplias metas, objetivos y estrategias de la organización
		b) La falla en lograr sus objetivos, o de una actividad específica, o de un proyecto en consideración, es un conjunto de riesgos que debe ser administrado.
		c) La política y las metas de la organización ayudan a definir los criterios mediante los cuales se decide si un riesgo es aceptable o no y constituye la base para las opciones del tratamiento de los riesgos.
	Establecer el contexto de administración de los riesgos	a) Definir el proyecto o actividad y establecer sus metas y objetivos.
		b) Definir la extensión del proyecto en tiempo y ubicación.
		c) Identificar cualquier estudio necesario y su alcance, objetivos y recursos requeridos; las fuentes genéricas de riesgo y las áreas de impacto pueden proveer una guía para ello.
		d) Definir el alcance y amplitud de las actividades de administración de los riesgos que se van a llevar a cabo.
	Definir la estructura: Separando la actividad o proyecto en un conjunto de elementos que provea una estructura lógica para la identificación y el análisis que ayuda a asegurar que no se pasen por alto riesgos significativos.	
Identificación del Riesgo	¿Qué puede suceder?	Generar una lista amplia de eventos que pueden afectar a cada elemento de la estructura; estos son luego considerados en mayor detalle para identificar lo que puede suceder.
	¿Cómo y por qué pueden suceder?	Habiendo identificado una lista de eventos, es necesario considerar causas y escenarios posibles.
	Herramientas y técnicas	checklists, juicios basados en la experiencia y en los registros, diagramas de flujo
		brainstorming, análisis de sistemas y de escenarios y técnicas de ingeniería de sistemas.
Análisis de Riesgos	**Determinar los controles existentes:** Identificar la administración, los sistemas técnicos y los procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades.	
	Consecuencias y probabilidades	a) Registros anteriores
		b) Experiencia relevante

		c) Prácticas y experiencia de la industria
		d) Literatura relevante publicada
		e) Comprobaciones de marketing e investigaciones de mercado
		f) Experimentos y prototipos
		g) Modelos económicos, de ingeniería u otros
		h) Opiniones y juicios de especialistas y expertos
	Tipos de análisis	Análisis cualitativo: Utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad
		Análisis semi-cuantitativo: El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo
		Análisis cuantitativo: La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.
Evaluación De Riesgo	Evaluación de los riesgos	Comparar el nivel de riesgo detectado durante el proceso de análisis con los criterios de riesgo establecidos previamente.
Tratamiento Del Riesgo	Reducir probabilidad	Reducir consecuencia
	Transferir	Evitar

NIST 800:30		
Caracterización del sistema	La identificación de riesgos para un sistema de TI requiere un profundo conocimiento del entorno de procesamiento del sistema. La persona o personas que llevan a cabo la evaluación del riesgo deben de información relacionada con el sistema	Hardware
		Software
		Acoplamientos del sistema (por ejemplo, la conectividad interna y externa)
		Datos e información •Las personas que apoyan y utilizan el sistema informático • misión del sistema (por ejemplo, los procesos realizados por el sistema IT)
		Sistema y criticidad de datos (por ejemplo, el valor del sistema o la importancia de una organización)
		Sistema y los datos de sensibilidad.
Identificación de amenazas	Historial de ataque del sistema	Naturales: Inundaciones, terremotos, tornados, deslaves, avalanchas, tormentas eléctricas y otros eventos
		Humanas: Eventos que son habilitados por o causados por seres humanos como: actos no intencionales (ingreso de datos inadvertida) o acciones deliberadas (ataques basados en red, software malicioso, acceso no autorizado a información confidencial)
	Información de agencias de inteligencia, organizaciones y medios	Ambientales: Fallas de energía de larga duración, contaminación, química y fuga de fluidos

ANEXO IV ARMONIZACIÓN DE ESTANDARES

FASE	ACTIVIDADES		SE OBTUVO DE:
ESTABLECER EL CONTEXTO INTERNO, EXTERNO Y CRITERIOS	Establecer el alcance		ISO 31000:2018 (objetivos, tipo) AS/NZS 43605 (establece el contexto de la administración de riesgo como metas, objetivos para llevar a cabo la implementación o sea su alcance)
	Establecer el contexto	Establecer el contexto externo	ISO 31000:2018 (social, cultural, legal, tecnológico, competitivo)
		Establecer el contexto interno	ISO 31000:2018 (Objetivos, estructura)
	Establecer criterios	Establecer criterios de valoración de activos (criticidad)	OCTAVE (Establece 3 indicadores para valorar a un activo, además de mencionar que solo se debe de valorar a los activos críticos) MAGERIT (También establece 3 indicadores y como establecer la escala de cada uno de estos)
		Establecer criterios de evaluación de riesgos	ISO 31000:2018 (Te da la definición de por qué son importante los criterios de valoración y aceptación)
		Establecer criterios de aceptación de riesgos	NTP 27005:2018 (Indica que indicadores tomar para establecer los criterios de impacto y aceptación y la opción de determinar el nivel del riesgo)
ANÁLISIS ESTRATÉGICO	Identificar activos	Identificar los procesos de las I.E	NTP 27005:2018 (Indica que se debe identificar los procesos, pero no como se puede identificar)
		Identificar los activos de TI	OCTAVE (Establece que los activos debes estar perfilados según un tipo de perfil) MAGERIT (Aquí se identificaron los perfiles a utilizar SERVICIOS, SOFTWARE Y SOPORTE

			DE TI, además de tener en cuenta sin son propios o no) NTP 27005:2018 (Menciona que se debe identificar a los propietarios de cada activo)
		Valorar los activos de TI	MAGERIT (También establece 3 indicadores y como establecer la escala de cada uno de estos)
VALORACIÓN DEL RIESGO	Identificar riesgos	Lista de amenazas	NTP 27005:2018 (Establece una lista clasificada de tipo de amenazas)
		Escenarios de riesgos de los activos	ISO 31000:2018 (te indica que tener en cuenta para identificar los riesgos) COBIT 5 (Te da una estructura para plasmar escenarios tomando en cuenta actores, tipo de amenaza, evento, recursos y tiempo)
		Listado de riesgos identificados	
	Análisis	Análisis de riesgos	NTP 27005:2018 (se debe evaluar según a los criterios establecidos y así ver el impacto) OCTAVE (Establece que se debe analizar evaluando la probabilidad + impacto=Riesgo)
	Evaluación	Posicionar el riesgo	AS/NZS 43605 (Establece que se debe comparar el nivel del riesgo detectado con el criterio)
		Valoración del riesgo	
TRATAMIENTO DE RIESGOS	Identificación de tratamiento del riesgo		OCTAVE (Establece tipos de tratamiento Mitigar, Mitigar o transferir, Transferir o aceptar y aceptar)
	Establecer planes de acción		ISO 31000:2018 (te indica que se debe tomar en cuenta para establecer el tratamiento.)
SEGUIMIENTO Y SUPERVISIÓN	Listado de planes de acción		ISO 31000:2018 (Menciona que se debe dar seguimiento para ver si los controles son eficientes)
	Revisión de los planes de acción		
COMUNICACIÓN Y CONSULTA	Comunicación y consulta		ISO 31000:2018

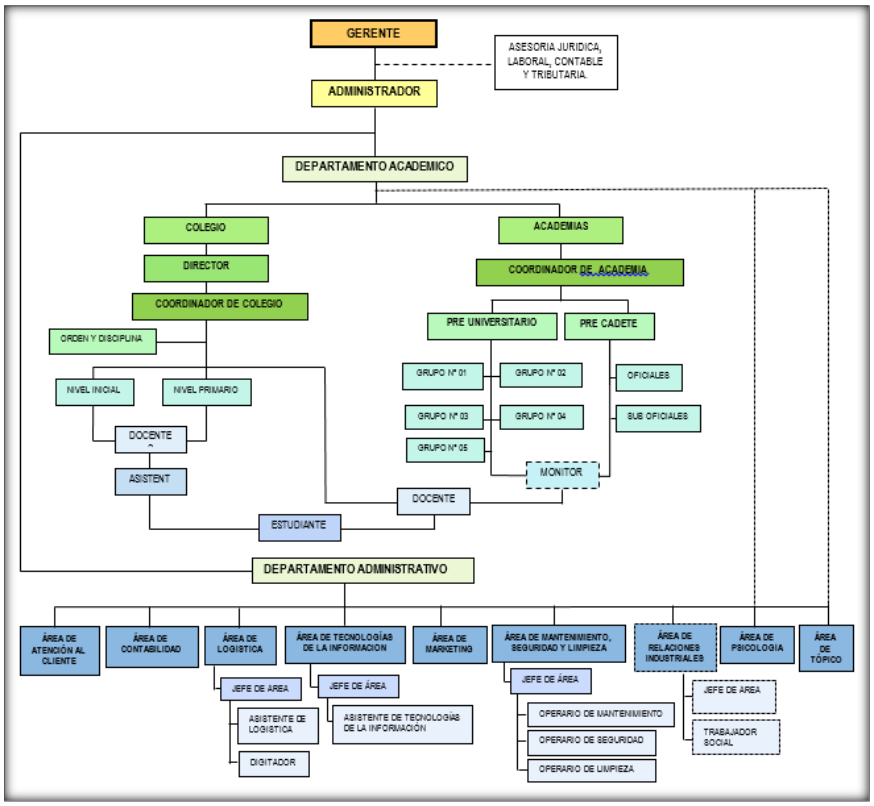
ANEXO V: IMPLEMENTACIÓN DE LA PROPUESTA

LOGO	ESTABLECER EL CONTEXTO EXTERNO					
	Fase:	1	**Proceso**	1	**Actividad**	-
	Código:	**GR001**		**Páginas:**		1/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

N°	CONTEXTO	FUENTE	DETALLE
1	**Socio-Cultural**	Datos censales	Personas que se encuentre en los niveles socioeconómicos A,B,C
2	**Entes regulatorios**	MINEDU, SUNAT, INDECOPI, INDECI	-Nuevas normas que controlan en sector educativo peruano. - Falta documentación relevante de la institución.
3	**Competitivo**	Análisis FODA	Instituciones educativas externas. - Utilizan aplicaciones móviles. - Cuentan con portales web. - Trasmisiones en vivo. - Documentos de evaluaciones y resultados en línea.
4	**Proveedores**	Lista de proveedores	-Play Store -Punto pe (Servicio de dominio) -Colegio de contadores (software) -Tayloit
5	**Tecnológico**	Revista o foros de tecnología.	Oportunidad: - Herramientas de Google. - GSuite Educación. - Fibra óptica. - Servidor proxi. - Firewall. Amenaza: - Cambios tecnológicos que influyen en estrategias (cloud computing). - Ataques cibernéticos (robo de datos institucionales) - Cultura de usuario. - Rastreo por cookies mediante R.S.

LOGO	ESTABLECER EL CONTEXTO INTERNO					
	Fase:	1	**Proceso**	2	**Actividad**	-
	Código:	**GR002**		**Páginas:**		1/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

N°	CONTEXTO	FUENTE	DETALLE
1	**Estructura organizacional:**	Organigrama de la institución educativa.	Plasmar el organigrama institucional.
2	**Objetivos organizacionales**	Plan estratégico.	- Brindar un buen servicio. - Infraestructura física. - Cumplir la visión y misión propuesta. - Nivel académico.
4	**Partes interesadas:**	Plan estratégico, Misión, Visión.	-Personal docente -Padres de familia -Alumnos. -MINEDU
5	**Recursos:**	Inventario de activos.	-Recursos humanos -Recursos tecnológicos (hardware y software)



LOGO	ESTABLECER CRITERIOS DE VALORACIÓN					
	Fase:	1	**Proceso**	2	**Actividad**	-
	Código:	**GR003**		**Páginas:**		1/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: A continuación, se presenta un ejemplo de cómo podemos llenar los siguientes criterios de valoración, la cual servirá para evaluar los activos de TI. Se debe tomar en cuenta que el valor va (1 al 5) siendo el 1 el valor más bajo y 5 el valor más crítico.

VALOR	CONFIDENCIALIDAD
1 (Muy bajo)	La información es pública.
2 (Bajo)	La información es de uso interno de la institución.
3 (Medio)	La información es confidencial y solo el personal de algunas áreas pueden acceder a ella
4 (Alto)	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5 (Muy alto)	La información es solo accedida por el personal de alto rango o con permisos a ella

VALOR	DISPONIBILIDAD
1 (Muy bajo)	El funcionamiento es normal en las actividades
2 (Bajo)	Disponible al 10% del tiempo.
3 (Medio)	Disponible al 30% del tiempo.
4 (Alto)	Disponible al 60% del tiempo.
5 (Muy alto)	Disponible al 90% del tiempo.

VALOR	INTEGRIDAD
1 (Muy bajo)	Se tolera pérdida o alteración de sus componentes en un 80% - 100%
2 (Bajo)	Se tolera pérdida o alteración de sus componentes en un 60% - 79%
3 (Medio)	Se tolera pérdida o alteración de sus componentes en un 40% - 59%
4 (Alto)	Se tolera pérdida o alteración de sus componentes en un 20% - 39%
5 (Muy alto)	Se tolera pérdida o alteración de sus componentes en un 0% - 19%

LOGO	CRITERIÓS DE EVALAUCIÓN DE RIESGOS					
	Fase:	1	**Proceso**	3	**Actividad**	1
	Código:	**GR004**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

PROBABILIDAD		
CATEGORIA	**ESCALA**	**PROBABILIDAD**
MUY ALTO	**5**	Ocurre al menos 1 vez a la semana .
ALTO	**4**	Puede ocurrir 1 vez al mes.
MODERADO	**3**	Puede ocurrir 1 vez cada 6 meses.
BAJO	**2**	Puede ocurrir 1 vez al año.
MUY BAJO	**1**	Puede ocurrir una vez cada 4 años

IMPACTO				
CATEGORIA	**ESCALA**	**PROBABILIDAD**		
		Interrupción del servicio	**Pérdida del activo**	**Interrupción laboral**
MUY ALTO	**5**	Mayor que un mes	Pérdida total	De una semana a más
ALTO	**4**	De una semana a un mes	Muy gran impacto	No mayor a 1 semana
MODERADO	**3**	De un día a una semana	Gran impacto	No mayor a 1 día
BAJO	**2**	3 horas a 1 día	Impacto menor	No mayor a 4 horas
MUY BAJO	**1**	Máximo 3 horas	Casi sin impacto	No hay interrupción

Análisis de los resultados de la probabilidad y el impacto para determinar el nivel del riesgo:

NIVEL	PXI	CATEGORÍA
1	[1-2]	Muy bajo
2	[3-4]	Bajo
3	[5-10]	Moderado
4	[11-15]	Alto
5	[16-25]	Muy alto

LOGO	CRITERIÓS DE ACEPTACIÓN DE RIESGOS					
	Fase:	1	**Proceso**	3	**Actividad**	2
	Código:	**GR005**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Matriz de probabilidad por impacto

IMPACTO						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		PROBABILIDAD				

Nivel de aceptación de riesgos, la institución educativa básica regular debe establecer el nivel de impacto y el nivel de probabilidad que está dispuesta asumir, y así establecer su tabla de aceptación de los riesgos como se muestra:

NIVEL	RANGO	CATEGORÍA
1	[1-4]	Aceptable
2	[5-9]	Tolerable
3	[10-25]	Intolerable

LOGO	IDENTIFICACIÓN DE ÁREA DE LA I.E.P					
	Fase:	II	**Proceso**	1	**Actividad**	-
	Código:	**GR006**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Indicaciones: El encargado tendrá que marcar (SI) si cuentan el proceso o (NO) si no cuentan con dichos procesos.

RESPONSABLE		Johnny Guevara		
N°	**LISTADO DE ÁREAS**	**RPTA**		**PERSONA A CARGO**
		SI	**NO**	
1	Área Académica	***x***		Noelia Arroyo
2	Área atención al cliente	***x***		María Oballe
3	Área de contabilidad	***x***		Yameliss Cruzalegui
4	Área de logística	***x***		Angel Sosa
5	Área de sistemas	***x***		Johnny Guevara
6	Área de marketing	***x***		Milagros Chavez
7	Área de psicología	***x***		Karol Dávila
8	Área de enfermería o tópico	***x***		Greisy Arroyo
Áreas adicionales				
9	Área de relaciones industriales	***x***		Yameliss Cruzalegui

LOGO	IDENTIFICACIÓN DE PROCESOS					
	Fase:	II	**Proceso**	1	**Actividad**	-
	Código:	**GR005**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ÁREA	Atención al cliente	**RESPONSABLE**	**MARIA OBALLE**

N°	**TIPO DE PROCESO**	**RPTA**		**OBSERVACION**
		SI	**NO**	
1	**ESTRATÉGICOS (PE)**			
	PE01. Gestionar la planificación	**x**		
	PE02. Gestionar las relaciones interinstitucionales		**x**	Encargada el director académico
	PE03. Gestionar el sistema de control interno		**x**	
	PE04. Gestionar el desarrollo e innovación	**x**		
	PE05. Marketing educativo	**x**		
	PE06. Análisis de las partes interesadas.		**x**	
2	**OPERATIVOS (PO)**			
	PO01. Gestionar el servicio educativo	**x**		
	PO02.Gestionar los recursos para los aprendizajes.	**x**		
	PO03. Gestionar el desarrollo del personal de servicio en las instituciones educativa	**x**		
	PO04. Gestionar la infraestructura educativa	**x**		
3	**SOPORTE (PS)**			
	PS01. Gestionar Recursos Humanos	**x**		
	PS02. Administrar los recursos financieros	**x**		
	PS03. Administrar sistema logístico.	**x**		
	PS03. Administrar los sistemas y TIC	**x**		
	PS03. Atender asuntos jurídicos legales		**x**	

Procesos adicionales

Proceso de admisión. (PE)

Proceso de atención al cliente (PO)

Proceso de matrícula (PO)

LOGO	IDENTIFICACIÓN DE PROCESOS					
	Fase:	II	**Proceso**	2	**Actividad**	-
	Código:	**GR005**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ÁREA	**T.I**	**RESPONSABLE**	**JHONY AGAPITO**

N°	**TIPO DE PROCESO**	**RPTA**		**OBSERVACION**
		SI	**NO**	
1	**ESTRATÉGICOS (PE)**			
	PE01. Gestionar la planificación	**x**		
	PE02. Gestionar las relaciones interinstitucionales		**x**	
	PE03. Gestionar el sistema de control interno		**x**	No hay un proceso en sí, solo se supervisa que estén cumpliendo con sus labores.
	PE04. Gestionar el desarrollo e innovación	**x**		Haciendo uso de nuevas tecnologías, automatizando muchas actividades dentro de la organización.
	PE05. Marketing educativo	**x**		
	PE06. Análisis de las partes interesadas.		**x**	
2	**OPERATIVOS (PO)**			
	PO01. Gestionar el servicio educativo	**x**		
	PO02.Gestionar los recursos para los aprendizajes.	**x**		
	PO03. Gestionar el desarrollo del personal de servicio en las instituciones educativa	**x**		
	PO04. Gestionar la infraestructura educativa	**x**		
3	**SOPORTE (PS)**			
	PS01. Gestionar Recursos Humanos	**x**		
	PS02. Administrar los recursos financieros	**x**		
	PS03. Administrar sistema logístico.	**x**		
	PS03. Administrar los sistemas y TIC	**x**		
	PS03. Atender asuntos jurídicos legales		**x**	

Procesos adicionales

No se cuenta con otros procesos.

LOGO	IDENTIFICACIÓN DE PROCESOS					
	Fase:	II	**Proceso**	2	**Actividad**	-
	Código:	**GR005**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ÁREA	**Contabilidad**	**RESPONSABLE**	**YAMELISS CRUZALEGUI**

N°	TIPO DE PROCESO	RPTA SI	RPTA NO	OBSERVACION
1	**ESTRATÉGICOS (PE)**			
	PE01. Gestionar la planificación	x		
	PE02. Gestionar las relaciones interinstitucionales		x	
	PE03. Gestionar el sistema de control interno	x		
	PE04. Gestionar el desarrollo e innovación	x		
	PE05. Marketing educativo	x		
	PE06. Análisis de las partes interesadas.		x	
2	**OPERATIVOS (PO)**			
	PO01. Gestionar el servicio educativo	x		
	PO02.Gestionar los recursos para los aprendizajes.	x		
	PO03. Gestionar el desarrollo del personal de servicio en las instituciones educativa	x		Capacitación al personal
	PO04. Gestionar la infraestructura educativa	x		Compra de equipos, nuevas sedes.
3	**SOPORTE (PS)**			
	PS01. Gestionar Recursos Humanos	x		En este proceso solo se ve el tema de planillas, incorporación de personal.
	PS02. Administrar los recursos financieros	x		Administración de ingresos y egresos de la institución.
	PS03. Administrar sistema logístico.	x		Control de inventarios (entradas y salidas)
	PS03. Administrar los sistemas y TIC	x		
	PS03. Atender asuntos jurídicos legales		x	Este tema lo atiende terceras personas

Procesos adicionales

Proceso de postulantes (PO)

LOGO	IDENTIFICACIÓN DE ACTIVOS DE TI					
	Fase:	II	**Proceso**	2	**Actividad**	1
	Código:	**GR006**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ÁREA	**T.I**	**RESPONSABLE**		**JHONNY**
N°	**ACTIVOS**	**PROPIO**		**OBSERVACION**
		SI	**NO**	
	SERVICIOS: *Medio para entregar valor a las diferentes áreas de las instituciones educativas, satisfaciendo las necesidades de sus usuarios para que logren sus objetivos*			
	Servicio de intranet.	**X**		Páginas web para el personal, alumnos y padres de familia.
	Aplicaciones móviles	**X**		Aplicación móvil para el personal, alumnos y padres de familia.
	Servicio de correo electrónico	**X**		Personal, alumnos y padre de familia
	Soporte informático	**X**		Mantenimiento de computadoras
	Video vigilancia	**X**		Dentro y fuera de la organización
	Biblioteca	**X**		
	Servicio de internet	**X**		Se cuenta con 2 líneas (claro y movistar) para el uso dentro de la organización
	Servicio de telefonía	**X**		
	Portal web	**X**		
	APLICACIONES: *Apartado se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático*			
	Sistema web V4CIMA	**X**		Para el uso del personal de la institución
	Sistema web de Ticket	**X**		Uso de atención del cliente
	Sistema web de resultados de la UNPRG	**X**		
	Sistema web de recuperar contraseñas	**X**		
	Intranet web PREU	**X**		
	Intranet web PRE CADETE	**X**		
	Intranet web COLEGIO	**X**		
	Sistema web de asistencia Offline	**X**		
	Sistema web de inscripción	**X**		
	Aplicación móvil Colegio	**X**		
	Aplicación móvil de Admisión	**X**		
	Sistema de inventarios (Kardex)	**X**		
	Sistema web convocatoria	**X**		
	Moodle	**X**		
	Classrroon		**X**	Para las clases virtuales
	Facturador Sunat	**X**		
	Sistema Concart		**X**	Para la gestión administrativa (corre dentro de nuestros servidores)
	SOPORTE DE TI: *Es la estructura tecnológica que da soporte directa o indirectamente a los servicios y aplicaciones que presta el área de TI.*			
	Servidor Aplicaciones	**X**		
	Servidor de base de datos	**X**		
	Servidor de archivos	**X**		
	Servidor del aula virtual	**X**		
	Switches	**X**		
	Antenas RADWIN	**X**		Para comunicar con las diferentes sedes
	Dispositivos de comunicación	**X**		Rauter, Acces point

LOGO	LISTADO DE ACTIVOS DE TI					
	Fase:	II	**Proceso**	2	**Actividad**	1
	Código:	**GR007**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

N°	Código	Perfil del activo	Activo	Responsable
1	SE_1	Servicio	Servicio de intranet.	T.I
2	SE_2	Servicio	Aplicaciones móviles	T.I
3	SE_3	Servicio	Servicio de correo electrónico	T.I
4	SE_4	Servicio	Soporte informático	T.I
5	SE_5	Servicio	Video vigilancia	T.I
6	SE_6	Servicio	Biblioteca	T.I
7	SE_7	Servicio	Internet	T.I
8	SE_8	Servicio	Portal web	T.I
9	SE_9	Servicio	Servicio de telefonía	T.I
10	SW_1	Software	Sistema web V4CIMA	T.I (Área de desarrollo)
11	SW_2	Software	Sistema web de Ticket	T.I (Área de desarrollo)
12	SW_3	Software	Sistema web de resultados de la UNPRG	T.I (Área de desarrollo)
13	SW_4	Software	Sistema web de recuperar contraseñas	T.I (Área de desarrollo)
14	SW_5	Software	Intranet web PREU	T.I (Área de desarrollo)
15	SW_6	Software	Intranet web PRE CADETE	T.I (Área de desarrollo)
16	SW_7	Software	Intranet web COLEGIO	T.I (Área de desarrollo)
17	SW_8	Software	Sistema web de asistencia Offline	T.I (Área de desarrollo)
18	SW_9	Software	Sistema web de inscripción	T.I (Área de desarrollo)
19	SW_10	Software	Aplicación móvil Colegio	T.I (Área de desarrollo)
20	SW_11	Software	Aplicación móvil de Admisión	T.I (Área de desarrollo)
21	SW_12	Software	Sistema de inventarios (Kardex)	T.I (Área de desarrollo)
22	SW_13	Software	Sistema web convocatoria	T.I (Área de desarrollo)
23	SW_14	Software	Moodle	T.I (Área de desarrollo)
24	SW_15	Software	Classrroon	T.I (Área de desarrollo)
25	SW_16	Software	Facturador Sunat	T.I (Área de desarrollo)
26	SW_17	Software	Sistema Concart	T.I (Área de desarrollo)
27	HW_1	Hardware	Servidor Aplicaciones	T.I (Área de redes)
28	HW_2	Hardware	Servidor de base de datos	T.I (Área de redes)
29	HW_3	Hardware	Servidor de archivos	T.I (Área de redes)
30	HW_4	Hardware	Servidor del aula virtual	T.I (Área de redes)
31	HW_5	Hardware	Switches	T.I (Área de redes)
32	HW_4	Hardware	Antenas RADWIN	T.I (Área de redes)
33	HW_6	Hardware	Dispositivos de comunicación	T.I (Área de redes)

LOGO	VALORACIÓN DE ACTIVOS					
	Fase:	II	**Proceso**	3	**Actividad**	-
	Código:	**GR008**		**Páginas:**		4/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CONFIDENCIALIDAD (C)	
1	La información es pública .
2	La información es de uso interno de la institución.
3	La información es confidencial y solo el personal de algunas área pueden acceder a ella
4	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5	La información es solo accedida por el personal de alto rango o con permisos a ella

DISPONIBILIDAD (D)	
1	El funcionamiento es normal en las actividades
2	Disponible al 10% del tiempo.
3	Disponible al 30% del tiempo.
4	Disponible al 60% del tiempo.
5	Disponible al 90% del tiempo.

INTEGRIDAD (I)	
1	Se tolera pérdida o alteración de sus componentes en un 80% - 100%
2	Se tolera pérdida o alteración de sus componentes en un 60% - 79%
3	Se tolera pérdida o alteración de sus componentes en un 40% - 59%
4	Se tolera pérdida o alteración de sus componentes en un 20% - 39%
5	Se tolera pérdida o alteración de sus componentes en un 0% - 19%

ÁREA	ATENCIÓN AL CLIENTE			RESPONSABLE				ROSALIN OBALLE
N°	ACTIVOS		USO	CRITERIOS				OBSERVACIÓN
	CÓDIGO	DESCRIPCION		C	D	I	TOTAL	
1	SE_1	Servicio de intranet.	X	4	4	4	12	PO02 – (Entrar a los sistemas en las diferentes sedes)
2	SE_2	Aplicaciones móviles	X	3	4	4	11	PO02 – (Para el uso interno del personal etc)
3	SE_3	Servicio de correo electrónico	X	3	4	4	11	Es indispensable para la fluidez de la información.
4	SE_4	Soporte informático	X	2	4	3	9	PS05
5	SE_5	Video vigilancia	X	4	4	4	12	PO04
6	SE_6	Biblioteca	-	-	-	-	-	-
7	SE_7	Internet	X	2	3	1	6	PS05
8	SE_8	Portal web	X	1	1	2	4	PE04
9	SE_9	Servicio de telefonía	X	1	1	1	3	-
10	SW_1	Sistema web V4CIMA	X	5	5	5	15	PE05, PO01, PO05,PO06,PO07, PS01,9S02
11	SW_2	Sistema web de Ticket	X	2	3	3	8	PO06
12	SW_3	Sistema web de resultados de la UNPRG	X	1	4	5	10	La información debe ser confiable , se muestra al público.
13	SW_4	Sistema web de recuperar contraseñas	-	-	-	-	-	-
14	SW_5	Intranet web PREU	X	2	5	5	12	PO02
15	SW_6	Intranet web PRE CADETE	X	2	5	5	12	PO02
16	SW_7	Intranet web COLEGIO	X	2	5	5	12	PO02
17	SW_8	Sistema web de asistencia Offline	X	2	4	3	9	PS01
18	SW_9	Sistema web de inscripción	X	3	5	5	13	PS01
19	SW_10	Aplicación móvil Colegio	-	-	-	-	-	PO02

20	SW_11	Aplicación móvil de Admisión	**X**	4	5	5	14	PO01, PO05, PO07,
21	SW_12	Sistema de inventarios (Kardex)	-	-	-	-	-	-
22	SW_13	Sistema web convocatoria	**X**	4	4	4	12	PS01
23	SW_14	Moodle	**X**	2	5	5	12	PO02 -(Esencial para las evaluaciones.)
24	SW_15	Classrroon	**X**	2	5	5	12	PO02 -(Esenciales para las clases virtuales)
25	SW_16	Facturador Sunat	-	-	-	-	-	-
26	SW_17	Sistema Concart	-	-	-	-	-	-

LOGO	VALORACIÓN DE ACTIVOS					
	Fase:	II	**Proceso**	3	**Actividad**	-
	Código:	**GR008**		**Páginas:**		4/2
NOMBRE DE LA I.E. P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CONFIDENCIALIDAD (C)	
1	La información es pública.
2	La información es de uso interno de la institución.
3	La información es confidencial y solo el personal de algunas áreas pueden acceder a ella
4	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5	La información es solo accedida por el personal de alto rango o con permisos a ella

DISPONIBILIDAD (D)	
1	El funcionamiento es normal en las actividades
2	Disponible al 10% del tiempo.
3	Disponible al 30% del tiempo.
4	Disponible al 60% del tiempo.
5	Disponible al 90% del tiempo.

INTEGRIDAD (I)	
1	Se tolera pérdida o alteración de sus componentes en un 80% - 100%
2	Se tolera pérdida o alteración de sus componentes en un 60% - 79%
3	Se tolera pérdida o alteración de sus componentes en un 40% - 59%
4	Se tolera pérdida o alteración de sus componentes en un 20% - 39%
5	Se tolera pérdida o alteración de sus componentes en un 0% - 19%

ÁREA	Contabilidad		RESPONSABLE				MILUSKA CRUZALEGUI
N°	ACTIVOS		USO	CRITERIOS			OBSERVACIÓN
	CÓDIGO	DESCRIPCION		C	D	I	TOTAL	
1	SE_1	Servicio de intranet.	**X**	2	4	5	11	PO03
2	SE_2	Aplicaciones móviles	**X**	2	4	5	11	PE01,PO01, PO03
3	SE_3	Servicio de correo electrónico	**X**	2	4	4	10	PE01
4	SE_4	Soporte informático	**X**	2	4	3	9	PS05
5	SE_5	Video vigilancia	-	-	-	-	-	-
6	SE_6	Biblioteca	-	-	-	-	-	-
7	SE_7	Internet	**X**	2	4	3	9	-
8	SE_8	Portal web	-	-	-	-	-	-
9	SE_9	Servicio de telefonía	**X**	1	1	1	3	-
10	SW_1	Sistema web V4CIMA	**X**	3	5	5	13	Todos los procesos operativos, PS01, PS02
11	SW_2	Sistema web de Ticket	-	-	-	-	-	-
12	SW_3	Sistema web de resultados de la UNPRG	-	-	-	-	-	-
13	SW_4	Sistema web de recuperar contraseñas	-	-	-	-	-	-
14	SW_5	Intranet web PREU	-	-	-	-	-	-
15	SW_6	Intranet web PRE CADETE	-	-	-	-	-	-
16	SW_7	Intranet web COLEGIO	-	-	-	-	-	-
17	SW_8	Sistema web de asistencia Offline	**X**	2	5	5	12	PS01 - Se utiliza para sacar reporte para los pagos de planilla
18	SW_9	Sistema web de inscripción	**X**	2	5	5	12	PA01
19	SW_10	Aplicación móvil Colegio	**X**	2	5	5	12	PO02
20	SW_11	Aplicación móvil de Admisión	**X**	2	5	5	12	PO05
21	SW_12	Sistema de inventarios (Kardex)	**X**	3	5	5	13	PS03 -Se lleva un control de inventarios (compra de insumos)

22	SW_13	Sistema web convocatoria	**X**	3	5	5	13	PS01
23	SW_14	Moodle	**-**	-	-	-	-	-
24	SW_15	Classrroon	**-**	-	-	-	-	-
25	SW_16	Facturador Sunat	**X**	5	5	5	15	PS02 –(Información que se remite a Sunat)
26	SW_17	Sistema Concart	**X**	5	5	5	15	PS01, PS02

LOGO	VALORACIÓN DE ACTIVOS					
	Fase:	II	**Proceso**	3	**Actividad**	-
	Código:	**GR008**		**Páginas:**		4/3
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CONFIDENCIALIDAD (C)	
1	La información es pública .
2	La información es de uso interno de la institución.
3	La información es confidencial y solo el personal de algunas área pueden acceder a ella
4	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5	La información es solo accedida por el personal de alto rango o con permisos a ella

DISPONIBILIDAD (D)	
1	El funcionamiento es normal en las actividades
2	Disponible al 10% del tiempo.
3	Disponible al 30% del tiempo.
4	Disponible al 60% del tiempo.
5	Disponible al 90% del tiempo.

INTEGRIDAD (I)	
1	Se tolera pérdida o alteración de sus componentes en un 80% - 100%
2	Se tolera pérdida o alteración de sus componentes en un 60% - 79%
3	Se tolera pérdida o alteración de sus componentes en un 40% - 59%
4	Se tolera pérdida o alteración de sus componentes en un 20% - 39%
5	Se tolera pérdida o alteración de sus componentes en un 0% - 19%

ÁREA	T. I		RESPONSABLE	JHONY AGAPITO			
N°	ACTIVOS		USO	CRITERIOS				OBSERVACIÓN
	CÓDIGO	DESCRIPCION		C	D	I	TOTAL	
1	SE_1	Servicio de intranet.	X	2	4	5	11	PO03
2	SE_2	Aplicaciones móviles	X	2	4	5	11	PE01, PO01, PO03
3	SE_3	Servicio de correo electrónico	X	2	4	4	10	PE01
4	SE_4	Soporte informático	X	2	4	3	9	PS05
5	SE_5	Video vigilancia	X	3	5	2	10	PO01, PS05
6	SE_6	Biblioteca	X	1	1	1	3	PO01
7	SE_7	Internet	X	2	2	1	5	PS05
8	SE_8	Portal web	X	1	1	3	5	PO01
9	SE_9	Servicio de telefonía	X	2	2	1	5	PS05
10	SW_1	Sistema web V4CIMA	X	3	5	5	13	Todos los procesos operativos
11	SW_2	Sistema web de Ticket	X	2	3	1	6	PO06
12	SW_3	Sistema web de resultados de la UNPRG	X	1	5	5	11	PO01, PS05
13	SW_4	Sistema web de recuperar contraseñas	X	2	3	5	10	PS05
14	SW_5	Intranet web PREU	X	2	5	5	12	PO02
15	SW_6	Intranet web PRE CADETE	X	2	5	5	12	PO02

16	SW_7	Intranet web COLEGIO	**X**	2	5	5	12	PO02
17	SW_8	Sistema web de asistencia Offline	**X**	2	5	5	12	PS01
18	SW_9	Sistema web de inscripción	**X**	2	5	5	12	PS01
19	SW_10	Aplicación móvil Colegio	**X**	2	5	5	12	PO01, PO02
20	SW_11	Aplicación móvil de Admisión	**X**	2	5	5	12	P001

LOGO	VALORACIÓN DE ACTIVOS					
	Fase:	II	**Proceso**	3	**Actividad**	-
	Código:	**GR008**		**Páginas:**		4/4
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CONFIDENCIALIDAD (C)	
1	La información es pública .
2	La información es de uso interno de la institución.
3	La información es confidencial y solo el personal de algunas área pueden acceder a ella
4	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5	La información es solo accedida por el personal de alto rango o con permisos a ella

DISPONIBILIDAD (D)	
1	El funcionamiento es normal en las actividades
2	Disponible al 10% del tiempo.
3	Disponible al 30% del tiempo.
4	Disponible al 60% del tiempo.
5	Disponible al 90% del tiempo.

INTEGRIDAD (I)	
1	Se tolera pérdida o alteración de sus componentes en un 80% - 100%
2	Se tolera pérdida o alteración de sus componentes en un 60% - 79%
3	Se tolera pérdida o alteración de sus componentes en un 40% - 59%
4	Se tolera pérdida o alteración de sus componentes en un 20% - 39%
5	Se tolera pérdida o alteración de sus componentes en un 0% - 19%

ÁREA	T.I		RESPONSABLE				JHONY AGAPITO
N°	ACTIVOS		USO	CRITERIOS				OBSERVACIÓN
	CÓDIGO	DESCRIPCION		C	D	I	TOTAL	
21	SW_12	Sistema de inventarios (Kardex)	X	3	5	5	13	PS03
22	SW_13	Sistema web convocatoria	X	3	4	5	12	PS01
23	SW_14	Moodle	X	2	5	5	12	PO01, PO02
24	SW_15	Classrroon	X	2	5	5	12	PO01, PO02
25	SW_16	Facturador Sunat	X	5	5	5	15	PS02
26	SW_17	Sistema Concart	X	5	5	5	15	PS01,PS02
27	HW_1	Servidor Aplicaciones	X	5	5	5	15	Todos procesos operativos y de soporte
28	HW_2	Servidor de base de datos	X	5	5	5	15	Todos procesos operativos y de soporte
29	HW_3	Servidor de archivos	X	5	5	5	15	Todos procesos operativos y de soporte
30	HW_4	Servidor del aula virtual	X	5	5	5	15	PO01, PO02, P03
31	HW_3	Switches	X	5	4	5	14	Importante para la comunicación entre las áreas de cada sede
32	HW_4	Antenas RADWIN	X	5	5	5	15	Importante para el uso de los sistemas en las diferentes sedes
33	HW_3	Dispositivos de comunicación	X	2	5	5	12	PO04

LOGO	VALORACIÓN DE ACTIVOS					
	Fase:	II	**Proceso**	3	**Actividad**	-
	Código:	**GR008**		**Páginas:**		2/2
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CONFIDENCIALIDAD (C)	
1	La información es pública .
2	La información es de uso interno de la institución.
3	La información es confidencial y solo el personal de algunas área pueden acceder a ella
4	La información es restringida y solo el personal de un proyecto específico puede acceder a ella
5	La información es solo accedida por el personal de alto rango o con permisos a ella

DISPONIBILIDAD (D)	
1	El funcionamiento es normal en las actividades
2	Disponible al 10% del tiempo.
3	Disponible al 30% del tiempo.
4	Disponible al 60% del tiempo.
5	Disponible al 90% del tiempo.

INTEGRIDAD (I)	
1	Se tolera pérdida o alteración de sus componentes en un 100%
2	Se tolera pérdida o alteración de sus componentes en un 80%
3	Se tolera pérdida o alteración de sus componentes en un 50%
4	Se tolera pérdida o alteración de sus componentes en un 15%
5	Se tolera pérdida o alteración de sus componentes en un 0%

ÁREA	T.I		RESPONSABLE				Jhony Agapito
N°	ACTIVOS		USO	CRITERIOS				OBSERVACIÓN
	CÓDIGO	DESCRIPCION		C	D	I	TOTAL	
21	APW _12	Sistema de inventarios (Kardex)	X	3	5	5	13	PS03
22	APW _13	Sistema web convocatoria	X	3	4	5	12	PS01
23	APW _14	Moodle	X	2	5	5	12	PO01, PO02
24	APW _15	Classrroon	X	2	5	5	12	PO01, PO02
25	APW _16	Facturador Sunat	X	5	5	5	15	PS02
26	APW_17	Sistema Concart	X	5	5	5	15	PS01,PS02
27	STI _1	Servidor Aplicaciones	X	5	5	5	15	Todos procesos operativos y de soporte
28	STI _2	Servidor de base de datos	X	5	5	5	15	Todos procesos operativos y de soporte
29	STI _3	Servidor de archivos	X	5	5	5	15	Todos procesos operativos y de soporte
30	STI _4	Servidor del aula virtual	X	5	5	5	15	PO01, PO02, P03
31	STI _5	Switches	X	5	4	5	14	Importante para la comunicación entre las áreas de cada sede
32	STI _6	Antenas RADWIN	X	5	5	5	15	Importante para el uso de los sistemas en las diferentes sedes
33	STI_7	Dispositivos de comunicación	X	2	5	5	12	PO04

LOGO	NIVEL DE CRITICIDAD DE ACTIVOS DE TI					
	Fase:	II	**Proceso**	2	**Actividad**	1
	Código:	**GR007**		**Páginas:**		1/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

Activos de TI			Total	Nivel de criticidad
#	ETIQUETA	ACTIVO		
1	SE_1	Servicio de intranet.	11	Alto
2	SE_2	Aplicaciones móviles	11	Alto
3	SE_3	Servicio de correo electrónico	10	Medio
4	SE_4	Soporte informático	9	Medio
5	SE_5	Video vigilancia	10	Medio
6	SE_6	Biblioteca	3	Bajo
7	SE_7	Internet	5	Bajo
8	SE_8	Portal web	4	Bajo
9	SE_9	Servicio de telefonía	3	Bajo
10	SW_1	Sistema web V4CIMA	13	Alto
11	SW_2	Sistema web de Ticket	6	Medio
12	SW_3	Sistema web de resultados de la UNPRG	10	Medio
13	SW_4	Sistema web de recuperar contraseñas	10	Medio
14	SW_5	Intranet web PREU	12	Alto
15	SW_6	Intranet web PRE CADETE	12	Alto
16	SW_7	Intranet web COLEGIO	12	Alto
17	SW_8	Sistema web de asistencia Offline	9	Medio
18	SW_9	Sistema web de inscripción	12	Alto
19	SW_10	Aplicación móvil Colegio	12	Alto
20	SW_11	Aplicación móvil de Admisión	12	Alto
21	SW_12	Sistema de inventarios (Kardex)	13	Alto
22	SW_13	Sistema web convocatoria	12	Alto
23	SW_14	Moodle	12	Alto
24	SW_15	Classrroon	12	Alto
25	SW_16	Facturador Sunat	15	Alto
26	SW_17	Sistema Concart	15	Alto
27	HW_1	Servidor Aplicaciones	15	Alto
28	HW_2	Servidor de base de datos	15	Alto
29	HW_3	Servidor de archivos	15	Alto
30	HW_4	Servidor del aula virtual	15	Alto
31	HW_5	Switches	14	Alto
32	HW_6	Antenas RADWIN	15	Alto
33	HW_7	Dispositivos de comunicación	12	Alto

LOGO	LISTADO DE AMENAZAS					
	Fase:	III	**Proceso**	1	**Actividad**	1
	Código:	**GR008**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

TIPO DE AMENAZA	AMENAZA
NATURALES	Polvo
	Corrección o Humedad
	Desastres naturales
	Corte de suministro eléctrico
SERVICIOS	Corte de suministro eléctrico
	Fallos eléctricos
	Fallo de servicio de comunicaciones
	Interrupción de servicios internos y externos.
	Espionaje
	Software dañado
USUARIO NO INTENCIONAL	Errores de usuarios
	Errores de configuración
	Escape de información
	Errores de mantenimiento
	Caídas del sistema
	Indisponibilidad del personal
	Perdidas de equipos
	Usuario mal entrenado
	Negligencia del usuario.
USUARIO INTENCIONAL	Usuario deshonesto
	Empleados despedidos
	Penetración del sistema
	Robo de información
	Acceso no autorizado
	Ingeniería social
INFORMACIÓN	Acceso no autorizado a la información
	Modificación no autorizada
	Eliminación no autorizada
	Robo de activo contenedores de información
	Corrupción de datos
	Ataques de hacking
	Fuga de información
	Alteración de información
SOFTWARE	Actualizaciones no controladas
	Instalaciones no autorizadas
	Saturación de operaciones en el software
	Virus informático

LOGO	ESCENARIO DE RIESGOS					
	Fase:	III	**Proceso**	1	**Actividad**	1
	Código:	**GR009**		**Páginas:**		__/__
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

CÓDIGO: *#identificador*	R0001	**TIEMPO:** *Duración del riesgo*	6 a 12 horas
TIPO DE AMENAZA: *Ver plantilla **GR008***		**AMENAZA:** *Ver plantilla Ver plantilla **GR008***	
NATURALES		Corte de suministro eléctrico	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No contar un UPS, para el suministro de energía		Paralizar todos los procesos de la institución educativa generando inconvenientes para cerrar caja, realizar pagos y que se realicen actividades.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_1 Servidor de aplicaciones, STI_2 Servidores de base de datos, STI _3 Servidor de archivos, STI_4 servidor del aula virtual, STI_5 Switches.			

CÓDIGO: *#identificador*	R0002	**TIEMPO:** *Duración del riesgo*	Varias semanas
TIPO DE AMENAZA: *Ver plantilla **GR008***		**AMENAZA:** *Ver plantilla Ver plantilla **GR008***	
NATURALES		Desastre naturales	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Mala ubicación de los servidores		Pérdida total de los equipos, de datos e interrupción de los servicios.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_1 Servidor de aplicaciones, STI_2 Servidores de base de datos, STI _3 Servidor de archivos, STI_4 servidor del aula virtual, STI_5 Switches.			

CÓDIGO: *#identificador*	R0003	**TIEMPO:** *Duración del riesgo*	Varias semanas
TIPO DE AMENAZA: *Ver plantilla **GR008***		**AMENAZA:** *Ver plantilla Ver plantilla **GR008***	
NATURALES		Polvo	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco mantenimiento en los equipos.		Lentitud en los servicios que son soportados en el servidor	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_1 Servidor de aplicaciones, STI_2 Servidores de base de datos, STI _3 Servidor de archivos, STI_4 servidor del aula virtual, STI_5 Switches.			

CÓDIGO: *#identificador*	R0004	**TIEMPO:** *Duración del riesgo*	Varias semanas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
Usuario no intencional		Negligencia del usuario.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco mantenimiento al aire acondicionado		Corto circuito y perdida de servidores	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_1 Servidor de aplicaciones, STI_2 Servidores de base de datos, STI _3 Servidor de archivos, STI_4 servidor del aula virtual, STI_5 Switches.			

CÓDIGO: *#identificador*	R0005	**TIEMPO:** *Duración del riesgo*	Máximo 1 hora.
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
NO INTENCIONAL		Negligencia del usuario.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Mala ubicación de la sala de servidores		Sobre calentamiento de los equipos y reinicio de estos, interrumpiendo los diferentes servicios soportados	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI _1 Servidor de aplicaciones, STI_2 Servidores de base de datos, STI_3 Servidor de archivos, STI 4 servidor del aula virtual.			

CÓDIGO: *#identificador*	R0006	**TIEMPO:** *Duración del riesgo*	1 a varios días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO INTENCIONAL		Acceso no autorizado	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
La mala ubicación de la sala de servidores, esta al acceso de personas que no pertenecen a la institución		Perdida de equipos tecnológicos paralizando los diferentes procesos de la organización.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_1 Servidor de aplicaciones, STI_2 Servidores de base de datos, STI_3 Servidor de archivos, STI STI_4 servidor del aula virtual.			

CÓDIGO: *#identificador*	R0007	**TIEMPO:** *Duración del riesgo*	6 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Instalación de programas no autorizados	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No hay control de permisos de acceso al servidor (todos los desarrolladores incluyendo practicantes pueden instalar o desinstalar programas)		Apagar o reiniciar los servicios internos dentro del servidor por un determinado tiempo, por una mala configuración	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI__1 Servidor de aplicaciones			

CÓDIGO: *#identificador*	R0008	**TIEMPO:** *Duración del riesgo*	6 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Usuario mal entrenado	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No hay control de permisos de acceso al servidor de base de datos (todos los desarrolladores incluyendo practicantes acceden con el rol de administrador a la base de datos)		Eliminar o alterar la información, generando inconsistencia en los datos a la hora de mostrar en las diferentes aplicaciones.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_2 Servidores de base de datos			

CÓDIGO: *#identificador*	R0009	**TIEMPO:** *Duración del riesgo*	1 o 2 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO INTENCIONAL		Penetración del sistema	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Mala gestión de seguridad		Eliminación de archivos confidenciales de la institución.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_3 Servidor de archivos			

CÓDIGO: *#identificador*	R00010	**TIEMPO:** *Duración del riesgo*	1 semana a más
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios internos y externos	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No tienen el control de construcción de edificios o instalaciones de antenas entre sus sedes		Denegación del servicio de internet y de los diferentes sistemas por la interrupción de comunicación entre las diferentes sedes.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_6 Antenas RADWIN			

CÓDIGO: *#identificador*	R0011	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SOFTWARE		Actualización no controlada	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Incompatibilidad entre sistemas		Retraso en las actividades para levantar los nuevos cambios de los sistemas.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_16 Facturador Sunat			

CÓDIGO: *#identificador*	R0012	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Errores de configuración.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco control en las actualizaciones de los sistemas		Retraso de trabajo y sanciones de Sunat por inconsistencia en él envió de información	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_16 Facturador Sunat			

CÓDIGO: *#identificador*	R0013	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios internos y externos.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poca banda ancha		Pérdida parcial o completa de información en registros enviados a Sunat. Lo que generar estar revisando uno por uno	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_16 Facturador Sunat			

CÓDIGO: *#identificador*	R0014	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Errores de configuración o actualización.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Falta de control de calidad.		Retraso de trabajo y sanciones de Sunat por inconsistencia en envió de información	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_16 Facturador Sunat			

CÓDIGO: *#identificador*	R0015	**TIEMPO:** *Duración del riesgo*	1 a 2 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Software desfasado		Actualización del sistema operativo, haciendo que el sistema deje de funcionar, logrando interrumpir la jornada laboral	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_17 Sistema Concar			

CÓDIGO: *#identificador*	R0016	**TIEMPO:** *Duración del riesgo*	1 a 2 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Control inadecuado de las actualizaciones y de configuraciones del sistema operativo		Haciendo que el sistema deje de funcionar, logrando interrumpir la jornada laboral	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_17 Sistema Concar			

CÓDIGO: *#identificador*	R0017	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Daño físico	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Mal manejo de los equipos (falta de capacitación)		Perdida del equipo, además de la interrupción de los equipos conectados al Switches	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_5 Switches			

CÓDIGO: *#identificador*	R0018	**TIEMPO:** *Duración del riesgo*	1día
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Errores de configuración	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No se cuenta con manuales de configuración		Interrupción laboral por mala configuración del equipo.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_5 Switches			

CÓDIGO: *#identificador*	R0019	**TIEMPO:** *Duración del riesgo*	Máximo 1 día
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
NATURALES		Polvo	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco mantenimiento		Se congestiona y no reconoce las configuración generando interrupción en los servicios.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_5 Switches			

CÓDIGO: *#identificador*	R0020	**TIEMPO:** *Duración del riesgo*	1día
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
NATURALES		Negligencia del usuario.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poca coordinación en la institución.		Pérdida de comunicación entre la antena y el Switches interrumpiendo las actividades las máquinas conectadas.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_5 Switches , STI_6 Antenas RADWIN			

CÓDIGO: *#identificador*	R0021	**TIEMPO:** *Duración del riesgo*	1 a n días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
INFORMACIÓN		Acceso no autorizado a la información	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Mal control de asignación de permisos en el sistema		Divulgar información confidencial a la competencia de la institución.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_1 Sistema web V4CIMA			

CÓDIGO: *#identificador*	R0022	**TIEMPO:** *Duración del riesgo*	1 a 3 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
INFORMACIÓN		Interrupción de servicios internos y externos.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Software muy antiguo.		Al actualizar se paralice el servicio, debido a incompatibilidad en el S.O.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_1 Sistema web V4CIMA			

CÓDIGO: *#identificador*	R0023	**TIEMPO:** *Duración del riesgo*	1 a más días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO INTENCIONAL		Empleados despedidos	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Falta de gestión de identidades y accesos.		Divulgar la información a personas externa de la información o extorción con información confidencial que puede generar multas.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_1 Sistema web V4CIMA			

CÓDIGO: *#identificador*	R0024	**TIEMPO:** *Duración del riesgo*	1 a varios días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO INTENCIONAL		Usuario deshonesto	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco control del personal		Alteración de la información para su propio beneficio.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_1 Sistema web V4CIMA			

CÓDIGO: *#identificador*	R0025	**TIEMPO:** *Duración del riesgo*	1 a 3 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SOFTWARE		Saturación de operaciones en el software	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Mala gestión de concurrencia de usuarios		Caídas del sistema en momentos críticos de la jornada laborar generando insatisfacción y lentitud en los procesos.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_1 Sistema web V4CIMA			

CÓDIGO: *#identificador*	R0026	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Errores de usuario	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Falta de control de calidad al actualizar el sistema		Envió de reporte inconsistente a la Sunat	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_12 Sistema de inventario (Kardex)			

CÓDIGO: *#identificador*	R0027	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Usuario mal entrenado	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poca capacitación al personal de la institución en el manejo de los sistema		Pérdida de tiempo del personal, retrasos de actividades e inconsistencia de datos	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_12 Sistema de inventario (Kardex)			

CÓDIGO: *#identificador*	R0028	**TIEMPO:** *Duración del riesgo*	1 a n días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO INTENCIONAL		Usuario deshonesto	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poca seguridad en los sistemas		Alteración de información para su propio beneficio, cambio de costos, stock, etc., generando pérdidas a la institución.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_12 Sistema de inventario (Kardex)			

CÓDIGO: *#identificador*	R0029	**TIEMPO:** *Duración del riesgo*	1 a 6 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Fallos de equipo de comunicaciones	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Conexión deficiente de cables		Perdida de horas de jornada laboral	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
STI_7 Dispositivos de comunicación			

CÓDIGO: *#identificador*	R0030	**TIEMPO:** *Duración del riesgo*	1 a n semanas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SOFTWARE		Actualizaciones no controladas	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco seguimiento de las actualizaciones de servicios de terceros		Interrupción de las diferentes actividades de las diferentes áreas, inconsistencia de datos.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
SE_2 Aplicaciones móviles			

CÓDIGO: *#identificador*	R0031	**TIEMPO:** *Duración del riesgo*	Máximo 1día
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Errores de mantenimiento	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Un mal control de calidad del software		Interrupción de las diferentes actividades de las diferentes áreas, inconsistencia de datos.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_10 Aplicación móvil colegio , APW_11 Aplicación móvil de Admisión			

CÓDIGO: *#identificador*	R0032	**TIEMPO:** *Duración del riesgo*	1 a 3 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
INFORMACIÓN		Corrupción de datos	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco control de datos e integración entre aplicaciones.		Reclamos hacia la institución por información inconsistente que se muestra en las aplicaciones.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_5 Intranet web PREU, APW_6 Intranet web PRE CADETE , APW_7 Intranet web COLEGIO, APW_10 Aplicación móvil colegio , APW_11 Aplicación móvil de Admisión			

CÓDIGO: *#identificador*	R0033	**TIEMPO:** *Duración del riesgo*	1 a 4 días
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Indisponibilidad del personal	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No contar con documentación de los diferentes sistemas.		No poder brindar el soporte de actualizaciones o configuración de los sistemas debido a la falta del personal	

ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*
SE_1 Servicio de intranet, SE_2 aplicaciones móviles

CÓDIGO: *#identificador*	R0034	**TIEMPO:** *Duración del riesgo*	Hasta 1 día
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios internos y externos.	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poca banda ancha		Perdida de información e inconformidad de los usuarios.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_14 Moodle			

CÓDIGO: *#identificador*	R0035	**TIEMPO:** *Duración del riesgo*	Hasta 1 día
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
USUARIO NO INTENCIONAL		Errores de configuración	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Configuración manual para la actualización.		Inconsistencia de información, generando pérdida de tiempo en hora de clases.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_14 Moodle			

CÓDIGO: *#identificador*	R0036	**TIEMPO:** *Duración del riesgo*	1 a 8 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios internos y externos	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
Poco control de la plataforma tercerizado		Problemas a la hora de acceder a los cursos y acceder a evaluaciones, archivos, etc.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_15 Classroon			
CÓDIGO: *#identificador*	R0037	**TIEMPO:** *Duración del riesgo*	1 a 8 horas
TIPO DE AMENAZA: *Ver plantilla* ***GR008***		**AMENAZA:** *Ver plantilla Ver plantilla* ***GR008***	
SERVICIOS		Interrupción de servicios internos y externos	

VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*	**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*
Poco control de la plataforma tercerizado	Problemas a la hora de acceder a los cursos y acceder a evaluaciones, archivos, etc.
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*	
APW_15 Classroon	

CÓDIGO: *#identificador*	R0038	**TIEMPO:** *Duración del riesgo*	1 a 6 horas
TIPO DE AMENAZA: *Ver plantilla **GR008***		**AMENAZA:** *Ver plantilla Ver plantilla **GR008***	
SERVICIOS		Interrupción de servicios internos y externos	
VULNERABILIDAD: *característica que puede ser aprovechada por una amenaza.*		**RIESGOS:** *probabilidad de que una amenaza se convierta en un desastre para la instituciones.*	
No contar con documentación para reanudar los procesos.		Demorar a la hora de restaurar los servicios generando incomodidad e insatisfacción a los usuarios externos de la institución.	
ACTIVOS AFECTADOS: *Son los activos que pueden verse afectados con la materialización del riesgo identificado.*			
APW_3 Sistema web de resultados de la UNPRG, APW_5 Intranet web PREU, APW_6 Intranet web PRE CADETE, APW_7 Intranet web COLEGIO, APW_9 Sistema web de inscripción, APW_10 Aplicación móvil colegio, APW_11 Aplicación móvil de Admisión, APW_13 Sistema web de convocatoria			

LOGO	LISTADO DE ESCENARIOS DE RIESGOS					
	Fase:	3	**Proceso**	1	**Actividad**	2
	Código:	**GR010**		**Páginas:**		__/_1_
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ACTIVO			ESCENARIO DE RIESGO			
N°	**ETIQUETA**	**NOMBRE**	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**
1	STI_1	Servidor de aplicaciones	R0001	Corte de suministro eléctrico	No contar un UPS, para el suministro de energía	Paralizar todos los procesos de la institución educativa generando inconvenientes para cerrar caja, realizar pagos y que se realicen actividades.
2	STI_2	Servidores de B. D				
3	STI _3	Servidor de archivos				
4	STI_4	Servidor del aula virtual				
5	STI_5	Switches				
6	STI_1	Servidor de aplicaciones	R0002	Desastres naturales	Mala ubicación de los servidores	Pérdida total de los equipos, de datos e interrupción de los servicios.
7	STI_2	Servidores de B. D				
8	STI _3	Servidor de archivos				
9	STI_4	Servidor del aula virtual				
10	STI_5	Switches				
11	STI_1	Servidor de aplicaciones	R0003	Polvo	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	Lentitud en los servicios que son ofrecidos por el área de T.I
11	STI_2	Servidores de B. D				
12	STI _3	Servidor de archivos				
13	STI_4	Servidor del aula virtual				
14	STI_5	Switches				
15	STI_1	Servidor de aplicaciones	R0004	Negligencia del usuario	Poco mantenimiento preventivo en los equipos que pertenece al área de T. I	Corto circuito y perdida de servidores por fuga de agua del aire acondicionado
16	STI_2	Servidores de B. D				
17	STI _3	Servidor de archivos				
18	STI_4	Servidor del aula virtual				
19	STI_5	Switches				
20	STI_1	Servidor de aplicaciones	R0005	Negligencia del usuario.	Mala ubicación de la sala de servidores	Sobre calentamiento de los equipos y reinicio de estos, interrumpiendo los diferentes servicios soportados
21	STI_2	Servidores de B. D				
22	STI _3	Servidor de archivos				
23	STI_4	Servidor del aula virtual				
24	STI_1	Servidor de aplicaciones	R0006	Acceso no autorizado	La mala ubicación de la sala de servidores, esta al acceso de personas que no pertenecen a la institución	Perdida de equipos tecnológicos paralizando los diferentes procesos de la organización.
25	STI_2	Servidores de B. D				
26	STI _3	Servidor de archivos				
27	STI_4	Servidor del aula virtual				

28	STI_1	Servidor de aplicaciones	R0007	Instalación de programas no autorizados	No hay control de permisos de acceso al servidor (todos los desarrolladores incluyendo practicantes pueden instalar o desinstalar programas)	Apagar o reiniciar los servicios internos dentro del servidor por un determinado tiempo, por una mala configuración

LOGO	**LISTADO DE ESCENARIOS DE RIESGOS**					
	Fase:	3	**Proceso**	1	**Actividad**	2
	Código:	**GR010**		**Páginas:**		4/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ACTIVO			**ESCENARIO DE RIESGO**			
N°	**ETIQUETA**	**NOMBRE**	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**
29	STI_2	Servidores de B.D	R0008	Usuario mal entrenado	No hay control de permisos de acceso al servidor de base de datos (todos acceden con usuario y contraseña de administrador)	Eliminar o alterar la información, generando inconsistencia en los datos a la hora de mostrar en las diferentes aplicaciones.
30	STI_3	Servidor de archivos	R0009	Penetración del sistema	Mala gestión de seguridad	Eliminación de archivos confidenciales de la institución.
31	STI_6	Antenas RADWIN	R0010	Interrupción de servicios internos y externos	No tienen el control de construcción de edificios o instalaciones de antenas entre sus sedes	Denegación del servicio de internet y de los diferentes sistemas por la interrupción de comunicación entre las diferentes sedes.
32	APW_16	Facturador Sunat	R0011	Actualización no controlada	Incompatibilidad entre sistemas	Retraso en las actividades para levantar los nuevos cambios de los sistemas.
33	APW_16	Facturador Sunat	R0012	Errores de configuración	Poco control en las actualizaciones de los sistemas	Retraso de trabajo y sanciones de Sunat por inconsistencia en él envió de información
34	APW_16	Facturador Sunat	R0013	Interrupción de servicios internos y externos	Poca banda ancha	Pérdida parcial o completa de información en registros enviados a Sunat. Lo que generar estar revisando uno por uno

35	APW_16	Facturador Sunat	R0014	Errores de configuración o actualización	Falta de control de calidad.	Retraso de trabajo y sanciones de Sunat por inconsistencia en envió de información
36	APW_17	Sistema Concar	R0015	Interrupción de servicios	Software desfasado	Actualización del sistema operativo, haciendo que el sistema deje de funcionar, logrando interrumpir la jornada laboral
37	APW_17	Sistema Concar	R0016	Interrupción de servicios	Control inadecuado de las actualizaciones y de configuraciones del sistema operativo	Haciendo que el sistema deje de funcionar, logrando interrumpir la jornada laboral

LOGO	**LISTADO DE ESCENARIOS DE RIESGOS**					
	Fase:	3	**Proceso**	1	**Actividad**	2
	Código:	**GR010**		**Páginas:**		3/2
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ACTIVO			**ESCENARIO DE RIESGO**			
N°	**ETIQUETA**	**NOMBRE**	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**
38	STI_5	Switches	R0017	Daño físico	Mal manejo de los equipos (falta de capacitación)	Perdida del equipo, además de la interrupción de los equipos conectados al Switches
39	STI_5	Switches	R0018	Errores de configuración	No se cuenta con manuales de configuración	Interrupción laboral por mala configuración del equipo.
40	STI_5	Switches	R0019	Polvo	Poco mantenimiento preventivo	Se congestiona y no reconoce las configuración generando interrupción en los servicios
41	STI_5	Switches	R0020	Negligencia del usuario	Poca coordinación en la institución.	Pérdida de comunicación entre la antena y el Switches interrumpiendo las actividades las máquinas conectadas.
42	STI_6	Antenas RADWIN				
43	APW_1	Sistema web V4CIMA	R0021	Acceso no autorizado a la información	Mal control de asignación de permisos en el sistema	Divulgar información confidencial a la competencia de la institución.
44	APW_1	Sistema web V4CIMA	R0022	Interrupción de servicios internos y externos.	Software muy antiguo.	Al actualizar se paralice el servicio, debido a incompatibilidad en el S.O.
45	APW_1	Sistema web V4CIMA	R0023	Empleados despedidos	Falta de gestión de identidades y accesos.	Divulgar la información a personas externa de la

						información o extorción con información confidencial que puede generar multas
46	APW_1	Sistema web V4CIMA	R0024	Usuario deshonesto	Poco control del personal	Alteración de la información para su propio beneficio.
47	APW_1	Sistema web V4CIMA	R0025	Saturación de operaciones en el software	Mala gestión de concurrencia de usuarios	Caídas del sistema en momentos críticos de la jornada laborar generando insatisfacción y lentitud en los procesos.
48	APW_12	Sistema de inventario (Kardex)	R0026	Errores de usuario	Falta de control de calidad al actualizar el sistema	Envió de reporte inconsistente a la Sunat

LOGO	LISTADO DE ESCENARIOS DE RIESGOS					
	Fase:	3	**Proceso**	1	**Actividad**	2
	Código:	**GR010**		**Páginas:**		4/3
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ACTIVO			ESCENARIO DE RIESGO			
N°	**ETIQUETA**	**NOMBRE**	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**
49	APW_12	Sistema de inventario (Kardex)	R0027	Usuario mal entrenado	Poca capacitación al personal de la institución en el manejo de los sistemas	Pérdida de tiempo del personal, retrasos de actividades e inconsistencia de datos
50	APW_12	Sistema de inventario (Kardex)	R0028	Usuario deshonesto	Poca seguridad en los sistemas	Alteración de información para su propio beneficio, cambio de costos, stock, etc., generando pérdidas a la institución.
51	STI_7	Dispositivos de comunicación	R0029	Fallos de equipo de comunicaciones	Conexión deficiente de cables	Perdida de horas de jornada laboral
52	SE_2	Aplicaciones móviles	R0030	Actualizaciones no controladas	Poco seguimiento de las actualizaciones de servicios de terceros	Interrupción de las diferentes actividades de las diferentes áreas, inconsistencia de datos.
53	APW_10	Aplicación móvil colegio	R0031	Errores de mantenimiento	Un mal control de calidad del software	Interrupción de las diferentes actividades de las diferentes áreas, inconsistencia de datos.
54	APW_11	Aplicación móvil de Admisión				
55	APW_5	Intranet web PREU	R0032	Corrupción de datos	Poco control de datos e integración entre aplicaciones.	Reclamos hacia la institución por información inconsistente que se muestra en las aplicaciones.
56	APW_6	Intranet web PRE CADETE				
57	APW_7	Intranet web COLEGIO				
58	APW_10	Aplicación móvil colegio				
59	APW_11	Aplicación móvil de Admisión				
60	SE_1	Servicio de intranet	R0033	Indisponibilidad del personal	No contar con documentación de los diferentes sistemas.	No poder brindar el soporte de actualizaciones o configuración
61	SE_2	aplicaciones móviles				

						de los sistemas debido a la falta del personal
62	APW_14	Moodle	R0034	Interrupción de servicios internos y externo	Poca banda ancha	Perdida de información e inconformidad de los usuarios.

LOGO	LISTADO DE ESCENARIOS DE RIESGOS					
	Fase:	3	**Proceso**	1	**Actividad**	2
	Código:	**GR010**		**Páginas:**		4/4
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

ACTIVO			ESCENARIO DE RIESGO			
N°	**ETIQUETA**	**NOMBRE**	**CÓDIGO**	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**
62	APW_14	Moodle	R0035	Errores de configuración	Configuración manual para la actualización.	Inconsistencia de información, generando pérdida de tiempo en hora de clases.
63	APW_15	Classroon	R0036	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	Problemas a la hora de acceder a los cursos y acceder a evaluaciones, archivos, etc.
64	APW_15	Classroon	R0037	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	Problemas a la hora de acceder a los cursos y acceder a evaluaciones, archivos, etc.
65	APW_3	Sistema web de resultados de la UNPRG	R0038	Interrupción de servicios internos y externos	No contar con documentación para reanudar los procesos.	Demorar a la hora de restaurar los servicios generando incomodidad e insatisfacción a los usuarios externos de la institución.
66	APW_5	Intranet web PREU				
67	APW_6	Intranet web PRE CADETE				
68	APW_7	7 Intranet web COLEGIO				
69	APW_9	Sistema web de inscripción				
70	APW_10	Aplicación móvil colegio				
71	APW_11	Aplicación móvil de Admisión				
72	APW_13	Sistema web de convocatoria				

LOGO	ANÁLISIS DE RIESGOS					
	Fase:	III	**Proceso**	**2**	**Actividad**	3
	Código:	**GR011**		**Páginas:**		4/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANALISIS			
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CÓDIGO	P	I	(PxI)	CAT.
1	STI_1	Servidor de aplicaciones	Corte de suministro eléctrico	No contar un UPS, para el suministro de energía	R0001	4	3	12	Alto
2	STI_2	Servidores de B.D							
3	STI _3	Servidor de archivos							
4	STI_4	Servidor del aula virtual							
5	STI_5	Switches							
6	STI_1	Servidor de aplicaciones	Desastres naturales	Mala ubicación de los servidores	R0002	5	5	25	Alto
7	STI_2	Servidores de B.D							
8	STI _3	Servidor de archivos							
9	STI_4	Servidor del aula virtual							
10	STI_5	Switches							
11	STI_1	Servidor de aplicaciones	Polvo	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	R0003	3	3	9	Moderado
11	STI_2	Servidores de B.D							
12	STI _3	Servidor de archivos							
13	STI_4	Servidor del aula virtual							
14	STI_5	Switches							
15	STI_1	Servidor de aplicaciones	Negligencia del usuario	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	R0004	3	3	9	Moderado
16	STI_2	Servidores de B.D							
17	STI _3	Servidor de archivos							
18	STI_4	Servidor del aula virtual							
19	STI_5	Switches							
20	STI_1	Servidor de aplicaciones	Negligencia del usuario.	Mala ubicación de la sala de servidores	R0005	2	4	8	Moderado
21	STI_2	Servidores de B.D							
22	STI _3	Servidor de archivos							
23	STI_4	Servidor del aula virtual							
24	STI_1	Servidor de aplicaciones	Acceso no autorizado	La mala ubicación de la sala de servidores, esta al acceso de personas que no pertenecen a la institución	R0006	1	4	4	Bajo
25	STI_2	Servidores de B.D							
26	STI _3	Servidor de archivos							
27	STI_4	Servidor del aula virtual							
28	STI_1	Servidor de aplicaciones	Instalación de programas no autorizados	No hay control de permisos de acceso al servidor (todos los desarrolladores	R0007	4	3	12	Alto

				incluyendo practicantes pueden instalar o desinstalar programas)					

LOGO	ANÁLISIS DE RIESGOS					
	Fase:	III	**Proceso**	**2**	**Actividad**	3
	Código:	**GR011**		**Páginas:**		4/2
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANALISIS			
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CÓDIGO	P	I	(PxI)	CAT.
29	STI_2	Servidores de B.D	Usuario mal entrenado	No hay control de permisos de acceso al servidor de base de datos (todos acceden con usuario y contraseña de administrador)	R0008	5	3	15	Alto
30	STI_3	Servidor de archivos	Penetración del sistema	Mala gestión de seguridad	R0009	2	4	8	Moderado
31	STI_6	Antenas RADWIN	Interrupción de servicios internos y externos	No tienen el control de construcción de edificios o instalaciones de antenas entre sus sedes	R0010	2	5	10	Moderado
32	APW_16	Facturador Sunat	Actualización no controlada	Incompatibilidad entre sistemas	R0011	3	3	9	Moderado
33	APW_16	Facturador Sunat	Errores de configuración	Poco control en las actualizaciones de los sistemas	R0012	3	2	6	Moderado
34	APW_16	Facturador Sunat	Interrupción de servicios internos y externos	Poca banda ancha	R0013	4	2	8	Moderado
35	APW_16	Facturador Sunat	Errores de configuración o actualización	Falta de control de calidad.	R0014	3	2	6	Moderado
36	APW_17	Sistema Concar	Interrupción de servicios	Software desfasado	R0015	3	3	9	Moderado
37	APW_17	Sistema Concar	Interrupción de servicios	Control inadecuado de las actualizaciones y de configuraciones del S. O	R0016	4	2	8	Moderado
38	STI_5	Switches	Daño físico	Mal manejo de los equipos (falta de capacitación)	R0017	2	2	4	Bajo
39	STI_5	Switches	Errores de configuración	No se cuenta con manuales de configuración	R0018	2	2	4	Bajo
40	STI_5	Switches	Polvo	Poco mantenimiento preventivo	R0019	3	3	9	Moderado
41	STI_5	Switches	Negligencia del usuario	Poca coordinación en la institución.	R0020	4	3	12	Alto
42	STI_6	Antenas RADWIN							

43	APW_1	Sistema web V4CIMA	Acceso no autorizado a la información	Mal control de asignación de permisos en el sistema	R0021	3	3	9	Moderado
44	APW_1	Sistema web V4CIMA	Interrupción de servicios internos y externos.	Software muy antiguo.	R0022	5	3	15	Alto
45	APW_1	Sistema web V4CIMA	Empleados despedidos	Falta de gestión de identidades y accesos.	R0023	4	1	4	Bajo

LOGO	**ANÁLISIS DE RIESGOS**					
	Fase:	III	**Proceso**	**2**	**Actividad**	3
	Código:	**GR011**		**Páginas:**		4/3
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

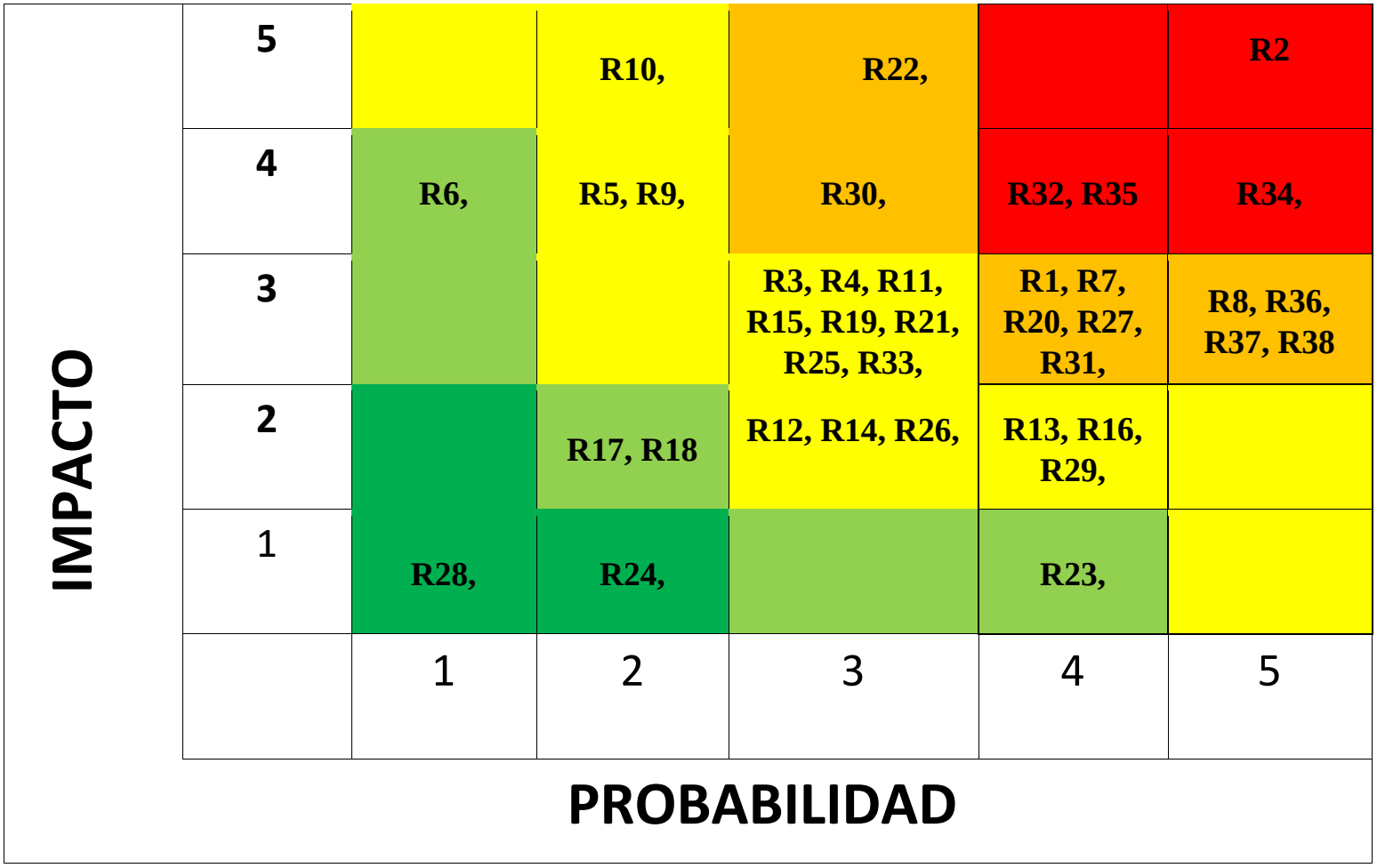
#	ACTIVO		RIESGO			ANALISIS			
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CÓDIGO	P	I	(PxI)	CAT.
46	APW_1	Sistema web V4CIMA	Usuario deshonesto	Poco control del personal	R0024	2	1	2	Muy bajo
47	APW_1	Sistema web V4CIMA	Saturación de operaciones en el software	Mala gestión de concurrencia de usuarios	R0025	3	3	9	Moderado
48	APW_12	Sistema de inventario (Kardex)	Errores de usuario	Falta de control de calidad al actualizar el sistema	R0026	3	2	6	Moderado
49	APW_12	Sistema de inventario (Kardex)	Usuario mal entrenado	Poca capacitación al personal de la institución en el manejo de los sistema	R0027	4	3	12	Alto
50	APW_12	Sistema de inventario (Kardex)	Usuario deshonesto	Poca seguridad en los sistemas	R0028	1	1	1	Muy bajo
51	STI_7	Dispositivos de comunicación	Fallos de equipo de comunicaciones	Conexión deficiente de cables	R0029	4	2	8	Moderado
52	SE_2	Aplicaciones móviles	Actualizaciones no controladas	Poco seguimiento de las actualizaciones de servicios de terceros	R0030	3	4	12	Alto
53	APW_10	Aplicación móvil colegio	Errores de mantenimiento	Un mal control de calidad del software	R0031	4	3	12	Alto
54	APW_11	Aplicación móvil de Admisión							
55	APW_5	Intranet web PREU	Corrupción de datos	Poco control de datos e integración entre aplicaciones.	R0032	4	4	16	Muy alto
56	APW_6	Intranet web PRE CADETE							

57	APW_7	Intranet web COLEGIO							
58	APW_10	Aplicación móvil colegio							
59	APW_11	Aplicación móvil de Admisión							
60	SE_1	Servicio de intranet	Indisponibilidad del personal	No contar con documentación de los diferentes sistemas.	R0033	3	3	9	Moderado
61	SE_2	aplicaciones móviles							
62	APW_14	Moodle	Interrupción de servicios internos y externo	Poca banda ancha	R0034	5	4	20	Muy alto

LOGO	**ANÁLISIS DE RIESGOS**					
	Fase:	III	**Proceso**	**2**	**Actividad**	3
	Código:	**GR011**		**Páginas:**		4/4
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANALISIS			
	ETIQUETA	ACTIVO	AMENAZA	VULNERABILIDAD	CÓDIGO	P	I	(PxI)	CAT.
62	APW_14	Moodle	Errores de configuración	Configuración manual para la actualización.	R0035	4	4	16	Muy alto
63	APW_15	Classroon	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	R0036	5	3	15	Alto
64	APW_15	Classroon	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	R0037	5	3	15	Alto
65	APW_3	Sistema web de resultados de la UNPRG	Interrupción de servicios internos y externos	No contar con documentación para reanudar los procesos.	R0038	5	3	15	Alto
66	APW_5	Intranet web PREU							
67	APW_6	Intranet web PRE CADETE							
68	APW_7	7 Intranet web COLEGIO							
69	APW_9	Sistema web de inscripción							
70	APW_10	Aplicación móvil colegio							
71	APW_11	Aplicación móvil de Admisión							
72	APW_13	Sistema web de convocatoria							

LOGO	POSICIONAR EL RIESGO					
	Fase:	III	Proceso	**3**	**Actividad**	2
	Código:	**GR012**		**Páginas:**		1/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__



LOGO	EVALUACIÓN DEL RIESGO					
	Fase:	III	Proceso	**3**	**Actividad**	2
	Código:	**GR012**		**Páginas:**		4/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANÁLISIS		EVALUACIÓN		
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	CATEGORÍA	A	T	VALOR
1	STI_1	Servidor de aplicaciones	Corte de suministro eléctrico	No contar un UPS, para el suministro de energía	R0001	12	Alto	3	9	Intolerable
2	STI_2	Servidores de B.D								
3	STI _3	Servidor de archivos								
4	STI_4	Servidor del aula virtual								
5	STI_5	Switches								
6	STI_1	Servidor de aplicaciones	Desastre naturales	Mala ubicación de los servidores	R0002	25	Alto	3	9	Intolerable
7	STI_2	Servidores de B.D								
8	STI _3	Servidor de archivos								
9	STI_4	Servidor del aula virtual								
10	STI_5	Switches								
11	STI_1	Servidor de aplicaciones	Polvo	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	R0003	9	Moderado	3	9	Tolerable
11	STI_2	Servidores de B.D								
12	STI _3	Servidor de archivos								
13	STI_4	Servidor del aula virtual								
14	STI_5	Switches								
15	STI_1	Servidor de aplicaciones	Negligencia del usuario	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	R0004	9	Moderado	3	9	Tolerable
16	STI_2	Servidores de B.D								
17	STI _3	Servidor de archivos								
18	STI_4	Servidor del aula virtual								
19	STI_5	Switches								
20	STI_1	Servidor de aplicaciones	Negligencia del usuario.	Mala ubicación de la sala de servidores	R0005	8	Moderado	3	9	Tolerable
21	STI_2	Servidores de B.D								
22	STI _3	Servidor de archivos								
23	STI_4	Servidor del aula virtual								
24	STI_1	Servidor de aplicaciones	Acceso no autorizado	La mala ubicación de la sala de servidores, esta al acceso de personas que no pertenecen a la institución	R0006	4	Bajo	3	6	Tolerable
25	STI_2	Servidores de B.D								
26	STI _3	Servidor de archivos								
27	STI_4	Servidor del aula virtual								

28	STI_1	Servidor de aplicaciones	Instalación de programas no autorizados	No hay control de permisos de acceso al servidor (todos los desarrolladores incluyendo practicantes pueden instalar o desinstalar programas)	R0007	12	Alto	3	9	Intolerable

LOGO	**EVALUACIÓN DEL RIESGO**					
	Fase:	III	Proceso	**3**	**Actividad**	2
	Código:	**GR012**		**Páginas:**		4/2
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANÁLISIS		EVALUACIÓN		
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	CATEGORÍA	A	T	VALOR
29	STI_2	Servidores de B.D	Usuario mal entrenado	No hay control de permisos de acceso al servidor de base de datos (todos acceden con usuario y contraseña de administrador)	R0008	15	Alto	4	9	Intolerable
30	STI_3	Servidor de archivos	Penetración del sistema	Mala gestión de seguridad	R0009	8	Moderado	4	9	Tolerable
31	STI_6	Antenas RADWIN	Interrupción de servicios internos y externos	No tienen el control de construcción de edificios o instalaciones de antenas entre sus sedes	R0010	10	Moderado	4	9	Intolerable
32	APW_16	Facturador Sunat	Actualización no controlada	Incompatibilidad entre sistemas	R0011	9	Moderado	4	9	Tolerable
33	APW_16	Facturador Sunat	Errores de configuración	Poco control en las actualizaciones de los sistemas	R0012	6	Moderado	4	8	Tolerable
34	APW_16	Facturador Sunat	Interrupción de servicios internos y externos	Poca banda ancha	R0013	8	Moderado	4	9	Tolerable
35	APW_16	Facturador Sunat	Errores de configuración o actualización	Falta de control de calidad.	R0014	6	Moderado	4	8	Tolerable
36	APW_17	Sistema Concar	Interrupción de servicios	Software desfasado	R0015	9	Moderado	4	9	Tolerable
37	APW_17	Sistema Concar	Interrupción de servicios	Control inadecuado de las actualizaciones y de configuraciones del S. O	R0016	8	Moderado	4	9	Tolerable
38	STI_5	Switches	Daño físico	Mal manejo de los equipos (falta de capacitación)	R0017	4	Bajo	4	5	Tolerable
39	STI_5	Switches	Errores de configuración	No se cuenta con manuales de configuración	R0018	4	Bajo	4	5	Tolerable

40	STI_5	Switches	Polvo	Poco mantenimiento preventivo	R0019	9	Moderado	4	9	Tolerable
41	STI_5	Switches	Negligencia del usuario	Poca coordinación en la institución.	R0020	12	Alto	4	9	Intolerable
42	STI_6	Antenas RADWIN								
43	APW_1	Sistema web V4CIMA	Acceso no autorizado a la información	Mal control de asignación de permisos en el sistema	R0021	9	Moderado	4	9	Tolerable
44	APW_1	Sistema web V4CIMA	Interrupción de servicios internos y externos.	Software muy antiguo.	R0022	15	Alto	4	9	Intolerable
45	APW_1	Sistema web V4CIMA	Empleados despedidos	Falta de gestión de identidades y accesos.	R0023	4	Bajo	4	6	Aceptable

LOGO	EVALUACIÓN DEL RIESGO					
	Fase:	III	Proceso	**3**	**Actividad**	2
	Código:	**GR012**		**Páginas:**		4/3
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANÁLISIS		EVALUACIÓN		
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	CATEGORÍA	A	T	VALOR
46	APW_1	Sistema web V4CIMA	Usuario deshonesto	Poco control del personal	R0024	2	Muy bajo	2	5	Aceptable
47	APW_1	Sistema web V4CIMA	Saturación de operaciones en el software	Mala gestión de concurrencia de usuarios	R0025	9	Moderado	4	9	Tolerable
48	APW_12	Sistema de inventario (Kardex)	Errores de usuario	Falta de control de calidad al actualizar el sistema	R0026	6	Moderado	4	6	Tolerable
49	APW_12	Sistema de inventario (Kardex)	Usuario mal entrenado	Poca capacitación al personal de la institución en el manejo de los sistema	R0027	12	Alto	4	9	Intolerable
50	APW_12	Sistema de inventario (Kardex)	Usuario deshonesto	Poca seguridad en los sistemas	R0028	1	Muy bajo	1	5	Aceptable
51	STI_7	Dispositivos de comunicación	Fallos de equipo de comunicaciones	Conexión deficiente de cables	R0029	8	Moderado	4	8	Tolerable
52	SE_2	Aplicaciones móviles	Actualizaciones no controladas	Poco seguimiento de las actualizaciones de servicios de terceros	R0030	12	Alto	4	9	Intolerable
53	APW_10	Aplicación móvil colegio	Errores de mantenimiento	Un mal control de calidad del software	R0031	12	Alto	4	8	Intolerable
54	APW_11	Aplicación móvil de Admisión								
55	APW_5	Intranet web PREU	Corrupción de datos	Poco control de datos e integración entre aplicaciones.	R0032	16	Muy alto	4	8	Intolerable
56	APW_6	Intranet web PRE CADETE								
57	APW_7	Intranet web COLEGIO								
58	APW_10	Aplicación móvil colegio								
59	APW_11	Aplicación móvil de Admisión								
60	SE_1	Servicio de intranet	Indisponibilidad del personal	No contar con documentación de los diferentes sistemas.	R0033	9	Moderado	4	9	Tolerable
61	SE_2	aplicaciones móviles								

62	APW_14	Moodle	Interrupción de servicios internos y externo	Poca banda ancha	R0034	20	Muy alto	4	9	Intolerable

LOGO	EVALUACIÓN DEL RIESGO					
	Fase:	III	Proceso	**3**	**Actividad**	2
	Código:	**GR012**		**Páginas:**		4/4
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			ANÁLISIS		EVALUACIÓN		
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	CATEGORÍA	A	T	VALOR
62	APW_14	Moodle	Errores de configuración	Configuración manual para la actualización.	R0035	16	Muy alto	4	9	Intolerable
63	APW_15	Classroon	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	R0036	15	Alto	4	9	Intolerable
64	APW_15	Classroon	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	R0037	15	Alto	4	9	Intolerable
65	APW_3	Sistema web de resultados de la UNPRG	Interrupción de servicios internos y externos	No contar con documentación para reanudar los procesos.	R0038	15	Alto	4	10	Intolerable
66	APW_5	Intranet web PREU								
67	APW_6	Intranet web PRE CADETE								
68	APW_7	7 Intranet web COLEGIO								
69	APW_9	Sistema web de inscripción								
70	APW_10	Aplicación móvil colegio								
71	APW_11	Aplicación móvil de Admisión								
72	APW_13	Sistema web de convocatoria								

LOGO	TRATAMIENTO DE RIESGOS					
	Fase:	IV	**Proceso**	**1**	**Actividad:**	1
	Código:	**GR013**		**Páginas:**		4/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			EVALUACIÓN		TRATAMIENTO
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	VALOR	
1	STI_1	Servidor de aplicaciones	Corte de suministro eléctrico	No contar un UPS, para el suministro de energía	R0001	12	Intolerable	Mitigar
2	STI_2	Servidores de B.D						
3	STI _3	Servidor de archivos						
4	STI_4	Servidor del aula virtual						
5	STI_5	Switches						
6	STI_1	Servidor de aplicaciones	Desastre naturales	Mala ubicación de los servidores	R0002	25	Intolerable	Mitigar
7	STI_2	Servidores de B.D						
8	STI _3	Servidor de archivos						
9	STI_4	Servidor del aula virtual						
10	STI_5	Switches						
11	STI_1	Servidor de aplicaciones	Polvo	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	R0003	9	Tolerable	Mitigar
11	STI_2	Servidores de B.D						
12	STI _3	Servidor de archivos						
13	STI_4	Servidor del aula virtual						
14	STI_5	Switches						
15	STI_1	Servidor de aplicaciones	Negligencia del usuario	Poco mantenimiento preventivo en los equipos que pertenece al área de T.I	R0004	9	Tolerable	Mitigar
16	STI_2	Servidores de B.D						
17	STI _3	Servidor de archivos						
18	STI_4	Servidor del aula virtual						
19	STI_5	Switches						
20	STI_1	Servidor de aplicaciones	Negligencia del usuario.	Mala ubicación de la sala de servidores	R0005	8	Tolerable	Mitigar
21	STI_2	Servidores de B.D						
22	STI _3	Servidor de archivos						
23	STI_4	Servidor del aula virtual						
24	STI_1	Servidor de aplicaciones	Acceso no autorizado	La mala ubicación de la sala de servidores, esta al acceso de personas que no pertenecen a la institución	R0006	4	Tolerable	Mitigar
25	STI_2	Servidores de B.D						
26	STI _3	Servidor de archivos						
27	STI_4	Servidor del aula virtual						

28	STI_1	Servidor de aplicaciones	Instalación de programas no autorizados	No hay control de permisos de acceso al servidor (todos los desarrolladores incluyendo practicantes pueden instalar o desinstalar programas)	R0007	12	Intolerable	Mitigar

a

LOGO	**TRATAMIENTO DE RIESGOS**					
	Fase:	IV	**Proceso**	**1**	**Actividad:**	1
	Código:	**GR013**		**Páginas:**		4/2
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			EVALUACIÓN		TRATAMIENTO
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	VALOR	
29	STI_2	Servidores de B.D	Usuario mal entrenado	No hay control de permisos de acceso al servidor de base de datos (todos acceden con usuario y contraseña de administrador)	R0008	15	Intolerable	Mitigar
30	STI_3	Servidor de archivos	Penetración del sistema	Mala gestión de seguridad	R0009	8	Tolerable	Mitigar
31	STI_6	Antenas RADWIN	Interrupción de servicios internos y externos	No tienen el control de construcción de edificios o instalaciones de antenas entre sus sedes	R0010	10	Intolerable	Aceptar
32	APW_16	Facturador Sunat	Actualización no controlada	Incompatibilidad entre sistemas	R0011	9	Tolerable	Aceptar
33	APW_16	Facturador Sunat	Errores de configuración	Poco control en las actualizaciones de los sistemas	R0012	6	Tolerable	Aceptar
34	APW_16	Facturador Sunat	Interrupción de servicios internos y externos	Poca banda ancha	R0013	8	Tolerable	Mitigar
35	APW_16	Facturador Sunat	Errores de configuración o actualización	Falta de control de calidad.	R0014	6	Tolerable	Aceptar
36	APW_17	Sistema Concar	Interrupción de servicios	Software desfasado	R0015	9	Tolerable	Aceptar
37	APW_17	Sistema Concar	Interrupción de servicios	Control inadecuado de las actualizaciones y de configuraciones del S. O	R0016	8	Tolerable	Aceptar
38	STI_5	Switches	Daño físico	Mal manejo de los equipos (falta de capacitación)	R0017	4	Tolerable	Mitigar
39	STI_5	Switches	Errores de configuración	No se cuenta con manuales de configuración	R0018	4	Tolerable	Aceptar
40	STI_5	Switches	Polvo	Poco mantenimiento preventivo	R0019	9	Tolerable	Mitigar

41	STI_5	Switches	Negligencia del usuario	Poca coordinación en la institución.	R0020	12	Intolerable	Aceptar
42	STI_6	Antenas RADWIN						
43	APW_1	Sistema web V4CIMA	Acceso no autorizado a la información	Mal control de asignación de permisos en el sistema	R0021	9	Tolerable	Mitigar
44	APW_1	Sistema web V4CIMA	Interrupción de servicios internos y externos.	Software muy antiguo.	R0022	15	Intolerable	Aceptar
45	APW_1	Sistema web V4CIMA	Empleados despedidos	Falta de gestión de identidades y accesos.	R0023	4	Aceptable	Mitigar

LOGO	TRATAMIENTO DE RIESGOS					
	Fase:	IV	**Proceso**	**1**	**Actividad:**	1
	Código:	**GR013**		**Páginas:**		4/3
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			EVALUACIÓN		TRATAMIENTO
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	VALOR	
46	APW_1	Sistema web V4CIMA	Usuario deshonesto	Poco control del personal	R0024	2	Aceptable	Mitigar
47	APW_1	Sistema web V4CIMA	Saturación de operaciones en el software	Mala gestión de concurrencia de usuarios	R0025	9	Tolerable	Mitigar
48	APW_12	Sistema de inventario (Kardex)	Errores de usuario	Falta de control de calidad al actualizar el sistema	R0026	6	Tolerable	Mitigar
49	APW_12	Sistema de inventario (Kardex)	Usuario mal entrenado	Poca capacitación al personal de la institución en el manejo de los sistema	R0027	12	Intolerable	Mitigar
50	APW_12	Sistema de inventario (Kardex)	Usuario deshonesto	Poca seguridad en los sistemas	R0028	1	Aceptable	Mitigar
51	STI_7	Dispositivos de comunicación	Fallos de equipo de comunicaciones	Conexión deficiente de cables	R0029	8	Tolerable	Aceptar
52	SE_2	Aplicaciones móviles	Actualizaciones no controladas	Poco seguimiento de las actualizaciones de servicios de terceros	R0030	12	Intolerable	Mitigar
53	APW_10	Aplicación móvil colegio	Errores de mantenimiento	Un mal control de calidad del software	R0031	12	Intolerable	Mitigar
54	APW_11	Aplicación móvil de Admisión						
55	APW_5	Intranet web PREU	Corrupción de datos	Poco control de datos e integración entre aplicaciones.	R0032	16	Intolerable	Mitigar
56	APW_6	Intranet web PRE CADETE						
57	APW_7	Intranet web COLEGIO						
58	APW_10	Aplicación móvil colegio						
59	APW_11	Aplicación móvil de Admisión						
60	SE_1	Servicio de intranet	Indisponibilidad del personal	No contar con documentación de los diferentes sistemas.	R0033	9	Tolerable	Mitigar
61	SE_2	aplicaciones móviles						
62	APW_14	Moodle	Interrupción de servicios internos y externo	Poca banda ancha	R0034	20	Intolerable	Transferir

LOGO	TRATAMIENTO DE RIESGOS					
	Fase:	IV	**Proceso**	**1**	**Actividad :**	1
	Código:	**GR013**		**Páginas:**		4/4
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

#	ACTIVO		RIESGO			EVALUACIÓN		TRATAMIENTO
	ETIQUETA	ACTIVO	RIESGO	VULNERABILIDAD	CODIGO	PXI	VALOR	
63	APW_14	Moodle	Errores de configuración	Configuración manual para la actualización.	R0035	16	Intolerable	Mitigar
65	APW_15	Classroon	Interrupción de servicios internos y externos	Poco control de la plataforma tercerizado	R0036	15	Intolerable	Mitigar
66	APW_3	Sistema web de resultados de la UNPRG	Interrupción de servicios internos y externos	No contar con documentación para reanudar los procesos.	R0038	15	Intolerable	Mitigar
67	APW_5	Intranet web PREU						
68	APW_6	Intranet web PRE CADETE						
69	APW_7	7 Intranet web COLEGIO						
70	APW_9	Sistema web de inscripción						
71	APW_10	Aplicación móvil colegio						
72	APW_11	Aplicación móvil de Admisión						
73	APW_13	Sistema web de convocatoria						

LOGO	PROPUESTA DEL PLAN DE ACCIÓN					
	Fase:	I4	**Proceso**	**1**	**Actividad:**	2
	Código:	**GR014**		**Páginas:**		1/1
NOMBRE DE LA I.E.P	**Versión**:	0.1		**Fecha de aplicación:**		__/__/__

"CAPACITACIÓN PERSONAL DE DESARROLLO"	001

OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*

Presentar el servicio de asesoría de manera remota a todo el equipo de desarrollo (5 desarrolladores) de la Institución Educativa "ABC" en las siguientes tecnologías:

1. Angular 10
2. Bootstrap 4
3. Java 11 - SPRING BOOT
4. Seguridad en desarrollo y base de datos postgres 12
5. Docker
6. Integración continua
7. Seguridad en aplicaciones informáticas.

RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
JHONY AGAPITO GUEVARA	20 días
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
[R0021], [R0023], [R0024], [R0025], [R0026], [R0028], [R0033], [R0030]	
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
- 5 computadoras - Internet	Tiempo= 80 Costo por hora= S/30 INC. IGV. S./ 2400

PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*

- PO01. Gestionar el servicio educativo
- PO02.Gestionar los recursos para los aprendizajes.
- PO05. Proceso de admisión. (PE)
- PO06. Proceso de atención al cliente (PO)
- PO07. Proceso de matrícula (PO)

OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*

Todas las clases serán grabadas, teniéndose como entregable los vídeos de cada una de las sesiones. En cada sesión se codifica una parte de la plataforma la cual se tomará como guía para el futuro desarrollo del mismo.

1. Se reunirá con el jefe del proyecto para tener el alcance del mismo.
2. El equipo tendrá diseñada la base de datos que brinde soporte al proyecto.
3. Se brindará varias sesiones explicando todas las tecnologías y cada sesión será grabada para su posterior revisión de cada uno de los integrantes del equipo de desarrollo.
4. Se hará una segunda explicación, como refuerzo del punto anterior y en esta etapa, cada participante se le asignará un CRUD (Crear, Leer, Actualizar y Borrar por sus iniciales en inglés), donde pondrá en ejecución los conocimientos aprendidos en el punto 3.
5. Se revisará, según coordinación, en el tiempo definido y en coordinación con el jefe del proyecto.

“CAPACITACIÓN AL PERSONAL DE REDES”	002
OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*	
Presentar el servicio de consultoría a todo el equipo de Seguridad y Redes de la Institución Educativa CIMA en las siguientes tecnologías: 1. Administración de Servidor con CENTOS SERVER 2. Gestión de Switch CISCO 3. Servidor Proxy PFSense 4. Seguridad Perimetral	
RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
JHONY AGAPITO GUEVARA	1 mes (120 horas)
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
[R0007], [R0008], [R0009], [R0017]	MODERADO
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
-Servidores -MVARE	120 horas * S/70
PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*	
PO02.Gestionar los recursos para los aprendizajes. PO04. Gestionar la infraestructura educativa PO05. Proceso de admisión. (PE) PO06. Proceso de atención al cliente (PO) PO07. Proceso de matrícula (PO) PS02. Administrar los recursos financieros	
OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*	
- Uno de los inconvenientes que se tiene, es que todos los usuarios del área de TI cuentan con acceso en modo administrador a los diferentes servidores que cuenta la institución. - El crecimiento institucional, se ha requerido adquirir equipos de alta gama para dar soporte a todos y cada uno de los procesos y áreas que conforman dicha institución. Esto implica que el personal responsable que administra los equipos se debe capacitar para poder gestionar de manera óptima los equipos. -	

“IMPLEMENTACIÓN DE FIBRA ÓPTICA”	003

OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*

Implementar una fibra óptica para así evitar las interrupciones constantes de los diferentes servicios que son utilizados por el personal de la institución “ABC”

RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
JHONY AGAPITO GUEVARA	60 días
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
[R0013], [R0025], [R0034]	MUY ALTO
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
Se contratará a una empresa para mejorar los servicio que brinda el área de TI a las diferentes sedes.	S/1521.86 mensual Sin. IGV.

PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*

Con la implementación de la fibra óptica en la sede principal, todos los servicios ofrecidos por el área de TI que hacen uso de banda ancha, mejorarán considerablemente.

- PE02. Gestionar el desarrollo e innovación
- PO01. Gestionar el servicio educativo
- PO02.Gestionar los recursos para los aprendizajes.

OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*

Inconveniente:

- Debido a las constantes caídas de los servicios de los operadores como claro y movistar, la cual genera un inconveniente a la hora de entrar los servicios de la institución educativa, además de tener en cuenta que el pago que se hace a estos operadores es un pago similar por el plan que se está planteando.
- Cuando el servicio que ofrecen estas operadoras cae, las actividades que se realizan en las diferentes sedes también paralizan porque dependen del internet la cual es ofrecido desde la sede principal.
- Los servicios brindados por estos operadores muchas veces generan saturación en la banda ancha, provocando una lentitud en los servicios utilizados por las diferentes áreas de las instituciones.

Para la contratación de la empresa que brinde el servicio de fibra óptica se debe de considerar lo siguiente:

- Que ofrezcan una línea dedicada
- Ancho de Banda al 100%
- Capacitaciones al personal de la institución por la empresa “XYZ”.
- Tengan sus propios criterios de seguridad.

“CAPACITACIÓN PERSONAL DE DESARROLLO”	004

OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*

Presentar el servicio de asesoría de manera remota a todo el equipo de desarrollo (5 desarrolladores) de la Institución Educativa “ABC” en las siguientes tecnologías:
1. Angular 10
2. Bootstrap 4
3. Java 11 - SPRING BOOT
4. Seguridad en desarrollo y base de datos postgres 12
5. Docker
6. Integración continua
7. Seguridad en aplicaciones informáticas.

RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
JHONY AGAPITO GUEVARA	20 días
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
[R0021], [R0023], [R0024], [R0025], [R0026], [R0028], [R0033], [R0030]	
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
- 5 computadoras - Internet	Tiempo= 80 Costo por hora= S/30 INC. IGV. S./ 2400

PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*

- PO05. Proceso de admisión. (PE)
- PO06. Proceso de atención al cliente (PO)
- PO07. Proceso de matrícula (PO)
- PS01. Gestionar Recursos Humanos
- PS02. Administrar los recursos financieros

OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*

Todas las clases serán grabadas, teniéndose como entregable los vídeos de cada una de las sesiones. En cada sesión se codifica una parte de la plataforma la cual se tomará como guía para el futuro desarrollo del mismo.

6. Se reunirá con el jefe del proyecto para tener el alcance del mismo.
7. El equipo tendrá diseñada la base de datos que brinde soporte al proyecto.
8. Se brindará varias sesiones explicando todas las tecnologías y cada sesión será grabada para su posterior revisión de cada uno de los integrantes del equipo de desarrollo.
9. Se hará una segunda explicación, como refuerzo del punto anterior y en esta etapa, cada participante se le asignará un CRUD (Crear, Leer, Actualizar y Borrar por sus iniciales en inglés), donde pondrá en ejecución los conocimientos aprendidos en el punto 3.
10. Se revisará, según coordinación, en el tiempo definido y en coordinación con el jefe del proyecto.

“Reubicación de la sala de servidores”	005

OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*

El objetivo de esta propuesta es reubicar la sala de servidores con el fin de asegurar este activo, debido a que es muy importante para la organización, tanto por el costo y por la información que en ella se almacena.

RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
JHONY AGAPITO GUEVARA	1 mes.
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
[R0001], [R0002], [R0005], [R0006]	MUY ALTO
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
-Transporte -Evaluar la nueva ubicación.	S/.1500 * 3 personas *1 mes

PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*

Todos los procesos de la institución se verían afectados.

- PE04. Proceso de admisión.
- PO01. Gestionar el servicio educativo
- PO02.Gestionar los recursos para los aprendizajes.
- PO03. Gestionar el desarrollo del personal de servicio en las instituciones educativa
- PO04. Gestionar la infraestructura educativa
- PO05. Proceso de admisión. (PE)
- PO06. Proceso de atención al cliente (PO)
- PO07. Proceso de matrícula (PO)
- PS01. Gestionar Recursos Humanos
- PS02. Administrar los recursos financieros
- PS03. Administrar sistema logístico.

OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*

La empresa requiere reubicar el centro de datos por los siguientes motivos

- El lugar donde se encuentra ubicado está rodeado por diversas tuberías de agua, la ruptura de alguna de ella puede generar considerables pérdidas para la institución.
- El lugar donde se encuentra ubicado puede generar sobre calentamiento debido a que el sol le da directamente a la sala de servidores.
- Se encuentra ubicado al acceso de todo el personal de la institución, además de personas ajenas a ella.

Por lo antes mencionado se debe de reubicar el centro de datos a un lugar más seguro, por el bienestar de la institución.

Adicionalmente se debe realizar la compra de un UPS, debido a los constantes cortes de fluido eléctrico que existe en las diferentes sedes que tiene la institución.

“CAPACITACIÓN AL PERSONAL DE LA INSTITUCIÓN”	006

OBJETIVO: *Describe el objetivo principal del plan de acción para la empresa.*

Implementar programas de capacitación al personal, según segregación de funciones para evitar alteraciones accidentales de información, con el objetivo de reducir el nivel de frecuencia de alteraciones accidentales de información provocadas por desconocimiento del usuario.

RESPONSABLE: *Encargado de la ejecución del plan.*	**TIEMPO:** *Tiempo que tomará la ejecución del proyecto.*
JHONY AGAPITO GUEVARA	1 semana
RIESGOS: *Se hace referencia a los diferentes riesgos que serán tratados con esta propuesta.*	**NIVEL DEL RIESGO:** *Se debe de indicar en nivel más alto de los riesgos que serán tratados con la propuesta.*
R0027	MODERADO
RECURSOS: ***Recursos que se van a utilizar a la hora llevar a cabo el plan de acción.***	**PRESUPUESTO:** *Número de personas*tiempo*costo hora*
-1 computadoras	El mismo personal lo realiza .

PROCESOS Y ACTIVOS BENEFICIADOS: *Listado de los procesos o activos que serán beneficiados a la hora de poner en marcha el plan de acción.*

- PE04. Proceso de admisión.
- PO01. Gestionar el servicio educativo
- PO02.Gestionar los recursos para los aprendizajes.
- PO03. Gestionar el desarrollo del personal de servicio en las instituciones educativa
- PO05. Proceso de admisión. (PE)
- PO06. Proceso de atención al cliente (PO)
- PO07. Proceso de matrícula (PO)
- PS01. Gestionar Recursos Humanos
- PS02. Administrar los recursos financieros
- PS03. Administrar sistema logístico.

OBSERVACIÓN: *Listado de observaciones o anexos que se tenga para llevar a cabo la propuesta.*

- La institución “ABC” requiere desarrollar una programación de capacitaciones dirigida a los usuarios, antiguos y nuevos, de las diferentes áreas que hace uso de los aplicativos informáticos. De lo contrario, los usuarios seguirán cometiendo errores al registrar sus operaciones en el sistema, causando daño a la integridad de la información. En tal sentido, considerando la necesidad de evitar la corrupción de la información, se realiza el presente proyecto

ANEXO V: VALIDACIÓN DE EXPERTO

ACTIVIDAD	EXPERTO 1				EXPERTO 2				EXPERTO 3			
	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
Establecer contexto externo.	4	4	4	4	4	4	4	4	4	4	4	4
Establecer el contexto interno.	4	3	3	4	4	4	4	4	4	3	4	4
Criterios de valoración de activo	4	4	4	4	4	4	4	4	4	4	4	4
Criterios de evaluación de activo	4	3	4	4	4	4	4	4	4	4	4	4
Criterios de aceptación de los riesgos	4	3	4	4	4	4	4	4	4	4	4	4
Identificación de los procesos I.E	4	4	4	4	4	4	4	4	4	4	4	4
Identificación de los activos de TI	4	4	4	4	4	4	4	4	4	4	4	4
Valoración de activos.	3	3	3	3	4	4	4	4	4	4	4	4
Escenarios de riesgos	4	4	4	4	4	4	4	4	4	4	4	4
Análisis de riesgos	4	4	4	4	4	4	4	4	4	4	4	4
Evaluación del riesgo	3	3	3	3	4	4	4	4	4	4	4	4
Identificación del tratamiento	4	4	4	4	4	4	4	4	4	4	4	4
Establecer plan de acción	4	4	4	4	4	4	4	4	4	4	4	4
Seguimiento del plan de acción	4	4	4	4	4	4	4	4	4	4	4	4
Comunicación del riesgo.	4	4	3	3	4	4	4	4	4	4	4	4

- **LOMPARTE ALVARADO RÓMULO**

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
FASE I: ESTABLECER EL CONTEXTO INTERNOS, EXTERNOS Y CRITERIOS	Establecer el contexto externo.	4	4	4	4	
	Establecer el contexto interno.	4	4	4	4	
	Criterios de valoración de activo.	4	4	4	4	
	Criterios de evaluación de activo.	4	4	4	4	
	Criterios de aceptación de los riesgos.	4	4	4	4	
FASE II: ANÁLISIS ESTRATÉGICO	Identificación de procesos.	4	4	4	4	
	Identificación de activos de TI.	4	4	4	4	
	Valoración de Activos	4	4	4	4	
FASE III: EVALUACIÓN DEL RIESGO	Escenarios de riesgos	4	4	4	4	
	Análisis de riesgos	4	4	4	4	
	Evaluación del riesgo	4	4	4	4	
FASE IV: TRATAMIENTO DE RIESGOS	Identificación del tratamiento	4	4	4	4	
	Establecer plan de acción.	4	4	4	4	
FASE V: SEGUIMIENTO Y REVISIÓN	Seguimiento del plan de acción.	4	4	4	4	
FASE VI: OMUNICACION DEL RIESGO	Comunicación del riesgo.	4	4	4	4	

X	ACEPTADO
	OBSERVADO
	DISCONFORME

FIRMA

- **VILLACORTA CHAVEZ PAUL MARTIN**

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
FASE I: ESTABLECER EL CONTEXTO INTERNOS, EXTERNOS Y CRITERIOS	Establecer el contexto externo.	4	4	4	4	
	Establecer el contexto interno.	4	3	3	4	
	Criterios de valoración de activo.	4	4	4	4	
	Criterios de evaluación de activo.	4	3	4	4	
	Criterios de aceptación de los riesgos.	4	3	4	4	
FASE II: ANÁLISIS ESTRATÉGICO	Identificación de procesos.	4	4	4	4	
	Identificación de activos de TI.	4	4	4	4	
	Valoración de Activos	3	3	3	3	
FASE III: EVALUACIÓN DEL RIESGO	Escenarios de riesgos	4	4	4	4	
	Análisis de riesgos	4	4	4	4	
	Evaluación del riesgo	3	3	3	3	**Debe contener las reservas de contingencia y de gestión.**
FASE IV: TRATAMIENTO DE RIESGOS	Identificación del tratamiento	4	4	4	4	
	Establecer plan de acción.	4	4	4	4	
FASE V: SEGUIMIENTO Y REVISIÓN	Seguimiento del plan de acción.	4	4	4	4	
FASE VI: OMUNICACION DEL RIESGO	Comunicación del riesgo.	4	4	3	3	

X	**ACEPTADO**
	OBSERVADO
	DISCONFORME

FIRMA

- **DIAZ ESPINO MIGUEL ANGEL**

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
FASE I: ESTABLECER EL CONTEXTO INTERNOS, EXTERNOS Y CRITERIOS	Establecer el contexto externo.	4	4	4	4	
	Establecer el contexto interno.	4	3	4	4	Mejorar redacción Partes Interesadas
	Establecer criterios de valoración de activo.	4	4	4	4	
	Establecer criterios de evaluación de activo.	4	4	4	4	
	Establecer criterios de aceptación de los riesgos.	4	4	4	4	
FASE II: ANÁLISIS ESTRATÉGICO	Identificación de procesos de I.E.P.	4	4	4	4	
	Identificación de activos de TI.	4	4	4	4	
	Valoración de activos de TI.	4	4	4	4	
FASE III: EVALUACIÓN DEL RIESGO	Identificación de amenazas.	4	4	4	4	
	Escenarios de riesgos	4	4	4	4	
	Análisis de riesgos (Probabilidad x Impacto)	4	4	4	4	
	Posicionar el riesgo	4	4	4	4	
	Valoración de los riesgos	4	4	4	4	
FASE IV: TRATAMIENTO DE RIESGOS	Identificación del tratamiento	4	4	4	4	
	Establecer plan de acción.	4	4	4	4	
FASE V: SEGUIMIENTO Y REVISIÓN	Seguimiento del plan de acción.	4	4	4	4	
FASE VI: COMUNICACIÓN DEL RIESGO	Comunicación del riesgo.	4	4	4	4	

X	**ACEPTADO**
	OBSERVADO
	DISCONFORME

FIRMA

Mgtr. Miguel Angel Diaz Espino

ANEXO VI: PERFILES DE LOS EXPERTOS

PERFIL DE EXPERTO	
	**Lomparte Alvarado Rómulo** Magister en Dirección de Empresas por la Universidad Peruana de Ciencias Aplicadas. Licenciado en computación por la Universidad Nacional Mayor de San Marcos. Business Management por Harvard University. Gerencia de Proyectos de Sistemas de Información por ESAN. Tiene certificaciones IRCA International Register of Certificated Auditors), CGEIT (Certified in the Governance of Enterprise IT), CRISC (Certified in Risk and Information Systems Control), ISO/IEC 27002, CRMA (Certification in Risk Management Assurance), CISM (Certified Information Security Manager), COBIT 5 y CISA (Certified Information Systems Auditor) y Capacitation's en Massachussetts Instiute of Technology (MIT) – OCW, Bureau Veritas, IBM del Peru, IBM de México, New Horizons, Arthur Andersen, COSAPI DATA y SAP.

DATOS ACADÉMICOS

- **ISACA**
  Certified Data Privacy Solutions Engineer™ (CDPSE™)
  COBIT 5 Foundations
  CISM
  Certified Information Security Manager® (CISM)
  CRMA
  ISO 27002
  Certified in Risk and Information Systems Control™ (CRISC)
  Certified in the Governance of Enterprise IT® (CGEIT)
  Certified Information Systems Auditor® (CISA)

- **APMG Accredited Trainer**
  Certified Information Systems Auditor® (CISA)
  Certified in the Governance of Enterprise IT® (CGEIT)

- **Harvard University**
  Business Management

- **Universidad Peruana de Ciencias Aplicadas**
  Master Dirección de Negocios

- **ESAN**
  Gerencia de Proyectos de Sistemas de Información

- **Universidad Nacional Mayor de San Marcos**
  Disciplina académica Computing

EXPERIENCIA LABORAL

- **IT Corporate Manager**
  EPENSA

- **Teacher of POST GRADE SCHOOL**
  Universidad del Pacifico
  Teacher of IT Governance course.

- **Consultor Senior**
  Software & Consulting S.A.C.

- **Teacher**
  BS Grupo
  Teacher of course ISO/27001

- **IT Audit Manager**
  Grupo Pacifico
  Responsible of reviewing and evaluation controls, application systems, IT procedures, hardware and software, their utilization, efficiency and security; work evaluation of multiple platforms environments, systems development tools, evaluation of development of IT projects and ISO17799. ACHIEVEMENTS: 1. Optimization of works of the Internal Audit Unit through implementation and administration of automated tools. 2. Implementation of quality control system for projects of Internal Audit. 3. Consulting at all levels of IT governance using COBIT and ITIL.

- **IT Security Consultant, Senior**
  ETEK International
  Responsible of advising to management and assessment IT security processes in customer companies based on ISO/27002. 1 ETEK-Perú 2 ETEK-Colombia 3 ETEK-USA 4 ETEK-Chile 5 ETEK-Argentina 6 ETEK-Brasil

- **IT Corporate Auditor**
  Yanbal International
  Responsible of reviewing and evaluation controls, application systems, IT procedures, hardware and software, their utilization, efficiency and security; work evaluation of multiple platforms environments (AS/400, Client/Server and Internet), systems development tools, evaluation of development of IT projects and ISO17799. In charge of execution of audits of our corporation enterprises in both Peru and abroad. 1 Unique - Perú 2 Yanbal (Ecuador, Colombia, Venezuela, México, Guatemala, USA, Bolivia y Spain)

- **Teacher of POST GRADE SCHOOL & CONTINUING EDUCATION**
  Universidad Privada del Norte
  Teacher of Information Security course. Teacher of Information Technology Auditing course. Teacher of Standards Applied on Information Security Management course. Teacher of Systems Audit Guidelines course. Teacher of Balance Score Card course. Teacher of Business Intelligence course.

- **Teacher of POST GRADE SCHOOL OF SYSTEMS ENGINEERING COLLEGE**
  Universidad Nacional Mayor de San Marcos

Teacher of Sarbanes-Oxley and other regulations course. Teacher of Management of IT Project course. Teacher of IT Governance course. Teacher of CMMI course.

- **Member CISA, CGEIT, CRISC**
  ISACA

- **Systems Auditor**
  Banco de Crédito BCP
  Responsible of review and evaluate controls, application systems, IT procedures, computation equipment, their utilization, efficiency and security; evaluation of works on multiple platforms environments (Main Frame, Client/Server and Internet), tools for systems development and evaluation of development of systems projects. In charge of execute audits to subsidiaries of Banco de Crédito del Perú and other companies of Credicorp Group in Perú and abroad, editing reports in Spanish and English directed to our Corporation Headquarters. Supervising works and reports of six qualified audit professionals.

- **Systems Analyst**
  Bellsouth
  In charge of analysis, development and maintenance of systems in Cobol language for Digital Systems.

- **Systems Analyst**
  BANCO DEL LIBERTADOR
  In charge of analysis, development and maintenance of systems in Cobol language for Wang Systems.

- **Systems Analyst**
  XEROX DEL PERU
  In charge of analysis and development of data base managers, AS/ 400 and Windows environment. Electronic Impression Services Chief managing projects with leader companies in their sectors and work groups of more than 30 people.

- **Analista de Sistemas**
  Banco Industrial del Perú

Objetivo:

El objetivo del presente informe es someter a evaluación del modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de los diversos marcos de trabajo, estándares y metodologías, para minimizar los riesgos que están expuestos los diferentes procesos que soporta el área de TI en las instituciones educativas básica regular.

Nombres y apellidos:

Rómulo Fernando, Lomparte Alvarado

Grado académico y profesión:

Licenciado en Computación

MBA

Área de experiencia profesional:

Magister en Dirección de Negocios y Licenciado en Computación; con certificaciones PMP, CISM, IRCA, CGEIT, CRISC, CISA, ISO 27002, Cobit 5 Foundations CDPSE y CRMA. Con sólida y amplia experiencia de 30 años en empresas nacionales e internacionales del ámbito comercial y financiero en funciones de consultoría, auditoría, seguridad y desarrollo de proyectos de sistemas de información.

Experiencia en uso de COSO, COBIT y procesos de Certificación Sarbanes-Oxley.

Estudios de pre-grado en la Universidad Nacional Mayor de San Marcos y de post-grado en la Universidad Peruana de Ciencias Aplicadas, Esan y la Universidad de Harvard.

Catedrático en escuelas de post-grado en diversas universidades. Con participación en ISACA International y otros organismos profesionales, donde se desempeña como expositor e integrante de diversos comités especializados, tales como:

- Miembro del CGEIT Test Enhancement Subcommitee
- Expositor en Latin CACS y CEIC Las Vegas.
- Miembro del Comité de Expertos sobre Cloud Computing – CSA
- Miembro del Consejo Directivo de ISACA, Capítulo Lima
- Miembro del Government and Regulatory Advocacy Regional Subcommittee 2
- Líder de la Comunidad de Entrega de Valor de TI – Val IT
- Experto Revisor de la publicación Journal
- Miembro del Consejo de Gobernabilidad de Tecnologías de Información - ISACA
- Presidente de la Asociación de Egresados de la Escuela de Postgrado de la UPC
- Decano del Colegio Nacional de Matemáticos

Institución donde trabaja:

ITG Consulting

Tiempo de experiencia:

30 años

PERFIL DE EXPERTO

VILLACORTA CHAVEZ PAUL MARTIN

Ingeniero Administrativo, Grado Magister (MBA), Certificación Internacional PMP®, con más 15 años en Consultoría y Entrenamiento en empresas públicas y privadas (ONPE: Proyecto Voto Electrónico), MEF (Proyecto: Cero Papeles), ONP (Proyecto Calificación Expedientes Pensionables), Jefe Capacitación COMSA, Jefe Centro Cómputo, Asociación Judía del Perú. Catedrático PostGrado (PUCP, UTP, UNFV, UNMSM, UPAGU) y PreGrado (UPC, UTP, USMP).

Presidente PMI® Lima Chapter (2015.2017) y VicePresidente Educación PMI® Lima Chapter (2013-2014). Actual Director Proyectos de IGP (Instituto Gestión Proyectos).

DATOS ACADÉMICOS

- **Certificación PMP**
  REP PM
- **Technological University of America - TUA**
  Master of Business Administration (MBA)
- **Universidad Tecnológico del Perú - UTP**
  Maestría en educación
- **Universidad Nacional Federico Villarreal**
  Maestría en Proyectos Empresariales (PMI)
- **Universidad Inca Garcilaso de la Vega**
  Ingeniero Administrativo

EXPERIENCIA LABORAL

- **Responsable de Dirigir los Proyectos de Outsourcing para las áreas de Tecnología (TI) y Recursos Humanos (RRHH)**
  Instituto de gestión de proyectos
- **Catedrático en Gestión de Proyectos - PMI**
  en la escuela de postgrado de la facultad de Ing. electrónica y de telecomunicaciones de la UNMSM.
- **Profesor en la Diplomatura de Gestión de Proyectos PMI**
  Instituto de Calidad de la PUCP
- **Consultor & Facilitador Proyectos (PMI)**
  COLEGIO DE INGENIEROS DEL PERU (CIP)
- **Presidente**

PMI Lima Perú Chapter

- Profesor de las cátedras de Informática Empresarial, Administración - Gestión Empresarial (Facultad Ing. Económica) y Taller PMP de Gestión de Proyectos (Facultad de Ing. Sistemas Industrial – UTP

- **Profesor TI/Proyectos**
  Centro de Informática - UNMSM

- **Gestor de Capacitación y Capacitador**
  Ministerio de Economía y Finanzas - Proyecto "MEF Sin Papeles"

- **Profesor Acreditado TI**
  CEUPS/FISI – UNMSM

- **Coordinador Capacitación**
  COMSA/INDRA

- **Jefe del Centro de Cómputo**
  Asociación Judía del Perú

- **Facilitador / Consultor TI**
  Independiente (BN, LAN, Rio Tinto, AUSA, Emape, IPSS, Aceros Arequipa, Cámara de Comercio de Lima, Senati, New Horizons, IPAE, GMD, Cosapi Data)

Objetivo:
El objetivo del presente informe es someter a evaluación del modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de los diversos marcos de trabajo, estándares y metodologías, para minimizar los riesgos que están expuestos los diferentes procesos que soporta el área de TI en las instituciones educativas básica regular.
Nombres y apellidos:
PAUL MARTIN VILLACORTA CHAVEZ
Grado académico y profesión:
INGENIERO ADMINISTRATIVO COLEGIADO, MBA, MG. EDUCACION. ESPECIALIZACION EN PROYECTOS (PMP), CANDIDATO A DOCTOR EN PROYECTOS.
Área de experiencia profesional:
DIRECCION DE PROYECTOS / EDUCACION.
Institución donde trabaja:
UPC.
Tiempo de experiencia:
+15 AÑOS.

PERFIL DE EXPERTO

DIAZ ESPINO MIGUEL ANGEL

Ingeniero en computación y sistemas. Magister en Sistemas con especialidad en gestión de TI. Conocimientos en Windows server 2012 R2. Conocimientos en gestión de proyectos PMBOOK. Gestión de servicios ITIL. Especialización en auditoria informática. Experiencia en la administración del área de sistemas. Conocimientos en seguridad Informática, ethical hacking V8. Conocimientos en planeamiento estratégicos de TI y COBIT 5.0. Ingeniero Certificado en Elastix (ECE). Docente en la Universidad Señor de Sipán

DATOS ACADÉMICOS

- **Universidad Católica Santo Toribio de Mogrovejo**
  Magister en Dirección Estratégica de TI
- **ELASTIX CERTIFIED ENGINEER - ECE**
  ELASTIX TRAINING
- **New Horizons**
  Project Management for Professionals - PMBOK 5ta. Ed.
- **Universidad Católica Santo Toribio de Mogrovejo - USAT**
  Auditoría de Tecnologías de Información y Seguridad Informática
- **Universidad Privada Antenor Orrego**
  Ingeniero en Computación y Sistemas

EXPERIENCIA LABORAL

- **ESPECIALISTA EN SISTEMAS DE INFORMACIÓN**
  PROYECTO ESPECIAL OLMOS TINAJONES
- **GERENTE DE SISTEMAS**
  MUNICIPALIDAD PROVINCIAL DE CHICLAYO
- **RESPONSABLE DEL CENTRO DE COMPUTO**
  PROYECTO ESPECIAL OLMOS TINAJONES
- **ADMINISTRADOR SISTEMA MANTENIMIENTO PECOMAN**
  HOSPITAL ALMANZOR AGUINAGA ASENJO
- **TECNICO EN COMPUTACIÓN**
  ELECTRONORTE S.A.

Objetivo:

El objetivo del presente informe es someter a evaluación del modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de los diversos marcos de trabajo, estándares y metodologías, para minimizar los riesgos que están expuestos los diferentes procesos que soporta el área de TI en las instituciones educativas básica regular.

Nombres y apellidos:

MIGUEL ANGEL DIAZ ESPINO

Grado académico y profesión:

PROFESION: INGENIERO EN COMPUTACIÓN Y SISTEMAS
GRADO ACADEMICO: MAGISTER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGIAS DE INFORMACION

Area de experiencia profesional:

- GESTION DE TI
- PLANIFICACIÓN Y PRESUPUESTO

Institución donde trabaja:

- UNIVERSIDAD SANTO TORIBIO DE MOGROVEJO
- PROYECTO ESPECIAL OLMOS TINAJONES

Tiempo de experiencia:

- GESTION DE TI: Más de 20 años
- PRESUPUESTO Y PLANIFICACIÓN: Más de 2 años