FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ANÁLISIS DE RIESGOS INFORMÁTICOS Y ELABORACIÓN DE UN PLAN DE CONTINUIDAD PARA LA UNIDAD DE EDUCACIÓN VIRTUAL CEC-EPN

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Sistemas de Computación e Informática

Profesor guía

Ing. Javier Enrique García Bailón

Autores:

Andrea Elizabeth Conza Gonsález

Leonardo Xavier Medrano Chimborazo

Año

2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Javier Enrique García Bailón
Ingeniero en Sistemas Informáticos y de Computación
CI: 1306287028

DECLARACIÓN DE AUDITORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original de nuestra auditoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____	_____
Andrea Elizabeth Conza Gonsález	Leonardo Xavier Medrano Chimborazo
CI: 1714568944	CI: 1716476807

AGRADECIMIENTOS

A Dios por su gran amor y ser el motor que mueve mi vida, a mis padres por su apoyo y guía, al equipo de la Unidad de Educación Virtual 2013 – 2015, y a todas las personas que me apoyaron a culminar este proyecto.

Andrea

AGRADECIMIENTOS

Por el apoyo incondicional de Dios y mis queridos padres, hermana y sobrina que siempre con sus palabras de aliento y amor me dieron el empuje para culminar un anhelado sueño y perseguir otros.

Leonardo

DEDICATORIA

A Dios y a mi Madre Santísima, a toda mi linda familia por todo el cariño, entregado, a mi compañero de toda la vida Leonardo por su amor, constancia y profesionalismo entregado.

Andrea

DEDICATORIA

A mi querida compañera, amiga y esposa Andrea que con su apoyo, amor y dedicación fue posible la realización del proyecto. A mi familia por enseñarme que no hay que rendirse frente a las adversidades.

Leonardo

RESUMEN

El presente proyecto de titulación realiza el Análisis de Riesgos y elaboración de un Plan de Continuidad para la Unidad de Educación Virtual (UEV) del Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN), mediante la búsqueda de las amenazas, vulnerabilidades, riesgos en los activos de información y los procesos críticos de la unidad, el análisis fue empleado para proponer un Plan de Continuidad acorde a las necesidades de la UEV. El proyecto se divide en cinco capítulos los mismos que se detallan a continuación:

En el primer capítulo se señala una breve descripción del CEC-EPN, y la UEV, por otra parte se define el alcance del proyecto y los objetivos que se pretenden alcanzar.

En el segundo capítulo se abordan conceptos sobre análisis de riesgos y continuidad del negocio, centrándose en las principales metodologías, buenas prácticas de Tecnologías de la Información (TI) y estándares conocidos en el mercado, además se revisa y selecciona las metodologías tanto para el desarrollo del Análisis de Riesgos como la propuesta del Plan de Continuidad para la UEV.

En el tercer capítulo se desarrolla el Análisis de Riesgos mediante la metodología OCTAVE Allegro a través de los ocho pasos que propone la misma, el cual permite la identificación de amenazas, vulnerabilidades y riesgos, con la intención de plantear estrategias para aceptar, transferir o mitigar los riesgos encontrados.

En el cuarto capítulo se propone un Plan de Continuidad a través de la combinación de la metodología de *Disaster Recovery Institute International* (DRII) y la Gestión de la Continuidad de los Servicios de Tecnologías de la Información (TI), de *Information Technology Infrastructure Library* (ITIL) v3.

Finalmente en el capítulo cinco se presentan las conclusiones a las que se llegaron después del desarrollo del presente trabajo y se exponen las recomendaciones que serán de utilidad para la UEV.

ABSTRACT

This project develops the Risk Analysis and development of a Continuity Plan for the Unidad de Educación Virtual (UEV) Centro de Educación Continua of the Escuela Politécnica Nacional (CEC-EPN), by searching for threats, vulnerabilities risks to information assets and critical processes of the unit, the analysis was employed to propose Continuity Plan according to the needs of the UEV. This project is divided into five chapters the same as detailed below:

In the first chapter a brief description of CEC-EPN and UEV, moreover the project scope and objectives to be achieved is defined.

In the second chapter the main concepts of risk analysis, business continuity, are reviewed and focusing on the main methodologies, best practices of Information Technology (IT) and standards known in the market are discussed further analysis and selection of the best methodologies for both the development of risk analysis as performed the proposal Continuity Plan for UEV.

In the third chapter Risk Analysis methodology developed by OCTAVE Allegro through the eight steps proposed it, which allows the identification of threats, vulnerabilities and risks, with the intention to propose strategies to accept, transfer or mitigate the risks encountered.

In the fourth chapter Continuity Plan is proposed by combining the methodology of Disaster Recovery Institute International (DRII) and Continuity Management Services Information Technology (IT) of the Information Technology Infrastructure Library (ITIL) v3.

Finally in chapter five the conclusions that were reached after the development this work and recommendations that will be useful for UEV.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Capítulo I

1 Introducción

En la actualidad un Plan de Continuidad es una necesidad básica de una empresa pequeña o grande, debido a que los ambientes del negocio son cada vez cambiantes y exigentes obligando a buscar alternativas que garanticen la continuidad de las operaciones en las organizaciones.

El uso de las Buenas Prácticas de TI apoyan a la elaboración de un Plan de Continuidad para la Unidad de Educación Virtual (UEV) del Centro de Educación Continua de la Escuela Politécnica Nacional, mediante el Análisis de Riesgos Informáticos, los mismos que permitirán determinar el impacto y las acciones necesarias a seguir para garantizar la disponibilidad, confidencialidad y calidad de los servicios considerados como críticos para la UEV.

1.1 Centro de Educación Continua (CEC)

En mayo de 1995 fue creado como Centro de Educación Continua (CEC), mediante normativo de la Escuela Politécnica Nacional (EPN), con el propósito de impartir conocimientos y desarrollar actividades académicas promoviendo así la actualización permanente de conocimientos de los miembros de la comunidad de la EPN, egresados de la institución, empresas públicas y privadas; y público en general.

El 11 de Octubre de 2005, el Consejo Politécnico resuelve suprimir el Centro de Transferencia y Desarrollo de Tecnologías de Estudios para la Comunidad nombrado en agosto del 2000 y dispone que las actividades se ejecuten ininterrumpidamente a través del Centro de Educación Continua reactivado el 4 de enero de 2005 por el mismo Consejo Politécnico (Centro de Educación Continua (CEC-EPN), 2013).

1.1.1. Estructura organizacional CEC-EPN

El CEC-EPN, se encuentra conformada por la Dirección, Subdirección y siete coordinaciones entre las cuales se destacan las coordinaciones denominadas

como productivas dado la misión de la organización: Lingüística, Capacitación y Consultoría, y la Unidad de Educación Virtual.

La siguiente figura muestra la estructura organizacional del CEC-EPN dentro de la EPN.

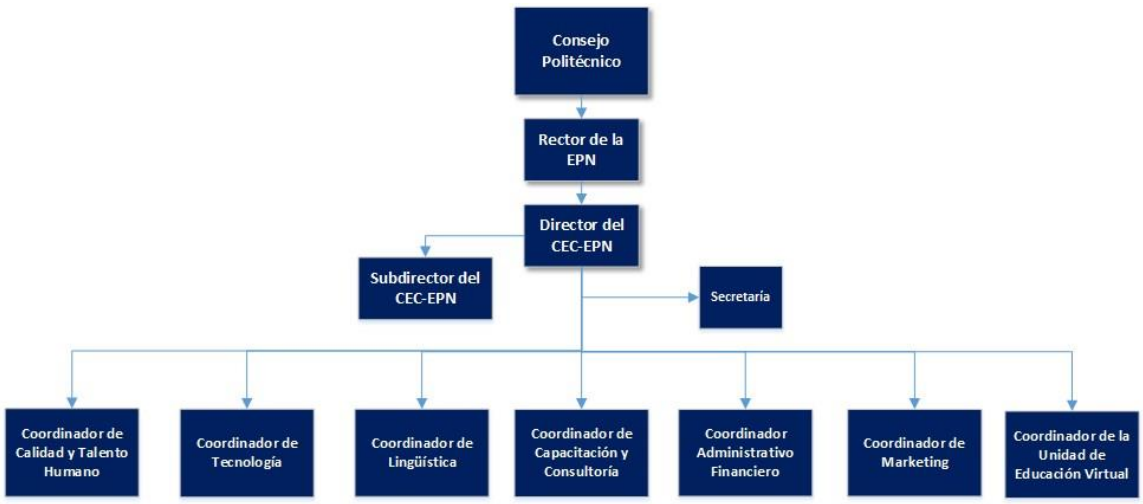

Figura 1. Organigrama del CEC-EPN

Adaptado de (CEC-EPN, 2013, p. 7)

1.1.2. Misión CEC-EPN

"El Centro de Educación Continua de la Escuela Politécnica Nacional ofrece servicios de capacitación y consultoría, con profesionales altamente calificados y tecnología avanzada para aportar al desarrollo y a la competitividad de la sociedad" (CEC-EPN, 2013, p. 8).

1.1.3. Visión CEC-EPN

"Ser el Centro de Educación Continua referente en el Ecuador, con estándares internacionales, en servicios de capacitación y consultoría, mediante una gestión efectiva y con responsabilidad social" (CEC-EPN, 2013, p. 8).

1.1.4. Valores CEC-EPN

- Transparencia: con cultura de rendición de cuentas en lo que a gestión, resultados y manejo financiero se refiere.
- Flexibilidad: apertura para aceptar y asimilar los cambios sin oponer resistencia por el simple hecho de hacerlo.

- Responsabilidad: reconocer la importancia del trabajo por realizar y cumplir con las actividades, con el fin de obtener resultados dentro de los plazos establecidos.
- Compromiso: preocupación permanente por satisfacer las necesidades y expectativas del cliente, con el fin de alcanzar cada vez mejores resultados.
- Respeto: valor que permite que la sociedad puede vivir en paz, en una sana convivencia a base de normas e instituciones. Todo se puede sintetizar en una sola frase: “no hagas a los demás lo que no quieres que te hagan a ti”. (CEC-EPN, 2013, p. 8)

1.1.5. Objetivos Estratégicos CEC-EPN

Los objetivos estratégicos del CEC-EPN son los siguientes:

- Asegurar la satisfacción de los clientes y partes interesadas.
- Implementar las mejores prácticas de gestión académica y administrativa en los procesos del Centro de Educación Continua de la Escuela politécnica nacional (CEC-EPN).
- Fortalecer el posicionamiento en el mercado.
- Fomentar una cultura organizacional en base a nuestros valores.
- Promover proyectos de responsabilidad social. (CEC-EPN, 2013, pp. 8-9)

1.1.6. Unidad de Educación Virtual CEC-EPN

La Unidad de Educación Virtual (UEV), inicia en el año 2008 como un proyecto de la Escuela Politécnica Nacional, siendo parte de sus objetivos diseñar y desarrollar una oferta académica a través de programas de educación continua virtuales. Dado su crecimiento y la fuerte relación con la capacitación profesional, pasó a formar parte del CEC-EPN, y desde su visión como proyecto ha ofrecido aulas virtuales en las plataformas Moodle como un recurso de apoyo a los docentes de la EPN (de manera opcional), en las

carreras de Pregrado y Posgrado, beneficiando al proceso educativo de manera integral.

La Unidad de Educación Virtual CEC-EPN, tiene como principal objetivo ofrecer soluciones *E-learning*, utilizando las Tecnologías de la Información y Comunicación - TIC, basados en tres ejes: educación, tecnología y organización (Unidad de Educación Virtual (UEV), s.f.).

1.1.6.1. Organigrama de la Unidad de Educación Virtual

La Unidad de Educación Virtual, está compuesta por cinco áreas de trabajo, en la figura 2, se indica las áreas y el orden jerárquico dentro de la Unidad de Educación Virtual CEC-EPN.

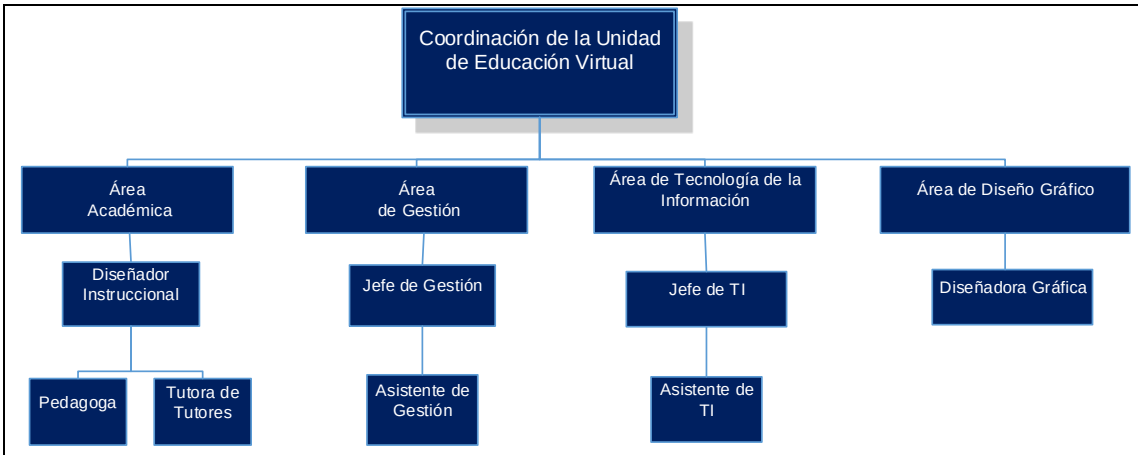

Figura 2. Organigrama de la UEV del CEC-EPN
Adaptado de (CEC-EPN, 2013, p. 7)

El equipo que lo conforma son nueve profesionales, a continuación la descripción de las áreas:

- Coordinación de la Unidad de Educación Virtual: es el área responsable de todas las actividades que se desarrollan en la UEV, a cargo del área se encuentra la Coordinadora.
- Área Académica: es responsable de las actividades pedagógicas, académicas y de seguimiento dentro de la UEV, a cargo del área se encuentra el Diseñador Instruccional, forman parte del área la Pedagoga y la Tutora de Tutores.

- Área de Gestión: es responsable de las actividades administrativas y de atención al cliente en la UEV, a cargo del área está el Jefe de Gestión, dentro del área se encuentra el Asistente de Gestión.
- Área de Tecnología de la Información: es responsable de gestionar y administrar las actividades relacionadas con las tecnologías de la información y comunicación dentro de la UEV, a cargo del área está el Jefe de TI (Tecnologías de la Información), dentro del área se encuentra el Asistente de TI.
- Área de Diseño Gráfico: es responsable de desarrollar el material gráfico y multimedia de los cursos virtuales e imagen de la UEV, a cargo del área se encuentra la Diseñadora Gráfica.

1.2 Objetivo General

Realizar el Análisis de Riesgos Informáticos y elaborar un Plan de Continuidad mediante la aplicación de metodologías y buenas prácticas de Tecnología de la Información, para mejorar la disponibilidad de los servicios críticos de la Unidad de Educación Virtual.

1.3 Objetivos específicos

- Seleccionar la metodología adecuada para analizar los riesgos identificados en la Unidad de Educación Virtual CEC-EPN.
- Seleccionar la metodología adecuada para elaborar el plan de continuidad para la Unidad de Educación Virtual CEC-EPN.
- Identificar las principales amenazas y riesgos para la Unidad de Educación Virtual CEC-EPN.
- Desarrollar un Plan de Continuidad para Unidad de Educación Virtual CEC-EPN.

1.4 Alcance del proyecto

El presente proyecto pretende analizar y seleccionar la metodología que se emplearán para el análisis de riesgos y plan de continuidad en la Unidad de Educación Virtual, considerando temas organizacionales y facilidad de uso, de tal forma que se realice la identificación y análisis de los riesgos informáticos,

así como también la propuesta de un Plan de Continuidad, que sirva de guía para que la unidad pueda implementarla.

1.5 Justificación

En la actualidad el Centro de Educación Continua no dispone de un plan de continuidad de TI que mantenga los servicios críticos de la organización disponibles en caso de un incidente o falla. Dado el crecimiento que experimenta la Unidad de Educación Virtual hace que los servicios de capacitación como los de apoyo académico se encuentren disponibles para garantizar así la calidad del servicio. En tal virtud se propone realizar el análisis de riesgos informáticos a fin de desarrollar un Plan de Continuidad que sirva de guía para la Unidad de Educación Virtual.

Capítulo II

2 Marco Teórico

En este capítulo se establecerán varios términos, conceptos, metodologías, estándares que se utilizarán a lo largo del desarrollo del presente proyecto.

2.1 Riesgo

Es la probabilidad de que una amenaza o evento no deseado se realice, de forma que no permita cumplir con los objetivos planteados en la organización por ejemplo: tiempo, coste, alcance o calidad (Salazar & Torres, 2008).

2.1.1. Elementos del Riesgo

2.1.1.1. Activos y/o Procesos

Consiste en todos los bienes físicos y lógicos sobre el cual permite a la organización funcionar. Se clasifican en:

- Activos físicos: Equipos de oficina, infraestructura, maquinarias.
- Activos de información: Archivos, aplicativos, base de datos, entre otros (Pazmiño, 2007, p. 2).

2.1.1.2. Impacto

El impacto es la materialización de un riesgo, el cual permite captar o medir el daño que provoca el riesgo (Instituto Nacional de Tecnologías de la Comunicación (INTECO), s.f.).

2.1.1.3. Probabilidad

El concepto de la probabilidad tiene dos concepciones: una objetiva el cual indica que es la posibilidad de que un evento ocurra según a una periodicidad o frecuencia determinada. Otra subjetiva el cual es construida en base a las creencias personales respecto a la ocurrencia de un determinado evento (Chena, s.f.).

2.1.2. Clasificación de Riesgos

Según las causas que provocan los riesgos se clasifican en:

- Fuentes de riesgos internos: son aquellos riesgos que tiene sus orígenes dentro de la organización.

- Fuentes de riesgos externos: son aquellos riesgos que tiene sus orígenes fuera de la organización (Instituto Nacional de Tecnologías de la Comunicación (INTECO), s.f.)

En la tabla 1 y tabla 2 se resume las fuentes de riesgo tanto internas como externas.

Tabla 1. Clasificación de riesgos internos

Tecnología	Programación	Financiera	Contractual y Legal
Tecnología nueva o no probada	Disponibilidad de recursos	Fondos y presupuesto	Propiedad intelectual
Disponibilidad de experiencia técnica	Planificación inadecuada	Exactitud de estimación	Políticas de gobierno
Actuación del subcontratista/vendedor	Restricción de programación	Cambio en coste de material	Derecho de datos
Personalización (riesgo de diseño)	Información insuficiente		Ambigüedades de contrato
Transición desde diseño a producción	Dependencia de la empresa		Multas
Disponibilidad de materiales	Dependencia del cliente		Derecho de patentes o incumplimientos

Adaptado de (INTECO, s.f., p. 12)

Tabla 2. Clasificación de riesgos externos

Impredecibles	Predecibles pero inciertos
Cambios reguladores	Cambios de mercados
Impacto ambiental, del entorno, sociales	Tasación
Desastres naturales	Inflación
Interés publico	Tipo de cambio
Relaciones industriales	Subcontratista o *partner* políticos
Mercados dinámicos	Mercados dinámicos

Adaptado de (INTECO, s.f., p. 12)

2.1.3. Riesgos en la tecnología de información

Entre los riesgos que presentan los activos que conforman una organización se categorizan en:

- Riesgos asociados a desastres naturales.

- Riesgos por variaciones y pérdidas de flujo eléctrico.
- Riesgo por configuración inadecuada de los equipos. Consiste en la manipulación incorrecta de los equipos ya sea por el personal interno o externo o el propietario del activo.
- Riesgos por pérdida de información. Debido al inadecuado almacenamiento de la información en el equipo o dispositivo.
- Riesgos por caída de sistemas. Producidos por recursos internos o externos que provocan pérdidas económicas y productividad.
- Riesgos por vandalismo.
- Riesgo por extravió de equipos.
- Riesgo por pérdida de confidencialidad de la información. Está vinculado al robo de información y divulgación por terceros.
- Riesgo de autentificación. Consiste en la violación de acceso a los sistemas por parte de usuarios no autorizados o por robo de identidad.
- Riesgos por violación de integridad. Producidos por un agente o circunstancia inesperada de forma deliberada o accidental que altera datos en un documento, archivo, base de datos, entre otros.
- Riesgos económicos. Consiste en la perdida monetaria, material, humana que afecta directamente al cumplimiento de los objetivos de la organización.
- Riesgos por pérdida de fidelización de clientes. Está relacionado con la pérdida de confiabilidad y prestigio por parte de los usuarios o clientes hacia la organización (Pazmiño, 2007).

2.2 Vulnerabilidad

Consiste en la debilidad existente en un sistema de información, procedimiento o control, el cual es aprovechado o explotado por una amenaza (Pazmiño, 2007).

2.2.1. Clasificación de las vulnerabilidades:

Las vulnerabilidades se clasifican en:

- Vulnerabilidades de diseño: consiste en el diseño erróneo de aplicación del software, hardware, entre otros.
- Vulnerabilidades de configuración: está vinculado con la incorrecta configuración y administración de acceso a un sistema.
- Vulnerabilidades de implementación: es provocado por un incorrecto análisis e implementación de hardware o software en algún proyecto de producción.
- Vulnerabilidades organizacionales: es provocado por la implementación de políticas y prácticas de seguridad erróneas en la organización.
- Vulnerabilidades tecnológicas: consisten en las vulnerabilidades de los sistemas el cual afectan a los servicios, arquitecturas y aplicaciones de la organización.
- Vulnerabilidades físicas: son aquellas que afectan a la infraestructura física de la organización por ejemplo la no existencia de sistemas de control de acceso.
- Vulnerabilidades geográficas: consiste en las inseguridades de la ubicación donde se encuentra la organización ya que puede existir fallas arquitectónicas o desastres naturales (Pazmiño, 2009).

2.3 Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgos y las acciones que se van a implementar. (Salazar & Torres, 2008, p. 43)

Consta de 3 etapas:

- Identificación de activos.
- Evaluación de las amenazas.
- Tratamiento del riesgo (Peña, p. 8).

2.3.1. Identificación de los activos

La identificación de los riesgos en los activos permite reconocer y determinar las causas principales de dichos riesgos que se presentan o no

en la empresa. Este proceso se lo debe realizar de forma constante con el propósito de detectar las amenazas que surgen a diario (Salazar & Torres, 2008).

2.3.1.1. Métodos de identificación de riesgo en los activos

Existen varios métodos que permiten la identificación de riesgos:

- Métodos Comparativos. Consiste en el uso de experiencias e instalaciones realizadas con el propósito de minimizar los riesgos. Existen varios métodos entre ellos esta los manuales técnicos, listas de comprobación, análisis históricos de incidentes y análisis preliminar de riesgos (Salazar & Torres, 2008).
- Métodos generalizados. El método generalizado consiste en la identificación de fallos, errores, procesos de la empresa. Existen varios métodos entre ellos está el análisis funcional de operatividad, análisis de árbol de fallos, análisis de árbol de sucesos y el análisis de modo y efecto de los fallos (Salazar & Torres, 2008).

2.3.2. Evaluación de las amenazas

Para la evaluación de las amenazas se tiene en cuenta la estimación o probabilidad en el cual se produzca un peligro en la integridad en el activo. Las amenazas dependen del negocio de la organización, ubicación y tipo de sistema a proteger. Entre los tipos de amenazas existen los errores o accidentes, intencionadas y por eventos naturales. Entre los objetivos principales de esta etapa consiste identificar la causa de la amenaza, identificar el activo afectado por la amenaza y calcular la probabilidad de que ocurra la amenaza. El resultado final de la evaluación permitirá realizar una lista de amenazas e identificar los activos afectados (Peña, s.f.).

2.3.3. Tratamiento del riesgo

El tratamiento del riesgo permite encontrar un equilibrio entre el nivel de seguridad versus el costo de la misma, así como también el costo de la protección versus el costo de exposición. Esto permite tomar la mejor

elección o decisión para reducir o eliminar la probabilidad de ejecución del riesgo (Peña, s.f.).

Entre las decisiones que se pueden tomar para tratar el riesgo, según a diversos enfoques, se tiene:

- Evitar el riesgo. Consiste en prevenir que el riesgo se materialice a través del uso de buenas prácticas.
- Reducir el riesgo. Consiste en minimizar la probabilidad que el riesgo suceda así como también el impacto.
- Transferir el riesgo. Consiste en trasladar el riesgo del activo a otras organizaciones o grupos para que asuman las pérdidas a través de contratos de seguros o de riesgos compartidos.
- Asumir el riesgo. Consiste en que la organización o empresa tomara el riesgo e impacto sobre el activo, tras haber realizado un análisis y reducido o transferido dicho riesgo (Salazar & Torres, 2008).

2.3.4. Elementos del análisis de riesgo

Entre los elementos que cuenta un análisis de riesgo están:

- Construcción de perfil de amenaza basado en los activos de la organización.
- Identificación de activos de la organización.
- Identificar las amenazas de cada uno de los activos listados.
- Conocer las prácticas actuales de seguridad.
- Identificar las vulnerabilidades de la organización: recursos humanos, técnicos y financieros.
- Identificar los requerimientos de seguridad de la organización.
- Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.
- Detección de los componentes claves.
- Desarrollar planes y estrategias de seguridad: riesgo para los activos críticos, medidas de riesgos, estrategias de protección y planes para reducción de riesgos. (Seguridad informática, s.f.)

2.4 Metodologías de análisis de riesgos

Para el análisis de riesgos existen varias metodologías en el mercado que permiten facilitar el desarrollo del análisis mediante la aplicación de métodos científicos. A continuación se detalla las cinco principales metodologías más usadas.

2.4.1. CRAMM – CCTA Risk Analysis and Management Method

Es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. La versión inicial se genera a partir de 1987 y la versión vigente es la 5.2. Su uso se realiza en la administración pública británica y en empresas e instituciones de gran tamaño (Huerta, 2012).

2.4.1.1. Fases

La metodología CRAMM consta de las siguientes fases:

Etapa 1: Establecimiento de objetos de seguridad:

- Definir el alcance del estudio.
- Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
- Identificar y evaluar los activos físicos y de software que forman parte del sistema.

Fase 2: Evaluación de riesgos:

- Identificar, valorar el tipo y nivel de las amenazas que pueden afectar el sistema.
- Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
- Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.

Fase 3: Identificación y selección de contramedidas.

Los productos o entregables que la metodología CRAMM produce son:

- Documento de inicio de proyecto
- Informe de análisis de riesgos

- Informe de gestión de riesgos
- Plan de implantación (Salazar & Rangel, 2012, pp. 6-13).

2.4.1.2. Características

- “Una metodología para el análisis y gestión de riesgos.
- Una metodología que aplica sus conceptos de una manera formal, estructurada y disciplinada.
- Una metodología orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos.
- Una metodología que, aunque se la encuadre, a veces, como cuantitativa, utiliza evaluaciones cuantitativas y cualitativas; de ahí su carácter de mixta” (Calle Guglieri, 1997, p. 58).

2.4.2. MAGERIT – Metodología de Análisis y Gestión de Riesgos IT

Metodología desarrollada por el Ministerio de Administraciones Publicas de Madrid. Esta metodología se enfoca en los sistemas de información y activos de la empresa con el propósito de protegerlos. La primera versión fue publicada en 1997, la versión vigente en la actualidad es la versión 3.0. Dispone de una herramienta de soporte llamado PILAR II (Proceso Informático-Lógico para el Análisis y Gestión de Riesgos) que es de uso gratuito para la Administración Pública Española y de manera comercial a las organizaciones privadas (Gaona, 2013).

2.4.2.1. Fases o guías

La metodología MAGERIT consta de tres volúmenes los cuales se mencionan a continuación:

Volumen I: Método.

Esta guía se estructura en ocho capítulos:

- Capitulo I. Introducción de la metodología.
- Capitulo II. Visión de conjunto. Contiene las actividades de análisis y tratamiento de riesgos para tener un proceso integral de gestión de riesgos.
- Capítulo III. Método de Análisis de Riesgos. Detalla los pasos para realizar dicho análisis.

- Capitulo IV. Proceso de Gestión de Riesgos. Detalla las actividades para realizar dicha gestión.
- Capitulo V. Proyecto de Análisis de Riesgos.
- Capítulo VI. Plan de Seguridad. Detalla las actividades para realizar un plan de seguridad, después de haber realizado el proyecto de Análisis y Gestión de Riesgos con el propósito de escoger las mejores decisiones para el tratamiento de los riesgos.
- Capitulo VII. Desarrollo de sistemas de información. Se centra en la seguridad de los sistemas de información con el propósito de mitigar los riesgos.
- Capitulo VIII. Consejos prácticos. Consiste en recomendaciones prácticas para ser utilizados en el análisis de riesgos.

Además recopila material adicional a través de cinco apéndices de consulta (Gaona, 2013).

Volumen II: Catálogo de Elementos

Es el complemento del Volumen I el cual contiene tareas para la aplicación de la metodología MAGERIT. Contiene además varios elementos como: Tipos de activos, dimensiones y criterios de valoración, amenazas y salvaguardas.

Sus objetivos principales son: facilitar la labor de las personas que realizan el proyecto así como también entregar terminología y criterios uniformes que permitan comparar e incluso integrar el análisis realizados por diferentes equipos (Gaona, 2013).

Volumen III: Guía de Técnicas

Describe algunas técnicas utilizadas en el análisis y gestión de riesgos. Para cada técnica referenciada explica brevemente el objetivo que se persigue al utilizarla, describe los elementos asociados básicos, expone los principios fundamentales de elaboración. Las técnicas que se utiliza son el análisis mediante tablas, algorítmicas, árbol de ataque, técnicas generales, análisis de coste-beneficio, diagrama de flujo de datos, diagrama de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo como entrevistas, reuniones, presentaciones y valoración Delphi (Gaona, 2013).

2.4.2.2. Características

A través del uso de la metodología MAGERIT, permite concienciar a los responsables de los sistemas de información sobre la existencia de riesgos y de la necesidad de detenerlos a tiempo. Así como también ofrecer un método sistemático para analizar los riesgos. Permite descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Apoya a la preparación a la organización para los procesos de evaluación, auditoría, certificación, etc (INTECO), s.f.).

2.4.3. MEHARI – Método Armonizado de Análisis de Riesgos

Metodología de evaluación y gestión de riesgos desarrollada por el Club de Seguridad de Información Francesa en 1995 derivada de las metodologías Melissa y Marion. Se trata de una guía de implantación de seguridad el cual evalúa los riesgos a partir de 3 principios: disponibilidad, integridad y confidencialidad conforme a los requerimientos de la ISO/IEC 27005:2008. (Huerta, 2012)

2.4.3.1. Fases

La metodología MEHARI tiene las siguientes fases:

- Fase Preliminar o estudio de contexto (alcance y límites).
- Fase Operacional o evaluación de riesgos (estimación de riesgos).
- Fase de Planeación o tratamiento de riesgos (Controles y pruebas).

2.4.3.2. Características

Es un conjunto de herramientas cuyo resultado permite un análisis directo e individual de cada escenario de riesgo. Esta metodología está dirigido para profesionales IT, gerentes y dueños de negocios. Los aspectos fundamentales son: el modelo de riesgos que son cualitativos y cuantitativos. La capacidad para evaluar y simular los niveles de riesgo derivados. La ventaja principal es el uso de las diferentes herramientas y métodos de forma separadas una de otras en cualquier etapa del desarrollo de la seguridad, utilizando diferentes enfoques de gestión garantizando la consistencia de las decisiones resultantes. (LLanos, 2010)

2.4.4. OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation)

Metodología de análisis de riesgos desarrollado por Estados Unidos por la Universidad Carnegie Mellon en 2001. Se trata de una metodología que sigue tres principios: Confidencialidad, Disponibilidad e Integridad. Su propósito es identificar y evaluar los riesgos en la seguridad de la información. Así como también desarrollar criterios de evaluación de riesgos cualitativos que describan el riesgo operacional de la organización. (Huerta, 2012)

Identificar los activos que son importantes para la misión de la organización e identificar las vulnerabilidades y amenazas a los activos.

La metodología OCTAVE clasifica los componentes de la organización en activos y los ordena de acuerdo a su importancia en amenazas y vulnerabilidades (Huerta, 2012).

La metodología OCTAVE divide a los activos en dos tipos:

- Sistemas (Hardware, Software y Datos).
- Personas.

La metodología OCTAVE se clasifica en:

- Método OCTAVE.
- Método OCTAVE – S.
- Método OCTAVE Allegro.

2.4.4.1. Método OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation)

El método OCTAVE está definido por una guía de implementación, procedimientos, hojas de trabajo, catálogos de información y encuestas. Se utiliza para grandes organizaciones de trescientos o más empleados. Específicamente se ha diseñado este método para organizaciones que tienen:

- Una jerarquía de varios niveles.
- Mantienen su propia infraestructura informática.

- Capacidad de ejecutar herramientas de evaluación de vulnerabilidades.
- Capacidad de interpretar los resultados de las evaluaciones de vulnerabilidad.

Se realizan varios talleres a través de un equipo de análisis interdisciplinarios, conformados entre tres o cinco personas de la misma organización.
Contiene tres fases que explora las cuestiones organizacionales y tecnológicas de la empresa.

En la primera fase el equipo de análisis identifica los activos que son importantes relacionados con la información de la organización y las estrategias de protección actuales de dichos activos. Posteriormente el equipo determina los activos críticos que están estrechamente relacionados a cumplir los objetivos de éxito en la organización con el propósito de documentar los requisitos de seguridad e identificar las amenazas.

En la segunda fase, el equipo de análisis realiza una evaluación de la infraestructura de la información para complementar el análisis de amenazas realizado en la primera fase e informar las decisiones de mitigación en la tercera fase.

En la tercera fase, el equipo de análisis realiza actividades de identificación de riesgos y desarrolla un plan de mitigación de riesgos para los activos críticos (Caralli, Stevens, Young, & Wilson, 2007, p. 14).

2.4.4.2. Método OCTAVE –S (Operationally Critical Threat Asset and Vulnerability Evaluation) Small

El método OCTAVE–S se utiliza para organizaciones manufactureras pequeñas de cien o menos empleados. Realiza el mismos criterios del método OCTAVE pero se encuentra limitado o restringido a las normas de la organización. De acuerdo con los criterios de OCTAVE, el enfoque de OCTAVE–S se compone de tres fases similares mencionados anteriormente. Requiere de un equipo de análisis que tengan un amplio conocimiento de la organización que puede ser entre tres a cinco personas. Una diferencia significativa entre OCTAVE–S y OCTAVE es más estructurado ya que los

conceptos de seguridad están integrados en las hojas de trabajo lo que permite menos desaciertos al identificar los riesgos. Otra ventaja de OCTAVE–S se requiere un estudio menos extenso de la infraestructura de información en la organización; dado que las organizaciones pequeñas pueden no poseer los recursos para obtener y ejecutar herramientas de detección de vulnerabilidades (Caralli et al., 2007, p.15).

2.4.4.3. Método OCTAVE Allegro (Operationally Critical Threat Asset and Vulnerability Evaluation) Allegro

Es una versión sintética del Método OCTAVE, realiza el mismo procedimiento con la diferencia que no se necesita un equipo interdisciplinario, al contrario es muy apropiado para personas que deseen realizar una evaluación de riesgo sin tanta participación de la organización y experiencia. El enfoque principal es centrarse en los activos de información en el contexto de cómo se utilizan, en el cual se conservan, transportan, procesan, la forma que se encuentran expuestas a las amenazas, vulnerabilidades y perturbaciones como resultado. Al igual que los métodos anteriores OCTAVE Allegro se puede realizar en un taller con un entorno colaborativo.

OCTAVE Allegro proporciona un conjunto estándar de plantillas de hojas de trabajo y cuestionarios los cuales se utilizarán durante la implementación del método.

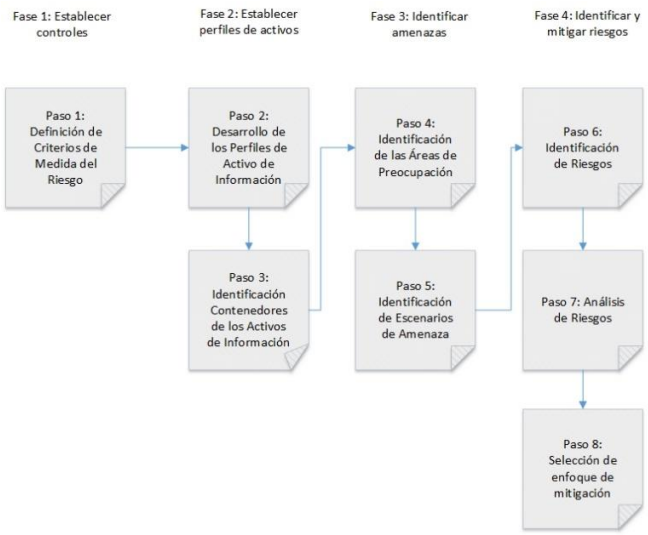

Figura 3. Diagrama del Método OCTAVE Allegro.

Adaptado de (Caralli et al., 2007, p. 4)

Características

- La principal característica del Método OCTAVE Allegro, permite el trabajo colaborativo entre las unidades de negocio y de TI con el propósito de identificar brechas de seguridad en la organización.
- Este método cuenta con cuatro fases de ocho pasos.

Fases:

- Fase I: Establecer controles.
- Fase II: Establecer perfiles de activos.
- Fase III: Identificar amenazas.
- Fase IV: Identificar y mitigar riesgos.

Fase 1: Establecer controles, la organización crea los controles que posteriormente se transformara en criterios de medición de riesgos, los cuales se relacionaran con los efectos que producen los riesgos a la misión y objetivos de la organización. Además de evaluar el grado de impacto en un área específica, una organización debe reconocer qué áreas de impacto son los más significativos para sus objetivos dentro de la organización. La priorización de áreas de impacto también se realiza en esta etapa inicial (Caralli et al., 2007).

La Fase I, se compone del Primer Paso y a su vez de dos actividades.

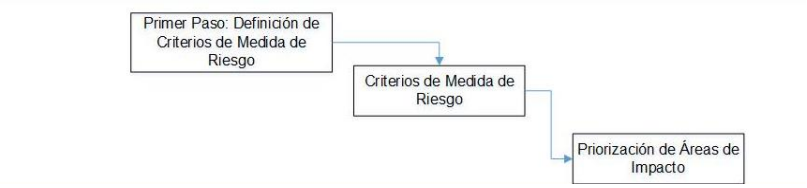

Figura 4. Actividades a desarrollar dentro del Primer Paso de la Fase I del Método OCTAVE Allegro.

- Primer Paso: Definición de Criterios de Medida del Riesgo, en este paso se establecen los controles para la organización, los cuales se utilizaran para evaluar el efecto de un riesgo sobre la misión y los objetivos del negocio de una organización (Caralli et al., 2007).

  Actividad 1: Criterios de Medida de Riesgo, son un conjunto de medidas cualitativas, son la base para la evaluación de riesgos de los activos de información, permite medir el grado de afectación si una amenaza se materializa. La metodología OCTAVE Allegro sugiere cinco criterios; pero será la organización quien las seleccione; de igual manera los criterios de medida de riesgo. Los criterios de medida de riesgo son: Reputación y Confianza del Cliente, Económico, Productividad, Seguridad y Salud; y Multas y Sanciones Penales.

  Actividad 2: Priorización de las Áreas de Impacto, se debe ordenar las áreas de impacto en base a los intereses de la organización desde la más importante con una valoración alta, hasta la menos importante con una valoración baja.

Fase II: Establecer perfiles de activos, esta fase establece límites claros para el activo de información, es decir identifica los requisitos de seguridad, lugares donde se almacenan, transporta y procesa, después se determina que activos son considerados como críticos para la organización.

Cabe mencionar que los activos críticos son considerados los más importantes ya que podrían sufrir un impacto negativo si:

- Se da a conocer a las personas no autorizadas.
- Es modificado sin autorización.
- Se pierde o destruye.
- El acceso es interrumpido.

En esta fase se desarrolla el Segundo y Tercer Paso del método OCTAVE Allegro.

Figura 5. Fase II, incluye el Segundo y Tercer Paso así como las actividades a desarrollar según el Método OCTAVE Allegro

- Segundo Paso: Desarrollo de los Perfiles de Activo de Información, consiste en definir los activos de información de la organización. Un perfil es una representación de un activo de información que describe sus características únicas, cualidades y valor. A través del perfilamiento se asegura que un activo se describe con claridad y coherencia, que no hay una definición inequívoca de los límites del activo y que los requisitos de seguridad para el activo se especifican adecuadamente (Caralli et al., 2007).

  Actividad 1: Identificación de la colección de activos de información, para identificar la lista de activos de información, la metodología OCTAVE Allegro, sugiere responder un banco de preguntas, a fin de obtener los activos de mayor importancia para la organización.

  Actividad 2: Identificación de los principales activos de información (críticos), una vez definidos los activos se seleccionan los que en caso de pérdida o daño afectarían al cumplimiento de la misión de la organización.

- Tercer Paso: Identificación de los Contenedores de los Activos de Información, se fundamenta en los contenedores de activos de información. Un contenedor se describe como el lugar de almacenamiento de los activos de información donde son transportados y procesados. Los activos de información no sólo residen en contenedores dentro de los límites de la organización, también a menudo residen en contenedores que no están en el control directo de la organización (Caralli et al., 2007).

  La identificación de los contenedores permite reconocer si existen puntos de vulnerabilidad y amenaza para los activos de información con el objetivo de implementar controles para ser asegurados.
  Los propietarios de los contenedores son los custodios, responsables del activo de información, son los individuos internos o externos que son parte de la organización, tienen la responsabilidad de proteger los activos de información.
  Actividad 1: Identificación de contenedor técnico, se incluyen generalmente los recursos de hardware, software, sistemas de aplicaciones, servidores y redes (activos tecnológicos).
  Actividad 2: Identificación de contenedor físico, se coloca la ubicación física de los activos de información también pueden ser archivos físicos (donde se guarda la información escrita, carpetas)
  Actividad 3: Identificación de contenedor personas, son quienes conocen la información importante en la organización, se incluye al personal interno y externo de la organización (Caralli et al., 2007).

Fase III: Identificar Amenazas, se identifican en el contexto de las ubicaciones donde se almacenan, transportan, o procesan los activos críticos. En esta fase se desarrolla el Cuarto y Quinto Paso del método OCTAVE Allegro.

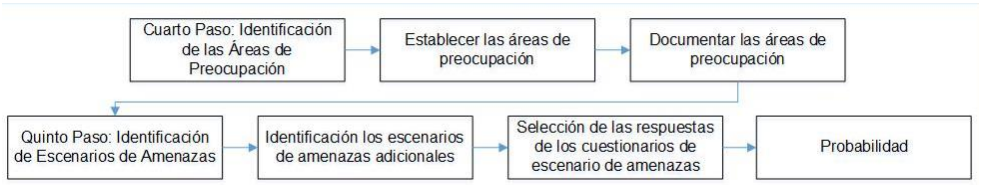

Figura 6. Fase III, incluye el Cuarto y Quinto Paso así como las actividades a desarrollar según el Método OCTAVE Allegro

- Cuarto Paso: Identificación de las Áreas de Preocupación, comienza el proceso de elaboración de los perfiles de riesgo de los activos de información,

  Amenaza (Condición) + Impacto (Consecuencia) = Riesgo

  Se aborda el componente de amenaza, a través de la ecuación del riesgo por medio de una lluvia de ideas sobre las posibles condiciones o situaciones que pueden poner en peligro los activos de información de una organización.

  Estos escenarios del mundo real se denominan áreas de preocupación y pueden representar amenazas y causar resultados indeseables para la organización.

  Actividad 1: Establecer las Áreas de Preocupación, el propósito de este paso no es capturar una lista completa de todos los posibles supuestos de amenazas para un activo de información; la idea es capturar rápidamente aquellas situaciones o condiciones que vienen inmediatamente a la mente del equipo de análisis.

  Actividad 2: Documentar las Áreas de Preocupación, una vez identificadas las áreas se debe evidenciar en la plantilla hoja de trabajo denominada Riesgos de Activos de Información, es importante además establecer los requisitos de seguridad como son: confidencialidad, integridad y disponibilidad (Caralli et al., 2007).

- Quinto Paso: Identificación de Escenarios de Amenazas, en este paso las áreas de preocupación se expanden en escenarios de amenaza, permitiendo conocer las propiedades de la misma, estos pueden ser

representados a través de una estructura conocida como árbol de amenaza.

El árbol de amenaza representa e identifica las amenazas potenciales del activo la información como base para determinar el riesgo. (Caralli et al., 2007)

El método OCTAVE Allegro considera cuatro árboles de amenaza, los cuales se describen en la siguiente tabla:

Tabla 3. Árboles de Amenaza

Definición de los distintos Árboles de Amenaza	
Árbol de Amenaza	**Descripción**
Actores Humanos utilizando medios técnicos.	Esta categoría se refiere a las amenazas a los activos de información realizadas por un actor humano de forma directa sea accidental o deliberada a la infraestructura técnica de la organización.
Actores Humanos utilizando acceso físico.	Esta categoría se refiere a las amenazas a los activos de información realizadas por un actor humano por acceso físico de manera directa o sobre su contenedor sea accidental o deliberada a la organización.
Problemas técnicos	Esta categoría se refiere a las amenazas a los activos de información por problemas con la tecnología y los sistemas de información de la organización. Incluye los defectos de hardware, software, virus y otros problemas relacionados con el sistema.
Otros problemas	Esta categoría se refiere a las amenazas a los activos de información son los problemas o situaciones que están fueran del alcance de control de la organización. Incluye los desastres naturales (inundaciones, terremotos, incendios) y los riesgos de interdependencia por ejemplo fuente de alimentación eléctrica.

Actividad 1: Identificación de los escenarios de amenazas adicionales, esta actividad consiste en responder a una serie de cuestionarios propuestos por el método OCTAVE Allegro, por cada uno de los activos críticos de información.

Actividad 2: Selección de los cuestionarios de escenario de amenazas, después de responder a los cuestionarios formulados en la actividad 1, se procede a escoger las respuestas afirmativas y negativas, para el primer caso se deberá registrar en una nueva hoja de trabajo Riesgos de Activos de Información, si la respuesta es negativa no se realizará ninguna tarea.

Actividad 3: Probabilidad, ayuda a la organización a determinar cuál de los escenarios de amenaza son más probables dado su entorno operativo único. Esto es útil para los pasos posteriores cuando la organización comienza el proceso de priorización de sus actividades de mitigación de riesgos. Sin embargo, debido a que a menudo es difícil de cuantificar con precisión la probabilidad, especialmente con respecto a las vulnerabilidades y los eventos de seguridad, la probabilidad se expresa de acuerdo al método OCTAVE Allegro de forma cualitativa como alta, media o baja. (Caralli et al., 2007)

Fase IV: Identificar y mitigar riesgos, se identifican y analizan los riesgos para los activos de información con el propósito de desarrollar enfoques de mitigación.

En esta fase se desarrolla el Sexto, Séptimo y Octavo Paso del método OCTAVE Allegro.

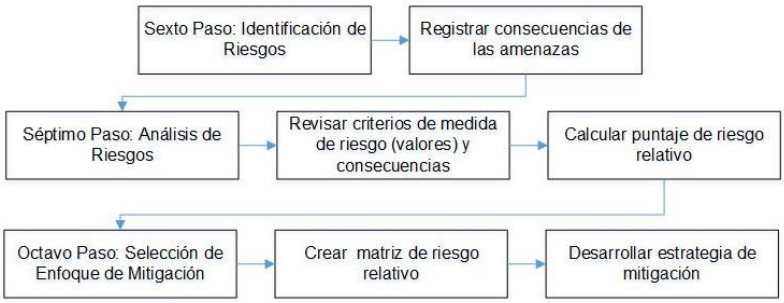

Figura 7. Fase IV, incluye el Sexto, Séptimo y Octavo Paso así como las actividades a desarrollar según el Método OCTAVE Allegro

- Sexto Paso: Identificación de Riesgos, en este paso se establecen las consecuencias, si estas amenazas se cumplen en la organización. Una amenaza puede tener múltiples impactos potenciales sobre la organización. Es importante asegurarse que se registren las diversas consecuencias de riesgo.

Amenazas + Impacto = Riesgo.

El registro de las consecuencias permite completar la ecuación del riesgo (Caralli et al., 2007).

Actividad 1: Revisar criterios de medida de riesgo (valores) y consecuencias

El valor de impacto es un valor cualitativo asignado para describir el grado de impacto que una organización recibe cuando se presenta la amenaza. El valor de impacto se deriva de los criterios de medición de riesgos. (Caralli et al., 2007)

- Séptimo Paso: Análisis de Riesgos, se calcula una medida cuantitativa del grado en que la organización se ve afectada por una amenaza. Esta puntuación de riesgo relativo se obtiene considerando en qué medida la consecuencia de un impacto del riesgo afecta a la organización tomando en cuenta la importancia relativa de la diversas áreas de impacto y posiblemente la probabilidad.
- Octavo Paso: Selección de Enfoque de Mitigación, en el último paso del método OCTAVE Allegro, la organización determina cuál de los riesgos que se han identificado requieren mitigarse y desarrollar una estrategia de mitigación de dichos riesgos. Esto se lleva a cabo en función de la puntuación del riesgo relativo. Una vez que los riesgos han sido priorizados, las estrategias de mitigación que se desarrollan se tomarán en cuenta: el valor del activo, sus requisitos de seguridad, los contenedores en los que se encuentran y el entorno operativo único de la organización (Caralli et al., 2007).

  Hay que recordar que el valor de impacto es un factor primordial, pero también lo es la probabilidad, porque si se presenta un riesgo grave podría afectar significativamente a la organización, pero si es muy poco probable que ocurra, puede que no sea necesario mitigarlo.

  Cuando se desarrolla e implementa el enfoque de mitigación de riesgos en los resultados de la implementación siempre aparecerá un riesgo residual.

  Este riesgo residual debe ser aceptable para la organización.

Para mitigar el riesgo adecuadamente hay que tomar las siguientes consideraciones:

- Evitar el riesgo, mediante la implementación de controles adecuados para prevenir amenazas y vulnerabilidades en los activos.
- Limitar el riesgo, mediante la implementación de estrategias que minimicen el impacto negativo sobre la organización si se presenta el riesgo.
- Contar con el apoyo de la alta dirección, colaborar con el departamento de Tecnologías de la Información, así como también otras partes interesadas para desarrollar estrategias de mitigación balanceadas y rentables. (Caralli et al., 2007)

La metodología OCTAVE Allegro sugiere utilizar una matriz de riesgo relativo, en la cual se ordenan cada uno de los riesgos identificados según a la puntuación de riesgo relativo y probabilidad.

Matriz de riesgo relativo			
Probabilidad	Puntaje de riesgo		
	30 A 45	16 A 29	0 A 15
Alta	Grupo 1	Grupo 2	Grupo 2
Media	Grupo 2	Grupo 2	Grupo 3
Baja	Grupo 3	Grupo 3	Grupo 4

Figura 8. Matriz de Riesgo Relativo

Tomado de *(Mendoza, 2014)*.

Los valores de la matriz dependen de los puntajes sobre los que se construyen los riesgos, es así que los riesgos se agrupan como se muestra en la figura 11.

La categorización de los riesgos permiten tomar decisiones sobre su tratamiento estos pueden ser: aceptar, mitigar y transferir.

Grupo	Enfoque de Mitigación
Grupo 1	Mitigar
Grupo 2	Mitigar o Transferir
Grupo 3	Transferir o Aceptar
Grupo 4	Aceptar

Figura 9. Enfoques de mitigación

En resumen los diferentes métodos OCTAVE permiten a la organización tener una visión fundada en el riesgo operativo de la seguridad y las direcciones de la tecnología en un contexto de negocios. (Caralli et al., 2007)

2.4.5. NIST SP800-30 National Institute of Standards and Technology

Metodología de análisis de riesgos desarrollado por NIST Estados Unidos en 1901. Se trata de una guía de documentos con información detallada sobre procedimientos técnicos que deberían ser adoptados para garantizar un alto nivel de desempeño y disponibilidad de los servicios dentro de una organización. El propósito principal es realizar la evaluación y gestión de riesgos en los sistemas de información. (Pazmiño, 2007, p. 17)

2.4.5.1. Fases

La metodología NIST SP 800-30 está compuesta por nueve pasos para el análisis de riesgo:

- Caracterización del sistema.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Control de análisis.
- Determinación de probabilidad.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de control.

- Resultado de la implementación o documentación (Matalobos, 2009).

2.4.5.2. Características

La metodología NIST SP 800-30 provee fundamentos para el desarrollo de un programa de administración de riesgos efectivo, conteniendo tanto las definiciones como una guía práctica necesaria para la evaluación y mitigación de riesgos identificados dentro de los sistemas de TI con el propósito de ayudar a las organizaciones mejorar la administración de riesgos relacionados con la misión de la TI. (Pazmiño, 2007)

2.4.6. COSO Committee of Sponsoring Organizations

Fue creada en el año de 1985 por el sector privado estadounidense. Está patrocinado y financiado por varias asociaciones e institutos de contabilidad como el Instituto Americano de Contadores Públicos Certificados (AICPA) y la Asociación de Contadores Americanos (AAA). El principal objetivo es identificar los motivos por el cual existen informes fraudulentos y realizar recomendaciones para minimizar el impacto. Contiene cinco componentes:

- Ambiente de control. Contiene varios puntos de control como: filosofía, estilo operativo de la gerencia, políticas y prácticas de recursos humanos, entre otros.
- Evaluación de riesgos. Su objetivo es identificar y analizar el riesgo.
- Actividades de control. Consiste en cerciorar que los empleados realicen las directivas de la gerencia a través de políticas y procedimientos entre ellos revisiones del sistema de control, control físico, control de sistemas de información.
- Información y comunicación. Consiste en recibir información y comunicar a toda la organización especialmente a los empleados, con el objetivo de comprender sus roles en el sistema de control interno. En el caso de que exista problemas estos deben ser comunicados o escalados a la alta gerencia.
- Monitoreo. En este componente se encarga la gerencia en monitorear las actividades de control y realizar evaluaciones en el sistema de control. Entre las actividades de control existe: comparación de los

activos físicos con los datos registrados, evaluaciones realizadas por auditores internos y externos. (Hidalgo, 2010)

2.4.6.1. Características

- COSO ofrece una guía para la elaboración de informes públicos sobre el control interno y provee materiales que la gerencia, auditores y otros pueden utilizar para evaluar un sistema de control interno.
- Brinda recomendaciones a la dirección sobre como evaluar, reportar y mejorar los sistemas de control.
- Provee un estándar contra el cual las organizaciones pueden evaluar sus sistemas de control y determinar cómo mejorarlos (Figueroa, 2014).
- Una de las principales características en el componente de evaluación de riesgos de COSO es que la gerencia es quien debe evaluar los riesgos. Para esto la gerencia debe establecer objetivos generales y específicos, e identificar y analizar los riesgos de no cumplirse los objetivos (Martínez, 2012).

2.5 Estándares de Análisis de Riesgos

2.5.1. ISO 27001

Es una norma internacional realizada por la Organización Internacional de Normalización (ISO) cuyo objetivo es gestionar la seguridad de la información en una empresa. Puede ser implementada en cualquier tipo y tamaño de organización ya sea con fines de lucro o no. El ISO 27001 se enfoca en la protección de la confidencialidad, integridad y disponibilidad de la información de la empresa, realizando una evaluación de riesgos para determinar los principales y potenciales problemas que podrían ser afectados la información. Para posteriormente mitigación o tratamiento del riesgo.

El procedimiento que realiza la norma ISO 27001 es brindar controles de seguridad o reglas organizacionales que se implementaran en la gestión de procesos, activos de información, recursos humanos, entre otros. En el cual permitirá prevenir violaciones de seguridad dentro de un sistema de gestión de seguridad de la información (SGSI). (27001 Academy, s.f.)

2.5.1.1. Beneficios

- Entre los beneficios que brinda la norma ISO 270001 se tiene:
- Cumplir requerimientos legales.
- Lograr ventaja comercial.
- Amenorar costos en implementar normas de seguridad.
- Lograr mejor organización (27001 Academy, s.f.).

2.5.1.2. Características

La norma ISO 27001 consta de 10 secciones y un anexo. Las secciones 0 a 3 son introductorias, de la sección 4 a 10 son obligatorias para la implementación en la organización para que cumplan las normas.

Puede ser implementada en cualquier tipo de organización, pública o privada.

Se orienta a la gestión de seguridad de una organización.

Es una de las normas principales a nivel mundial para la seguridad de la información (27001 Academy, s.f.).

2.5.1.3. Implementación

Para la implementación de la norma ISO 27001 se debe seguir los siguientes pasos:

- Obtener el apoyo de la dirección.
- Utilizar una metodología para gestión de proyectos.
- Definir el alcance del SGSI.
- Redactar una política de alto nivel sobre seguridad de la información.
- Definir la metodología de evaluación de riesgos.
- Realizar la evaluación y el tratamiento de riesgos.
- Redactar la Declaración de aplicabilidad.
- Redactar el Plan de tratamiento de riesgos.
- Definir la forma de medir la efectividad de sus controles y de su SGSI.
- Implementar todos los controles y procedimientos necesarios.
- Implementar programas de capacitación y concienciación.

- Realizar todas las operaciones diarias establecidas en la documentación de su SGSI.
- Monitorear y medir su SGSI.
- Realizar la auditoría interna.
- Realizar la revisión por parte de la dirección.
- Implementar medidas correctivas. (ISO27000.es, s.f.)

2.5.2. COBIT Control Objetives for Information and related Technology

Fue creado por la Asociación para la Auditoría y control de Sistemas de Información (ISACA) y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992. Su principal objetivo es ayudar a las organizaciones a mantener un balance entre las necesidades de control, cuestiones técnicas y los riesgos de control de la TI. COBIT permite que la información y tecnología sean administrados de forma holística en toda la organización; es decir que tanto la información y la tecnología conforma un sistema completo que se comporta de un modo distinto que la suma de sus partes. La última versión de COBIT es COBIT 5. Entre los objetivos principales:

- Incrementar la satisfacción del usuario con los acuerdos y resultados de la seguridad de información.
- Mejorar la integración de la seguridad de información y la organización.
- Reducir impacto de los incidentes de seguridad.
- Administrar costos relacionados con la seguridad de información.
- Proteger información sensible contra la divulgación (Sperat, 2010).

2.5.2.1. Características e implementación

Los principios y facilitadores son genéricos y útiles para las organizaciones o empresas de cualquier tamaño, ya sean públicas o privadas, con o sin fines de lucro. COBIT contiene cinco principios:

- Satisfacer las necesidades del accionista o partes interesadas. Consiste en mantener en equilibrio la realización de beneficios, el uso de recursos y gestión de riesgo.

- Cubrir a la organización de forma integral. Se lo realiza mediante la integración del Gobierno corporativo y el Gobierno de TI.
- Aplicar un único modelo de referencia integrado. Mediante el uso de COBIT permite la integración de modelos y buenas prácticas.
- Habilitar un enfoque holístico.
- Separar gobierno de la gestión. (Pastor, 2012)

COBIT contiene siete facilitadores:

- Principios, políticas y modelos de referencia. Consiste en guías para realizar tareas de gestión de TI.
- Procesos. Son un conjunto de prácticas y actividades que permiten alcanzar objetivos de las TI.
- Estructuras organizaciones.
- Culturas, éticas y comportamiento.
- Información.
- Servicios, infraestructura y aplicaciones.
- Gente, habilidades y competencias. (Pastor, 2012)

2.5.3. AS/NZS 4360:2004 Australia/ Estándar Nueva Zelanda 4360:2004

Es un estándar creado por el Comité Conjunto de Estándares de Australia/ Estándares Nueva Zelanda. Su primera versión fue en 1995. La versión más actual es la 2004. Siendo la última versión utilizada por varias empresas multinacionales. Su objetivo principal es proporcionar una guía para manejar el riesgo. Esta guía especifica los elementos del proceso de gestión de riesgos, pero no es el propósito de esta norma para hacer cumplir la uniformidad de los sistemas de gestión de riesgos. Es genérico e independiente de cualquier industria específica o sector económico. El diseño e implementación del sistema de gestión de riesgos se verán influenciadas por las diferentes necesidades de una organización, sus objetivos particulares, sus productos y servicios, y los procesos y prácticas específicas empleadas (Bueno, Correa, & Echeverry, 2010).

Los objetivos principales:

- Permitir la identificación de amenazas y oportunidades.
- Realizar una gestión proactiva y no reactiva.
- Mejorar la confianza con las partes interesadas.
- Mejorar el gobierno corporativo.
- Reducir pérdidas.

Características e implementación

Está conformado por cinco pasos:

- Alcance, ámbito de aplicación y definiciones. El estándar provee la identificación, análisis, tratamiento, monitoreo y alcance en varias actividades sean públicas, comerciales con y sin fines de lucro.
- Requerimientos de administración de riesgos. En este paso, el estándar indica a la organización que debe haber “un programa sistemático de administración de riesgos”, realizando lo siguiente: desarrollar una política de administración de riesgos. Precisar y planear los recursos, roles y responsabilidades de las personas que realizan dicho proceso. Programar la implementación. Realizar una revisión gerencial.
- Vista general de administración de riesgos. En este paso el estándar se concentra en: establecer el contexto, identificar, analizar, evaluar y tratar los riesgos para su posterior monitoreo y revisión.
- Establecer el contexto. En esta etapa se define tres tipos de contextos (organizacional, estratégico y administrativo) y cinco aspectos básicos para proveer una guía para la administración del riesgo.
- Identificación de riesgo. Consiste en identificar los riesgos a través de un proceso sistemático por ejemplo: lista de verificación, identificación basada en experiencia e historia, tormenta de ideas.
- Análisis de riesgo. En esta etapa el estándar se ocupa en clasificar los riesgos entre los que se necesita mitigar y cuáles no. Para realizar esta etapa se determina controles, probabilidad de ocurrencia y consecuencias. Señala además utilizar registros anteriores,

experiencia de la organización, prácticas, experimentos y prototipos, entre otros.

- Evaluación de riesgo. Consiste en realizar una lista de riesgos con prioridades para su posterior mitigación o aceptación del riesgo. Aquellos riesgos que se realizara dicha mitigación se procederá en la siguiente etapa (tratamiento de riesgo).
- Tratamiento de riesgo. Esta es la última etapa en el cual se encarga de identificar, evaluar y preparar el plan de tratamiento de riesgos e implementación.
- Proceso de administración de riesgos. Consiste en ejecutar los sietes pasos expuestos en la vista general de administración de riesgos.
- Documentación. Consiste en documentar la ejecución de cada paso expuesto en la vista general de administración de riesgos (Bueno, et al., 2010).

2.6 Cuadro de Revisión de las metodología para realizar el Análisis de Riesgos para la Unidad de Educación Virtual CEC-EPN

2.6.1. Metodologías para realizar el Análisis de Riesgos

Tabla 4. Metodologías de Análisis de Riesgos

Nombre	Fases	Documentación	Habilidad	Entregables	Acceso / Costo
CRAMM	1. Definir marco de gestión del riesgo. 2. Identificar riesgos. 3. Identificar propietarios de los riesgos. 4. Evaluar riesgos. 5. Definir niveles aceptables de riesgo. 6. Identificar respuestas adecuadas al riesgo. 7. Implantar respuestas. 8. Obtener garantías de la efectividad. 9. Monitorear y revisar.	Medianamente dispone documentación	Introducción: Especialistas Uso: Especialistas Mantenimiento: Especialistas	➢ Documento de inicio del proyecto. ➢ Informes de análisis de riesgos. ➢ Informes de Gestión de riesgos Plan de implementación.	Restringido / Pago
MAGERIT	1. Identificar los activos de la empresa. 2. Determinar las amenazas. 3. Establecer las respectivas salvaguardas. 4. Estimar Impacto. 5. Determinar Riesgo.	Existe documentación	Introducción: Sin experiencia Uso: Profesional de ITC Mantenimiento: Directivos	➢ Modelo de valor. ➢ Mapa de riesgos. Evaluación de salvaguardas. ➢ Estado de riesgo Informe de insuficiencias. ➢ Plan de seguridad.	Público / Gratis

Nombre	Fases	Documentación	Habilidad	Entregables	Acceso / Costo
MEHARI	1. Valorar de riesgo. 2. Tratar de riesgo. 3. Gestionar de riesgo.	Medianamente dispone documentación	Introducción: Nivel Estándar, Directivos Uso: Nivel Estándar, Auditores, Directores de Riesgo Mantenimiento: Nivel Estándar.	➢ Modelo de riesgos (cualitativo y cuantitativo). ➢ Escala de valores de malfuncionamiento. ➢ Clasificación de información y activos de TI.	Público / Gratis
OCTAVE	1. Construir perfiles de amenazas basados en los activos. 2. Identificar vulnerabilidades en la infraestructura. 3. Desarrollar estrategias y planes de seguridad.	Existe documentación	Introducción: Sin experiencia Uso: Sin experiencia Mantenimiento: Sin experiencia	➢ Estrategia de protección. ➢ Plan de Mitigación Lista de Acción.	Público / Gratis
NIST SP 800-30	1. Caracterizar el sistema. Identificar amenazas. 2. Identificar vulnerabilidades. 3. Controlar el análisis. 4. Determinar el riesgo. 5. Analizar el impacto. 6. Realizar recomendaciones de control. 7. Presentar resultado de la implementación o documentación.	Medianamente dispone documentación	Introducción: Sin experiencia Uso: Sin experiencia Mantenimiento: Sin experiencia	➢ Funciones del sistema. ➢ Criticidad de datos y sistemas. ➢ Sensibilidad de datos y sistemas. ➢ Definición de amenazas. ➢ Lista de vulnerabilidades. ➢ Lista de controles actuales y planificados. ➢ Rating de probabilidades e impacto. ➢ Riesgos y niveles de riesgo.	

Nombre	Fases	Documentación	Habilidad	Entregables	Acceso / Costo
COSO	1. Ambiente de control. 2. Evaluar riesgos. 3. Realizar actividades de control. 4. Informar y comunicar. Monitorear.	Medianamente dispone documentación	Introducción: Nivel Estándar, Directivos Uso: Nivel Estándar, Auditores, Directores de Riesgo Mantenimiento: Nivel Estándar.	➢ Visión Global de riesgo. ➢ Priorización de objetivos. ➢ Alineación de objetivos. ➢ Soporte a las actividades de planificación estratégica y control interno.	

2.6.2. Estándares para realizar el Análisis de Riesgos

Tabla 5. Estándares para realizar Análisis de Riesgos

Nombre	Fases / Principios	Documentación	Habilidad	Entregables	Acceso / Costo
ISO 27001	1. Fase de planificación 2. Fase de implementación 3. Fase de revisión 4. Fase de mantenimiento y mejora	Existe documentación	Introducción: Especialista Uso: Nivel Estándar Mantenimiento: Nivel Estándar	➢ Alcance y límites del Sistema de Gestión de Seguridad de la Información (SGSI). ➢ Documentación y puesta en marcha de la política de seguridad de la información. ➢ Roles y responsabilidades relativas a seguridad de la información. ➢ Análisis de riesgos y amenazas. ➢ Políticas, estándares, guías y procedimientos de seguridad de la información. ➢ Plan de tratamiento de riesgos. ➢ Declaración de Aplicabilidad (SoA). ➢ Programa de concientización. ➢ Modelo de control de documentación y registros del sistema.	Público / Pago
COBIT	1. Satisfacer las necesidades de las partes interesadas. 2. Cubrir a la empresa extremo a extremo. 3. Aplicar un marco de referencia único integrado. 4. Posibilitar enfoque holístico. 5. Separar el gobierno de la gestión. 6. Habilitadores: Gobierno corporativo de TI y Administración de TI corporativa.	Existe documentación	Introducción: Nivel Estándar Uso: Profesional de ITC Mantenimiento: Directivos	➢ Análisis de brechas e identificación del nivel de madurez de Cobit. ➢ Mejora del nivel de madurez de Cobit. ➢ Entendimiento de estrategia de TI.	Privado / Pago

Nombre	Fases	Documentación	Habilidad	Entregables	Acceso / Costo
AS/NZS 4360	1. Establecer el contexto estratégico, organizacional y de administración del riesgo. 2. Identificar y analizar los riesgos. 3. Determinar los controles existentes y los riesgos analizados en términos de consecuencia y probabilidad una vez aplicados los controles. 4. Comparar los niveles de riesgo contra los criterios preestablecidos. 5. Tratar, aceptar y monitorear los riesgos. 6. Comunicar al personal interno y terceros a la organización la gestión de riesgo realizada.	Medianamente dispone documentación	Introducción: Nivel Estándar, Directivos Uso: Nivel Estándar, Auditores, Directores de Riesgo Mantenimiento: Nivel Estándar	➢ Establecer el contexto. ➢ Identificación de riesgos. ➢ Análisis de riesgos. ➢ Evaluación de riesgos. ➢ Tratamiento de riesgos. ➢ Monitoreo y revisión. ➢ Comunicación y consulta.	Público / Pago

2.6.3. Selección, justificación de la metodología para elaborar el Análisis de Riesgos para la Unidad de Educación Virtual CEC-EPN

Con el objetivo de evidenciar las principales metodologías y estándares existentes en el mercado para la elaboración de análisis de riesgos, se realizó los cuadros de revisión, tablas 4 y 5, en ellas se reunión los siguientes aspectos:

- Fases o etapas que las componen.
- Disponibilidad de la documentación.
- Habilidades o experticia en el manejo.
- Entregables al final de la implementación.
- Tipo de acceso y costo.

Una vez realizado el cuadro de revisión se procedió a seleccionar una metodología acorde a las necesidades de la organización y especialmente que cumpla con los siguientes criterios:

- Simplicidad de las fases o pasos.
- Accesibilidad a la información a través de una guía práctica.
- Facilidad en la aplicación y manejo de la metodología (habilidad).
- El o los productos finales (entregables) se adapten a las necesidades de la organización.
- El enfoque principal sean los activos de información.

En función de los aspectos mencionados anteriormente se procedió a seleccionar a la metodología OCTAVE Allegro porque cumplió con todos los criterios.

En el Capítulo Tres se desarrollará el Análisis de Riesgos para la Unidad de Educación Virtual CEC-EPN empleando la metodología seleccionada.

2.7 Gestión de Continuidad del Negocio

El *Business Continuity Management* (BCM), se define como un proceso de gestión integral que identifica las amenazas potenciales de una organización y los impactos de estas sobre las operaciones del negocio, proporcionando una estructura organizacional resistente y una capacidad efectiva de respuesta que resguarde los intereses de los directivos, empleados, clientes, reputación, marca y las actividades que generen valor para la organización (Business Continuity Institute (BCI), s.f.).

2.7.1. Plan de Continuidad de Negocio

El *Business Continuity Plan* (BCP), es un conjunto de directrices, criterios, normas que ante la interrupción total o parcial de las operaciones del negocio, permite la recuperación de la operatividad de las mismas en el menor tiempo posible, de tal manera que las pérdidas económicas sean mínimas. (Instituto Nacional de Tecnologías de la Comunicación (INTECO) y Deloitte, s.f.)

2.7.2. Plan de Recuperación de Desastres

El *Disaster Recovery Plan* (DRP), es una parte del Plan de Continuidad de Negocio, es guía para la reanudación de las operaciones del negocio con respecto a los servicios de tecnología datos, hardware y software crítico, en caso de un desastre o incidente que afecte la continuidad del negocio. (Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior ICETEX, s.f.)

2.7.3. Plan de Contingencias

“Es un documento desarrollado en forma preventiva, con el objetivo de servir de guía de acción antes, durante y después de la ocurrencia de un imprevisto” (M&M Auditores de Colombia Ltda, p. 8).

2.7.4. Análisis de Impacto del Negocio

El *Business Impact Analysis* (BIA), es el proceso en el cual se analiza las actividades de negocio y las consecuencias que provocaría la interrupción de las mismas sobre la organización (INTECO) y Deloitte, s.f.).

2.7.5. Actividades a desarrollar en el BIA

Para el desarrollo del Análisis de Impacto es necesario realizar las siguientes actividades:

- Definir objetivos, alcance y suposiciones.
- Identificar áreas y procesos fundamentales.
- Evaluar el impacto financiero y estratégico.
- Identificar las funciones y procesos críticos del negocio.
- Identificar los sistemas y aplicaciones críticas de TI.
- Identificar MTD's (*Maximum Tolerable Downtimes*) y priorizar los procesos del negocio.
- Determinar RTO (*Recovery Time Objetive*) y WRT (Work Recovery Time).
- Determinar RPO (*Recovery Point Objetive*).
- Analizar el daño causado por una interrupción en el negocio (Montesdeoca, 2011).

2.8 Metodologías para elaborar un Plan de Continuidad

La Continuidad del Negocio es una buena práctica que debe replicarse en cualquier tipo de organización, su aplicación debe funcionar sin afectar a los procesos propios de la misma.

Para la elaboración del Plan de Continuidad del Negocio es necesario una estructura o metodología que permita establecer la estrategia a seguir para alcanzar el objetivo deseado.

2.8.1. DRII (Disaster Recovery Institute International)

DRI International (originalmente conocido como *Disaster Recovery Institute*) es una organización sin ánimo de lucro que proporciona formación a nivel internacional y está constituido como organismo de certificación de profesionales para la Gestión de la Continuidad de Negocio (BCM por sus siglas en inglés). DRI establece estándares profesionales para la planificación de la continuidad del negocio y sustenta las certificaciones de profesionales y de programas de formación de mayor prestigio en este área desde 1988. (Disaster Recovery Institute Spain, s.f.)

El objetivo principal es brindar las estrategias necesarias para la continuidad del negocio.

En el año de 1997 DRII publicó ocho mejores prácticas profesionales y en mayo de 2013 el DRII actualizó a diez prácticas.

De esta forma, según menciona DRII en su página web “Las secciones de estas normas no se presentan en ningún orden particular de importancia o secuencia, ya que puede ser necesario llevar a cabo o aplicar las secciones en paralelo durante el desarrollo del Programa de BCM” (Disaster Recovery Institute, s.f.).

2.8.1.1. Prácticas Profesionales del DRII

Las prácticas profesionales o áreas del conocimiento se describen a continuación:

- Inicio y Administración del Programa: establecer la necesidad de un programa BCM con los componentes de estrategias de resiliencia, planes de respuesta, restauración y recuperación, la continuidad del negocio. Los requisitos de la práctica incluyen obtener el apoyo de la administración, organizar y manejar la creación de las funciones o proceso requeridos para crear la estructura de BCM. (Disaster Recovery Institute, s.f.)
- Evaluación y Control de Riesgos: identificar los riesgos/amenazas y vulnerabilidades que pueden afectar adversamente a la entidad y a sus

recursos (ejemplos: personal, comodidades, tecnologías) a causa de la interrupción del negocio; la perdida potencial de estos eventos puede causar y los controles necesarios para evitar o mitigar los efectos de los riesgos. Como resultado, se requiere un análisis de los beneficios del costo para justificar la inversión en controles. (Disaster Recovery Institute, s.f.)

- Análisis del Impacto al Negocio: identificar los impactos de interrupciones del negocio que pueden afectar a la entidad y técnicas que pueden cuantificar y calificar dichos impactos. Identificar los procesos sensibles al tiempo, los requisitos para recuperarlos y las interdependencias para que los objetivos del tiempo de la recuperación puede ser establecidos y aprobados. (Disaster Recovery Institute, s.f.)
- Estrategias de Continuidad del Negocio: utilizar la información que fue obtenida durante el BIA y la evaluación de riesgos para desarrollar y recomendar estrategias de continuidad del negocio. La base de estas estrategias es el tiempo de recuperación y objetivos que apoyan las funciones críticos de la entidad. (Disaster Recovery Institute, s.f.)
- Preparación y Respuesta de Emergencia: esta práctica profesional define los requisitos para desarrollar e implementar el plan de la entidad para responder a emergencias y situaciones que pudieran impactar la seguridad de los empleados, visitantes u otros activos. El plan de respuesta de emergencia documenta cómo la entidad debe responder a emergencias de una forma coordinada, oportuna y efectiva, para atender la seguridad de vida y la estabilización de situaciones de emergencia hasta la llegada de personal entrenado o externo de primera respuesta. (Disaster Recovery Institute, s.f.)
- Planes de la Continuidad del Negocio: “crear, desarrollar e implementar planes de la continuidad del negocio que provee la continuidad y/o la recuperación como son identificados por los requisitos de la entidad” (Disaster Recovery Institute, s.f.)

- Programas de Concientización y Entrenamiento: “preparar un programa para establecer y mantener la concientización corporativa y mejorar las habilidades requisitas para desarrollar e implementar un plan de la continuidad del negocio” (Disaster Recovery Institute, s.f.).
- Ejercicio, Auditoría y Mantenimiento del Plan de Continuidad de Negocio: establecer un programa de ejercicios/pruebas que recuerda los requisitos del ejercicio del plan, incluyendo la planificación, horarios, facilitación, comunicación, auditoría y la documentación después de la revisión. Establecer un programa de mantenimiento para actualizar los planes. Establecer un proceso de auditoría que va a validar el cumplimiento con los estándares, revisar soluciones, verificar niveles aptas de mantenimiento y ejercer actividades y validar que los planes son actuales, correctos, y completos. (Disaster Recovery Institute, s.f.).
- Comunicación de Crisis: “desarrollar y recordar los planes de acción para facilitar la comunicación de información crítica de la continuidad. Coordinar, ejercer y asegurar con los involucrados la claridad de las comunicaciones de crisis” (Disaster Recovery Institute, s.f.)
- Coordinación con Dependencias Externas: “establecer políticas y procedimientos para coordinar actividades de respuesta, continuidad y recuperación con las dependencias externas, a nivel local, regional y nacional, a la vez que asegura el cumplimiento con los estatutos y regulaciones aplicables” (Disaster Recovery Institute, s.f.).

2.8.1.2. Fases de la Metodología DRII

La metodología del DRII se compone de siete fases, a continuación el siguiente gráfico

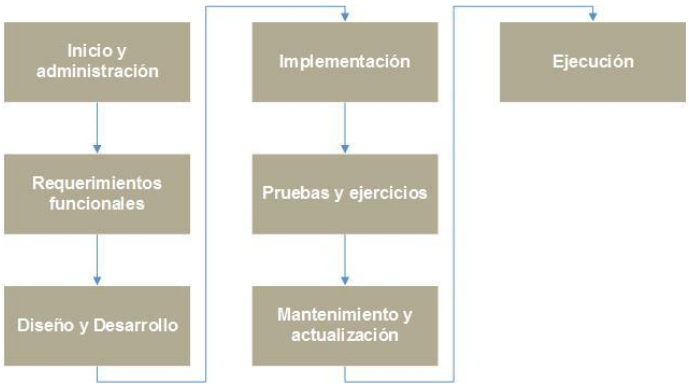

Figura 10. Fases de la metodología de DRII

Adaptado de (Romero, 2002, p.15)

Fase 1. Inicio y administración: en esta fase se define el problema, los objetivos, el alcance y los escenarios del plan, así como también la conformación del equipo de trabajo, sociabilización de la metodología y apoyo de los directivos al plan.

Entre las tareas a desarrollarse se tiene:

- Conformación de equipo de trabajo.
- Familiarización de la metodología con el equipo de trabajo.
- Especificar los objetivos, alcance y escenarios del problema.
- Estructurar la administración del proyecto: consiste en definir tareas y duración, establecer relaciones entre tareas y recursos, además se realizará el seguimiento, reportes de progreso y ajustes para la aprobación de los directivos.
- Aprobación de los directivos: al culminar las tareas, el equipo de trabajo presentará un informe a los directivos el cual será revisado y aprobado en caso de que no exista ninguna observación. (Asociación Bancaria y de Entidades Financieras, s.f.)

Fase 2. Requerimientos Funcionales: consiste en el estudio de las amenazas, vulnerabilidades, análisis de riesgos e impacto del negocio, así como también los

tiempos críticos los cuales permiten determinar estrategias con el propósito de disminuir el riesgo en las operaciones críticas del área.

Se realiza las siguientes actividades:

- Identificación de las funciones y servicios críticos del área: en esta actividad se enumera y prioriza las funciones y servicios que se realiza en el área, así como también los tiempos de espera para que se reanuden los servicios.
- Identificación de recursos críticos: consiste en establecer para cada función y servicio que recursos tecnológicos o lógicos se apoya, logrando así establecer la criticidad de los recursos en la organización.
- Recopilación de información: se recolecta la información sobre los empleados, clientes y proveedores que se encuentran dentro de los procesos y servicios del área.
- Análisis de riesgos y controles. está vinculado con la identificación de amenazas y riesgos de los recursos. Así como también con la verificación de controles existentes para las aplicaciones.
- Análisis de impacto. Se realizará una evaluación del impacto sobre los recursos y operaciones del área a través del análisis costo/beneficio del establecimiento de un control.
- Aprobación por parte de los directivos: después de terminar con las tareas anteriores el grupo debe presentar un informe de recomendaciones a los directivos quienes después de revisarlo consideren aprobarlo o solicitar cambios y continuar adelante con el proyecto. (Asociación Bancaria y de Entidades Financieras, s.f.)

Fase 3 y 4. Diseño e implementación: se especifica las estrategias y controles para mitigar los riesgos encontrados, se identifica los recursos necesarios, (personas, equipos de trabajo), además el organigrama de contingencias y notificación de sucesos.

Dentro de esta fase se realiza las siguientes actividades:

- Diseñar estrategias y controles.

- Identificar equipo para operación en contingencia.
- Realizar organigrama de contingencia.
- Diseñar sistema de notificación.
- Conectar con planes ya existentes de otras áreas funcionales.
- Elaborar el contenido del plan tentativo.
- Aprobar del proyecto por parte de los directivos. (Asociación Bancaria y de Entidades Financieras, s.f.)

Fase 5. Pruebas y ejercicios: consiste en diseñar las primeras pruebas, enfrentarse a situaciones que se contemplaron en el plan, probar los controles, calcular los tiempos de respuesta del personal, además establecer conclusiones para retroalimentar el plan. (Asociación Bancaria y de Entidades Financieras, s.f.)

Fase 6. Mantenimiento y actualización: se genera una bitácora de cambios al plan, para que permanezca vigente y funcional. (Asociación Bancaria y de Entidades Financieras, s.f.)

Fase 7. Ejecución: es la realización es sí del plan, el equipo de trabajo sabe qué hacer, a donde ir, a quien debe notificar durante una emergencia e inicia el procedimiento de recuperación del negocio. (Romero, 2002)

2.8.2. BCI (Business Continuity Institute)

El Instituto de Continuidad de Negocios (BCI) se creó en 1994 el cual ofrece una orientación y soporte en cuanto a las actividades profesionales relacionadas con la Continuidad del Negocio. A través de su sistema de certificación, el BCI provee reconocimiento internacional y competencia para llevar a cabo la gestión de continuidad del negocio al máximo nivel.

El principal objetivo es...“orientar a sus miembros y promocionar las normas más elevadas en materia de competencias profesionales y ética de las prestaciones y del mantenimiento de servicios y planificación de la continuidad de los negocios” (SGS Academy, s.f.).

Figura 11. Buenas Prácticas de BCI

Tomado de (Bird & Higgins, 2013, p. 7)

Su última actualización se realizó en Mayo de 2013, a continuación el código de buenas prácticas de BCI.

2.8.2.1. Buenas prácticas de BCI:

La guía de buenas prácticas es una herramienta diseñada para proporcionar una base de conocimiento en el área de Continuidad de Negocio, a continuación la descripción de las buenas prácticas:

PP1. Política y Administración del Programa: este punto se enfoca en definir una política para la organización en relación con el Plan de Continuidad, establecer cómo va a hacer implementado, controlado y validado a través de un programa de Gestión de Continuidad del Negocio (BCM).

Dentro de este punto se realiza las siguientes actividades:

- Establecer la Política de Plan de Continuidad y determinar el alcance del programa de BCM.
- Definir el gobierno y asignación de roles y responsabilidades.
- Implementar un programa de BCM, gestión de documentación usando programas y técnicas de gestión de proyectos.
- Gestión de las actividades subcontratadas y la cadena de suministros de continuidad. (Bird & Higgins, 2013)

PP2. Incorporando la Continuidad del Negocio (Cultura): la administración de las prácticas profesionales busca integrar el Plan de Continuidad en el día a día en las actividades del negocio y la cultura organizacional, a través de:

- Cultura Organizacional.
- Habilidades y Competencias.
- La gestión de un programa de formación.
- La gestión de una campaña de sensibilización. (Bird & Higgins, 2013)

PP3. Análisis: evalúa una organización en términos de cuáles son sus objetivos, su funcionamiento y las limitaciones del entorno en el que opera a través de:

- Análisis de Impacto del Negocio (BIA) o BIA inicial, estratégico, táctico y operacional.
- Análisis de Amenazas (incluye evaluación de riesgos). (Bird & Higgins, 2013)

PP4. Diseño: en este punto se identifica y selecciona las estrategias y tácticas apropiadas para la continuidad de los servicios, además las medidas para la mitigación de las amenazas y la estructura para la respuesta frente a incidentes. (Bird & Higgins, 2013)

PP5. Implementación: ejecuta las estrategias acordadas a través del proceso de desarrollo del Plan de Continuidad de Negocio. (Bird & Higgins, 2013)

PP6. Validación: confirma si el programa de BCM cumple con los objetivos establecidos en la política de Plan de Continuidad y si el plan adecuado para el propósito.

En este parte se realiza las siguientes tareas.

- Planificar un programa de ejercicios.
- Desarrollar un plan de ejercicios.
- Realizar el mantenimiento del programa BCM.
- Revisar el programa de BCM. (Bird & Higgins, 2013)

2.9 Estándares y Buenas Prácticas para el desarrollo de un Plan de Continuidad.

Existen diferentes estándares internacionales que ayudan a la elaboración de un Plan de Continuidad a continuación los más destacados.

2.9.1. Normal Internacional de Gestión de Continuidad de Negocio ISO 22301

"El nombre completo de esta norma es ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio – Requisitos. Esta norma fue redactada por los principales especialistas en el tema y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización" (27001 Academy, s.f.).

El propósito de este estándar es disminuir los daños potenciales provocados por incidentes gestionando la continuidad del negocio, así como también prepara al equipo de la organización a responder a dichos incidentes.

Este estándar puede ser implementado en cualquier tipo de organización con o sin fin de lucro ya sea pública o privada (27001 Academy, s.f.).

2.9.2. ITIL® (IT Infraestructure Library)

Aparece en la década de 1980, elaborada por el gobierno de Gran Bretaña, con el objetivo de desarrollar una metodología estándar para garantizar una entrega

eficaz y eficiente de los servicios de TI, el resultado fue la publicación de la Biblioteca de la Infraestructura de Tecnología de la Información (ITIL), la cual está conformada por varias “Mejores Prácticas” para los servicios de TI (Van Bon, y otros, 2008).

2.9.2.1. Ventajas

La implementación de ITIL permitirá a la organización gestionar de mejor manera los servicios de TI en el negocio, así como también:

- Desarrollar una estructura más clara y se orienta hacia los objetivos de la empresa.
- Mejorar la utilización de recursos.
- Permitir que la organización sea más competitiva.
- Reducir y eliminar tareas repetitivas.
- Mejor gestión de la calidad, la disponibilidad, confianza y seguridad de los servicios de TI.
- Justificar el coste de la calidad de servicio, entre otros (Van Bon, y otros, 2008) .

2.9.2.2. Características e Implementación

Consta de cinco libros en el cual se centra y procede con los siguientes puntos:

- ITIL Estrategia del servicio. Se encarga de garantizar la optimización de procesos, tomando como base la administración de portafolios de servicio, administración de demandas y administración financiera. Entre los procesos a optimizar se tiene: gestión financiera, generación de la estrategia, gestión de la demanda y gestión de la cartera de servicios.
- ITIL Diseño del servicio. Se encarga de convertir los objetivos estratégicos de la organización en portafolios de servicios y activos de servicios; mediante el diseño y desarrollo de servicios y procesos de administración de servicios.
- ITIL Transición del servicio. Define como los procesos de estrategia y diseño del servicio se realizan en la operación del servicio, con el propósito de controlar los riesgos en caso de que exista una falla en los procesos

anteriores, así como también realiza una mejora de las capacidades de transición a producción de los servicios nuevos o modificados.

- ITIL Operación del servicio. Presenta los procesos y actividades diarias de soporte y administración de los niveles de servicios con los usuarios finales. Con el propósito de que el negocio de la organización cumpla sus objetivos, reducir el costo y mejorar la calidad de servicio al usuario final.
- ITIL Mejora Continua de Servicio. Consiste en guías y en mejores prácticas para la administración de la calidad en los servicios para los usuarios finales (Van Bon, y otros, 2008).

En este apartado se hará referencia únicamente a la Gestión de la Continuidad del Servicio, sobre el punto llamado Gestión de Continuidad de Servicios de TI (ITSCM).

En la figura 12, se muestra los pasos para el desarrollo del Plan de Continuidad.

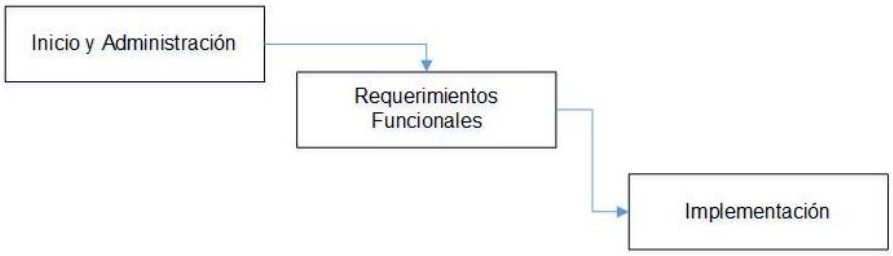

Figura 12. Proceso para el desarrollo del Plan de Continuidad.

Al final se obtendrá un documento escrito para la Dirección del CEC-EPN, como una guía para la Unidad de Educación Virtual.

2.10 Cuadro de Revisión y Selección de la Metodología para elaborar un Plan de Continuidad para la Unidad de Educación Virtual CEC-EPN

2.10.1. Metodologías para elaborar un Plan de Continuidad

Tabla 6. Revisión de diversas metodologías de Plan de Continuidad

Nombre	Mejores prácticas /Código de buenas prácticas	Documentación	Habilidad	Entregable	Acceso /costo
DRII	1. Inicio y administración del programa. 2. Evaluación y control de riesgos. 3. Análisis de impacto al negocio. 4. Estrategias de continuidad del negocio. 5. Respuesta y operaciones de emergencia. 6. Planes de continuidad del negocio. 7. Programas de creación de conciencia y entrenamiento. 8. Ejercicios, auditoría y mantenimiento del plan de continuidad del negocio. 9. Comunicación en crisis. 10. Coordinación con agencias públicas externas.	Existe documentación	Introducción: Nivel Estándar Uso: Nivel Estándar Mantenimiento: Especialista	Plan de Continuidad de Negocio (BCP)	Público / Gratis
BCI	PP1. Administración del Programa. PP2. Incorporando la Continuidad del Negocio (Cultura). PP3.Análisis. PP4.Diseño. PP5.Implementación. PP6. Validación.	Medianamente dispone documentación	Introducción: Especialistas Uso: Especialistas Mantenimiento: Especialistas	Plan de Continuidad de Negocio (BCP)	Privado/pago

2.10.2. Estándares para elaborar un Plan de Continuidad

Tabla 7. Revisión de diversos estándares para elaborar un Plan de Continuidad

Nombre	Mejores prácticas /Código de buenas prácticas	Documentación	Habilidad	Entregable	Acceso /costo
ISO 22301	1. Introducción. 2. Alcance. 3. Referencia a Normativas. 4. Términos y Definiciones. 5. Contexto de la Organización. 6. Liderazgo. 7. Planeamiento. 8. Soporte. 9. Operación. Evaluación de Desempeño. 10. Mejora continua.	Medianamente dispone documentación	Introducción: Nivel Estándar, Directivos Uso: Nivel Estándar, Auditores, Directores de Riesgo Mantenimiento: Nivel Estándar	Sistema de Continuidad del Negocio (BSI)	Público / Gratis
COBIT	1. Planeación y organización. 2. Adquisición e implementación. 3. Servicios y Soporte.	Existe documentación	Introducción: Sin experiencia Uso: Profesional de ITC Mantenimiento: Directivos	Plan de Continuidad de Negocio (BCP)	Privado/pago
ITIL	1. Política y Alcance. 2. Análisis de Impacto. 3. Evaluación de Riesgos. 4. Estrategias de Continuidad. 5. Organización y Planificación. 6. Supervisión.	Existe documentación	Introducción: Nivel Estándar, Directivos Uso: Nivel Estándar, Auditores, Directores de Riesgo Mantenimiento: Nivel Estándar.	Gestión de Servicios Informáticos	Público / Gratis

2.10.3. Selección, justificación de la metodología y estándar para elaborar un Plan de Continuidad para la Unidad de Educación Virtual CEC-EPN

Al igual que la selección de la metodología para análisis de riesgo, en las tablas 6 y 7, se tomaron en consideración los siguientes criterios: simplicidad en los pasos o fases para desarrollar la metodología, disponibilidad de la documentación (consulta), grado de conocimiento de los analistas, habilidad de las personas que utilizan y manejan los diferentes sistemas, y el producto final (entregables).

Para elaborar el Plan de Continuidad se seleccionó la metodología DRII y las buenas prácticas de ITIL por las siguientes razones:

- La metodología DRII es práctica y detallada, identifica claramente los recursos con los que cuenta la organización a fin de elaborar el plan de continuidad, además se complementa con ITIL.
- El uso de las buenas prácticas de ITIL permiten elaborar un plan robusto y acorde a las necesidades de la organización a través de los entregables.
- Accesibilidad a la información a través de guías y experiencias de empresas en el desarrollo de planes de continuidad.
- Conocimientos básicos y experiencia del CEC-EPN en el uso de la metodología DRII y las buenas prácticas de ITIL.

En el Capítulo Cuatro se elaborará el Plan de Continuidad para la Unidad de Educación Virtual CEC-EPN empleando la metodología DRII y las buenas prácticas de ITIL.

Capítulo III

3 Análisis de riesgos informáticos en la Unidad de Educación Virtual CEC-EPN

3.1 Portafolio de Servicios de la Unidad de Educación Virtual

Para realizar el análisis de riesgos es necesario conocer los servicios que presta la UEV a través del portafolio se puede conocer las actividades que presta cada una de las áreas, el siguiente catálogo de servicios, los cuales están divididos en las siguientes áreas:

Tabla 8. Portafolio de Servicios UEV

Área	Servicios
Coordinación	➢ Gestiona y desarrolla los planes operativos y estratégicos de la UEV. ➢ Define políticas y normativas para el desarrollo de cursos virtuales. ➢ Identifica nuevas oportunidades de diseño de cursos virtuales. ➢ Brinda asesoría sobre la implementación de nuevos proyectos *e-learning.* ➢ Gestiona alianzas estratégicas y convenios interinstitucionales en beneficio de la UEV. ➢ Evalúa los resultados de la gestión académica y administrativa de la unidad para la aplicación de planes y proyectos de mejora continua.
Académica	➢ Diseño Pedagógico de cursos virtuales. ➢ Diseño Instruccional de cursos virtuales. ➢ Diseña recursos utilizando objetos de aprendizaje. ➢ Desarrollo de cursos virtuales. ➢ Adaptación de contenidos a formato *e-learning*. ➢ Desarrollo de informes finales de cursos virtuales. ➢ Seguimiento a tutores y estudiantes de cursos virtuales CEC-EPN. ➢ Evaluación a tutores virtuales.
Gestión	➢ Gestión de estudiantes matriculados en cursos virtuales CEC-EPN. ➢ Genera información estadística de los cursos virtuales. ➢ Elaboración de proformas y cotizaciones para clientes internos y externos de la UEV. ➢ Análisis financieros. ➢ Gestionar envió de certificados de aprobación de cursos virtuales. ➢ Administra contratos, pagos y facturas de los clientes internos y externos de la UEV. ➢ Atención al cliente.

Área	Servicios
Tecnologías de la Información	➢ Autentificación de usuarios y recursos. ➢ Gestión de roles y perfiles. Soporte técnico a estudiantes de cursos virtuales. ➢ Creación y renovación de cursos virtuales. ➢ Almacenamiento de copias de seguridad de cursos virtuales. ➢ Servicio de asignación de claves para las plataformas virtuales. ➢ Soporte de aplicaciones de la UEV. ➢ Mantenimiento de plataformas virtuales. ➢ Administración de Servidores de la UEV. ➢ Configuración de plataformas virtuales. ➢ Gestión de plataforma de videoconferencia. ➢ Análisis y viabilidad tecnológica de soluciones *E-learning*.
Diseño Gráfico	➢ Desarrollo de objetos y materiales gráficos. ➢ Desarrollo de recursos multimedia. ➢ Desarrollo de artes gráficos para la imagen UEV. ➢ Elaboración de propuestas gráficas para proyectos *E-learning*.

3.2 Aplicación de la Metodología OCTAVE Allegro

3.2.1. Fase I. Establecer controles

3.2.1.1. Primer Paso: Definición de Criterios de Medida del Riesgo

Como parte de este paso se desarrollan dos actividades iniciales.

Actividad 1: Criterios de Medida de Riesgo

Antes de mencionar los criterios de medida de riesgo es necesario considerar ciertos factores dentro de la UEV:

- Estudiantes CEC-EPN, forman parte de la misión de la organización, las decisiones y planificaciones se realiza en función de ellos.
- Empleados de la UEV, son las personas que se encargan de cumplir actividades y tareas, para la consecución de los objetivos dentro de la unidad.

Tabla 9. Número de estudiantes y empleados en el año 2013

Año	Descripción	Valor
2013	Número de estudiantes CEC-EPN	**2798 estudiantes**
	Número de empleados UEV	8 empleados

Adaptado de (Martínez , 2015)

Tabla 10. Número de estudiantes y empleados en el año 2014

Año	Descripción	Valor
2014	Número de estudiantes CEC-EPN	**3651 estudiantes**
	Número de empleados UEV	9 empleados

Adaptado de (Martínez, 2015)

Para esta actividad la Coordinación de la Unidad de Educación Virtual ha seleccionado tres criterios de los cinco que incluye la metodología, a continuación las razones que motivaron la selección y los criterios de medida de riesgo:

1. Posicionamiento y Fidelización de los Clientes: es una adaptación del área de impacto de Reputación y Confianza del Cliente de la metodología de OCTAVE Allegro, por otro lado el criterio se enfoca en el cliente, ya que para el CEC- EPN los clientes son su razón de ser, este criterio permite conocer el grado de afectación del posicionamiento del cliente y su fidelidad frente a la organización.

   Dentro del Manual de Calidad en la Política de Calidad del CEC-EPN se indica: “Mantener permanentemente, en el campo de la Educación Continua, un compromiso de servicio de calidad con nuestros clientes, entendiendo sus requerimientos, logrando su satisfacción con oportunidad, mejoramiento continuo, creatividad y visión de país; cumpliendo la legislación pertinente” (CEC-EPN, 2013, p. 9).

Tabla 11. Criterio de medida de riesgo – Posicionamiento y Fidelización de los Clientes

Hoja de trabajo Metodología OCTAVE Allegro			
Criterio de medida del Riesgo - Posicionamiento y Fidelización de los Clientes			
Área de Impacto	**Bajo**	**Moderado**	**Alto**
Posicionamiento de la UEV-CEC-EPN	El posicionamiento es: Mínimamente afectado; poco o ningún esfuerzo o gasto es requerido para recuperarse.	El posicionamiento es: Afectado y algún esfuerzo y gasto es requerido para recuperarse.	El posicionamiento es: Irreparablemente afectado o destruido.

Hoja de trabajo Metodología OCTAVE Allegro			
Criterio de medida del Riesgo - Posicionamiento y Fidelización de los Clientes			
Área de Impacto	**Bajo**	**Moderado**	**Alto**
Fidelización del cliente	Reducción de clientes de cursos virtuales debido a la pérdida de confianza menor al 1% anual.	Reducción de clientes debido a la pérdida de confianza de 2% al 4% anual.	Reducción de clientes debido a la pérdida de confianza mayor al 5 anual%.

Nota. El valor total de estudiantes considerados para el cálculo de los porcentajes en el área Fidelización del cliente se basan en el promedio de estudiantes en los años 2013 – 2014, (promedio 3225 estudiantes).

2. Económico, es una de las áreas primordiales para la organización porque permite identificar el grado de afectación sobre los costos de operación, ingresos de la Unidad, este criterio apoya a la toma de decisiones de la alta gerencia.

Tabla 12. Criterio de medida de riesgo – Económico

Hoja de trabajo Metodología OCTAVE Allegro			
Criterio de medida del Riesgo - Económico			
Área de Impacto	**Bajo**	**Moderado**	**Alto**
Costos de Operación	Aumento de los costos de operación menor al 1% anual.	Aumento de los costos de operación de 2% al 4% anual.	Aumento de los costos de operación mayores al 5% anual.
Disminución de los Ingresos	Perdida de los ingresos menor al 1% anual.	Perdida de los ingresos de 2% al 4% anual.	Perdida de los ingresos mayores al 5% anual.

Nota. Los valores considerados para el cálculo de los porcentajes en las dos áreas se basan en los ingresos y costos de operación de la UEV, esta información es confidencial por esta razón no fueron incluidas en las tablas 9 y 10.

3. Productividad, se refiere a la productividad laboral, a través de este criterio se analizará la relación entre las horas de trabajo de una persona y la producción alcanzada en el mismo período de trabajo. El personal

es un recurso importante con el que cuenta la UEV para la consecución de sus objetivos.

Tabla 13. Criterio de medida de riesgo – Productividad

Hoja de trabajo Metodología OCTAVE Allegro			
Criterio de medida del Riesgo - Productividad			
Área de Impacto	**Bajo**	**Moderado**	**Alto**
Productividad de la mano de obra,	Disminución de la productividad del personal por interrupción de los servicios necesarios para cumplir con las actividades diarias en el lugar de trabajo menor al 1% anual.	Disminución de la productividad del personal por interrupción de los servicios necesarios para cumplir con las actividades diarias en el lugar de trabajo entre el 2% y 5% anual.	Disminución de la productividad del personal por interrupción de los servicios necesarios para cumplir con las actividades diarias en el lugar de trabajo mayor al 6% anual.
Carga laboral de la mano de obra.	Aumento de la carga laboral del personal menor al 1% anual.	Aumento de la carga laboral del personal entre el 2 y 5% anual.	Aumento de la carga laboral del personal mayor al 6% anual.

Nota. Para realizar el cálculo de los porcentajes en las dos áreas indicadas, se consideran 1736 horas anuales realizada por un empleado de la UEV, se descuentan las vacaciones y feriados.

Una vez identificados los criterios de medición de riesgos, la metodología OCTAVE Allegro menciona que se debe reconocer las áreas de impacto de la organización que sean más significativas.

Actividad 2: Priorización de las Áreas de Impacto

Todas las áreas de impacto deben ser clasificadas y tener una ponderación según los intereses de la organización tal como se realizó en las tablas 11, 12 y 13; la priorización se utilizará después para la evaluación del riesgo, la puntuación obtenida ayudará a la organización a determinar la forma como se deben abordar los riesgos identificados.

De igual manera la Coordinación de la UEV estableció el orden de priorización de las áreas de impacto de la siguiente manera:

Tabla 14. Priorización de las Áreas de Impacto

Prioridad	Áreas de Impacto
3	Posicionamiento y Fidelización de los Clientes.
2	Económica
1	Productividad

3.2.2. Fase II. Establecer perfiles de activos de información

3.2.2.1. Segundo Paso: Desarrollo de los Perfiles de Activo de Información

En este paso se identifican la colección de activos de información para la UEV, los mismos que servirán para la evaluación de riesgos.

Actividad 1: Identificación de la colección de activos de información para la UEV

La identificación se la realizó a través de un banco de preguntas, las mismas que fueron empleadas en una encuesta. Esta actividad contó con la participación de seis personas del equipo de la UEV.

Las preguntas y resultados se muestran en el Anexo 1, página 165.

Las tablas 15, 16, 17 y 18 muestran un resumen de los resultados obtenidos, se seleccionaron los activos de información que se ubican en los tres primeros lugares para un mejor análisis.

Tabla 15. Resumen de la pregunta 1 ¿Cuáles son los activos de información de mayor valor para la organización, según su criterio?

Número	Activos de Información	Respuesta
1	Plataforma Gestor de Cursos Virtuales Moodle	100%
2	Respaldos de Cursos Virtuales	100%
3	Contratos y Convenios	86%
4	Sistema Académico SIICECW	71%
5	Materiales para diseño de cursos virtuales	71%
6	Recursos Multimedia e Imágenes	71%
7	Planes y programa de cursos	71%
8	Archivos de accesos y claves	71%

Nota: Los tres primeros puestos se determinan por el valor que representan dentro de la tabulación de los resultados.

Tabla 16. Resumen de la pregunta 2 ¿Qué activos de información se utiliza en los procesos de trabajo del día a día, según su criterio?

Número	Activos de Información	Respuesta
1	Plataforma Gestor de Cursos Virtuales Moodle	100%
2	Sistema Académico SIICECW	71%
3	Respaldos de Cursos Virtuales	57%
4	Materiales para diseño de cursos virtuales.	57%
5	Objetos de aprendizaje	57%
6	Recursos Multimedia e Imágenes	57%
7	Proformas y Cotizaciones	57%
8	Archivos de accesos y claves	57%

Nota: Los tres primeros puestos se determinan por el valor que representan dentro de la tabulación de los resultados.

Tabla 17. Resumen de la pregunta 3 ¿Qué activos de información, en caso de pérdida, interrumpiría considerablemente la capacidad de su organización para cumplir sus objetivos y contribuir a la consecución de la misión de la organización?

Número	Activos de Información	Respuesta
1	Plataforma Gestor de Cursos Virtuales Moodle	100%
2	Sistema Académico SIICECW	86%
3	Proformas y Cotizaciones	71%

Tabla 18. Resumen de la pregunta 4 ¿Qué activos en su lista, si es comprometida, tendría un impacto negativo en la organización si sucede una o más situaciones?

Número	Activos de Información	Resultados
1	Plataforma Gestor de Cursos Virtuales Moodle	86%
2	Sistema Académico SIICECW	57%
3	Respaldos de Cursos Virtuales	57%
4	Correo electrónico	43%
5	Planes operativos y estratégicos de la UEV	43%
6	Informes Académicos	43%
7	Proformas y Cotizaciones	43%

Nota: El enunciado completo de la pregunta se encuentra en el Anexo 1, página 165, los tres primeros puestos se determinan por el valor que representan dentro de la tabulación de los resultados.

Actividad 2: Identificación de los principales activos de información para la UEV.

Después de conocer los resultados de la encuesta, se validó con la Coordinación de la UEV los activos críticos de información, que fueron recopilados en la actividad anterior Anexo N°1 página 165. De esta manera se seleccionaron solo tres activos críticos ya que son los más representativos y significativos dentro la UEV. El análisis se centra en los activos críticos de información, ya que estos deben responder con el cumplimiento de la misión de la organización.

Para evitar imprecisiones en los límites de los activos, es importante describir con claridad y definir los requisitos de seguridad adecuadamente. Para ello se utilizará la hoja de trabajo proporcionada por la metodología OCTAVE Allegro denominada: Perfil de los Activos Críticos.

Tabla 19. Plantilla hoja de trabajo N°1, Perfil de los Activos Críticos

Hoja de trabajo Metodología OCTAVE Allegro			
Perfil de los Activos Críticos			
Activo Crítico (a)	**Justificación (b)**	**Descripción (c)**	
Propietarios (d)			
Requisitos de Seguridad (e)			
Confidencialidad			
Integridad			
Disponibilidad			
Requisitos de seguridad más importantes (f)			
Confidencialidad ☐	Integridad ☐	Disponibilidad ☐	Autentificación ☐

Los ítems o campos que se presentan en la tabla 19 son:

- Activo crítico: describe al recurso más importante para una organización. Son utilizados para alcanzar objetivos, proporcionan un retorno de la inversión y generar ingresos.

- Justificación: es la razón por la cual el activo de información es importante para la organización.
- Descripción: son los detalles y características que tiene el activo.
- Propietarios: es o son los dueños del activo de información.
- Requisitos de Seguridad: cómo se ve afectado el activo si es vulnerado a nivel de confidencialidad, disponibilidad e integridad.
- Requisitos de Seguridad que son más importantes: en este campo se señala cuál de los requisitos (confidencialidad, integridad, disponibilidad y otros) es el más importante para el activo analizado. (Caralli et al., 2007)

Una vez identificada la plantilla para registrar los perfiles de los activos de información, se procede a describir los tres principales activos críticos de información encontrados en la UEV:

1. Sitios Web CEC-EPN: considerando que este activo no aparece en los primeros puestos de la lista de los activos de información en la encuesta realizada Anexo N°1 página 165 es necesario incluirlo como activo crítico porque son los medios de información y promoción de los cursos de capacitación de la organización, siendo parte del proceso de inscripción y matriculación de los cursos virtuales; cualquier inconveniente afecta directamente al giro del negocio, especialmente en temporada de matrículas.

   Esta información es ratificada por la investigación que presentó la Coordinación de Marketing del CEC-EPN, sobre la forma de enterarse de los cursos por instituciones dice que: “CEC-EPN: Búsqueda en página web, junto con las recomendaciones recibidas son los principales aspectos por los que los encuestados afirmaron enterarse de los cursos…” (EKOS Unidad de Investigación Económica y de Mercado, 2014, p. 14).

   También la investigación manifiesta que “…el internet es la principal herramienta de búsqueda para recibir información de cursos de capacitación con un 66.6% en Quito…” (EKOS Unidad de Investigación Económica y de Mercado, 2014, p. 15).

En la actualidad el Centro de Educación Continua dispone de dos sitios web:

- Sitio Web CEC: es el sitio web general del Centro de Educación Continua, el cual contiene la información institucional y la promoción de los cursos de las tres áreas productivas: Lingüística, Capacitación Presencial y Unidad de Educación Virtual.

  El sitio web posee un módulo especial para la inscripción y matriculación de los cursos, el cual es suministro para el sitio web de Virtual. La información es gestionada por un responsable de cada unidad productiva y la Coordinación de Tecnología, en el caso de los cursos virtuales es gestionada por el Área de TI de la UEV. Apoya a los procesos de Inscripción, Matriculación y Promoción de Cursos Virtuales de la UEV.
- Sitio Web de Virtual: es el sitio web que contiene la información de la unidad, sirve para la promoción, difusión de cursos virtuales y eventos. Es la primera línea de la publicidad de los cursos virtuales. Apoya al proceso de Inscripción, Matriculación y Promoción de cursos virtuales, la diferencia entre el sitio web CEC y sitio web de Virtual es que este último activo es gestionado por el Área de TI de la UEV.

2. Sistema Integrado de Información del CEC-EPN (SIICECW): se considera como un activo crítico porque es el sistema que se encarga de gestionar, almacenar la información personal y académica de los estudiantes de los cursos virtuales.

   Este sistema es conocido como SIICECW, aquí se registran los datos de las empresas y personas, las calificaciones obtenidas por los estudiantes, así como también se genera los certificados de aprobación de los cursos de capacitación del CEC-EPN.

   Apoya al proceso de Inscripción, Matriculación y Contratación de Instructores de Cursos Virtuales. Este activo es gestionado por la Coordinación de Tecnología CEC-EPN.

3. Gestores de Cursos Virtuales CEC-EPN y EPN: son los Sistemas de Gestión de Aprendizaje o también conocidos como *Learning Management System* (LMS) a través de los cuales se realiza el proceso de capacitación virtual, almacenan las actividades, recursos y calificaciones de los estudiantes de los cursos virtuales CEC-EPN, así como también son el soporte académico de las materias de la EPN. Los gestores son parte de los pilares fundamentales del negocio de la UEV.

   En función de lo antes mencionado cabe resaltar que son los espacios donde el personal de la unidad, docentes, tutores virtuales y estudiantes ejecutan el proceso de capacitación, permitiendo así cumplir con las actividades diarias; son estas razones que lo convierten en un activo crítico.

   La Unidad de Educación Virtual administra cinco plataformas virtuales, distribuidas de la siguiente manera:

- Gestores de cursos virtuales CEC-EPN, son LMS's que almacenan las calificaciones, actividades, recursos, participaciones de los estudiantes y tutores virtuales del CEC-EPN. Apoyan al proceso de Desarrollo y Ejecución de Cursos Virtuales.
  Plataforma Moodle CEC-EPN.
  Plataforma Moodle CEC-EPN V2.
  Plataforma Moodle CEC-INEPE.
- Gestores de cursos virtuales como apoyo académico para la EPN, son LMS's que almacenan calificaciones, actividades, recursos, participaciones de los estudiantes y docentes EPN, estos gestores son utilizados como apoyo académico a las clases presenciales. Apoyan al proceso de Soporte EPN.
  Plataforma Moodle PREGRADO.
  Plataforma Moodle POSGRADO

Los perfiles de los activos de información críticos descritos anteriormente se encuentran detallados en el Anexo N°2 página 169.

3.2.2.2. Tercer Paso: Identificación de los Contenedores de los Activos de Información para la UEV

El método OCTAVE Allegro propone el uso de la hoja de trabajo: Mapa de Ambiente de Riesgos de los Activos de Información, el cual describe las características e información del contenedor y el propietario del activo.
La información presentada en este paso fue obtenida a través de entrevistas realizadas a la Coordinadora de Tecnología del CEC-EPN y al personal UEV.

Actividad 1: Identificación de contenedor técnico

Dentro de este contenedor se colocan los recursos de hardware, software (sistemas), para la UEV. A continuación la explicación de la plantilla hoja de trabajo.

Tabla 20. Plantilla hoja de trabajo N°2 (a): Mapa de Ambiente de Riesgos de los Activos de Información – Técnico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información - Técnico	
INTERNO	
Descripción del Contenedor (1)	Propietario(s) (2)
EXTERNO	
Descripción del Contenedor	Propietario(s)

Adaptado de (Caralli et al., 2007, p. 83)

Los ítems o campos que se presentan en la tabla 20 son:

1. Descripción del Contenedor: detalla los sistemas y hardware utilizados para almacenar, transportar o procesar los activos de información.
2. Propietario(s): es el custodio del activo de información.

Actividad 2: Identificación de contenedor físico

En este contenedor se indica la localización física de los activos de información para la UEV. A continuación la explicación de la plantilla hoja de trabajo.

Tabla 21. Plantilla hoja de trabajo N°2 (b): Mapa de Ambiente de Riesgos de los Activos de Información – Físico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información - Físico	
INTERNO	
Descripción del Contenedor (1)	Propietario(s) (2)
EXTERNO	
Descripción del Contenedor	Propietario(s)

Adaptado de (Caralli et al., 2007, p. 85)

Los ítems o campos que se presentan en la tabla 21 son:

1. Descripción del Contenedor: detalla los lugares donde los activos se almacenan, transportan o procesan.
2. Propietario(s): es el custodio del activo de información.

Actividad 3: Identificación de contenedor personas

En este contenedor se indica el personal interno y externo de la UEV que conoce del activo de información. A continuación la plantilla hoja de trabajo que se utilizará en esta actividad.

Tabla 22. Plantilla hoja de trabajo N°2 (c), Mapa de Ambiente de Riesgos de los Activos de Información – Personas

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información - Personas	
PERSONAL INTERNO	
Nombre o Rol/Responsabilidad (1)	Área/Departamento (2)
PERSONAL EXTERNO	
Contratista, Proveedor (3)	Organización (4)

Adaptado de (Caralli et al., 2007, p. 87)

Los ítems o campos que se presentan en la tabla 22 son:

1. Nombre o Rol/Responsabilidad: son los datos de las personas que intervienen en los activos de información (interno).
2. Área/Departamento: indica el área al que pertenece la persona responsable del activo de información.
3. Contratista, Proveedor: indica los datos del responsable del activo de información (externo).
4. Organización: indica el nombre de la empresa a la que pertenece el contratista, proveedor.

Los contenedores de los activos de información se encuentran definidos en el Anexo N°3 página 176.

3.2.3. Fase III. Identificar Amenazas

3.2.3.1. Cuarto Paso: Identificación de las Áreas de Preocupación para la UEV

La identificación de las áreas se realizó en base a los requisitos de seguridad analizados en el Segundo Paso, creación de perfiles de activos de información Anexo N°2 página 169.

Actividad 1: Establecer las Áreas de Preocupación para la UEV

Las principales Áreas de Preocupación fueron identificadas de manera conjunta entre la coordinación de la UEV y los desarrolladores del proyecto a través de entrevistas y lluvia de ideas, de manera resumida las áreas se encuentran registradas en la siguiente tabla:

Tabla 23. Principales Áreas de Preocupación para la UEV CEC-EPN.

Activo de Información	Áreas de Preocupación
➢ Sitios Web CEC-EPN ➢ Sistema Integrado de Información del CEC-EPN ➢ Gestores de Cursos Virtuales CEC-EPN	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.
	Exposición de los activos de información, acceso no autorizado a la infraestructura física.
	Desconocimiento en el manejo de los sistemas o equipos informáticos.
	Interrupción en el servicio de energía eléctrica.

Activo de Información	Áreas de Preocupación
	Problemas de conectividad en la red interna de la organización.
	Interrupción en el servicio de internet.
	Cambio de Proveedor de Servicios.
	Falla en los componentes de hardware de los equipos informáticos.
	Desactualización de los sistemas.
	Alta Rotación de Personal.
	Desastres Naturales.
	Fallo o defecto de Software.

En la tabla 23 se encuentran los tres activos críticos de información y las doce áreas de preocupación para la Unidad de Educación Virtual CEC-EPN.

Actividad 2: Documentar las Áreas de Preocupación para la UEV

La Guía de OCTAVE Allegro sugiere el uso de la hoja de trabajo: Riesgos de Activos de Información, la misma se utilizará en los pasos: cuatro, cinco, seis, siete y ocho del método descrito en este capítulo.

Tabla 24. Plantilla hoja de trabajo N°3: Riesgos de Activos de Información

	Hoja de trabajo Metodología OCTAVE Allegro		
	Riesgos de Activos de Información		
CUARTO PASO	Activos de Información		
	Área de Preocupación		
	(1) Actor		
	(2) Medios		
	(3) Motivo		
	(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☐ Interrupción
	(5) Requisitos de seguridad		

	Hoja de trabajo Metodología OCTAVE Allegro			
	Riesgos de Activos de Información			
QUINTO PASO	(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☐
	SEXTO PASO	SÉPTIMO PASO		
	(7) Consecuencias	**(8) Gravedad**		
		Área de Impacto	**Valor de Impacto**	**Puntaje**
	Puntuación del Riesgo Relativo			
OCTAVO PASO	(8) **Mitigación de Riesgo** **Acciones a tomar**			
	☐ Aceptar	☐ Aplazar	☐ Mitigar	☐ Transferir
	Si se decide mitigar se realizará lo siguiente:			
	Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**		

La hoja de trabajo se encuentra conformada por los siguientes ítems:

Activo: es la información que tiene un valor para la organización, se caracteriza por ser físico, electrónico o intangible. En este caso es el activo crítico.

Área de preocupación: es la condición o situación que podría afectar a un activo de información.

1. Actor: es quien o que puede violar los requisitos de seguridad de un activo.
2. Medio: es la manera como el actor puede actuar sobre el activo.
3. Motivo: es la intención deliberada o accidental que tiene el actor en ejercer sobre un activo.
4. Resultado: es la consecuencia de violar los requisitos de seguridad de un activo sea por (divulgación, interrupción, modificación, destrucción y perdida).

5. Requisitos de seguridad: son las condiciones de seguridad necesarias que debe cumplir un activo (Disponibilidad, Autenticación, Integridad, Confidencialidad).
6. Probabilidad: es la posibilidad de que los escenarios de amenaza puedan ocurrir
7. Consecuencias: son los resultados que pueden sufrir la organización o el propietario de los activos de información por el incumplimiento de los requisitos de seguridad.
8. Gravedad: es el grado de afectación de las consecuencias producidas sobre el activo de información por el área de impacto.
9. Mitigación de Riesgo: de acuerdo al puntaje total para el riesgo, qué medidas se deben tomar (Caralli et al., 2007).

Para cada activo crítico de información se debe llenar la hoja de trabajo: Riesgos de Activos de Información, en los puntos 1 al 5 de acuerdo a la tabla 24, la información analizada en este paso se encuentra en el Anexo N°4 página 184.

3.2.3.2. Quinto Paso: Identificación de Escenarios de Amenaza para la UEV

Después de haber definido y descrito los árboles de amenaza, se realizará el árbol de amenaza para cada uno de los activos críticos de información de la UEV, a través de la evaluación de riesgos estructurado, para ello el método OCTAVE Allegro propone utilizar por cada activo crítico de información cuestionarios denominados: Cuestionarios de Escenarios de Amenaza, para ello se utilizará la información de las hojas de trabajo N°2(a), 2(b), 2(c) que se encuentran en el Anexo N°3 página 176. En este paso se realizan tres actividades:

Actividad 1: Identificar los escenarios de amenazas adicionales

Este paso consiste en responder a los cuestionarios sugeridos por el método OCTAVE Allegro.

Para el Cuestionario 1: Escenario de Amenazas Contenedor Técnico se considera los contenedores técnicos que se identificaron en la hoja de trabajo

N°2(a), se responde a las preguntas planeadas identificando a los contenedores respectivos.

En el Cuestionario 2: Escenario de Amenazas Contenedor Físico se considera los contenedores físicos que se identificaron en la hoja de trabajo N°2(b), se responde a las preguntas planeadas identificando a los contenedores respectivos.

Finalmente en el Cuestionario 3: Escenario de Amenazas Contenedor Personas se considera los contenedores personas que se identificaron en la hoja de trabajo N°2(c), se responde a las preguntas identificando a los contenedores respectivos.

En el Anexo N°5 pagina 253, se observa las respuestas de los cuestionarios realizados.

Actividad 2: Selección de las respuestas de los cuestionarios de escenario de amenaza

Esta actividad considera las respuestas afirmativas y negativas del cuestionario, si las respuestas fueron afirmativas se deberá registrar en una nueva hoja de trabajo Riesgos de Activos de Información, Plantilla hoja de trabajo N°3: tabla 24, si las respuestas son negativas no se realizará ninguna tarea adicional.

Actividad 3: Probabilidad

La probabilidad es necesaria para determinar que escenarios son más propensos a ocurrir, en este caso se consideró la probabilidad subjetiva debido a que en la mayoría de los casos no existe un registro o control de las ocurrencias presentadas. La frecuencia que se tomó en cuenta fue de un año para el presente análisis. A continuación se establece los valores y frecuencias que se utilizó en la probabilidad subjetiva:

Tabla 25. Probabilidad Subjetiva

Valor	Frecuencia
Alto	Más de 5 veces al año
Medio	De 2 a 4 veces al año
Bajo	1 vez al año

La probabilidad deberá ser colocada para cada uno de los activos en el Anexo N° 4 pagina 184, en la hoja de trabajo Riesgos de Activos de Información, en el ítem (6) de acuerdo a la Plantilla hoja de trabajo N°3: tabla 24.

Resumen de los árboles de amenaza de los activos críticos de información

Para obtener los resultados es necesario tomar la información que se encuentra en el Anexo N° 4 pagina 184, en la hoja de trabajo Riesgos de Activos de Información, en el ítem (4) de acuerdo a la Plantilla hoja de trabajo N°3: tabla 24.

Los árboles de amenaza fueron agrupados por cada activo de información, los cuales se detallan en las tablas 26, 27 y 28.

Tabla 26. Árbol de amenazas Sitios Web CEC-EPN

Árbol de Amenaza: Activo de Información Sitios Web CEC-EPN		
Árbol de Amenaza	**Área de Preocupación**	**Resultados**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Interrupción
	Desconocimiento en el manejo de los sistemas informáticos.	Interrupción
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos informáticos	Interrupción
	Desactualización de los sistemas	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Cambio de Proveedor de Servicios	Interrupción
	Alta Rotación de Personal	Interrupción
	Desastres Naturales	Destrucción

Nota: Los resultados fueron obtenidos del ítem (4) del Anexo N°4 página 184 Riesgos de Activos de Información, activo crítico Sitios Web CEC-EPN.

Tabla 27. Árbol de amenaza: Árbol de amenaza: Sistema Integrado de Información del CEC-EPN

Árbol de Amenaza: Activo de Información SIICECW		
Árbol de Amenaza	**Área de Preocupación**	**Resultados**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas informáticos.	Interrupción
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos informáticos.	Interrupción
	Desactualización de los sistemas	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Cambio de Proveedor de Servicios	Interrupción
	Alta Rotación de Personal	Interrupción
	Desastres Naturales	Destrucción

Nota: Los resultados fueron obtenidos del ítem (4) del Anexo N°4 página 184 Riesgos de Activos de Información, activo crítico Sistema Integrado de Información del CEC-EPN

Tabla 28. Árbol de amenaza: Activo de Información Gestores de Cursos Virtuales CEC-EPN y EPN

Árbol de Amenaza: Activo de Información Gestores de Cursos Virtuales CEC-EPN y EPN		
Árbol de Amenaza	**Área de Preocupación**	**Resultados**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Interrupción
	Desconocimiento en el manejo de los sistemas informáticos.	Interrupción

Árbol de Amenaza: Activo de Información Gestores de Cursos Virtuales CEC-EPN y EPN		
Árbol de Amenaza	**Área de Preocupación**	**Resultados**
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos informáticos.	Interrupción
	Desactualización de los sistemas	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Cambio de Proveedor de Servicios	Interrupción
	Alta Rotación de Personal	Interrupción
	Desastres Naturales	Destrucción

Nota: Los resultados fueron obtenidos del ítem (4) del Anexo N°4 página 184 Riesgos de Activos de Información, activo crítico Gestores de Cursos Virtuales CEC-EPN y EPN

El ítem Resultados: son los respuestas obtenidas de los Anexos N°4 ítem (4), esta información de acuerdo a la metodología OCTAVE Allegro puede ser: divulgación cuando el activo fue expuesto por un sujeto, sin el consentimiento del propietario del activo; modificación cuando fue realizado un cambio en el activo por un sujeto sin el consentimiento del propietario, destrucción cuando una persona o fenómeno natural destrozan el activo, por ultimo interrupción cuando los servicios o el activo falla ya sea por un fenómenos naturales, eléctricos, virus o personal no autorizado.

3.2.4. Fase IV. Identificar y mitigar riesgos

3.2.4.1. Sexto Paso: Identificación de Riesgos

En el Cuarto y Quinto Paso de la Fase III del método OCTAVE Allegro se encontraron las áreas de preocupación y escenarios de amenazas a los que están expuestos los activos críticos de información de la UEV.

En este paso se determina como se vería afectada la organización si las áreas de preocupación y los escenarios de amenazas se cumplen.

Actividad 1: Registrar consecuencias de las amenazas

Para ello se documentarán las consecuencias de las amenazas en el Anexo N° 4 página 184, en la hoja de trabajo Riesgos de Activos de Información, en el ítem (7) de acuerdo a la Plantilla hoja de trabajo N°3: tabla 24.

3.2.4.2. Séptimo Paso: Análisis de Riesgos

En este paso se mide cualitativamente el grado en que la organización se ve afectada por una amenaza mediante el cálculo de una puntuación para cada riesgo de cada activo de información.

La información del puntaje se utiliza para determinar qué riesgos se necesita mitigar inmediatamente y para dar prioridad a las acciones de mitigación para el resto de los riesgos en el paso ocho de la metodología OCTAVE Allegro.

Actividad 1: Revisar criterios de medida de riesgo (valores) y las consecuencias

Esta actividad utilizará la hoja de trabajo Riesgos de Activos de Información que se encuentra en el Anexo N° 4.

- Revisar los criterios de medición de riesgo que se creó en el Paso Uno, en las tablas 11, 12 y 13 páginas 61, 62 y 63, enfocándose en los valores de priorización de impacto definido por la organización, es decir en los valores alto, moderado y bajo.
- Usar el criterio de medición de riesgos como guía, se debe evaluar las consecuencias del Anexo N° 4, ítem (7) y relacionar con cada una de las áreas de impacto ítem (8) de la hoja de trabajo Riesgos de Activos de Información.

- Registrar en el ítem valor de impacto los valores cualitativos "alto", "moderado" o "bajo".

Actividad 2: Calcular el puntaje de riesgo relativo

Los valores de impacto se clasificaron en Alto con valor 3, Moderado con valor 2 y Bajo valor 1.

Con estas consideraciones se calcula el puntaje de riesgo relativo que es la suma total del producto de los valores del área de impacto por el valor de impacto.

Tabla 29. Ejemplo de cálculo del Puntaje Riesgo Relativo

Consecuencias	Gravedad		
	Área de Impacto	Valor de Impacto	Puntaje
Desconfianza de los clientes por no garantizar la seguridad de la información proporcionada a la organización.	Posición y Fidelización de los Clientes (3)	Bajo (1)	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 5%, por la falta de credibilidad de la organización a los clientes.	Económica (2)	Alto (2)	4
Disminución de la productividad del personal de la UEV por ataques de Denegación de Servicios.	Productividad (1)	Bajo (1)	1
Puntuación del Riesgo Relativo			**8**

El riesgo relativo ayudará a priorizar los riesgos, los resultados de cada activo crítico se encuentran en el Anexo N° 4 página 184 Riesgos de Activos de Información.

Los resultados del análisis realizado se muestran de manera resumida en las siguientes tablas 30, 31 y 32.

Tabla 30. Identificación de Riesgos: Activo de Información Sitios Web CEC-EPN

Área de Preocupación	Puntaje Riesgo Relativo	Probabilidad Subjetiva
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	6	Bajo
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	6	Bajo
Desconocimiento en el manejo de los sistemas informáticos.	6	Medio

Área de Preocupación	Puntaje Riesgo Relativo	Probabilidad Subjetiva
Interrupción en el servicio de energía eléctrica.	6	Medio
Problemas de conectividad en la red interna de la organización.	7	Medio
Interrupción en el servicio de internet	12	Medio
Cambio de Proveedor de Servicios.	6	Bajo
Falla en los componentes de hardware de los equipos informáticos.	11	Medio
Desactualización de los sistemas	7	Alto
Alta Rotación de Personal	7	Alto
Desastres Naturales	18	Bajo
Fallo o defecto de Software	11	Medio

Nota: Los valores colocados en la tabla se obtienen del Anexo N° 4 página 184 hoja de trabajo Riesgos de Activos de Información en donde: Valor del Puntaje de riesgo relativo es la suma total del producto de los valores del área de impacto por el valor de impacto, ítem (7) e ítem (8). El valor de la Probabilidad Subjetiva es el ítem (8)

Tabla 31. Identificación de Riesgos: Sistema Integrado de Información del CEC-EPN

Área de Preocupación	Puntaje Riesgo Relativo	Probabilidad Subjetiva
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	7	Bajo
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	6	Medio
Desconocimiento en el manejo de los sistemas informáticos.	8	Medio
Interrupción en el servicio de energía eléctrica.	6	Medio
Problemas de conectividad en la red interna de la organización.	7	Medio
Interrupción en el servicio de internet	12	Medio
Cambio de Proveedor de Servicios.	6	Bajo

Área de Preocupación	Puntaje Riesgo Relativo	Probabilidad Subjetiva
Falla en los componentes de hardware de los equipos informáticos.	6	Medio
Desactualización de los sistemas	12	Bajo
Alta Rotación de Personal	7	Alto
Desastres Naturales	18	Bajo
Fallo o defecto de Software	7	Bajo

Nota: Los valores colocados en la tabla se obtienen del Anexo N° 4 página 184 hoja de trabajo Riesgos de Activos de Información en donde: Valor del Puntaje de riesgo relativo es la suma total del producto de los valores del área de impacto por el valor de impacto, ítem (7) e ítem (8). El valor de la Probabilidad Subjetiva es el ítem (8)

Tabla 32. Identificación de Riesgos: Activo de Información Gestores de Cursos Virtuales CEC-EPN y EPN

Área de Preocupación	Puntaje Riesgo Relativo	Probabilidad Subjetiva
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	12	Bajo
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	6	Medio
Desconocimiento en el manejo de los sistemas informáticos.	7	Medio
Interrupción en el servicio de energía eléctrica.	6	Bajo
Problemas de conectividad en la red interna de la organización.	7	Medio
Interrupción en el servicio de internet	6	Medio
Cambio de Proveedor de Servicios.	6	Bajo
Falla en los componentes de hardware de los equipos informáticos.	12	Medio
Desactualización de los sistemas	7	Alto
Alta Rotación de Personal	12	Alto
Desastres Naturales	18	Bajo
Fallo o defecto de Software	13	Medio

Los valores colocados en la tabla se obtienen del Anexo N° 4 página 184, en las hojas de trabajo Riesgos de Activos de Información en donde: Valor del Puntaje de riesgo relativo es la suma total del producto de los valores del área de impacto por el valor de impacto, ítem (7) e ítem (8). El valor de la Probabilidad Subjetiva es el ítem (8)

La probabilidad y el Puntaje de Riesgo Relativo se utilizaran en el octavo paso del método OCTAVE Allegro para realizar la mitigación de riesgos.

3.2.4.3. Octavo Paso: Selección de enfoque de mitigación

En este paso se consideran los riesgos que se necesita mitigar y la manera de cómo hacerlo. OCTAVE Allegro sugiere realizar una priorización y seleccionar una estrategia para mitigar el riesgo.

En este paso se elabora la matriz de riesgos relativos, para su construcción se debe considerar el valor que se encuentra en el Anexo N°4, en el ítem (6) de las hojas de trabajo: Riesgos de Activos de Información y los resultados del Puntaje de Riesgo Relativo de cada activo.

Los intervalos representados en la Puntuación de Riesgo son los valores mínimos y máximos que pueden existir como resultado de la sumatoria de los valores de impacto (1 a 18) en las tablas 30, 31 y 32.

MATRIZ DE RIESGO RELATIVO			
Probabilidad	Puntuación de riesgo		
	13 a 18	7 a 12	1 a 6
Alto	Gripo 1	Grupo 2	Grupo 3
Medio	Grupo 2	Grupo 2	Grupo 3
Bajo	Grupo 3	Grupo 3	Grupo 4

Figura 13. Matriz de Riesgo Relativo para la UEV

Una vez obtenida la matriz de riesgo relativo para la UEV, figura 13, se procede a relacionar el valor de la puntuación del riesgo relativo (columna) y el valor de la probabilidad (fila).

La puntuación de riesgo se agrupa como se muestra en la figura 14.

Grupo	Enfoque de Mitigación
Grupo 1	Mitigar
Grupo 2	Mitigar o Transferir
Grupo 3	Transferir o Aceptar
Grupo 4	Aceptar

Figura 14. Enfoques de mitigación para la UEV

Los perfiles de riesgo que se decidieron mitigar corresponden al (grupo 2), OCTAVE Allegro sugiere desarrollar una estrategia de mitigación, de la siguiente manera:

- Considerar los contenedores técnicos, físicos y personas del paso tres, Anexo 3, página 176, en el cual se llevará a cabo los controles.
- Describir el control a ser implementado y cualquier riesgo residual de los activos críticos, una vez que se implementa el control.

Los resultados de la agrupación y tratamiento de la amenaza se muestran en las tablas 33, 34 y 35

Activo de Información: Sitio Web CEC-EPN

Tabla 33. Cuadro Resumen de enfoque de mitigación - Sitio Web CEC-EPN

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	6	Bajo	Grupo 4	Aceptar		
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	6	Bajo	Grupo 4	Aceptar		
Desconocimiento en el manejo de los sistemas informáticos.	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta y Coordinadora de UEV Lic. Gabriela Martínez.
Interrupción en el servicio de energía eléctrica.	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo al Administrador del Edificio Aulas y Relación con el Medio Externo EPN, cuyo responsable es Ing. Andrea Plaza.
Problemas de conectividad en la red interna de la organización.	7	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Interrupción en el servicio de internet	12	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
Cambio de Proveedor de Servicios	6	Bajo	Grupo 4	Aceptar		
Falla en los componentes de hardware de los equipos informáticos.	11	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta y Coordinadora de UEV Lic. Gabriela Martínez.
Desactualización de los sistemas	7	Alto	Grupo 2	Mitigar	➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios en los servidores. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	
Alta Rotación de Personal	7	Alto	Grupo 2	Mitigar	➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral.	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
					➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV.	
Desastres Naturales	18	Bajo	Grupo 3	Transferir		Se transfiere a los proveedores de los distintos servicios Servidor Dedicado, responsables: Undermedia, Ecualinux y aseguradora de equipos.
Fallo o defecto de Software	11	Medio	Grupo 2	Mitigar	➢ Planificar configuración de Servidores. Instalar herramienta antivirus de acuerdo a las capacidades de los servidores y estaciones de trabajo de TI. ➢ Programar ejecución de herramienta antivirus para analizar de forma periódica a las aplicaciones y sistemas operativos huésped. ➢ Escoger un Sistema Operativo adecuado a los componentes instalados de los servidores. ➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios. ➢ Realizar pruebas de carga al sistema operativo. ➢ El ingreso y actualizaciones	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
					remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	

Activo de Información: Sistema Integrado de Información del CEC-EPN

Tabla 34. Cuadro Resumen de enfoque de mitigación - Sistema Integrado de Información del CEC-EPN

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	7	Bajo	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Desconocimiento en el manejo de los sistemas informáticos.	8	Medio	Grupo 2	Mitigar	➢ Elaborar diagramas y esquemas donde se pueda apreciar los procedimientos administrativos del área. ➢ Elaborar manual de manejo de los sistemas que utilice el área. ➢ Crear una base de conocimientos de los incidentes más conocidos para su posterior resolución. ➢ Realizar pruebas pilotos y entrevistas con el personal para obtener retroalimentación y realizar mejoras. ➢ Mantener actualizado los manuales y realiza capacitaciones a los nuevos elementos.	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
Interrupción en el servicio de energía eléctrica.	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo al Administrador del Edificio Aulas y Relación con el Medio Externo EPN, cuyo responsable es Ing. Andrea Plaza.
Problemas de conectividad en la red interna de la organización.	7	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Interrupción en el servicio de internet	12	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Cambio de Proveedor de Servicios	6	Bajo	Grupo 4	Aceptar		
Falla en los componentes de hardware de los equipos informáticos.	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta y Coordinadora de UEV Lic. Gabriela Martínez.
Desactualización de los sistemas	12	Bajo	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Alta Rotación de Personal	7	Alto	Grupo 2	Mitigar	➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral.	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
					➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV.	
Desastres Naturales	18	Bajo	Grupo 3	Transferir		Se transfiere a los proveedores de los distintos servicios Servidor Dedicado, responsables: Undermedia, Ecualinux y aseguradora de equipos.
Fallo o defecto de Software	7	Bajo	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.

Activo de Información: Gestores de Cursos Virtuales CEC-EPN y EPN

Tabla 35. Cuadro Resumen de enfoque de mitigación - Gestores de Cursos Virtuales CEC-EPN y EPN

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	12	Bajo	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología. Se transfiere el riesgo a la Coordinadora de la UEV cuyo responsable del área es Lic. Gabriela Martínez y al Proveedor Undermedia.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo al Proveedor Undermedia.
Desconocimiento en el manejo de los sistemas informáticos.	7	Medio	Grupo 2	Mitigar	➢ Elaborar diagramas y esquemas donde se pueda apreciar los procedimientos administrativos del área. ➢ Elaborar manual de manejo de los sistemas que utilice el área. ➢ Crear una base de conocimientos de los incidentes más conocidos para su posterior resolución. ➢ Realizar pruebas pilotos y entrevistas con el personal para obtener retroalimentación y realizar mejoras. ➢ Mantener actualizado los	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
					manuales y realiza capacitaciones a los nuevos elementos. ➢ Capacitar al personal.	
Interrupción en el servicio de energía eléctrica.	6	Bajo	Grupo 4	Aceptar		
Problemas de conectividad en la red interna de la organización.	7	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Interrupción en el servicio de internet	6	Medio	Grupo 3	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología responsable del área Ing. Ximena Uchupanta.
Cambio de Proveedor de Servicios	6	Bajo	Grupo 4	Aceptar		
Falla en los componentes de hardware de los equipos informáticos.	12	Medio	Grupo 2	Transferir		Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta y el Proveedor Undermedia.
Desactualización de los sistemas	7	Alto	Grupo 2	Mitigar	➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios en los servidores. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH.	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
					➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	
Alta Rotación de Personal	12	Alto	Grupo 2	Mitigar	➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral. ➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV	
Desastres Naturales	18	Bajo	Grupo 3	Transferir		Se transfiere a los proveedores de los distintos servicios Servidor Dedicado, responsables: Undermedia, Ecualinux y aseguradora de equipos.
Fallo o defecto de Software	13	Medio	Grupo 2	Mitigar	➢ Planificar configuración de Servidores. ➢ Instalar herramienta antivirus de acuerdo a las capacidades de los servidores y estaciones de trabajo de TI.	

Áreas de Preocupación	Puntaje de Riesgo Relativo	Probabilidad Subjetiva	Categorización	Acción	Controles	Observaciones
					➢ Programar ejecución de herramienta antivirus para analizar de forma periódica a las aplicaciones y sistemas operativos huésped. ➢ Escoger un Sistema Operativo adecuado a los componentes instalados de los servidores. ➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios. ➢ Realizar pruebas de carga al sistema operativo. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	

Capítulo IV

4 Desarrollo del Plan de Continuidad para la Unidad de Educación Virtual CEC-EPN

En el Capítulo dos se realizó el análisis y selección de la metodología para el desarrollo del Plan de Continuidad, en este caso realizará la combinación de las metodologías de DRII y las buenas prácticas de ITIL v3, centrándose principalmente en la Gestión de la Continuidad de los Servicios de TI, conocida por su siglas en inglés (ITSCM).

En este capítulo se detallará adecuadamente la propuesta de Plan de Continuidad para la UEV del CEC-EPN, el mismo que se compone de un conjunto de planes que cubren áreas del negocio, en base a las fases definidas en la metodología de DRII y las fases del ciclo de vida de ITSCM.

4.1 Inicio y Administración

En esta fase se abordan aspectos esenciales para el desarrollo del Plan de Continuidad de la UEV del CEC-EPN.

En la figura 15, se indican los pasos a seguir en la fase de Inicio y Administración.

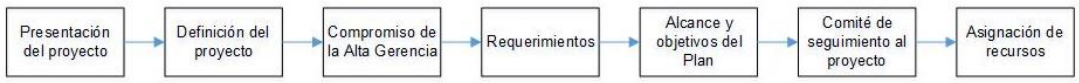

Figura 15. Pasos a desarrollar en la fase I – Inicio y Administración

4.1.1. Presentación del proyecto

4.1.1.1. Participantes

El Plan cuenta con el apoyo de la Coordinadora de la Unidad de Educación Virtual, es quien se encargará de definir el alcance y evaluar el Plan de

Continuidad. Los participantes son las personas que intervendrán en la elaboración y ejecución del Plan de Continuidad.

Para la Coordinación de la UEV, es de gran interés el desarrollo del Plan y los resultados que provengan del mismo, en la tabla 36 se muestra la información de los participantes del plan:

Tabla 36. Personal que interviene en el desarrollo del Plan de Continuidad

Responsable	Rol	Actividad
Tlgo. Leonardo Medrano	Desarrollador del Plan de Continuidad.	Elaboración del Plan de Continuidad
Tlga. Andrea Conza	Desarrolladora del Plan de Continuidad y Jefe del Área de TI	
Lic. Gabriela Martínez MgS.	Coordinadora de la Unidad de Educación Virtual	Proveedores de la información para el desarrollo del Plan de Continuidad
Ing. Christian Hidalgo	Jefe del Área de Gestión	
Ing. Cristhian Castillo	Jefe del Área Académica	

Nota: Unidad de Educación Virtual. Los nombres, roles y actividades que desempeñarán los participantes en el Plan de Continuidad para la UEV.

4.1.2. Definición del problema

El crecimiento de capacitación virtual en los últimos años ha permitido que la Unidad de Educación Virtual crezca a un ritmo exponencial, siendo definida como una unidad productiva dentro del Centro de Educación Continua, esto la convierte en generadora de recursos económicos, como resultado, todos sus procesos están encaminados a la prestación de servicios de calidad y a entera satisfacción de los clientes.

En la actualidad la UEV no cuenta con un plan o acciones que permita garantizar la continuidad del negocio ante un desastre, fallo e interrupción de alguno de los procesos críticos. En vista de esto es necesario contar con un Plan de Continuidad que permita evidenciar los riesgos, amenazas e impactos a los que está expuesta la unidad y plantear las mejores alternativas para prevenir, reducir, asumir o trasladar los riesgos encontrados.

4.1.3. Compromiso de la Alta Gerencia

La Dirección del CEC-EPN, es quien define las estrategias, toma las decisiones y proporciona los recursos financieros necesarios para el éxito del Plan.

4.1.4. Requerimientos

Para el desarrollo del Plan de Continuidad es necesario cumplir con los siguientes requerimientos:

- Realizar el Análisis de Impacto de Negocio (BIA).
- Realizar la Evaluación de riesgos.
- Análisis de Estrategias.

4.1.5. Alcance y objetivos del plan

4.1.5.1. Alcance

Realizar el Plan de Continuidad para los procesos críticos de la Unidad de Educación Virtual, siendo los mismos: Proceso de Inscripción y Matriculación, Proceso de Diseño de Cursos y Ejecución de curso.

4.1.5.2. Objetivos

- Garantizar la continuidad de las actividades y servicios, aplicando la metodología de DRII y las buenas prácticas de ITIL sobre los procesos críticos de la Unidad de Educación Virtual CEC-EPN
- Seleccionar las mejores estrategias para la implementación del Plan de Continuidad.

4.1.6. Comité de seguimiento al proyecto

El Comité de Seguimiento del Proyecto tiene la responsabilidad de evaluar los avances y objetivos planteados. El Comité está conformado por:

- Coordinadora de la Unidad de Educación Virtual CEC-EPN.
- Coordinadora de la Unidad de Gestión de Tecnología CEC-EPN.
- Jefe del Área de Tecnologías de la Información UEV.

4.1.7. Asignación de recursos

Complementando esta etapa de acuerdo a ITIL sobre la asignación de recursos es necesario mencionar los recursos con los que cuenta la CEC-EPN para el desarrollo del plan de continuidad del negocio.

4.1.7.1. Recursos financieros

La UEV cuenta con un presupuesto anual, planificado para cumplir con los objetivos estratégicos de la organización.

4.1.7.2. Recursos Humanos

La UEV cuenta con un grupo humano de nueve profesionales en las áreas administrativas, pedagógicas y tecnológicas para el desarrollo de proyectos de *e-learning*.

4.1.7.3. Recursos Tecnológicos

El recurso tecnológico es una de sus principales preocupaciones a través del plan de continuidad se desea establecer estrategias y controles que permitan garantizar la disponibilidad y continuidad del servicio.

4.2 Requerimientos Funcionales

La Unidad de Educación Virtual maneja seis procesos, en esta fase se describirá cada uno de ellos y se identificará que procesos son críticos para la UEV.

En la figura 16, se indica las actividades que se desarrollarán en esta fase:

Figura 16. Pasos a desarrollar en la fase II – Requerimientos Funcionales

4.2.1. Conocimiento del negocio

4.2.1.1. Descripción funcional del negocio

La Unidad de Educación Virtual ofrece los siguientes servicios:

- Cursos de capacitación en modalidad virtual en temáticas como: (Empresariales, Tecnológicos y Educativos).
- Desarrollos de cursos virtuales.
- Formación de tutores virtuales.

- Adaptación de contenidos a formato *e-learning*.
- Administración del campus virtual de la Escuela Politécnica Nacional. (UEV, s.f.)

4.2.1.2. Procesos de la Unidad de Educación Virtual

Desde noviembre de 2013, la UEV se encuentra trabajando en sus procesos, con el objetivo de ser parte del Sistema de Gestión de Calidad que maneja el CEC-EPN. De esta manera, la unidad actualmente maneja siete procesos:

1. Diseño de propuestas.
2. Diseño de cursos.
3. Promoción de cursos.
4. Inscripción y matriculación.
5. Selección y contratación de tutores.
6. Ejecución de cursos.
7. Gestión de pagos.

De manera general se pueden apreciar en la siguiente figura:

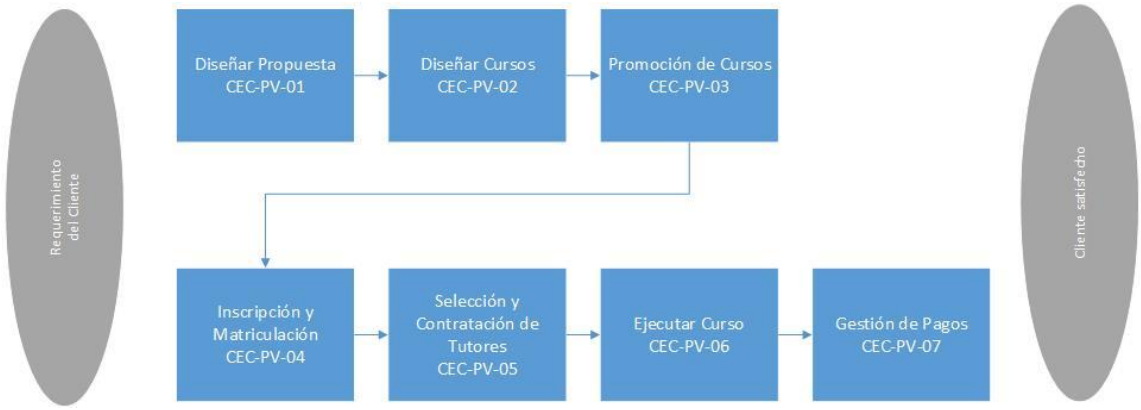

Figura 17. Procesos de la Unidad de Educación Virtual 2014

Los siete procesos se describen a través de las tablas 37, 38, 39, 40, 41, 42 y 43.

El detalle de las tablas corresponde a:

- Número de Proceso, es la codificación interna dentro del CEC-EPN.
- Nombre del Proceso, nombre con el que se conoce al proceso.
- Descripción del proceso, una breve explicación del proceso.

- Producto o servicio relacionado con el proceso, como interactúa con otros recursos.

Tabla 37. Proceso UEV– Diseño de Propuesta

Número de Proceso	CEC-PV-01
Nombre del Proceso	Diseño de Propuesta
Descripción del proceso	Este proceso se encarga de realizar las cotizaciones que solicitan los posibles clientes (personas, empresas) sobre cursos de capacitación virtual o implementación de soluciones *e-learning.*
Producto o servicio relacionado con el proceso	Conocimientos y competencias del personal de la UEV coordinadora, diseñador instruccional, técnico y gráfico. Cursos ofertados por la UEV.

Tabla 38. Proceso UEV – Diseño de Cursos

Número de Proceso	CEC-PV-02
Nombre del Proceso	Diseño de Cursos
Descripción del proceso	Este proceso genera los cursos de capacitación virtual de acuerdo a la demanda del mercado, y necesidades de los clientes.
Producto o servicio relacionado con el proceso	Plataforma de aprendizaje Moodle. Conocimientos y competencias de los diseñadores instruccional y gráfico. Servicios Profesionales de Capacitación

Tabla 39. Proceso UEV – Promoción de cursos

Número de Proceso	CEC-PV-03
Nombre del Proceso	Promoción de cursos
Descripción del proceso	Este proceso se encarga de ofertar los cursos virtuales en los medios con mayor demanda en el Ecuador.
Producto o servicio relacionado con el proceso	Medios impresos (prensa, revistas) y medios digitales. Cursos ofertados por la UEV.

Tabla 40. Proceso UEV – Inscripción y Matriculación

Número de Proceso	CEC-PV-04
Nombre del Proceso	Inscripción y Matriculación
Descripción del proceso	Este proceso se encarga de realizar el registro de los estudiantes que deciden capacitarse en modalidad virtual, tiene por objeto gestionar la información de los nuevos y antiguos estudiantes que desean participar en un curso virtual.
Producto o servicio relacionado con el proceso	Servicio de correo electrónico. Servicio de internet. Sitio Web UEV y CEC-EPN

Tabla 41. Proceso UEV – Selección y Contratación de Tutores

Número de Proceso	CEC-PV-05
Nombre del Proceso	Selección y Contratación de Tutores
Descripción del proceso	Este proceso gestiona el ingreso de nuevos profesionales como Tutores Virtuales de acuerdo a los requerimientos de la UEV.
Producto o servicio relacionado con el proceso	Servicio de correo electrónico. Servicio de internet. Telefonía fija o móvil.

Tabla 42. Proceso UEV – Ejecutar Curso

Número de Proceso	CEC-PV-06
Nombre del Proceso	Ejecutar Curso
Descripción del proceso	Este proceso muestra cómo se realiza la capacitación de un curso virtual, el mismo tiene por objeto el desarrollo, transmisión y seguimiento del aprendizaje a los estudiantes.
Producto o servicio relacionado con el proceso	Plataforma de aprendizaje Moodle. Servidor Dedicado ubicado en el exterior. Conocimientos y competencias del personal UEV y Tutores Virtuales.

Tabla 43. Proceso UEV – Gestión de Pagos

Número de Proceso	CEC-PV-07
Nombre del Proceso	Gestión de Pagos
Descripción del proceso	Este proceso se encarga de la gestión de pagos a los proveedores de la Unidad de Educación Virtual.
Producto o servicio relacionado con el proceso	Informes de actividades. Sistema Integrado de Información del CEC-EPN Sistema Financiero denominado e-Sigef. Quipux CEC-EPN

4.2.1.3. Procesos críticos

En la tabla 44, se muestra la Matriz de Holmes, la misma que ayudará a identificar los procesos críticos de la Unidad de Educación Virtual.

Para elaborar la tabla se coloca en la primera columna y fila los siete procesos de la unidad, en la intersección de la fila y la columna no se pondera, después se empieza a cotejar los procesos de fila a columna, se asigna un valor de 0.5 si el proceso (fila) es menos importante que el proceso (columna), el valor 1 si el proceso (fila) y proceso (columna) tienen igual importancia, el valor 2 si el proceso (fila) es más importante que el proceso (columna).

Se obtiene la suma total y porcentaje para cada proceso, al final se establece la importancia de los procesos por la posición de los porcentajes en forma descendente.

Tabla 44. Matriz de priorización de los procesos críticos de la UEV

PROCESOS	Diseño de Propuesta	Diseño de Cursos	Promoción de cursos	Inscripción y Matriculación	Selección y Contratación de Tutores	Ejecutar Curso	Gestión de Pagos	Suma total de la fila	% de total	Orden de Importancia
Diseño de Propuesta		0,5	0,5	1	0,5	0,5	0,5	3,5	7,4%	6
Diseño de Cursos	2		2	0,5	2	0,5	0,5	7,5	16,0%	3
Promoción de cursos	0,5	0,5		2	1	0,5	0,5	5	10,6%	5
Inscripción y Matriculación	1	2	1		2	1	1	8	17,0%	2
Selección y Contratación de Tutores	0,5	0,5	1	0,5		2	2	6,5	13,8%	4
Ejecutar Curso	2	1	2	1	2		0,5	7	18,1%	1
Gestión de Pagos	2	1	2	0,5	2	0,5		8	17,0%	2
SUMA TOTAL	8	5,5	8,5	5,5	9,5	5	5	47	100,0%	

Valores	**Descripción:**
0.5	Si la fila es menos importante que la columna
1	Si la fila y columna tienen igual importancia
2	Si la fila es más importante que la columna

Nota: El valor 8 se repite dos veces en la columna Suma total, este valor se considerará como una posición 2, según el Orden de importancia.

En resumen los procesos críticos son los siguientes:

Tabla 45. Resumen de procesos críticos

Valor	Ponderación
3	Diseño de Cursos
2	Gestión de Pagos
2	Inscripción y Matriculación
1	Ejecutar curso

Nota: El valor se encuentra ordenado en forma descendente.

Para el desarrollo del presente proyecto no se considerará el proceso crítico Gestión de Pagos debido a que este proceso es realizado en su mayoría por la Coordinación Administrativa Financiera del CEC-EPN, el alcance no contempla este análisis.

- Ponderación de criticidad de los procesos

Los valores están representados por los resultados de la matriz de priorización, de acuerdo a la columna orden de importancia.

Tabla 46. Ponderación para los procesos críticos

Nivel	Ponderación
4 - 6	Bajo
3	Medio
1 - 2	Crítico

4.2.1.4. Información externa de apoyo

Se considera los procesos con los niveles críticos de 1 a 3 de la tabla 43 Resumen de procesos críticos, se analiza la información que no pertenece al área pero que apoya el proceso.

El detalle de las tablas corresponde a:

- Nivel de Criticidad, ponderación del proceso dado su criticidad.
- Número de Proceso, es la codificación interna dentro del CEC-EPN.
- Nombre del Proceso, nombre con el que se conoce al proceso.
- Áreas de Origen, áreas de donde nace la información.

- Áreas de Destino, áreas hacia donde se dirige la información.

Tabla 47. Descripción del proceso crítico de la UEV – Ejecutar Curso

Nivel de Criticidad	1 - Crítico
Número de Proceso	CEC-PV-06
Nombre del Proceso	Ejecutar Curso
Áreas de Origen	Área de Tecnología de la Información UEV Área Académica UEV
Áreas de Destino	Área Académica UEV: Tutora de tutores Área de Gestión UEV

Tabla 48. Descripción del proceso crítico de la UEV – Inscripción y Matriculación

Nivel de Criticidad	2 - Crítico
Número de Proceso	CEC-PV-04
Nombre del Proceso	Inscripción y Matriculación
Áreas de Origen	Área de Gestión UEV Coordinación UEV
Áreas de Destino	Área de Tecnologías de la Información UEV Coordinación Administrativa Financiera CEC-EPN

Tabla 49. Descripción del proceso crítico de la UEV – Diseño de Cursos

Nivel de Criticidad	3 - Medio
Número de Proceso	CEC-PV-02
Nombre del Proceso	Diseño de Cursos
Áreas de Origen	Área Académica: ➢ Diseñador Instruccional UEV ➢ Experto en Contenidos UEV Coordinación UEV
Áreas de Destino	Área de Diseño Gráfico UEV Área de Tecnología de la Información UEV Área Académica: Pedagoga UEV

4.2.1.5. Identificación de tiempos críticos

Se establecen los horarios críticos de ejecución de los procesos con prioridades de 1, 2 y 3 considerando el RTO (Recovery Time Objetive) y RPO (Recovery Point Objetive) para cada uno de ellos.

En las tablas 50, 51 y 52 se encuentran varios ítems que a continuación se explican:

- Frecuencia de ejecución, determina el período de repetición del proceso analizado.
- Tiempo esperado de recuperación, es el tiempo máximo en que el proceso puede esperar sin impactar de manera considerable a los clientes, internos y externos.
- Tiempo límite de ejecución, es el horario máximo en que los procesos se deben ejecutar (fecha, hora).

Tabla 50. RTO para el proceso de Ejecutar Curso

Nivel de Criticidad	1 - Crítico
Número de Proceso	CEC-PV-06
Nombre del Proceso	Ejecutar Curso
Frecuencia de ejecución: D: Diario; S: Semanal; Q: Quincenal; M: Mensual; B: Bimestral; T: Trimestral; R: Semestral; A: Anual; O: Ocasional.	El proceso se ejecuta **Diariamente.**
Tiempo esperado de recuperación (RTO)	El tiempo máximo de espera son **2 horas**.
Tiempo límite de ejecución	Fecha máxima de ejecución: **Todos los días** durante la ejecución de capacitaciones **por 35 días**. El período se repite después de **1 a 2 semanas.** Hora máxima de ejecución: **10:00 pm diariamente** ejecución de respaldos.

Tabla 51. RTO para proceso de Inscripción y Matriculación

Nivel de Criticidad	2 - Crítico
Número de Proceso	CEC-PV-04
Nombre del Proceso	Inscripción y Matriculación

Frecuencia de ejecución: D: Diario; S: Semanal; Q: Quincenal; M: Mensual; B: Bimestral; T: Trimestral; R: Semestral; A: Anual; O: Ocasional.	El proceso se ejecuta **Diariamente.**
Tiempo esperado de recuperación (RTO)	El tiempo máximo de espera son **2 horas**.
Tiempo límite de ejecución	Fecha máxima de ejecución: **Todos los días** en período de matrículas **por 15 días**. El período se repite después de **5 semanas.** Hora máxima de ejecución: **10: 00 am en el día 15.**

Tabla 52. RTO para proceso de Diseño de Cursos

Número de Proceso	CEC-PV-02
Nombre del Proceso	Diseño de Cursos
Nivel de Criticidad	3 - Medio
Frecuencia de ejecución: D: Diario; S: Semanal; Q: Quincenal; M: Mensual; B: Bimestral; T: Trimestral; R: Semestral; A: Anual; O: Ocasional.	El proceso se ejecuta **Diariamente.**
Tiempo esperado de recuperación (RTO)	El tiempo máximo de espera son **2 horas**.
Tiempo límite de ejecución	Fecha máxima de ejecución: **Todos los días** durante el desarrollo de cursos **por 1 mes**. El período se repite 7 veces al año. Hora máxima de ejecución: **10: 00 am en el día 1.**

4.2.2. Inventario de recursos

Constan todos los recursos que son soportados por cada proceso crítico de la Unidad de Educación Virtual, esta información es un insumo fundamental para el análisis de riesgo; el inventario contiene una descripción detallada de cada recurso, considerando si es esencial para el sistema o proceso, o si se puede realizar de manera parcial en caso de ausencia.

4.2.2.1. Inventario de información

Se incluye el tipo de información, una descripción y la forma en que se actualiza cada uno de los procesos críticos.

El inventario de información se subdivide en entidades externas y clientes; y proveedores.

- Entidades externas y clientes

Este inventario se compone de la información entre los clientes y las entidades externas, en las tablas 53, 54 y 55 se muestra como la Unidad de Educación Virtual entrega y recibe la información, el medio de transmisión y la periodicidad.

Tabla 53. Interacción entre Entidades externas y clientes en el proceso Ejecutar de Curso

Número de Proceso	CEC-PV-06
Nombre del Proceso	Ejecutar Curso
Entidad externa o cliente:	➢ Cliente ➢ Tutor Virtual
Entrega/Recepción:	**Entrega:** La Unidad de Educación Virtual, entrega: ➢ El material para el desarrollo del curso. **Recibe:** ➢ La información de seguimiento. ➢ Informes de desarrollo del curso. ➢ Retroalimentación del desenvolvimiento del curso.
Descripción:	Se intercambia los siguientes datos entre las áreas o personas: **UEV- Entrega:** ➢ Acceso al curso virtual. ➢ Acceso a la plataforma de video conferencia. ➢ Soporte técnico a los estudiantes y tutores durante la ejecución del curso. **UEV- Recibe:** ➢ Datos de encuestas realizados a los estudiantes de cada curso. ➢ Informes de la ejecución de los cursos virtuales. ➢ Solicitudes de soporte técnico. **UEV- Entrega:** ➢ Calificaciones obtenidas en los cursos virtuales. ➢ Certificados de aprobación de los cursos.
Medio de transmisión o intercambio: Listado: L; Correo: C; Unidad de CD: CD; Unidad de DVD; DVD; Internet: I, Pen drive: USB, Plataforma de aprendizaje: LMS, Plataforma de videoconferencia: VC, Presencial: P, Llamada telefónica: T	Accesos al curso: LMS Acceso a plataforma de video conferencia: VC Soporte técnico: C, I, T, P Encuestas: LMS Informes de seguimiento: C, CD, USB, DVD Calificaciones: LMS, C, T

Periodicidad: Diario: D; Semanal: S; Quincenal: Q; Mensual: M; Trimestral: T; Semestral: S; Anual: A; Ocasional: O	Accesos al curso: D Acceso videoconferencia: S Soporte técnico: D Encuestas: Q Informes de seguimiento: M Calificaciones: D

Tabla 54. Interacción entre Entidades externas y clientes en el proceso Inscripción y Matriculación

Número de Proceso	CEC-PV-04
Nombre del Proceso	Inscripción y Matriculación
Entidad externa o cliente:	Cliente
Entrega/Recepción:	**Recepción:** La Unidad de Educación Virtual, recibe: ➢ La lista de los cursos que se programan para la inscripción y matriculación. ➢ La información de los inscritos y matriculados a través del sitio web y de forma presencial.
Descripción:	Se intercambia los siguientes datos entre la Unidad de Educación Virtual y los clientes: **UEV- Entrega:** ➢ Información de los cursos virtuales. ➢ Los formularios para la inscripción y matriculación de cursos virtuales. **UEV- Recibe:** ➢ Datos personales de los clientes inscritos y matriculados en los cursos virtuales. ➢ Datos de pagos realizados por los clientes para los cursos a realizar. **UEV- Entrega:** ➢ Confirmación de matrículas realizadas. ➢ Información de acceso para los clientes matriculados.
Medio de transmisión o intercambio: Listado: L; Correo: C; Internet: I, Medios Impresos: M, Presencial: P, Llamada telefónica: T	Información de cursos: C, I, M, P, T Formularios de Inscripción: C, I, P Datos Personales: C, I, P Datos de pagos: C, I, P Confirmación de matrículas: C, P, T Información de acceso: C, P, T
Periodicidad: Diario: D; Semanal: S; Quincenal: Q; Mensual: M; Trimestral: T; Semestral: S; Anual: A; Ocasional: O	Información de cursos: D Formularios de Inscripción: D Datos Personales: D Datos de pagos: D Confirmación de matrículas: D Información de acceso: M

Tabla 55. Interacción entre Entidades externas y clientes en el proceso Diseño de Curso

Número de Proceso	CEC-PV-02
Nombre del Proceso	Diseño de Curso
Entidad externa o cliente:	➢ Experto en Contenidos ➢ Cliente ➢ Lingüista ➢ Tutor Virtual
Entrega/Recepción:	**Recepción:** ➢ La Unidad de Educación Virtual, recibe: ➢ Los requerimientos para el desarrollo de nuevos cursos virtuales. ➢ La información para la construcción de los cursos virtuales por parte del Experto en Contenidos.
Descripción:	Se intercambia los siguientes datos entre las siguientes unidades, áreas o personas: **UEV- Recibe:** Informe y solicitudes de necesidades. **UEV- Entrega:** Formatos para el desarrollo del curso virtual: ➢ Plan, Programa de curso. ➢ Instructivo para la realización de materiales. **UEV- Recibe:** Materiales para la construcción de contenidos del curso: ➢ Documentos con los contenidos en bruto. ➢ Presentaciones en PowerPoint, Videos, Canciones. ➢ Enlaces. Archivos, imágenes. ➢ Instrucciones de Actividades y Evaluaciones
Medio de transmisión o intercambio: Listado: L; Correo: C; Unidad de CD: CD; Unidad de DVD; DVD; Internet: I, Pen drive: USB	Informe: C, I Solicitudes de necesidades: C, I Formatos: C, I Materiales para el desarrollo de contenidos: C, USB, CD, DVD, I
Periodicidad: Diario: D; Semanal: S; Quincenal: Q; Mensual: M; Trimestral: T; Semestral: S; Anual: A; Ocasional: O	Informe: S Solicitudes de necesidades: M Formatos: T Materiales para el desarrollo de contenidos: T

- Proveedores

En este inventario consta el intercambio de información entre los proveedores, considerando la información que se envía o recibe y el medio de intercambio.

Tabla 56. Interacción con los Proveedores en el proceso de Ejecutar Curso

Número de Proceso	CEC-PV-06
Nombre del Proceso	Ejecutar Curso
Nombre del proveedor:	Nuestro Server - Undermedia
Servicio Prestado:	Este proveedor proporciona el servicio de servidor dedicado, en este servidor funciona el servidor web, plataformas virtuales y base de datos.
Entrega/Recepción	El Proveedor entrega el servicio de servidor dedicado a la Unidad de Educación Virtual y los estudiantes reciben el servicio de capacitación en las plataformas virtuales. Toda la información de los cursos virtuales se encuentra en el servidor dedicado.
Descripción:	La información que se intercambia con el proveedor es: ➢ Solicitudes de nuevos requerimientos, ➢ Reportes de incidentes. ➢ Soporte técnico.
Medio de transmisión o intercambio: Listado: L; Correo: C; Internet: I, Medios Impresos: M, Presencial: P, Llamada telefónica: T	Solicitudes de nuevos requerimientos: C, I, T Reportes de incidentes: C, I, M, P,T Soporte técnico: C, I, M, T
Periodicidad: Diario: D; Semanal: S; Quincenal: Q; Mensual: M; Trimestral: T; Semestral: S; Anual: A; Ocasional: O	Solicitudes de nuevos requerimientos: T Reportes de incidentes: M Soporte técnico: O

Tabla 57. Interacción con los Proveedores en el proceso de Inscripción y Matriculación

Número de Proceso	CEC-PV-04
Nombre del Proceso	Inscripción y Matriculación
Nombre del proveedor:	Nuestro Server – Undermedia Ecualinux
Servicio Prestado:	**Nuestro Server – Undermedia** Este proveedor proporciona el servicio de servidor dedicado, en este servidor funcionan las plataformas virtuales, el servidor web de la UEV y

	base de datos. **Ecualinux** Este proveedor proporciona el servicio de servidor dedicado, en este servidor funciona el servidor web del CEC-EPN
Entrega/Recepción	**Nuestro Server – Undermedia** El Proveedor entrega el servicio de servidor dedicado y el Área de Tecnologías de la Información de la UEV se encarga de actualizar el sitio web de la UEV y se asocia la información con el sitio web del CEC-EPN, para que los clientes realicen la inscripción y matriculación de los cursos virtuales en los períodos planificados. **Ecualinux** El Proveedor entrega el servicio de servidor dedicado y la Coordinación de Tecnología CEC-EPN se encarga de actualizar parcialmente el sitio web del CEC-EPN.
Descripción:	La información que se intercambia con el proveedor es: ➢ Solicitudes de nuevos requerimientos, ➢ Reportes de incidentes. ➢ Soporte técnico.
Medio de transmisión o intercambio: Listado: L; Correo: C; Internet: I, Medios Impresos: M, Presencial: P, Llamada telefónica: T	Solicitudes de nuevos requerimientos: C, I, T Reportes de incidentes: C, I, M, P,T Soporte técnico: C, I, M, T
Periodicidad: Diario: D; Semanal: S; Quincenal: Q; Mensual: M; Trimestral: T; Semestral: S; Anual: A; Ocasional: O	Solicitudes de nuevos requerimientos: T Reportes de incidentes: M Soporte técnico: O

Tabla 58. Interacción con los Proveedores en el proceso de Diseño de Curso

Número de Proceso	CEC-PV-02
Nombre del Proceso	Diseño de Curso
Nombre del proveedor:	Experto en Contenidos
Servicio Prestado:	El Experto en Contenidos, proporciona los materiales necesarios para la construcción de los cursos virtuales, los cuales serán adaptados pedagógicamente y digitalizados para generar un curso virtual.
Entrega/Recepción	La Unidad de Educación Virtual, entrega los formatos e instructivos para la realización del material del curso. El Experto de Contenidos entrega la información para la construcción del aula virtual.

Descripción:	La información que se intercambia con el Experto en Contenidos es: Materiales para la construcción de contenidos del curso: ➢ Documentos con los contenidos en bruto. ➢ Presentaciones en PowerPoint, Videos, Canciones. ➢ Enlaces. Archivos, imágenes. ➢ Instrucciones de Actividades y Evaluaciones.
Medio de transmisión o intercambio: Listado: L; Correo: C; Internet: I, Medios Impresos: M, Presencial: P, Llamada telefónica: T	Materiales para la construcción de contenidos: C, USB, CD, DVD, I
Periodicidad: Diario: D; Semanal: S; Quincenal: Q; Mensual: M; Trimestral: T; Semestral: S; Anual: A; Ocasional: O	Materiales para el desarrollo de contenidos: T

4.2.2.2. Inventario tecnológico

El recurso tecnológico cumple un papel importante en el apoyo a los procesos que se gestionan diariamente en la UEV.

- Diagrama de estructura tecnológica, muestra la estructura de la Unidad de Educación Virtual así como también parte de los servidores de la Coordinación de Tecnología CEC-EPN para soportar cada proceso.

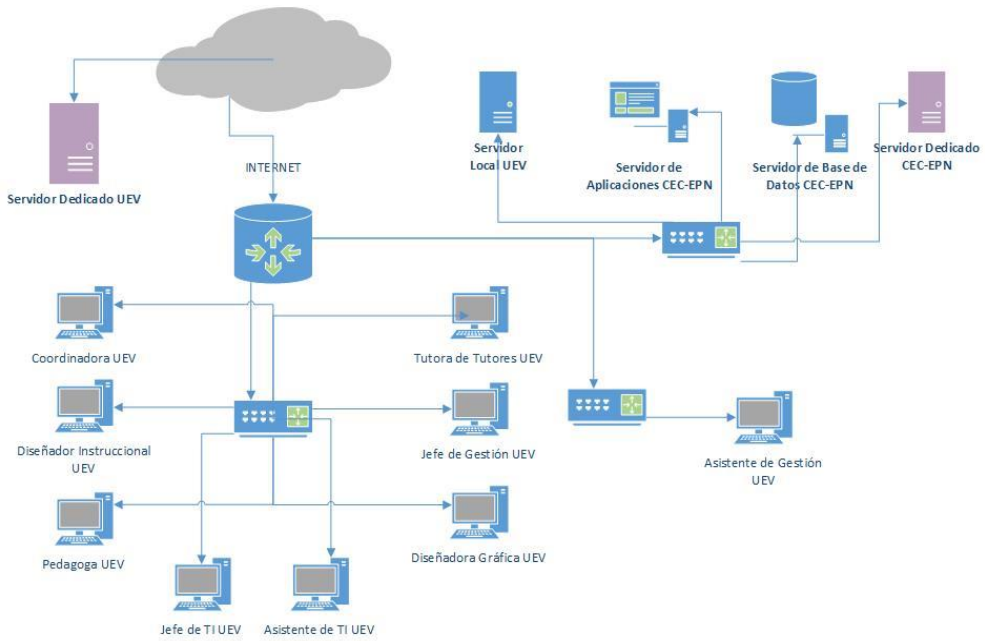

Figura 18. Diagrama de red de la UEV y Servicios adicionales

- Software

Son los distintos programas, herramientas y plataformas se utilizan en el desarrollo de las actividades de cada proceso crítico.

Tabla 59. Inventario de Software necesario para la realización de los procesos críticos en la UEV

Software	Procesos			Versión	Última actualización	Interacción con otros sistemas
	Ejecutar Curso	Inscripción y Matriculación	Diseño de Curso			
Adobe Photoshop			X	CS5	2013	LMS Moodle
Adobe Ilustrator			X	CS5	2013	LMS Moodle
Adobe Dreamweaver			X	CS5	2013	LMS Moodle
Adobe Flash			X	CS5	2013	LMS Moodle
Adobe Flash Player	X	X	X	11.0	2014	LMS Moodle
Adobe Reader	X	X	X	11.0	2014	LMS Moodle SIICECW Sitio web CEC Sitio Web UEV
Articulate			X	9	2013	LMS Moodle
CodeIgniter			X			SIICECW
Exe-learning			X			LMS Moodle
GIMP			X			LMS Moodle
gCMS		X		1	2007	Sitio web CEC Sitio Web UEV
iSpring Presenter			X	7	2013	LMS Moodle
Joomla		X		1.5	2009	SIICECW Sitio web CEC Sitio Web UEV
McAfee Antivirus	X	X	X			
Moodle	X		X	1.9 2.5	2010	SIICECW
MS. Excel	X	X	X	2010	2010	
MS. PowerPoint	X		X	2010		Articulate

Software	Procesos			Versión	Última actualización	Interacción con otros sistemas
	Ejecutar Curso	Inscripción y Matriculación	Diseño de Curso			
MS. Word	X	X	X	2010	2010	
MS. SQL Server		X		2008	2010	CodeIgniter SIICECW
MySQL	X	X	X	5.3	2013	LMS Moodle
PHP	X	X	X	5.3	2013	LMS Moodle
Picasa			X			LMS Moodle
Prezi online			X		2013	LMS Moodle
SSH Secure Shell	X		X		2010	LMS Moodle
Winzip	X	X	X			LMS Moodle
WinRar	X	X	X			LMS Moodle

Nota: la tabla 59, muestra el nombre del software, el proceso en el que interviene, la versión, la última fecha en qué fue actualizado y la interacción que tiene con otros programas o sistemas.

- Hardware

Se refiere a las especificaciones técnicas de los servidores, estaciones de trabajo que intervienen en los procesos críticos, además incluye a los responsables de los equipos.

Para un mejor entendimiento se describe que áreas de la UEV intervienen en cada proceso crítico.

1. Hardware del proceso Diseño de Curso (DC): los equipos que intervienen en este proceso son de las áreas de Coordinación UEV, Académica UEV, Tecnología de la Información UEV y la de Diseño Gráfico UEV.
2. Hardware del proceso Inscripción y Matriculación (IM): los equipos que intervienen en este proceso son de las áreas de Coordinación UEV, Gestión y Tecnología de la Información CEC-EPN.
3. Hardware del proceso Ejecutar curso (EC): los equipos que intervienen en este proceso son de las áreas de Coordinación UEV, Académica UEV, Gestión y Tecnología de la Información CEC-EPN.

Tabla 60. Inventario de Hardware de los equipos necesario para la realización de los procesos críticos.

Equipos	Cargo/Responsable	Procesos			Características	Sistema Operativo	Tipo de Mantenimiento
		Ejecutar Curso	Inscripción y Matriculación	Diseño de Curso			
Servidor 1	Jefe de TI	X	X	X	Procesador: RAM: 32 GB Disco Duro: 1 TB Comunicación remota	Centos 6	Correctivo
Servidor 2	Jefe de TI			X	Procesador: RAM: 32 GB Disco Duro: 2 TB	Centos 6	Correctivo
Equipo 1	Coordinadora UEV Diseñador Instruccional Experta Pedagoga Tutora de Tutores Asistente de TI Asistente de Gestión	X X X X X X	X X X	X X X X X	INTEL CORE QUAD Procesador: 2.4 GHZ RAM: 4 GB Disco Duro: 250 GB	Windows 7	Preventivo y Correctivo
Equipo 2	Jefe de TI Diseñadora Gráfica	X X	X	X X	INTEL CORE I7 Procesador: 3.4 GHZ RAM: 4 GB Disco Duro: 300 GB	Windows 7	Preventivo y Correctivo
Equipo 3	Jefe de Gestión	X	X		INTEL CORE I7 Procesador: 3.1 GHZ RAM: 4 GB Disco Duro: 1 TB	Windows 7	Preventivo y Correctivo
Equipo 4	Diseñadora Gráfica	X		X	Procesador: 2.7 GHZ RAM: 4 GB Disco Duro: 1TB	MAC OS X 10.85	Preventivo y Correctivo

La tabla 60, muestra el nombre del equipo, el responsable del equipo, en que proceso interviene el equipo, las características técnicas (Procesador, RAM y Disco Duro), sistema operativo instalado y el tipo de mantenimiento que se realiza sobre ellos.

Existen equipos adicionales que se utilizan para la ejecución de los procesos especialmente en el proceso CEC-PV-04 Inscripción y Matriculación, estos son:

1 Impresora Samsung CPL-620 ND

2 Impresoras HP LaserJet 1536DNF

1 Scanner HP Color LaserJet C91515N

- Comunicaciones

Son los recursos empleados en los procesos críticos, para que se pueda llevar a cabo la comunicación. Las tablas 61, 62 y 63 describen el origen de la comunicación, el receptor, el medio físico de transmisión y el proveedor del servicio.

Tabla 61. Recursos necesarios para la comunicación en el proceso Ejecutar Curso

Número de Proceso	CEC-PV-06		
Nombre del Proceso	Ejecutar Curso		
Descripción de la comunicación	En este proceso interactúan los siguientes actores: ➢ Cliente (estudiante), la persona que decide capacitarse en los cursos ofertados por la UEV. ➢ Tutora de tutores, supervisa y gestiona el proceso de capacitación es el medio de comunicación entre el Tutor virtual y el Cliente (estudiante). ➢ Área de Tecnología de Información, supervisa y gestiona el correcto funcionamiento de la plataforma virtual, así como también brinda el soporte técnico a los Tutores Virtuales y Clientes (estudiantes).		
Origen	➢ Receptor	Medio físico	Proveedor
Cliente/Tutor Virtual Solicita soporte técnico durante el proceso de capacitación.	➢ Jefe de TI ➢ Asistente de TI	➢ Teléfono convencional ➢ Teléfono celular ➢ Estación de trabajo ➢ Internet	➢ CNT ➢ Movistar ➢ Gmail ➢ Cedia
Tutora de Tutores Tutoriza el correcto desenvolvimiento de las actividades planificadas en los cursos virtuales.	➢ Tutores virtuales ➢ Cliente (estudiante).	➢ Teléfono convencional ➢ Teléfono celular ➢ Estación de trabajo ➢ Internet	➢ CNT ➢ Movistar ➢ Gmail ➢ Cedia

En la tabla 61, se puede observar la comunicación que existe entre el cliente/Tutor Virtual y la de TI, además la relación entre la Tutora de Tutores y cliente/Tutor Virtual.

La Tutora de Tutores canaliza la información de los clientes y Tutores Virtuales hacia las distintas áreas de la UEV.

Tabla 62. Recursos necesarios para la comunicación en el proceso de Inscripción y Matriculación

Número de Proceso	CEC-PV-04		
Nombre del Proceso	Inscripción y Matriculación		
Descripción de la comunicación	En este proceso interactúan los siguientes actores: ➢ Cliente, persona que decide capacitarse en los cursos ofertados por la UEV. ➢ Jefe de Gestión, supervisa y gestiona el proceso de inscripción y matriculación. ➢ Asistente de Gestión, el encargado de receptar: pedidos de información, inscripción y matriculación de cursos virtuales.		
Origen	➢ Receptor	Medio físico	Proveedor
Cliente Realiza la solicitud de información previa la inscripción de un curso virtual.	➢ Jefe de Gestión ➢ Asistente de Gestión	➢ Teléfono convencional ➢ Teléfono celular ➢ Estación de trabajo ➢ Internet	➢ CNT ➢ Movistar ➢ Gmail ➢ Cedia
Cliente Registra la inscripción y matriculación de los cursos virtuales.	➢ Jefe de Gestión ➢ Asistente de Gestión	➢ Estación de trabajo	➢ Gmail ➢ Cedia
Área de Gestión Confirma la recepción de la inscripción en el curso virtual.	➢ Cliente	➢ Teléfono convencional ➢ Teléfono celular ➢ Estación de trabajo ➢ Internet	➢ CNT ➢ Movistar ➢ Gmail ➢ Cedia
Cliente **E**nvía confirmación de pago realizado al curso virtual.	➢ Jefe de Gestión ➢ Asistente de Gestión	➢ Estación de trabajo ➢ Agencia Bancaria	➢ Gmail ➢ Cedia ➢ Banco de Guayaquil
Área de Gestión Confirma la recepción del pago del curso virtual.	➢ Cliente	➢ Teléfono convencional ➢ Teléfono celular ➢ Estación de trabajo ➢ Internet	➢ CNT ➢ Movistar ➢ Gmail ➢ Cedia

En la tabla 62, se muestra como el proceso de Inscripción y Matriculación requiere que una comunicación en doble vía, ambas partes deben confirmar para continuar con el proceso.

Tabla 63. Recursos necesarios para la comunicación en el proceso de Diseño de Cursos

Número de Proceso	CEC-PV-02		
Nombre del Proceso	Diseño de Cursos		
Descripción de la comunicación	En este proceso interactúan dos actores principales: ➢ Experto en Contenidos, la persona experta, conocedora de la temática del nuevo curso a desarrollar. ➢ Diseñador Instruccional, la persona que se comunica directamente con el experto durante el proceso de diseño de un curso virtual. La comunicación es importante porque ambos entregan/reciben información y retroalimentación del curso nuevo.		
Origen	Receptor	Medio físico	Proveedor
Diseñador Instruccional Solicita cambios, reunión de trabajo, sobre los contenidos desarrollados.	Experto en Contenidos	➢ Teléfono convencional ➢ Teléfono celular ➢ Estación de trabajo ➢ Internet	➢ CNT ➢ Movistar ➢ Gmail ➢ Cedia

La tabla 63, muestra la comunicación del Diseñador Instruccional y el Experto en Contenidos, ambas partes se mantienen en constante comunicación hasta la entrega del curso terminado.

4.2.2.3. Inventario de instalaciones físicas

Identifica el lugar donde se desarrollan las actividades de las personas que intervienen en cada proceso, incluye los empleados, usuarios externos, considerando la ciudad y edificación.

Tabla 64. Inventario de instalaciones físicas donde se realiza el proceso de Ejecutar Curso

Número de Proceso	CEC-PV-06
Nombre del Proceso	Ejecutar Curso
Ubicación - Personal interno	Unidad de Educación Virtual Edificio Aulas y Relación con el Medio Externo, Av. Toledo N23-55 y Madrid, Planta Baja Quito - Ecuador
Ubicación - Personal externo	➢ Los Tutores virtuales son nacionales y extranjeros, su lugar de residencia se específica en la Hoja de Vida que se solicita al iniciar el proceso de capacitación virtual. ➢ Los clientes son nacionales, las principales provincias de residencia son: Quito, Guayaquil, Cuenca, Ambato, Riobamba, Loja. ➢ La identificación de los clientes se lo realiza a través de los formularios de inscripción/matriculación, allí se encuentran sus datos personales.

Tabla 65. Inventario de instalaciones físicas donde se realiza el proceso de Inscripción y Matriculación

Número de Proceso	CEC-PV-04
Nombre del Proceso	Inscripción y Matriculación
Ubicación - Personal interno	Unidad de Educación Virtual Edificio Aulas y Relación con el Medio Externo, Av. Toledo N23-55 y Madrid, Planta Baja Quito - Ecuador
Ubicación - Personal externo	Los clientes son nacionales, las principales provincias de residencia son: Quito, Guayaquil, Cuenca, Ambato, Riobamba, Loja. La identificación de los clientes se lo realiza a través de los formularios de inscripción/matriculación, allí se encuentran sus datos personales.

Tabla 66. Inventario de instalaciones físicas donde se realiza el proceso de Diseño de Cursos

Número de Proceso	CEC-PV-02
Nombre del Proceso	Diseño de Cursos
Ubicación - Personal interno	Unidad de Educación Virtual Edificio Aulas y Relación con el Medio Externo, Av. Toledo N23-55 y Madrid, Planta Baja Quito - Ecuador
Ubicación - Personal externo	Los expertos en contenidos son nacionales y extranjeros, su lugar de residencia se específica en la Hoja de Vida que se solicita al iniciar el proceso de Diseño de Curso.

4.2.2.4. Inventario del recurso humano

El recurso humano es otro de los factores importantes en la realización de los procesos, en esta sección se identifica a las personas que intervienen en cada uno de ellos a nivel interno como externo.

Las tablas 67, 68 y 69 muestran el nombre y cargo del personal que interviene en el proceso a nivel interno como externo. Además se describe una de sus actividades principales y en caso de ausencia que persona puede apoyar.

Tabla 67. Inventario Recursos Humanos en el proceso de Ejecutar Curso

Número de Proceso: CEC-PV-06		
Proceso: Ejecutar Curso		
PERSONAL INTERNO		
Nombre Cargo	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
Lic. Gabriela Martínez MgS. **Coordinadora de la Unidad de Educación Virtual**	➢ Evalúa los resultados de la gestión académica y administrativa de la unidad para la aplicación de planes y proyectos de mejora continua.	**Jefe de Tecnologías de la Información** **Diseñador Instruccional**
Ing. Silvana Calderón **Tutora de Tutores**	➢ Desarrollo de informes finales de cursos virtuales. ➢ Seguimiento a tutores y estudiantes de cursos virtuales CEC-EPN. ➢ Evaluación a tutores virtuales.	**Diseñador Instruccional** **Experta Pedagoga**
Tlga. Andrea Conza **Jefe de Tecnologías de la Información** Sr. Iván Mullo **Asistente de Tecnologías de la Información**	➢ Soporte técnico a estudiantes de cursos virtuales. ➢ Mantenimiento de plataformas virtuales. ➢ Gestión de plataforma de videoconferencia.	**Asistente de Tecnologías de la Información.** **Coordinación de Tecnología CEC-EPN**
PERSONAL EXTERNO		
Contratista, Proveedor	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
Tutor Virtual	➢ Capacita a los estudiantes de los cursos virtuales ➢ Genera informes finales de ejecución de curso (calificaciones y observaciones).	Nuevo tutor virtual de acuerdo a la Base de Expertos UEV.

Tabla 68. Inventario Recursos Humanos en el proceso de Inscripción y Matriculación

Número de Proceso: CEC-PV-04		
Proceso: Inscripción y Matriculación		
PERSONAL INTERNO		
Nombre Cargo	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
Lic. Gabriela Martínez MgS. **Coordinadora de la Unidad de Educación Virtual**	➢ Realiza el calendario anual de cursos virtuales.	**Jefe de Tecnologías de la Información** **Diseñador Instruccional**

Número de Proceso: CEC-PV-04		
Proceso: Inscripción y Matriculación		
PERSONAL INTERNO		
Nombre Cargo	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
Ing. Christian Hidalgo **Jefe de Gestión UEV**	➢ Supervisa y gestiona el proceso de inscripción y matriculación.	**Coordinadora de la Unidad de Educación Virtual** **Asistente de Gestión UEV**
Sr. David Valencia **Asistente de Gestión UEV**	➢ Recibe la información de inscripciones y matrículas de los sitios web CEC-EPN. ➢ Elaboración de proformas y cotizaciones para clientes internos y externos de la UEV.	**Jefe de Gestión UEV** **Tutora de Tutores**
Tlga. Andrea Conza **Jefe de Tecnologías de la Información** Sr. Iván Mullo **Asistente de Tecnologías de la Información**	➢ Administra los sitios web CEC-EPN y UEV.	**Asistente de Tecnologías de la Información.** **Coordinación de Tecnología CEC-EPN**
Ing. Carla Gómez **Diseñadora Gráfica**	➢ Desarrollo de artes gráficos para la imagen UEV.	**Diseñador Gráfico CEC-EPN.** **Personal Unidad de Producción CEC-EPN.**

Tabla 69. Inventario Recursos Humanos en el proceso de Diseño de Cursos

Número de Proceso: CEC-PV-02		
Proceso: Diseño de Cursos		
PERSONAL INTERNO		
Nombre Cargo	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
Lic. Gabriela Martínez MgS. **Coordinadora de la Unidad de Educación Virtual**	➢ Define políticas y normativas para el desarrollo de cursos virtuales. ➢ Identifica nuevas oportunidades de diseño de cursos virtuales.	**Jefe de Tecnologías de la Información** **Diseñador Instruccional**
Ing. Cristhian Castillo **Diseñador Instruccional**	➢ Realiza el Diseño Instruccional de cursos virtuales. ➢ Diseña recursos utilizando objetos de aprendizaje. ➢ Desarrollo de cursos virtuales.	**Coordinadora de la Unidad de Educación Virtual**
Lic. Leticia Correa **Experta Pedagoga**	➢ Diseño Pedagógico de cursos virtuales.	**Coordinadora de la Unidad de Educación Virtual**

Número de Proceso: CEC-PV-02		
Proceso: Diseño de Cursos		
PERSONAL INTERNO		
Nombre Cargo	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
Ing. Silvana Calderón **Tutora de Tutores**	➢ Desarrollo del curso piloto previo a la apertura del curso virtual.	**Diseñador Instruccional**
Tlga. Andrea Conza **Jefe de Tecnologías de la Información** Sr. Iván Mullo **Asistente de Tecnologías de la Información**	➢ Gestión de materiales y recursos en el aula diseñada.	**Asistente de Tecnologías de la Información**
Ing. Carla Gómez **Diseñadora Gráfica**	➢ Desarrollo de objetos y materiales gráficos.	**Diseñador Gráfico CEC-EPN.** **Personal Unidad de Producción CEC-EPN.**
PERSONAL EXTERNO		
➢ **Contratista, Proveedor**	**Descripción de las actividades**	**Personal de apoyo en caso de ausencia**
➢ Experto en contenidos	Desarrolla los contenidos para el nuevo curso virtual.	Nuevo experto de acuerdo a la Base de Expertos UEV.
➢ Lingüista	Revisión ortográfica de los contenidos enviados por los Expertos en contenidos	**Coordinadora de la Unidad de Educación Virtual**

4.2.3. Análisis de riesgos

Para esto se utilizará el análisis realizado en el Capítulo Tres sobre los activos críticos de la Unidad de Educación Virtual.

En esta etapa el objetivo es determinar el conjunto de estrategias que deberá implementar la UEV para que los procesos críticos puedan reanudarse en condiciones mínimas.

Tabla 70. Interacción de Activos Críticos y Procesos Críticos

Nombre del Proceso	Activos críticos
Ejecutar Curso	➢ Sistema Integrado de Información del CEC-EPN. ➢ Gestores de Cursos Virtuales CEC-EPN y EPN.
Inscripción y Matriculación	➢ Sitios Web CEC-EPN. ➢ Sistema Integrado de Información del CEC-EPN. ➢ Gestores de Cursos Virtuales CEC-EPN y EPN.
Diseño de Cursos	➢ Gestores de Cursos Virtuales CEC-EPN y EPN.

En la tabla 70 se puede observar los tres activos críticos y como estos forman parte de los procesos críticos de la UEV.

Los resultados considerados en este apartado se encuentran en el Séptimo Paso del Capítulo 3, en las tablas 30, 31 y 32.

4.2.3.1. Recomendación de controles preventivos.

Los controles preventivos eliminan las causas del riesgo con el propósito de prevenir la ocurrencia o materialización.

Los resultados considerados en este apartado se encuentran en el Octavo Paso del Capítulo 3, en las tablas 33, 34 y 35.

4.2.4. Análisis de Impacto del Negocio (BIA)

Para recopilar la información que se emplearán en el BIA, se realizó varias entrevistas con el equipo de trabajo de la Unidad de Educación Virtual y la Coordinadora de Tecnología del CEC-EPN.

4.2.4.1. Definición de objetivo, alcance y suposiciones del BIA

- Objetivo

  Identificar el impacto ocasionado por la interrupción de los servicios críticos de la Unidad de Educación Virtual CEC-EPN.

- Alcance

  El BIA se centra únicamente en la Unidad de Educación Virtual del CEC-EPN, a fin de analizar el impacto que ocasionaría y las estrategias que se necesitarían para recuperar el negocio.

- Suposiciones

  Las suposiciones permiten establecer una categorización de los posibles eventos que pueden llegar a transformarse en interrupciones, además permite comprobar la capacidad que tendría el personal para enfrentar la interrupción del servicio.

  Las suposiciones se basan en el proyecto de titulación (Montesdeoca, 2011).

- Si la interrupción ocurre cuando el procesamiento es máximo.
- Si no existe facilidad para operar y producir de forma alterna.
- Si el sitio afectado se vuelve inaccesible una vez ocurrida la interrupción.

- Si el personal clave no se encuentra disponible en el momento que ocurre la interrupción.
- Si el sitio afectado se vuelve accesible después de un período de tiempo después de ocurrida la interrupción.

4.2.4.2. Identificar áreas y procesos fundamentales.

Las actividades que se realizan en los procesos son desarrolladas por tres áreas del negocio, en la tabla 71 se muestra la interacción de las áreas y los procesos.

Tabla 71. Áreas y procesos fundamentales de la UEV

Área del Negocio	Procesos del Negocio
Coordinación UEV Área Académica Área Tecnológica	Ejecutar Curso
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos

4.2.4.3. Evaluar el impacto financiero y estratégico

En etapa evalúa el impacto financiero y operacional suponiendo que exista una interrupción o desastre. La evaluación se realizará de manera cualitativa dado que los valores revelados son de uso confidencial de la organización.

Impacto Financiero

La evaluación del impacto financiero permite determinar la pérdida económica que representaría para la organización la interrupción de los procesos críticos.

A continuación las ponderaciones establecidas para determinar el nivel de impacto en la UEV:

- Impacto 0: no hay pérdidas
- Impacto 1: nivel bajo
- Impacto 2: nivel medio
- Impacto 3: nivel alto

Tabla 72. Impacto financiero de los procesos fundamentales de la UEV

Área del Negocio	Procesos del Negocio	Nivel de Impacto
Coordinación UEV Área Académica Área Tecnológica	Ejecutar Curso	3
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación	3
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos	2

A continuación el análisis realizado sobre los valores colocados en la tabla 72:

El proceso **Diseño de Cursos**, tiene un nivel de impacto financiero 2 (medio), debido a que si se suspende el proceso no habrá producción de nuevos cursos y repercute en los ingresos de la UEV.

En el proceso **Inscripción y Matriculación**, el impacto financiero por la suspensión de este proceso es de nivel 3 (alto) debido a que los ingresos se reducen, por falta de estudiantes, afecta además de manera directa al siguiente proceso Ejecución de Cursos.

Finalmente el proceso **Ejecutar Curso**, es crítico debido a que todas las actividades de capacitación virtual se realizan aquí. El prescindir del servicio ocasiona que los ingresos se reduzcan, la devolución de valores son la opción tras el incumplimiento de la capacitación. El impacto financiero es de nivel 3 (alto).

Impacto Estratégico

Para el impacto estratégico u operacional se consideraran los mismos factores empleados en el análisis de riesgos (posicionamiento, fidelización del cliente, productividad).

- Impacto 0: no produce impacto
- Impacto 1: nivel bajo
- Impacto 2: nivel medio
- Impacto 3: nivel alto

Tabla 73. Impacto estratégico de los procesos fundamentales de la UEV

Área del Negocio	Procesos del Negocio	Factores de Impacto Estratégico		
		Posicionamiento	Fidelización	Productividad
Coordinación UEV Área Académica Área Tecnológica	Ejecutar Curso	3	3	3
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación	3	3	2
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos	2	2	3

A continuación el análisis realizado sobre los valores colocados en la tabla 73:

El proceso **Diseño de Cursos**, en los factores de posicionamiento y fidelización tiene un nivel de impacto estratégico 2 (medio), la competencia aprovecharía esta oportunidad para captar nuevos clientes. La productividad laboral se ve afectada, el personal de la UEV deja de producir nuevos cursos, el nivel de impacto estratégico es 3 (alto).

El proceso **Inscripción y Matriculación**, tiene un impacto estratégico en los factores posicionamiento y fidelización 3 (alto), al no poder brindar la capacitación los clientes cambiarían su opción y elegirían a la competencia. La productividad tendría un impacto 2 (medio) el personal de la UEV no realizaría sus actividades diarias.

En el proceso **Ejecutar Curso**, todos los factores tienen un impacto estratégico 3 (alto), la confianza de los clientes en la modalidad se vería cuestionada, la revisión del material por parte de los estudiantes y la tutoría no se realizaría, porque no se cumpliría con el servicio 24x7.

4.2.4.4. Identificar las funciones y procesos críticos del negocio.

Sustentado y justificado en los pasos anteriores los procesos que cumplen con los siguientes criterios se denominan como procesos críticos:

- Si el valor de impacto financiero es 2 (medio) o 3 (alto)
- Si en al menos dos factores en el impacto estratégico, es 2 (medio) o 3 (alto).

La tabla 74, muestra el impacto financiero y estratégico para la organización, se evalúa el tiempo máximo que un proceso tardará en estar activo, para ello es necesario sumar los valores totales de las tablas.

Tabla 74. Impactos financiero y estratégico

Área del Negocio	Procesos	Imp. Financiero	Factores de Impacto Estratégico			Total Suma de Impactos
			Posicionamiento	Fidelización	Productividad	
Coordinación UEV Área Académica Área Tecnológica	Ejecutar Curso	3	3	3	3	12
Coordinación UEV, Área de Gestión Administrativa y Área Tecnológica	Inscripción y Matriculación	3	3	3	2	11
Coordinación UEV, Área Académica, Área Tecnológica,	Diseño de Cursos	2	2	2	3	9

4.2.4.5. Identificar MTD's (Maximum Tolerable Downtimes) y priorizar los procesos del negocio.

Después de conocer e identificar los procesos críticos, es necesario conocer los tiempos que la UEV puede tolerar que un proceso no se encuentre disponible o fuera de servicio, para ello se empleara los MTD's (Máximo Tiempo Tolerable de Caída).

La estimación de los MTD's se ha considerado de acuerdo a la experiencia y el consenso con la Coordinación de la UEV, en función del resultado obtenido de la suma del impacto financiero y estratégico.

Tabla 75. Estimación de MTD's

MTD	Total de puntos	Escala de priorización
De 1 a 24 horas (1 día)	12	A
De 25 a 48 horas (2 días)	11	B
De 49 a 72 horas (3 días)	10	C
De 73 a 96 horas (4 días)	9	D

Tomado de (Leiva, 2008, pp. 37-38).

Esto permite priorizar los procesos críticos de la UEV, a continuación la tabla con los elementos mencionados.

Tabla 76. Definición de MTD's para la UEV

Área del Negocio	Procesos del Negocio	Total Suma de Impactos	MTD's Días	Priorización de Proceso
Coordinación UEV Área Académica Área Tecnológica	Ejecutar Curso	12	1	A
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación	11	2	B
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos	9	4	D

4.2.4.6. Identificar los sistemas y aplicaciones críticas de TI

Se denominan así a los sistemas y aplicaciones de TI que apoyan a la realización de los procesos críticos, esta tabla se apoya en lo registrado en el apartado 4.2.2.2 sobre Inventario tecnológico Software.

Tabla 77. Sistemas y aplicaciones críticas de TI

Área del Negocio	Procesos del Negocio	Sistemas, aplicaciones y recursos críticos de TI
Coordinación UEV Área Académica Área Tecnológica	Ejecutar Curso	Adobe Reader MS. Office SSH Secure Shell Gestores de aprendizaje: CEC-EPN, CEC-EPN v2, CEC-INEPE, PREGRADO, POSGRADO Winzip WinRar Internet Correo electrónico Telefonía fija y móvil Impresora Estaciones de trabajo
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación	Adobe Reader MS. Office Sitio web CEC-EPN Sitio web UEV SIICECW Winzip WinRar Internet Correo electrónico Telefonía fija y móvil Impresora Estaciones de trabajo / Escáner

Área del Negocio	Procesos del Negocio	Sistemas, aplicaciones y recursos críticos de TI
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos	Adobe Cloud MS Office Herramientas de autor SSH Secure Shell Gestores de aprendizaje: CEC-EPN, CEC-EPN v2, CEC-INEPE, PREGRADO, POSGRADO Winzip WinRar Internet Correo electrónico Telefonía fija y móvil Impresora Estaciones de trabajo Escáner

4.2.4.7. Determinar RTO (Recovery Time Objetive) y WRT (Work Recovery Time).

En este apartado se determinará el RTO y el WRT con los que cuenta la UEV para la recuperación de los procesos identificados en la tabla 75.

Para un mejor entendimiento se muestra el siguiente gráfico que explica la interacción de los tiempos frente a un incidente.

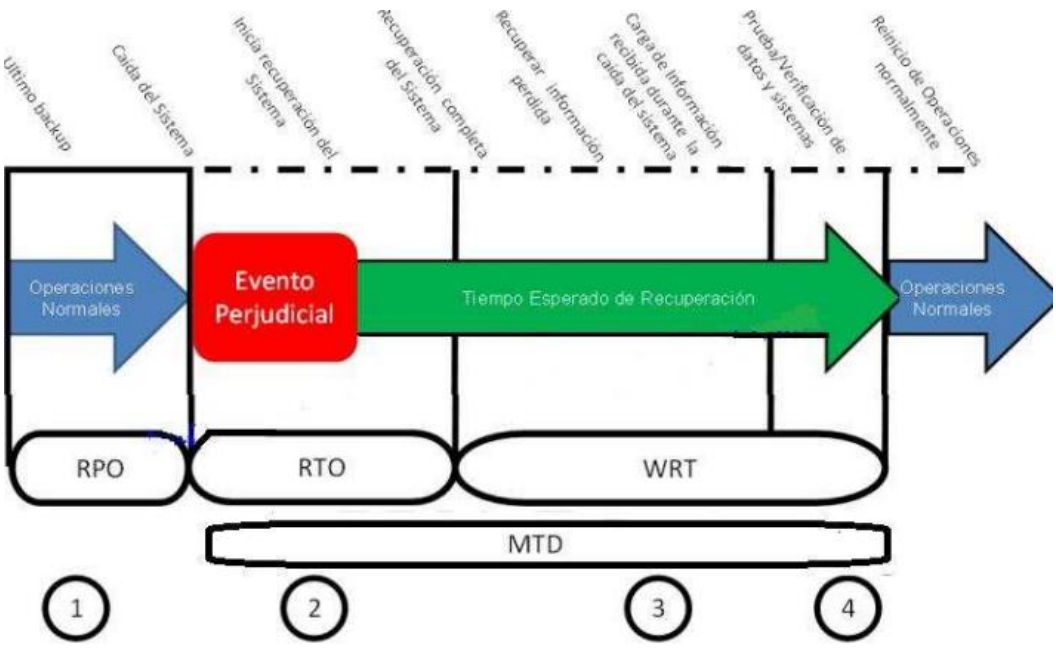

Figura 19. Interacción de tiempo

Tomado de (Camelo, 2010)

La escala empleada para el RTO está definida por los siguientes valores:

- A: De 1 a 24 horas
- B: De 25 a 48 horas
- C: De 49 a 72 horas
- D: De 73 a 125 horas

El WRT, es el tiempo disponible para recuperar los datos, perdidos o capturados manualmente mientras se recuperan los sistemas o recursos. Los valores WRT evalúan a los sistemas y aplicaciones de TI que almacenan datos.

$$WRT = MTD\text{-}RTO$$

Como base para establecer los tiempos RTO en primer lugar se debe considerar las actividades prioritarias de TI para que se pueda recuperar los diferentes recursos.

Tabla 78. Determinación del RTO

Actividad	RTO
Recuperar el enlace de red interna (LAN).	12 horas
Recuperar el enlace de red externa (WAN).	12 horas
Servidor de Archivos	72 horas
Servidor de Aplicaciones	12 horas
Servidor de Base de Datos (SQL Server)	24 horas
Servidor dedicado UEV (Servidor web, Servidor de Base de Datos MySQL y Gestor de aprendizaje).	16 horas

Nota: muestra las actividades prioritarias de TI con su respectivo tiempo,

- RTO.

El RTO y WRT para los servicios y aplicaciones críticas de la UEV se detallan a continuación:

Tabla 79. Identificación de RTO y WRT para los servicios y aplicaciones críticas de la UEV

Área del Negocio	Procesos del Negocio	Sistemas, aplicaciones y recursos críticos de TI	MTD	RTO	WRT
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos	Adobe Cloud	4 días	4 h	5 h
		MS Office		2 h	3 h
		Herramientas de autor		4 h	2 h
		SSH Secure Shell		6 h	1 h
		Gestores de aprendizaje: CEC-EPN, CEC-EPN v2, CEC-INEPE, PREGRADO, POSGRADO		2 h	4 h
		Winzip		1 h	-
		WinRar		1 h	-
		Internet		30 min	-
		Correo electrónico		30 min	-
		Telefonía fija y móvil		1 h	-
		Impresora		2 h	-
		Estaciones de trabajo		2 h	4 h
		Escáner		8 h	2 h
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación	Adobe Reader	2 días	4 h	5 h
		MS Office		2 h	3 h
		Sitio web CEC-EPN		2 h	4 h
		Sitio web UEV		2 h	4 h
		SIICECW		2 h	4 h
		Winzip		1 h	-
		WinRar		1 h	-
		Internet		30 min	-
		Correo electrónico		30 min	-
		Telefonía fija y móvil		1 h	-
		Impresora		2 h	-
		Estaciones de trabajo		2 h	4 h
		Escáner		8 h	2 h
Coordinación UEV Área Académica Área Tecnológica	Ejecutar curso	Adobe Reader	1 días	4 h	5 h
		MS Office		2 h	3 h
		SSH Secure Shell		1h	2 h
		Gestores de aprendizaje: CEC-EPN, CEC-EPN v2, CEC-INEPE, PREGRADO, POSGRADO		2 h	4 h
		Winzip		1 h	-
		WinRar		1 h	-
		Internet		30 min	-
		Correo electrónico		30 min	-
		Telefonía fija y móvil		1 h	-
		Impresora		2 h	-
		Estaciones de trabajo		2 h	4 h

4.2.4.8. Determinar RPO (Recovery Point Objetive)

Es el punto objetivo de recuperación, esto se refiere cuanta información está dispuesta a perder la UEV, de acuerdo a la última copia de seguridad o

respaldo en el momento del desastre, en otras palabras es la cantidad aceptable de pérdida de datos. En la tabla 80 se establece los tiempos definidos para el indicador RPO.

Tabla 80. Tabla de recursos según área y procesos de negocio RPO

Área del Negocio	Procesos del Negocio	Sistemas, aplicaciones y recursos críticos de TI	RPO
Coordinación UEV Área Académica Área Tecnológica	Diseño de Cursos	Adobe Cloud	30 min
		MS Office	Menor a 30 min
		Herramientas de autor	30 min
		SSH Secure Shell	-
		Gestores de aprendizaje: CEC-EPN, CEC-EPN v2, CEC-INEPE, PREGRADO, POSGRADO	30 min
		Internet	30 min
		Correo electrónico	30 min
		Telefonía fija y móvil	-
		Impresora	-
		Estaciones de trabajo	1 h
Coordinación UEV Área de Gestión Administrativa Área Tecnológica	Inscripción y Matriculación	Adobe Reader	30 min
		MS Office	Menor a 30 min
		Sitio web CEC-EPN	Menor a 1día
		Sitio web UEV	Menor a 1día
		SIICECW	Menor a 30 min
		Internet	30 min
		Correo electrónico	30 min
		Telefonía fija y móvil	-
		Impresora	-
		Estaciones de trabajo	1 h
Coordinación UEV Área Académica Área Tecnológica	Ejecutar curso	Adobe Reader	30 min
		MS Office	Menor a 30 min
		SSH Secure Shell	-
		Gestores de aprendizaje: CEC-EPN, CEC-EPN v2, CEC-INEPE, PREGRADO, POSGRADO	Menor a 30 min
		Internet	30 min
		Correo electrónico	30 min
		Telefonía fija y móvil	-
		Impresora	-
		Estaciones de trabajo	1 h

4.2.4.9. Analizar el daño causado por una interrupción en el negocio

En este punto se analiza los posibles daños que ocasionaría a la organización la interrupción de los servicios de TI.

Tabla 81. Consecuencias ocasionadas por la paralización de los servicios de TI

Servicios de TI	Consecuencias ocasionadas por la paralización de los servicios de TI
Adobe Cloud	La interrupción de esta herramienta provocaría que el área de diseño gráfico no pueda realizar las imágenes y objetos de aprendizaje en las aulas virtuales.
MS Office (Word, Excel, PowerPoint)	La ausencia de esta herramienta causaría que los usuarios no puedan realizar sus informes, presentaciones y cálculos, esto retrasaría la entrega de trabajo.
Herramientas de autor	La ausencia de estas herramientas haría que las áreas Académica y de Diseño Gráfico puedan desarrollar los objetos de aprendizaje en las aulas virtuales.
SSH Secure Shell	La falta de esta herramienta influenciaría en la comunicación con el servidor dedicado de la UEV vía SSH.
Gestores de aprendizaje CEC-EPN, CEC-EPN v2 CEC-INEPE, PREGRADO POSGRADO	La ausencia de los gestores de aprendizaje (LMS Moodle) ocasionaría que los procesos de capacitación no se ejecuten, causando serios problemas a la UEV.
Winzip/WinRar	La ausencia de estos programas afectaría al momento de adjuntar archivos por correo electrónico, subir archivos a los gestores de aprendizaje.
Sitio web CEC-EPN/ Sitio web UEV	La falta de los sitios web CEC-EPN y UEV ocasionaría que no haya estudiantes matriculados en los cursos virtuales, esto afectaría a los ingresos de la UEV.
SIICECW	La ausencia de este sistema provocaría que las actividades de registro académico se realicen manualmente, retrasando los procesos en toda la organización.

4.2.5. Identificación de las estrategias

En este apartado se determinan los recursos mínimos para evitar la interrupción de los servicios y continuar con los procesos críticos en los niveles de tiempo aceptables por la organización.

A través de las estrategias de continuidad del negocio, la organización puede identificar los recursos que se esperan recuperar y cuál es la mejor opción para realizarla.

4.2.5.1. Identificar el área y los recursos a recuperar

En este apartado se identifica el área y los recursos a ser recuperados, a nivel de área, recursos de TI.

La identificación de las estrategias toma como referencia al proyecto de titulación (Montesdeoca, 2011).

Se identifican dos categorías en este apartado:

Categoría de área de recuperación

- Oficina y centro de control de servidores

Categoría de recursos de TI e información a recuperar

- Aplicaciones y sistemas de TI
- Recursos y servicios de TI
- Servidores
- Base de datos

Tabla 82. Recursos de TI e información a recuperar

Aplicaciones y sistemas de TI	Recursos y servicios de TI	Servidores	Base de Datos
Adobe Cloud	Internet	Servidor dedicado UEV	Servidor de Base de Datos
MS Office (Word, Excel, PowerPoint)	Correo electrónico	Servidor dedicado CEC-EPN	
Herramientas de autor	Telefonía fija y móvil	Servidor de aplicaciones	
SSH Secure Shell	Impresora	Servidor de archivos	
Moodle	Estaciones de trabajo		
PHP-MySQL	Escáner		
Joomla	Discos externos		
gCMS			
CodeIgniter			
SIICECW			
Winzip/WinRar			

4.2.5.2. Determinar la opción de recuperación

"La continuidad de los servicios TI puede conseguirse bien mediante medidas preventivas, que eviten la interrupción de los servicios, o medidas reactivas, que recuperen unos niveles aceptables de servicio en el menor tiempo posible" (Osiatis, s.f.).

Existen tres opciones de recuperación del servicio a continuación de manera general:

- Cold standy: esta opción es la apropiada si los planes de recuperación consideran que la organización puede mantener sus niveles de servicio durante un período de tiempo sin el apoyo de la infraestructura de TI.
- Warm standy: esta opción demanda un período con sistemas activos, está diseñada para recuperar servicios críticos en un plazo de entre 24 y 72 horas.
- Hot standy: esta opción demanda un período con una réplica continua de datos y todos los sistemas activos, listos para una inmediata sustitución de la estructura de producción. Es la opción más costosa, se utiliza si la interrupción del servicio de TI tuviera repercusiones comerciales.

Aplicando lo visto en el apartado anterior tenemos:

Categoría de área de recuperación

Oficina y centro de control de servidores: las opciones de recuperación se menciona en la siguiente tabla:

Tabla 83. Área de preocupación a recuperar

Área de recuperación	Opción de recuperación	Descripción
Oficina (institución)	Utilizar las instalaciones de las sedes que posee el CEC-EPN.	Una oficina adecuada con estaciones de trabajo, sistemas, redes para iniciar el trabajo.
Centro de control de servidores (Datacenter)	Utilizar la propiedad o domicilio de un colaborador de TI como un sitio alterno.	Un espacio que se encuentre provisto con estaciones de trabajo, sistemas, material de oficina, redes y telefonía.

Área de recuperación	Opción de recuperación	Descripción
Centro de control de servidores (Datacenter)	Contratar un sitio alterno con un proveedor de servicios.	Un espacio especializado provisto de servidores de réplica base de datos, redes y conexión con el CEC-EPN.

Categoría de recursos de TI e información a recuperar

- Aplicaciones y sistemas de TI
- Recursos y servicios de TI
- Servidores
- Base de datos

Las opciones de recuperación para los recursos dentro de esta categoría se encuentran:

Tabla 84. Evaluación de las opciones de recuperación de los recursos de TI

Recursos de TI e información	Opción de recuperación	Descripción
Aplicaciones y sistemas de TI	Almacenar y mantener una copia de los instaladores de las aplicaciones y sistemas.	De los instaladores de las aplicaciones de software deben mantenerse una copia. En el caso de los sistemas se necesita contar con equipos, servidores configurados con el software base listos para entrar en funcionamiento.
Recursos y servicios de TI	Emplear las garantías de funcionamiento con los proveedores. Contratar un seguro para los equipos si ocurriera un incidente.	Establecer un acuerdo con el proveedor o aseguradora para establecer los criterios de recuperación, reparación de los equipos.
Servidores	Establecer acuerdos con el proveedor de los servidores.	Establecer los acuerdos del servicio en caso de falla de los componentes de hardware.
	Mantener copias de seguridad local en un equipo local y externo.	Mantener un servidor de respaldos local para subir un sitio alterno.

Recursos de TI e información	Opción de recuperación	Descripción
Base de Datos	Contar con servidores con respaldos (incremental, diferencial o completo), establecer la frecuencia de respaldo (diario, semanal o continuo),	Contar con servidores de base de datos donde los respaldos puedan ser subidos y colocar la información.

Las aplicaciones y sistemas son administrados por la Coordinación de Tecnología del CEC-EPN, la instalación y configuración es responsabilidad de la misma, excepto los sistemas de gestión de aprendizaje y sitio web de la UEV.

4.2.5.3. Evaluar las opciones viables

Esta actividad evalúa las opciones de recuperación, considerando la realidad diaria y económica de la UEV, la siguiente escala muestra el criterio de aplicación opciones de recuperación:

- Aplicable
- Recomendable
- No recomendable
- No aplicable

La prioridad que tiene la implementación de la opción de recuperación para la UEV, se basa en la escala:

- Nivel bajo: 1
- Nivel medio: 2
- Nivel alto: 3

Tabla 85. Evaluación de las opciones de recuperación por área de preocupación

Área de recuperación	Opción de recuperación	Criterios de aplicación	Prioridad	Justificación
Oficina (institución)	Utilizar las instalaciones de las sedes que posee el CEC-EPN.	Recomendable	2	El CEC-EPN cuenta con dos sedes en distintos lugares de la ciudad, sería una alternativa Recomendable si sucede algún inconveniente en la oficina principal.

Área de recuperación	Opción de recuperación	Criterios de aplicación	Prioridad	Justificación
Centro de control de servidores (Datacenter)	Utilizar la propiedad o domicilio de un colaborador de TI como un sitio alterno.	No recomendable	1	El colaborador podría salir de la organización sin previo aviso.
Centro de control de servidores (Datacenter)	Contratar un sitio alterno con un proveedor de servicios.	Recomendable	3	La UEV en los últimos años ha considerado mantener un sitio alterno dado la sensibilidad de los datos y criticidad de los servicios. Esto implica un costo alto al inicio pero al ser implementado las consecuencias positivas para el negocio se justifican.

A continuación la evaluación de la categoría de recursos de TI e información.

Tabla 86. Opciones de recuperación por recursos de TI e información

Recursos de TI e información	Opción de recuperación	Criterios de aplicación	Prioridad	Justificación
Aplicaciones y sistemas de TI	Almacenar y mantener una copia de los instaladores de las aplicaciones y sistemas.	Aplicable	1	Con esto se logra reinstalar y configurar las aplicaciones en caso de interrupción o daño de las mismas.
Recursos y servicios de TI	Emplear garantías de funcionamiento y acuerdos de servicio con los proveedores. Contratar un seguro para los equipos si ocurriera un incidente.	Recomendable	1	Si un equipo ha sufrido un daño, se solicita al proveedor cumplir con la garantía del equipo para reemplazar un componente o la reposición completa del mismo, en el caso de un servicio solicitar el cumplimiento de los acuerdos de servicio para transferir el riesgo y continuar con las actividades planificadas. En caso de robo se transfiere el riesgo al proveedor.
Servidores	Establecer acuerdos con el proveedor de los servidores.	Recomendable	2	La UEV debe definir los acuerdos de servicio con el proveedor, establecer líneas de soporte que permitan

Recursos de TI e información	Opción de recuperación	Criterios de aplicación	Prioridad	Justificación
				contar con la disponibilidad del servicio.
	Mantener copias de seguridad en un equipo local y externo.	Recomendable	2	Permite recuperar parcial o completamente la información de la UEV (sitio web, bases de datos y los gestores de aprendizaje) en caso de falla del servidor dedicado.
Base de Datos	Contar con servidores con respaldos (incremental, diferencial o completo), establecer la frecuencia de respaldo (diario, semanal o continuo),	Aplicable	1	Una correcta obtención de respaldos permite recuperar la información de la UEV y permite que el punto anterior se cumpla.

4.2.5.4. Evaluar según el criterio costo – beneficio

Este criterio es fundamental al momento de seleccionar la mejor opción, el valor económico no es lo único a considerar, sino el esfuerzo y el beneficio de la inversión que se realiza (confiabilidad, control y seguridad).

Los siguientes criterios se consideran en las tablas 87 y 88 para la evaluación del costo beneficio:

- Esfuerzo (E): es el nivel de esfuerzo y recurso humano que demanda la opción de recuperación.
- Confiabilidad (C): es el nivel de satisfacción de las necesidades a nivel de servicio y económico.
- Control (R): es el nivel de control que la UEV tendría sobre las aplicaciones y equipos al aplicar la recuperación.
- Seguridad (S): considera las condiciones físicas y de información al aplicar la recuperación.

De la misma manera que en los puntos anteriores la escala a emplear en la evaluación será:

- BAJO

- MEDIO
- ALTO

A continuación el análisis considerando el área de preocupación:

Tabla 87. Evaluación Costo – Beneficio de las opciones de recuperación por área de preocupación

Área de recuperación	Opción de recuperación	COSTO - BENEFICIO			
		E	C	R	S
Oficina (institución)	Utilizar las instalaciones de las sedes que posee el CEC-EPN.	MEDIO	ALTA	ALTO	ALTA
Centro de control de servidores (Datacenter)	Utilizar la propiedad o domicilio de un colaborador de TI como un sitio alterno.	ALTO	ALTA	ALTO	ALTA
Centro de control de servidores (Datacenter)	Contratar un sitio alterno con un proveedor de servicios.	MEDIO	ALTA	ALTO	ALTA

Tabla 88. Evaluación Costo – Beneficio de las opciones de recuperación por recursos de TI e información

Recursos de TI e información	Opción de recuperación	COSTO - BENEFICIO			
		E	C	R	S
Aplicaciones y sistemas de TI	Almacenar y mantener una copia de los instaladores de las aplicaciones y sistemas.	BAJO	MEDIA	MEDIO	MEDIA
Recursos y servicios de TI	Emplear garantías de funcionamiento y acuerdos de servicio con los proveedores. Contratar un seguro para los equipos si ocurriera un incidente.	ALTO	MEDIA	MEDIO	MEDIA
Servidores	Establecer acuerdos con el proveedor de los servidores.	ALTO	MEDIA	MEDIO	MEDIA
	Mantener copias de seguridad en un equipo local y externo.	BAJO	MEDIA	MEDIO	MEDIA
Base de Datos	Contar con servidores con respaldos (incremental, diferencial o completo), establecer	ALTO	ALTA	ALTO	ALTO

Recursos de TI e información	Opción de recuperación	COSTO - BENEFICIO			
		E	C	R	S
	la frecuencia de respaldo (diario, semanal o continuo),				

4.2.5.5. Consideraciones para las estrategias de recuperación

- Es importante considerar que las acciones a realizar no son un gasto sino una inversión a largo plazo que traerá beneficios para la UEV.
- El disponer de un sitio alterno para la UEV es importante porque permite garantizar la disponibilidad de los servicios ofertados por la unidad, amparándose en la primera consideración mencionada.
- Realizar una adecuada gestión de los respaldos de información es imprescindible, porque permitirá acortar el tiempo de recuperación y contar con los datos en el momento de interrupción del servicio.
- Las garantías y acuerdos de servicio deben ser claros para ambas partes (cliente – proveedor), ya que en el caso de un incidente se pueda solicitar el cumplimiento de las mismas (daño de componentes de hardware, reposición de equipos, tiempos de respuesta, soporte técnico).
- En el caso de la UEV, la gestión de los servicios de TI es compartida, en su mayor parte por la Coordinación de Tecnología del CEC-EPN y otra parte por el Área de TI de la UEV, ambas unidades deben trabajar de manera conjunta para coordinar los roles y responsabilidades dentro de cada área de preocupación y recursos de TI e información.

4.3 Implementación

La elaboración de esta etapa se basa en ITIL v3, la cual abarca los temas de organización y planificación dentro de la Gestión de la Continuidad de los Servicios de TI.

4.3.1. Organización y Planificación

Después de determinar el alcance del plan, analizar los riesgos y vulnerabilidades, y definir las estrategias de prevención y recuperación es

momento de establecer los recursos necesarios para la aplicación del plan de continuidad.

Figura 20. Pasos a desarrollar en la fase III – Implementación

Parte de los documentos que se incluyen están:

- Plan de prevención de riesgos.
- Plan de gestión de emergencias.
- Plan de recuperación.

4.3.1.1. Equipo de recuperación

La persona encargada de gestionar la recuperación inicial ante un incidente será la Jefe del Área de TI, quien notificará y convocará a los miembros de TI para evaluar el incidente presentado, posteriormente se notificará a la coordinación y miembros de la UEV sobre las acciones a realizar para la recuperación de los procesos críticos y aplicación del plan de continuidad.

4.3.1.2. Punto de reunión alterno en caso de desastre

En los siguientes casos, el lugar de reunión alterno para los miembros de la UEV son los siguientes:

- Si la Planta Baja del edificio EARME se encuentra inaccesible
  CEC-EPN: punto de encuentro, en los exteriores del edificio EARME.
  EPN: Biblioteca General.
- Si el edificio EARME se encuentra inaccesible
  EPN: Biblioteca General.
  EPN: Biblioteca Facultad de Sistemas.
- Si la zona de la universidad se encuentre inaccesible
  CEC-EPN – Sede Araucaria: Sala de Reuniones

CEC-EPN – Sede Reina Victoria: Sala de Reuniones

4.3.1.3. Acuerdos con proveedores

Es un convenio entre el proveedor y la organización por la prestación de un bien o servicio. Si la UEV no dispone de acuerdos, es necesario definir, actualizar y fortalecer para garantizar el cumplimiento de acuerdo a las políticas internas y normativas vigentes.

4.3.1.4. Requerimientos tecnológicos

Es necesario contar con respaldos de información de la UEV, estos se convierten en un insumo indispensable en el proceso. Los respaldos deben ser gestionados fuera de la UEV.

El recurso humano forma parte del proceso, es por esta razón que el equipo de trabajo debe contar con un alto sentido de responsabilidad y compromiso con la organización, en especial la disponibilidad 24/7 si se presentará una eventualidad.

4.3.2. Equipo de la Continuidad del Negocio

El Comité del BCP se encuentra definido por varios miembros de la UEV, los mismos que cumplen varios roles en el equipo; además se cuenta con el apoyo de miembros de la coordinación de Gestión Tecnológica del CEC-EPN.

4.3.2.1. Roles y funciones del equipo

Los roles y tareas que desempeñarán los miembros del comité del Plan de Continuidad se encuentra definido de la siguiente manera (Camelo, 2010):

Tabla 89. Roles, tareas y responsabilidades del equipo de la continuidad del negocio

Rol	Tareas - responsabilidades
Líder Ejecutivo	➢ Responsable general del Comité del BCP. ➢ Solicitar el apoyo de la Dirección. ➢ Solicitar el financiamiento necesario para el BCP.
Coordinador del BCP	➢ Asegurar el apoyo de la Dirección. ➢ Considerar los requisitos de financiamiento. ➢ Desarrollar la política del BCP. ➢ Coordinar y supervisar el proceso del BIA. ➢ Asegurar las participaciones eficaces de los líderes de procesos. ➢ Coordina y supervisar el desarrollo de los planes y disposiciones

Rol	Tareas - responsabilidades
	para la continuidad del negocio. ➢ Establecer grupos de trabajo y definir las responsabilidades. ➢ Coordinar el proceso de capacitación. ➢ Establecer revisiones periódicas, pruebas y de auditorías del BCP.
Oficial de Seguridad	➢ Garantizar que todos los aspectos del BCP se cumplan con los requisitos de seguridad de la organización.
Jefe de Información	➢ Cooperar estrechamente con el coordinador del BCP y especialistas de tecnología en los planes de continuidad.
Líderes de procesos	➢ Responsables de suministrar la información precisa y oportuna sobre las actividades de la organización, y revisar los resultados del BIA.

4.3.2.2. Equipo de la continuidad del negocio para la Unidad de Educación Virtual

El equipo se encargará de revisar, recuperar y retornar a las actividades normales en la UEV está definido por las siguientes personas:

Tabla 90. Responsables y rol dentro del comité del plan de continuidad del negocio

Responsable	Rol	Departamento o Coordinación
Tlga. Andrea Conza	Líder Ejecutivo Coordinador del BCP	Área de TI de la UEV
Lic. Gabriela Martínez MgS.	Coordinador del BCP Líder de proceso	Coordinación de la UEV
Sr. Iván Mullo	Oficial de Seguridad Líder de proceso	Área de TI de la UEV
Ing. Ximena Uchupanta	Jefe de Información	Coordinación de Tecnología CEC-EPN
Ing. Christian Hidalgo	Líder de proceso	Área de Gestión de la UEV
Ing. Cristhian Castillo	Líder de proceso	Área Académica de la UEV

4.3.3. Información de contactos

Para una adecuada gestión del plan de continuidad es necesario contar con la información de cada uno de los miembros del comité. La plantilla para recopilar la información de los contactos del BCP se encuentra en el Anexo 6, página 273, los datos colocados deben ser validados y actualizados periódicamente.

La información personal de los miembros no se colocará por motivos de confidencialidad pero la coordinación de la UEV dispone una documento con de esta información.

4.3.4. Actividades para la ejecución de las fases del BCP

Las actividades que se desarrollan en la administración de un incidente han sido adaptadas de acuerdo a las necesidades de la UEV e incluyen las siguientes fases: “Respuesta, Continuar entregando servicios o productos críticos, Recuperación y Restauración” (Camelo, 2010).

4.3.4.1. Respuesta

La respuesta frente a incidentes implica actuar con los equipos conformados, a través de planes, medidas y acuerdos establecidos.

La primera actividad a realizar es evaluar el impacto de los daños, notificar a los miembros del comité del plan de continuidad y ejecutar el plan que se adapte al incidente.

Las actividades que se ejecutan en esta fase se describen a continuación:

Gestión de Incidente

Las actividades que se desarrollarán son:

- Notificar a la Coordinación de la UEV, Coordinación de Tecnología CEC-EPN, Dirección del CEC-EPN y funcionarios.
- Tomar el control de la situación.
- Definir un punto de encuentro o reunión si fuera necesario.
- Identificar el alcance del daño presentado.
- Ponderar el impacto ocasionado.
- Implementar planes de acción de acuerdo al tipo de incidente, soportados en los controles de riesgo. Esto se puede visualizar en el Octavo Paso del Capítulo 3, en las tablas 30, 31 y 32.
- Estimar las pérdidas económicas generadas de acuerdo al Impacto financiero realizado en los procesos críticos.
- Identificar los daños en la infraestructura.

- Coordinar el apoyo de fuentes externas (proveedores) e internas (Coordinación de Tecnología CEC-EPN).
- Realizar un informe preliminar, mencionando las posibles causas del incidente y las acciones realizadas.

Gestión de comunicaciones

La comunicación es primordial para evitar rumores, establecer contacto con la Coordinación de la UEV, funcionarios, proveedores, tutores virtuales, estudiantes, servicios de emergencia.

Dentro de los requerimientos de comunicaciones se debe considerar el mantener equipos redundantes de información, con el objetivo de mantener la información segura y disponible para utilizarla.

Gestión de operaciones

Al presentarse una interrupción, la UEV puede trabajar desde un lugar alterno, denominado un centro de operaciones de emergencia, el análisis se encuentra mencionado en la tabla 85. **Evaluación de las opciones de recuperación por área de preocupación**.

4.3.4.2. Continuidad del servicio

Una vez identificado los procesos críticos para la UEV, en esta fase se debe asegurar que dichos procesos continúen operativos para los clientes, de no ser así que el tiempo de espera no sea superior a los establecidos en el BIA, considerando la tabla 79. Definición de RTO y WRT y tabla 80 Definición del RPO,

4.3.4.3. Recuperación y restauración

El objetivo es recuperar la operatividad de la UEV, manteniendo la entrega de los servicios críticos.

En esta fase se realizan las siguientes actividades:

Definir el sitio alterno de reunión y operaciones hasta la reparación de las instalaciones afectadas, si es necesario.

- Definir el sitio alterno de reunión y operaciones hasta la reparación de las instalaciones afectadas, si es necesario.
- Verificar que los recursos a utilizar en el sitio alterno se encuentren en óptimas condiciones para su funcionamiento.
- Revisar la configuración de los recursos.
- Revisar los respaldos y la integridad de los mismos.
- Revisar la ejecución de los procesos y procedimientos.
- De ser necesario adquirir recursos adicionales para restablecer por completo los procesos críticos de la UEV.
- Restaurar las operaciones en los puntos anteriores a la interrupción.
- Revisar que toda la infraestructura, redes e información se encuentre disponible para gestionar el regreso del personal a las instalaciones, además verificar que la información en los gestores de aprendizaje se encuentre disponible para los estudiantes.
- Leer minuciosamente el informe de incidentes, para considerar las acciones de prevención y registrarlas en el Plan de Continuidad del Negocio.

4.3.5. Análisis de la situación actual

Mediante el análisis de situación actual la UEV conocerá como debe actuar para poner en marcha los planes desarrollados.

En base a los procesos críticos encontrados se presenta los planes para mitigar y prevenir los riesgos.

4.3.5.1. Procesos críticos de la UEV

Tiempo: 1 día (24 horas) - Ejecutar Curso

- Realizar tareas programadas.
- Realizar evaluaciones.
- Revisar material de consulta.
- Descargar tareas y registrar las calificaciones.

Tiempo: 2 días (de 25 a 48 horas) - Inscripción y Matriculación

- Colocar información actualizada de los cursos.

- Descargar nuevos registros de clientes.
- Verificar pagos realizados.
- Registrar en el sistema los datos de clientes.

Tiempo: 4 días (73 a 96 horas) - Diseño de Cursos

- Generar material especializado.
- Diseñar los objetos de aprendizaje.
- Crear objetos de aprendizaje.
- Validar el curso nuevo.

4.3.5.2. Plan de prevención de riesgos

El objetivo principal es reducir los riesgos y evitar posibles inconvenientes y desastres.

A continuación se describen las estrategias por amenazas.

Tabla 91. Identificación de estrategias por amenaza Desactualización de los sistemas.

Número de estrategia:	R-UEV-001
Amenaza:	Desactualización de los sistemas
Actividades de prevención:	
➢ Instalar actualizaciones y parches de seguridad en los servidores. Desinstalar y deshabilitar servicios y programas innecesarios en los servidores. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	

Tabla 92. Identificación de estrategias por amenaza Alta Rotación de Personal.

Número de estrategia:	R-UEV-002
Amenaza:	Alta Rotación de Personal
Actividades de prevención:	
➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral. ➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV.	

Tabla 93. Identificación de estrategias por amenaza Fallo o defecto de Software.

Número de estrategia:	R-UEV-003
Amenaza:	Fallo o defecto de Software
Actividades de prevención:	
➢ Planificar configuración de Servidores. ➢ Instalar herramienta antivirus de acuerdo a las capacidades de los servidores y estaciones de trabajo de TI. ➢ Programar ejecución de herramienta antivirus para analizar de forma periódica a las aplicaciones y sistemas operativos huésped. ➢ Escoger un Sistema Operativo adecuado a los componentes instalados de los servidores. ➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios. ➢ Realizar pruebas de carga al sistema operativo. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	

Tabla 94. Identificación de estrategias por amenaza Desconocimiento en el manejo de los sistemas o equipos informáticos.

Número de estrategia:	R-UEV-005
Amenaza:	Desconocimiento en el manejo de los sistemas o equipos informáticos.
Actividades de prevención:	
➢ Elaborar diagramas y esquemas donde se pueda apreciar los procedimientos administrativos del área. ➢ Elaborar manual de manejo de los sistemas que utilice el área. ➢ Crear una base de conocimientos de los incidentes más conocidos para su posterior resolución. ➢ Realizar pruebas pilotos y entrevistas con el personal para obtener retroalimentación y realizar mejoras.	

Tabla 95. Identificación de estrategias por amenaza Problemas de conectividad en la red interna de la organización.

Número de estrategia:	R-UEV-006
Amenaza:	Problemas de conectividad en la red interna de la organización.
Actividades de prevención:	
➢ Proteger todos los elementos de red interna, hardware, software, datos ante cualquier intento de acceso no autorizado mediante la seguridad perimetral. ➢ Implementar restricciones en firewall. ➢ Asignar usuarios internos con permiso de salida para servicios restringidos.	

4.3.5.3. Plan de gestión de emergencias

El objetivo principal es establecer estrategias de respuesta apropiadas acordes a la situación actual de la UEV.

La primera actividad es establecer comunicación con los miembros del comité de plan de continuidad para ejecutar las estrategias de respuesta.

Dentro de la primera estrategia es establecer el punto de encuentro, el mismo que se encuentra definido en la sección 4.3.1.2 Punto de reunión alterno en caso de desastre.

Incidente: Si existe una caída en los sistemas o aplicaciones y procesos críticos de TI

- Identificar los sistemas gestionados y reportar a las unidades respectivas para una solución (Coordinación de Tecnología CEC-EPN o Área de TI UEV).
- Establecer un sitio alterno para el funcionamiento de las copias de seguridad y sitio web.

Incidente: Si existe una caída con los servidores dedicados CEC-EPN y UEV

- Notificar a la Coordinación de Tecnología CEC-EPN para obtener una solución en cuanto al servidor dedicado CEC-EPN.
- Establecer acuerdos con los proveedores, para recibir soporte técnico especializado.
- Trabajar con servidores espejo para que entren en funcionamiento mientras se restablece el servicio.

Incidente: Si existe problemas en los enlaces de datos y voz

- Notificar a la Coordinación de Tecnología CEC-EPN para obtener una solución.
- Conectarse a la red inalámbrica de la EPN.
- Conectarse a la red móvil de uno de los funcionarios para continuar con trabajo.

Incidente: Si existe interrupción en el servicio eléctrico

- Activar la planta generadora de energía eléctrica en el tiempo establecido por la administración del edificio.
- Utilizar los UPS's para los equipos sensibles (servidores, estaciones de trabajo de los funcionarios),
- Utilizar computadoras portátiles.

4.3.5.4. Plan de recuperación o continuidad

Las estrategias adecuadas para mantener la continuidad del servicio para la UEV son las siguientes:

- Contar con servidores de base de datos donde los respaldos puedan ser subidos y colocar la información.
- Disponer de un sitio alterno para la UEV, para garantizar la disponibilidad de los servicios ofertados por la unidad, para ser utilizado en caso de falla del servidor principal.
- Realizar una adecuada gestión de los respaldos de información es imprescindible, porque permitirá acortar el tiempo de recuperación y contar con los datos en el momento de interrupción del servicio.
- Mantener la frecuencia de los respaldos diarios y almacenarlos adecuadamente en cinta o discos duros externos,
- Las garantías y acuerdos de servicio deben ser claros para ambas partes (cliente – proveedor), ya que en el caso de un incidente se pueda solicitar el cumplimiento de las mismas (daño de componentes de hardware, reposición de equipos, tiempos de respuesta, soporte técnico).

Capítulo V

5 Conclusiones y Recomendaciones

5.1 Conclusiones

- La metodología OCTAVE Allegro demostró ser de mucha utilidad, ya que se enfoca en los activos de información y ofrece opciones para crear escenarios de amenaza, permitiendo un mayor alcance en la identificación de los riesgos y prevenirlos.
- La metodología OCTAVE Allegro permitió crear un ambiente colaborativo en las reuniones de trabajo con el equipo de la UEV, cada miembro evidencio que los recursos que utilizan, las actividades y procesos realizados son esenciales para el cumplimiento de los objetivos de la organización.
- La metodología OCTAVE Allegro brinda cinco criterios de medición de riesgo, pero la organización fue la que decidió que criterios utilizaría; así como también la ponderación de acuerdo a las necesidades del negocio.
- Al principio del proyecto se mencionó usar COBIT para la mitigación de riesgos encontrados, pero en el transcurso de la realización del análisis se comprobó que a través de la metodología OCTAVE Allegro en la fase denominada “Identificación y mitigación de riesgos” permite aminorar los riesgos encontrados a través de la integración de controles.
- El Análisis de Impacto del Negocio permitió conocer las repercusiones negativas de los riesgos en la Unidad de Educación Virtual y proponer las estrategias necesarias para mitigarlas.
- El apoyo de la alta dirección fue necesario para la elaboración del Plan de Continuidad.
- El equipo de trabajo fue implementando controles, políticas para fortalecer los acuerdos con los proveedores de servicios.
- El Análisis de Riesgos se convierte en un elemento de entrada para realizar el Plan de Continuidad.
- De la combinación de las buenas prácticas de Tecnologías de Información ITIL con una metodología como DRII se puede obtener un

Plan de Continuidad acorde a las necesidades de la Unidad de Educación Virtual.

- Para la realización del Plan de Continuidad es necesario contar con procesos claros y bien definidos para evitar imprecisiones en el análisis realizado.

5.2 Recomendaciones

- Con los resultados obtenidos en el presente trabajo se recomienda ampliar el análisis de riesgos y el plan de continuidad a todo el Centro de Educación Continua.
- La metodología OCTAVE Allegro puede ser utilizada por personas que están incursionando en el análisis de riesgos, ya que ofrece una guía técnica didáctica completa.
- Mantener un control y registro de los sucesos existentes en la UEV respecto a los servicios de TI a fin de establecer la probabilidad y frecuencia de ocurrencia de un evento.
- Ejecutar los planes de recuperación y emergencia periódicamente y evaluar los resultados obtenidos.
- El Comité debería evaluar periódicamente el Plan de Continuidad inicialmente dos veces al año para comprobar la efectividad y después anualmente para actualizar el mismo.
- Sociabilizar las políticas de seguridad del CEC-EPN, para minimizar las amenazas en la organización.

REFERENCIAS

27001 Academy. (s.f.). *¿Qué es la norma ISO 27001?* Recuperado el 12 de mayo de 2014, de http://advisera.com/27001academy/es/que-es-iso-27001/

27001 Academy. (s.f.). *Conceptos básicos sobre ISO 22301*. Recuperado el 20 de mayo de 2014, de http://advisera.com/27001academy/es/que-es-iso-22301/

Asociación Bancaria y de Entidades Financieras. (s.f.). *Guía para la Elaboración de Planes de Contingencia*. Recuperado el 16 de Febrero de 2014, de http://www.asobancaria.com/portal/pls/portal/docs/1/4389157.PDF

Bird, L., & Higgins, D. (2013). *Good Practice Guidelines 2013.* Recuperado el 29 de enero de 2015, de http://www.bcifiles.com/GPG2013PresentationforBCAW.pdf

Bueno, G., Correa, C., & Echeverry, J. I. (2010). *Administración de riesgos - una visión global y moderna*. Recuperado el 14 de agosto de 2014, de https://www.colibri.udelar.edu.uy/bitstream/123456789/201/1/M-CD4026.pdf

Business Continuity Institute (BCI). (s.f.). *What is BC?* Recuperado el 14 de marzo de 2014, de http://www.thebci.org/index.php/resources/what-is-business-continuity

Calle Guglieri, J. A. (1997). *Reingeniería y seguridad en el ciberespacio.* Madrid España: Ediciones Díaz de Santos, S.

Camelo, L. (2010). *Análisis de Impacto de Negocios / Business Imact Analysis (BIA)*. Recuperado el 10 de junio de 2014, de http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html

Camelo, L. (2010). *Plan de Continuidad de Negocios o Business Continuity Plan (BCP)*. Recuperado el 10 de junio de 2014, de http://seguridadinformacioncolombia.blogspot.com/2010/06/plan-de-continuidad-de-negocios-o.html

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process - 2007_005_001_14885.pdf:.* Recuperado el 16 de marzo de 2014, de http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Centro de Educación Continua (CEC-EPN). (2013). *Manual de Calidad.* Quito. Recuperado el 01 de marzo de 2014, de intranet/virtualcec-epn

Chena, P. (s.f.). *Tutorial Matriz*. Recuperado el 19 de diciembre de 2014, de http://www.uif.gov.ar/uif/images/tutorial_matriz.pdf

Disaster Recovery Institute International. (s.f.). *Prácticas Profesionales*. Recuperado el 10 de febrero de 2014, de https://www.drii.org/certification/professionalprac_spanish.php

Disaster Recovery Institute. (s.f.). *Las diez prácticas profesionales*. Recuperado el 10 de febrero de 2014, de http://drimexico.org/las-diez-practicas-profesionales/

Disaster Recovery Institute Spain. (s.f.). *Acerca de DRI*. Recuperado el 03 de enero de 2014, de http://www.dri-spain.org/acerca.html

EKOS Unidad de Investigación Económica y de Mercado. (2014). *Informe Diagnóstico de cursos de capacitación PROFESIONALES - 2014.* Recuperado el 12 de marzo de 2015, de intranet/virtualcec-epn

Figueroa, P. (2014). *COBIT SAC COSO.* Recuperado el 24 de junio de 2015, de http://myslide.es/documents/cobit-sac-coso.html

Gaona, K. (2013). *Aplicación de la Metología Magerit para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la Empresa Pesquera e Indusrial Bravito S.A en la Ciudad de Machala.* Recuperado el 20 de enero de 2015, de http://dspace.ups.edu.ec/handle/123456789/5272

Hidalgo, Y. (2010). *Comparacion de Controles Internos*. Recuperado el 28 de enero de 2015, de http://yomairahidalgo.jimdo.com/app/download/7112331068/COBIT,+SAC,+COSO.pdf?t=1402764769

Huerta, A. (2012). *Introducción al análisis de riesgos – Metodologías (I)*. Recuperado el 27 de junio de 2015, de http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Huerta, A. (2012). *Introducción al análisis de riesgos – Metodologías (II)*. Recuperado el 20 de agosto de 2014, de http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior ICETEX. (s.f.). *Manual de Administación del Plan de Continuidad de Negocios*. Recuperado el 20 de marzo de 2014, de http://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (s.f.). *Guía Avanzada de Gestión de Riesgos LNCS*. (Laboratorio Nacional de Calidad del Software (LNCS)) Recuperado el 9 de marzo de 2014, de https://www.incibe.es/file/TnOIvX7kM5r8OY-S8r9Bmg

Instituto Nacional de Tecnologías de la Comunicación (INTECO) y Deloitte. (s.f.). *Guía práctica para PYMES: como implantar un Plan de Continuidad de Negocio*. Recuperado el 23 de enero de 2015, de https://www.incibe.es/CERT/guias_estudios/guias//guia_continuidad

ISO27000.es. (s.f.). Recuperado el 10 de febrero de 2014, de http://www.iso27000.es/iso27000.html

Leiva, A. (2008). *Desarrollo del Plan de Continuidad del Negocio para el Departamento de TI de una Empresa Farmacéutica.* Recuperado el 11 de marzo de 2014, de http://bibdigital.epn.edu.ec/handle/15000/952

LLanos, H. (2010). *Mehari 2010.* Paris, Francia: CLUSIF.

M&M Auditores de Colombia Ltda. (s.f.). *Planes de Continuidad del Negocio.* Recuperado el 02 de julio de 2014, de http://www.acis.org.co/fileadmin/Conferencias/ConferenciaBCP.pdf

Martínez, E. (2012). *Auditoria Interna*. Recuperado el 28 de junio de 2015, de http://escarletteauditoria.blogspot.com/2012/11/modelos-de-control-losmodelos-han-sido.html

Martínez, G. (2015). *Informe Historico Inscripción Personal Cursos Virtual (General).* Quito. Recuperado el 29 de enero de 2015, de intranet/virtualcec-epn

Matalobos, J. (2009). *Análisis de riesgos de Seguridad de la Información.* Recuperado el 18 de abril de 2014, de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Mendoza, M. (2014). *8 pasos para hacer una evaluación de riesgos (parte II)*. Recuperado el 21 de junio de 2015, de http://www.welivesecurity.com/la-es/2014/09/30/8-pasos-evaluacion-de-riesgos-2/

Montesdeoca, A. E. (2011). *Desarrollo de un Plan de Continuidad del Negocio en la Unidad de Gestión de TI del Ministerio de Coordinación de Desarrollo Social.* Recuperado el 02 de febrero de 2014, de http://bibdigital.epn.edu.ec/handle/15000/4614

Osiatis. (s.f.). *Gestión de la Continuidad de los Servicios TI*. Recuperado el 10 de octubre de 2014, de http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti/estrategias_continuidad.php

Pastor, A. (2012). *Novedades de Cobit 5*. Recuperado el 15 de mayo de 2014, de http://www.crisoltic.com/2012/04/cobit-5-que-hay-de-nuevo.html

Pazmiño, P. (2007). *Análisis de riesgos y vulnerabilidades de la red de datos de la EPN.* Recuperado el 20 de marzo de 2014, de http://bibdigital.epn.edu.ec/handle/15000/695

Peña, J. (s.f.). *Metodologías y Normas para el Análisis de Riesgos*. Recuperado el 26 de abril de 2013, de http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

Romero, N. (2002). *Planes de Contingencia: Un enfoque práctico.* Recuperado el 24 de abril de 2014, de www.acis.org.co/memorias/JornadasSeguridad/IIJNSI/contingencia.ppt

Salazar, F., & Torres, J. (2008). *Análisis de riesgos y diseño de políticas de seguridad para una empresa de producción cuencana.* Recuperado el 20 de agosto de 2014, de http://dspace.ups.edu.ec/handle/123456789/573

Salazar, S., & Rangel, J. (2012). *Análisis de la Gestión de Riesgos en la División de Sistemas de la Universidad Francisco de Paula Santander, mediante la Aplicación de la metodología CRAMM.* Recuperado el 12 de mayo de 2015, de https://seguridadinformaticaufps.wikispaces.com/file/view/Metodologia+Cramm+1150198-1150226.docx

Seguridad informática. (s.f.). *Elementos de un análisis de riesgo*. Recuperado el 16 de febrero de 2015, de https://informaticsecurity.wordpress.com/elementos-de-un-analisis-de-riesgo/

SGS Academy. (s.f.). *Principios y Buenas Prácticas en Continuidad de Negocio*. Recuperado el 03 de julio de 2014, de http://www.sgs.com/~/media/Local/Spain/Documents/Brochures/SGS-Curso-Continuidad-de-Negocio-BCI-ES-12.pdf

Sperat, S. (2010). *Cobit 5*. Recuperado el 23 de julio de 2014, de http://estratega.org/todo-lo-que-usted-queria-saber-sobre-cobit-5-y-no-se-animo-a-preguntar/

Unidad de Educación Virtual (UEV). (s.f.). *Educación Virtual*. Recuperado el 20 de mayo de 2014, de http://www.virtualepn.edu.ec

Van Bon, J., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Verheijen, T. (2008). *Fundamentos de ITIL® V3.* Holanda: Van Haren Publishing, Zaltbommel. Recuperado el 15 de mayo de 2014

ANEXOS

Anexo N° 1. Criterios de medida del Riesgo

Los resultados de la encuesta realizada al equipo de la UEV se muestran en las siguientes figuras:

Pregunta 1: ¿Cuáles son los activos de información de mayor valor para la organización, según su criterio?

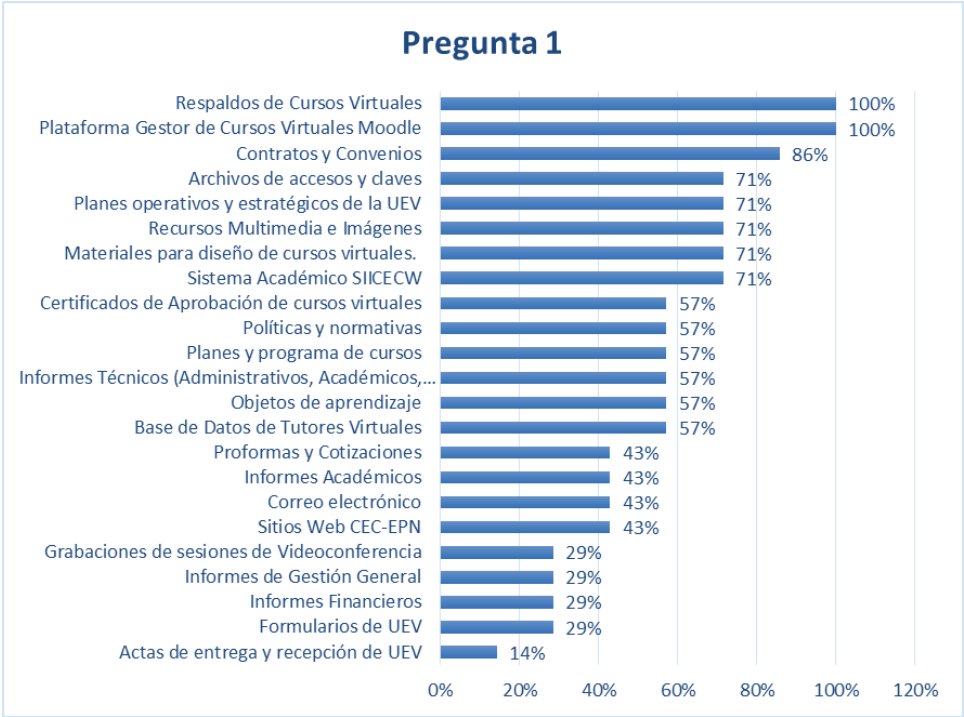

Figura 21. Resultados de la pregunta 1 sobre los activos de información

Pregunta 2: ¿Qué activos de información se utiliza en los procesos de trabajo del día a día, según su criterio?

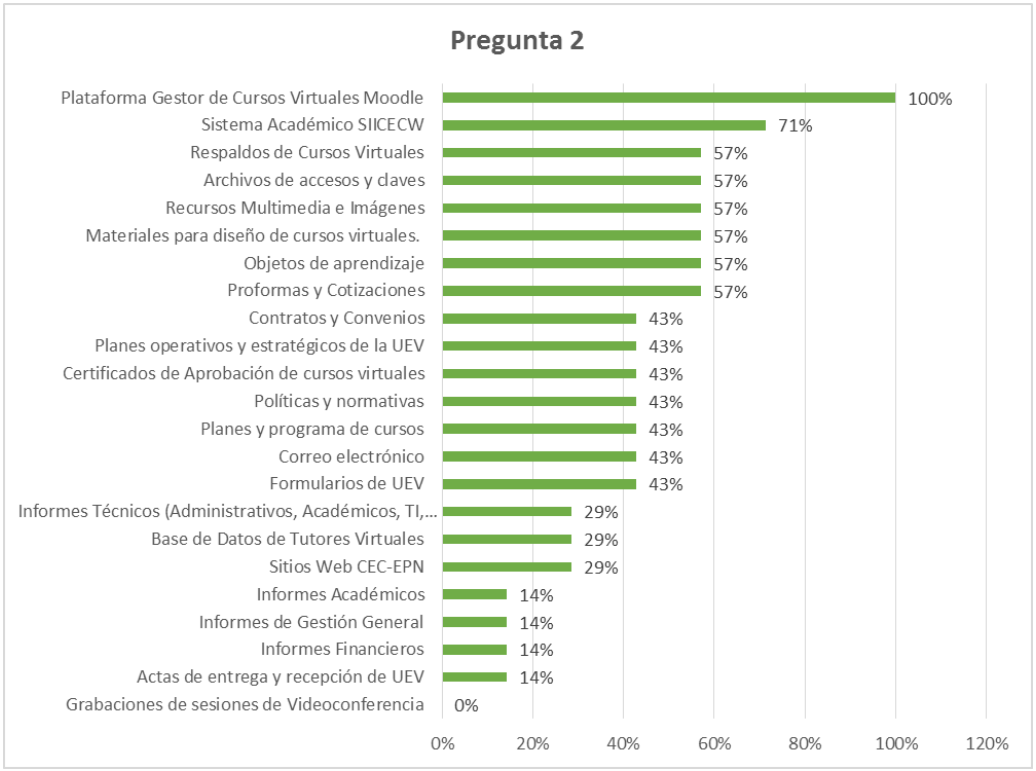

Figura 22. Resultados de la pregunta 2 sobre los activos de información

Pregunta 3: ¿Qué activos de información, en caso de pérdida, interrumpiría considerablemente la capacidad de su organización para cumplir sus objetivos y contribuir a la consecución de la misión de la organización?

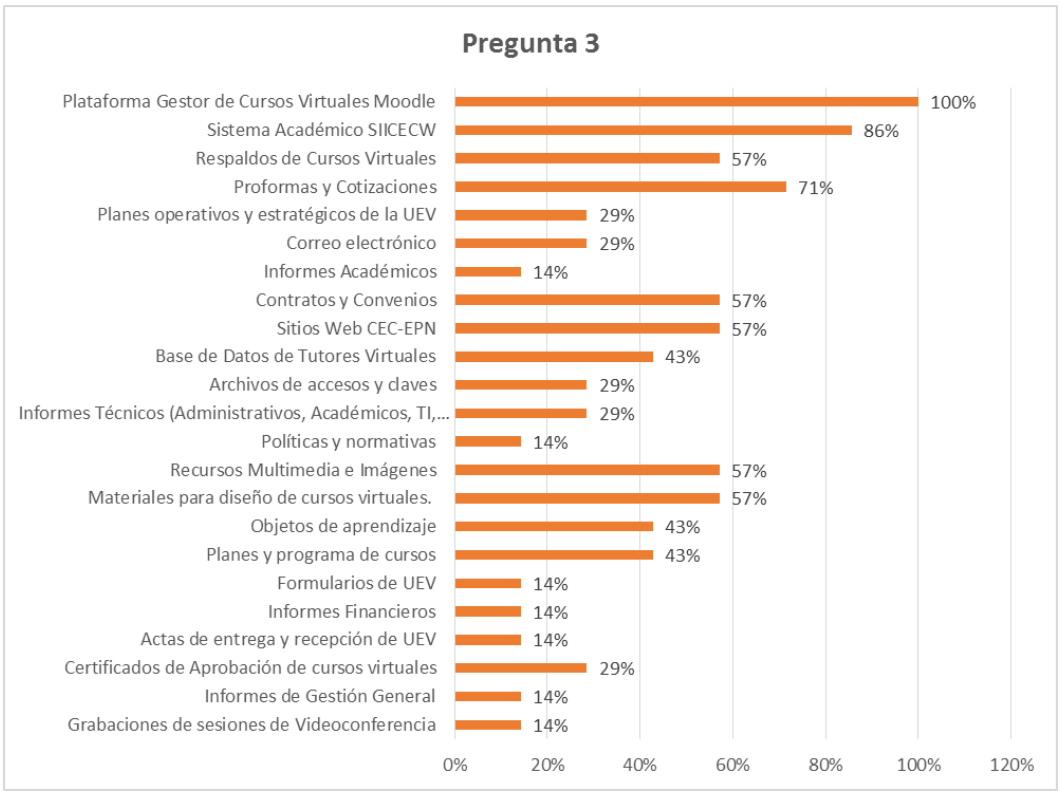

Figura 23. Resultados de la pregunta 3 sobre los activos de información

Pregunta 4: ¿Qué activos en su lista, si es comprometida, tendría un impacto negativo en la organización si sucede una o más de las siguientes situaciones?

a) Si el activo fuera revelado por personas no autorizadas.
b) Si el activo fuera modificado sin autorización.
c) Si el activo fuera destruido o perdido.
d) Si el acceso al activo fuera interrumpido.

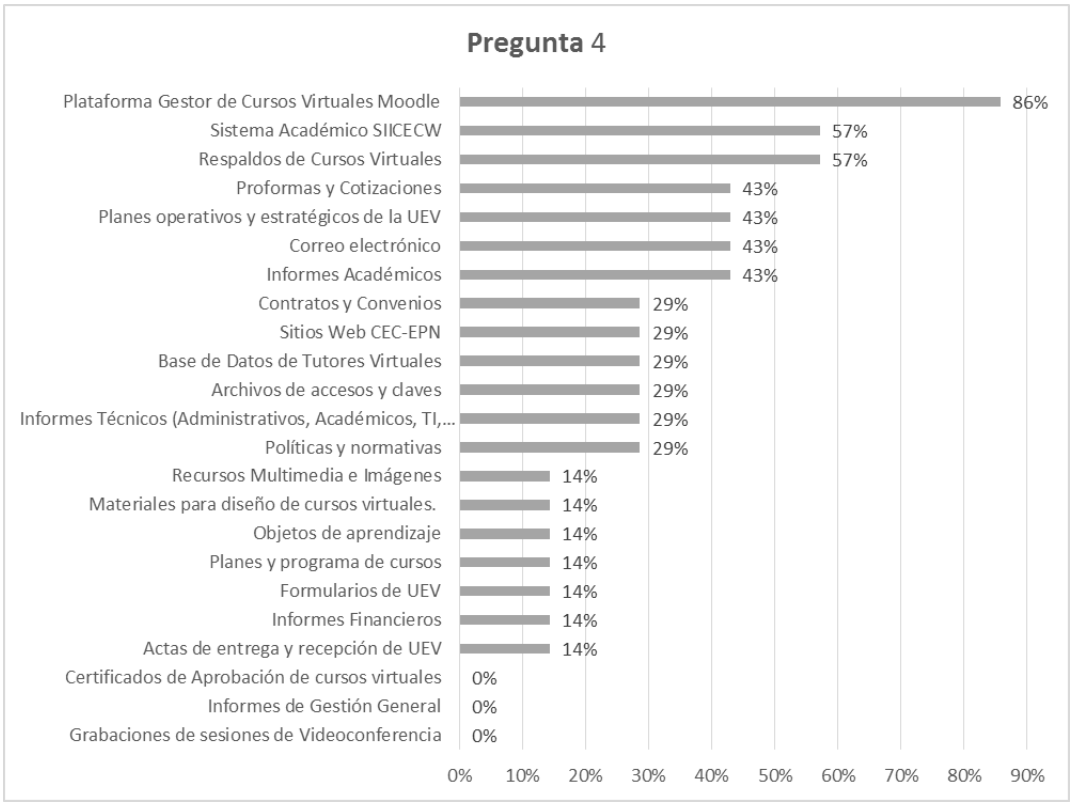

Figura 24. Resultados de la pregunta 4 sobre los activos de información

Anexo N° 2. Perfil de los Activos Críticos

- **Sitios Web CEC-EPN**

Tabla 96. Perfil de Activos Críticos – Sitios Web CEC-EPN

Hoja de trabajo Metodología OCTAVE Allegro		
Perfil de los Activos Críticos		
Activo Crítico	**Justificación**	**Descripción**
Sitios Web CEC-EPN	Son parte de los medios de información donde las personas se inscriben/matriculan a los cursos virtuales y eventos organizados por el Centro de Educación Continua.	El Centro de Educación Continua dispone dos sitios web: El primero es el sitio web del Centro de Educación el cual contiene la información institucional y los cursos de las tres áreas productivas del CEC-EPN (Lingüística, Capacitación Presencial y Unidad de Educación Virtual), de manera especial se gestiona los formularios de inscripción empresarial y personal que son la base para la inscripción y matriculación de las personas. Este activo se denomina **Sitio Web CEC.** La información de los cursos virtuales es gestionada por el Área de TI de la UEV. Apoya al proceso de Inscripción, Matriculación y Promoción de Cursos Virtuales. El segundo es el sitio web de la Unidad de Educación Virtual, el cual contiene la información de la UEV y los cursos virtuales; es el sitio web que se proporciona como primera línea en la promoción de los cursos virtuales. Este activo se denomina **Sitio Web de Virtual.** Apoya al proceso de Inscripción, Matriculación y Promoción de Cursos Virtuales.
Propietarios		
Coordinación de Tecnología CEC-EPN y Área de TI UEV.		
Requisitos de Seguridad		
Confidencialidad	Sólo el autorizado (personal administrativo y técnico del CEC-EPN) puede ver este activo de información, de la siguiente manera:	Con un perfil, usuario y contraseña proporcionado por los responsables de Coordinación de Tecnología CEC-EPN y Área de TI UEV los propietarios pueden realizar actividades dentro del activo de información.

Integridad	Sólo personal autorizado (personal administrativo y técnico del CEC-EPN) puede modificar este activo de información, de la siguiente manera:	Ingresando al activo con su usuario y contraseña, pueden modificar y actualizar la información de los cursos ofertados.
Disponibilidad	Este activo debe estar disponible para este personal pueda hacer su trabajo de la siguiente manera:	La Coordinación de Tecnología CEC-EPN y Área de TI UEV gestionan la publicación de información y se encarga del óptimo funcionamiento del activo de información. El Área de Gestión UEV recibe los datos de las nuevas personas matriculadas en los cursos virtuales.
	Este activo debe estar disponible las 24H, 7D, 52S del año.	Los Sitios Web del CEC-EPN deben estar disponibles las 24x7 porque es el centro de información de la UEV, es el medio por el cuál las personas se inscriben y matriculan. Interrupciones breves de 5 a 10 minutos no causarían problemas significativos pero prolongados y en especial en período de matrículas por más de 8 horas causaría una pérdida de ingresos.

Requisitos de seguridad más importantes			
Confidencialidad [ ]	Integridad [ ]	Disponibilidad [X]	Otros [ ]

En la tabla 95 se seleccionó como Requisitos de seguridad más importantes: la Disponibilidad, porque es el medio por el cual los futuros clientes se informan e ingresan sus datos para realizar el proceso de Inscripción y matriculación.

- **Sistema Integrado de Información del CEC-EPN**

Tabla 97. Perfil de Activos Críticos – Sistema Integrado de Información del CEC-EPN

Hoja de trabajo Metodología OCTAVE Allegro		
Perfil de los Activos Críticos		
Activo Crítico	**Justificación**	**Descripción**
Sistema Integrado de Información del CEC-EPN	Este sistema es importante porque registra la información personal y académica de los estudiantes de los cursos virtuales.	Es un sistema, conocido como **SIICECW.** En este sistema se registran los datos de las empresas y personas, así como también las notas obtenidas por las personas que deciden capacitarse en el CEC-EPN. Apoya al proceso de Inscripción, Matriculación y Contratación de Instructores de Cursos Virtuales.
Propietarios		
Coordinación de Tecnología CEC-EPN.		
Requisitos de Seguridad		
Confidencialidad	Sólo el personal autorizado (personal administrativo y técnico del CEC-EPN) puede ver este activo de información, de la siguiente manera:	Con el perfil, usuario y contraseña generado a través del Directorio Activo.
Integridad	Sólo personal autorizado (personal administrativo y técnico del CEC-EPN) puede modificar este activo de información, de la siguiente manera:	El Área de Gestión UEV modifica los datos del curso, del estudiante y tutor virtual.
Disponibilidad	Este activo debe estar disponible para este personal pueda hacer su trabajo de la siguiente manera:	El Área de Gestión UEV crea nuevos cursos, ingresa información de estudiantes, tutores virtuales y empresas. Gestiona la emisión de certificados. El Área Académica UEV ingresa notas de los estudiantes de cursos virtuales.
	Este activo debe estar disponible las 24H, 7D, 52S del año.	El SIICECW debe estar disponible las 24x7, en especial en las horas de trabajo del personal, porque a través de este medio se registran los datos de los estudiantes y empresas para apoyar al proceso de facturación. Interrupciones breves de 5 a 10 minutos no causarían problemas significativos; pero prolongados y

		en especial en período de matrículas por más de 2 horas causaría una pérdida de ingresos.	
Requisitos de seguridad más importantes			
Confidencialidad [ ]	Integridad [X]	Disponibilidad [ ]	Autentificación [ ]

En la tabla 96 se seleccionó como Requisitos de seguridad más importantes: la Integridad, porque la información almacenada deben ser válida y confiable, apoya a la toma de decisiones en la UEV.

- **Gestores de Cursos Virtuales CEC-EPN y EPN**

Tabla 98. Perfil de Activos Críticos – Gestores de Cursos Virtuales CEC-EPN Y EPN

Hoja de trabajo Metodología OCTAVE Allegro		
Perfil de los Activos Críticos		
Activo Crítico	**Justificación**	**Descripción**
Gestores de Cursos Virtuales CEC-EPN y EPN.	Son las plataformas donde se encuentran todos los registros de actividades, notas y tareas de los estudiantes de los cursos virtuales CEC-EPN y EPN.	La Unidad de Educación Virtual administra en total cinco plataformas virtuales, distribuidas de la siguiente manera: Gestores de cursos virtuales CEC-EPN para el desarrollo de la capacitación virtual: ➢ **Plataforma Moodle CEC-EPN.** ➢ **Plataforma Moodle CEC-EPN V2.** ➢ **Plataforma Moodle CEC-INEPE** En estos activos se encuentran las notas, tareas, recursos y participaciones de los estudiantes y tutores virtuales del CEC-EPN. Apoyan al proceso de Desarrollo y Ejecución de Cursos Virtuales. Gestores de cursos virtuales como apoyo académico para la EPN: ➢ **Plataforma Moodle PREGRADO.** ➢ **Plataforma Moodle POSGRADO** En estos activos se encuentran las notas, tareas, recursos y participaciones de los estudiantes EPN y docentes EPN, estos gestores son utilizados como apoyo académico a las clases presenciales. .Apoyan al proceso de Soporte EPN; cabe indicar que este proceso se denomina de esta manera en la UEV.
Propietarios		
Área de TI, Área Académica, Docentes EPN		
Requisitos de Seguridad		
Confidencialidad	Sólo el personal autorizado (personal académico y técnico de la UEV-CEC-EPN) puede ver este activo de	Con un perfil, usuario y contraseña proporcionado por los responsables de TI, los propietarios pueden realizar

	información, de la siguiente manera:	actividades dentro del activo de información.
Integridad	Sólo personal autorizado (personal académico y técnico de la UEV-CEC-EPN) puede modificar este activo de información, de la siguiente manera:	Ingresando al activo con su usuario y contraseña al curso respectivo.
Disponibilidad	Este activo debe estar disponible para este personal para que puedan hacer su trabajo de la siguiente manera:	**En los Gestores de cursos virtuales CEC-EPN:** Los Tutores Virtuales UEV participan y guían a los estudiantes de el/los cursos virtuales. El Área Académica UEV monitorea la participación de los estudiantes y tutores virtuales de los cursos virtuales. El Área de TI brinda el soporte a los estudiantes y tutores virtuales de los cursos virtuales. Gestiona el óptimo funcionamiento del activo de información. El Área de Diseño Gráfico gestiona el material y contenido gráfico para cada curso virtual. El Área de Gestión obtiene datos de los estudiantes para la gestión de contratos de los tutores virtuales. **Gestores de cursos virtuales EPN**: Los Docentes EPN participan y guían a los estudiantes de el/los cursos virtuales. El Área de TI brinda el soporte a los estudiantes y docentes EPN de los cursos virtuales. Gestiona el óptimo funcionamiento del activo de información.
	Este activo debe estar disponible las 24H, 7D, 52S del año.	Para los estudiantes, tutores y personal UEV debe estar disponible las 24x7, en especial en el período de ejecución de cursos virtuales, porque a través de este medio se realiza el proceso de capacitación. Interrupciones breves de 5 a 10 minutos no causarían problemas significativos; pero prolongados y en especial en período de ejecución de cursos virtuales y clases regulares EPN, por más de 10 minutos causaría molestias y pérdida de confianza en los estudiantes e improductividad en el personal UEV.

Requisitos de seguridad más importantes			
Confidencialidad [ ]	Integridad [ ]	Disponibilidad [X]	Autentificación [ ]

En la tabla 97 se seleccionó como Requisitos de seguridad más importantes: la Disponibilidad, porque los cursos virtuales deben estar accesible a cualquier hora para los estudiantes, tutores virtuales a fin de realizar la capacitación.

Anexo N° 3. Identificación de los Contenedores de los Activos de Información

Activo de Información Sitios Web CEC-EPN: El Centro de Educación Continua dispone de dos sitios web, los mismos que son administrados por la Coordinación de Tecnología CEC-EPN y la Unidad de Educación Virtual CEC-EPN.

Tabla 99. Mapa de Ambiente de Riesgos, Activo Sitios Web CEC-EPN – contenedor técnico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Técnico	
INTERNO	
Descripción del Contenedor	**Propietario(s)**
1. **Sistema de Gestión de Contenidos CEC-EPN**: este sistema es bajo licencia propietaria utilizado para gestionar la información del CEC-EPN.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
2. **Sistema de Gestión de Contenidos UEV Joomla**: este sistema es bajo licencia libre, desarrollada en PHP y MySQL.	Este contenedor es gestionado por el Área de TI UEV.
3. **Estaciones de Trabajo de TI:** se utilizan para procesar la información que se coloca en los Sitios Web del CEC-EPN. El sistema operativo de las Estaciones de Trabajo es Windows 7.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
EXTERNO	
Descripción del Contenedor	**Propietario(s)**
1. **Servidor dedicado del CEC-EPN: c**uenta con el sistema operativo Centos 6. Únicamente se accede por SSH por el personal autorizado de la Coordinación de Tecnología CEC-EPN.	Proveedor del Servicio Servidor Dedicado.
2. **Servidor dedicado de la UEV**: cuenta con el sistema operativo Centos 6. Únicamente se accede por SSH por el personal autorizado de TI de la UEV.	Proveedor del Servicio Servidor Dedicado.
3. El **Correo electrónico institucional**: se encuentra bajo el servicio de Google Apps for Education.	Google
4. El **Internet**: se utiliza para el proceso de inscripción y matriculación, para la realización de la mayoría de las actividades de la UEV. Este servicio es contratado por la EPN.	CEDIA

Tabla 100. Mapa de Ambiente de Riesgos, Activo Sitios Web CEC-EPN – contenedor físico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Físico	
INTERNO	
Descripción del Contenedor	**Propietario(s)**
1. *Sistema de Gestión de Contenidos UEV Joomla:* se respalda la base de datos. Los respaldos son almacenados en: Un Disco Externo de la UEV ubicado en la **oficina de la UEV** en la Estación de Trabajo del Jefe de TI. En el Servidor Local ubicado en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por el Área de TI UEV.
2. *Estaciones de Trabajo de TI***:** la información es procesada en las estaciones de trabajo, las cuales se encuentran ubicadas en la **oficina de la Unidad de Educación Virtual.**	Este contenedor es gestionado por el Área de TI UEV.
3. Red Interna: la información que será subida al sitio web también es gestionada en la red interna del CEC-EPN, el cual es almacenado en un Servidor de Archivos en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
4. Respaldos de la unidad de red: es la información que se respalda de las distintas unidades de red del CEC-EPN, este activo es almacenado en cintas en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
EXTERNO	
Descripción del Contenedor	**Propietario(s)**
1. *Servidor dedicado del CEC-EPN*: este servidor es contratado a una empresa en Ecuador que a su vez **se encuentra en un Data Center EEUU.** Los respaldos son almacenados por el proveedor y los facilitan cuando el CEC-EPN lo requiere en caso de fallo del sitio web. Únicamente se accede por SSH por el personal autorizado de la Coordinación de Tecnología CEC-EPN.	Proveedor del Servicio Servidor Dedicado.
2. *Servidor dedicado de la UEV*: este servidor es contratado a una empresa en Ecuador que a su vez **se encuentra en un Data Center EEUU.** Únicamente se accede por SSH por el personal autorizado de TI de la UEV.	Proveedor del Servicio Servidor Dedicado.

Tabla 101. Mapa de Ambiente de Riesgos, Activo Sitios Web CEC-EPN – contenedor personas

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Personas	
PERSONAL INTERNO	
Nombre o Rol/Responsabilidad	**Área/ Departamento**
1. Lic. Gabriela Martínez, MgS. **Coordinadora de la Unidad de Educación Virtual** Aprueba el material a publicar en los sitios web CEC-EPN correspondiente a la UEV	Coordinación Unidad de Educación Virtual
2. Ing. Christian Hidalgo **Jefe de Gestión UEV** Gestiona el calendario de nuevos cursos virtuales para ser publicados en los sitios web.	Área de Gestión - Coordinación Unidad de Educación Virtual
3. Sr. David Valencia **Asistente de Gestión UEV** Recibe la información de inscripciones y matrículas de los sitios web CEC-EPN.	Área de Gestión - Coordinación Unidad de Educación Virtual
4. Tlga. Andrea Conza **Jefe de Tecnologías de la Información UEV.** Administrador del sitio web UEV CEC-EPN.	Área de TI - Coordinación Unidad de Educación Virtual
5. Sr. Iván Mullo **Asistente de Tecnologías de la Información UEV.** Administrador del sitio web UEV CEC-EPN.	Área de TI - Coordinación Unidad de Educación Virtual
6. Ing. Carla Gómez **Diseñadora Gráfica UEV.** Gestiona los artes a ser publicados en los sitios web CEC-EPN.	Área de Diseño Gráfico - Coordinación Unidad de Educación Virtual
7. Ing. Ximena Uchupanta **Coordinadora de Tecnología CEC-EPN** Administra y gestiona los nuevos requerimientos únicamente del sitio web CEC-EPN.	Coordinación de Tecnología CEC-EPN
PERSONAL EXTERNO	
Contratista, Proveedor	**Organización**
1. Proveedor del Servicio de Servidor Dedicado con el Centro de Educación Continua,	Ecualinux
2. Proveedor del Servicio de Servidor Dedicado con la Unidad de Educación Virtual	Undermedia
3. Proveedor de Nombre de Dominio	NIC.ec
4. Proveedor del Correo electrónico	Google
5. Proveedor de Internet	CEDIA

Activo de Información Sistema Integrado de Información del CEC-EPN: La Coordinación de Tecnología CEC-EPN es la propietaria y quien se encarga de la administración del sistema.

Tabla 102. Mapa de Ambiente de Riesgos, Activo Sistema Integrado de Información del CEC-EPN - contenedor técnico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Técnico	
INTERNO	
Descripción del Contenedor	**Propietario(s)**
1. **Servidor de Aplicaciones CEC-EPN**: **c**uenta con el sistema operativo Centos 6. Utilizado para diferentes sistemas a través de máquinas virtuales.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
2. **Framework para aplicaciones web CodeIgniter:** es bajo licencia código abierto, en PHP.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
3. **Servidor de Base de Datos CEC-EPN**: cuenta con el sistema operativo Windows Server 2008, gestor de base de datos SQL Server 2008.	Este contenedor es gestionado por la Coordinación Tecnológica del CEC-EPN.
4. **Estaciones de Trabajo de la UEV,** se utilizan para procesar la información que se utilizará en el sistema académico. El sistema operativo de las Estaciones de Trabajo es Windows 7.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
EXTERNO	
Descripción del Contenedor	**Propietario(s)**
1. Proveedor de Internet	CEDIA

Tabla 103. Mapa de Ambiente de Riesgos, Activo Sistema Integrado de Información del CEC-EPN - contenedor físico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información - Físico	
INTERNO	
Descripción del Contenedor	**Propietario(s)**
1. *Servidor de Aplicaciones CEC-EPN:* se encuentra en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
2. *Servidor de Base de Datos CEC-EPN:* se respalda a través de una tarea programada que se almacenan en cintas al igual que el servidor en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
3. *Estaciones de Trabajo de la UEV***:** la información es procesada en las estaciones de trabajo, las cuales se encuentran ubicadas en la **oficina de la Unidad de Educación Virtual.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.

4. *Red Interna:* es el medio por el cual se tienen acceso al sistema académico.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
5. *Formularios de inscripción/matriculación:* son los documentos que permiten ingresar la información de los estudiantes y empresas, se utilizan como soporte del sistema académico, estos son almacenados **en un archivador a través de carpetas en la ventanilla de la UEV.**	Este contenedor es gestionado por el Área de Gestión UEV.
6. *Certificados de Aprobación de Cursos Virtuales:* son los documentos que se entregan a los estudiantes que aprobaron un curso virtual, estos son almacenados **en un archivador a través de carpetas en la ventanilla de la UEV.**	Este contenedor es gestionado por el Área de Gestión UEV.
7. *Informes de Tutores Virtuales:* son los documentos que entregan los tutores virtuales al área académica con respecto al desarrollo de los cursos virtuales en especial las notas obtenidas por los estudiantes, estas se registran en el sistema académico. Los informes son almacenados **en un archivador a través de carpetas en la oficina de la UEV.**	Este contenedor es gestionado por el Área Académica UEV.
EXTERNO	
Descripción del Contenedor	**Propietario(s)**
No existe personal externo	N/A

Tabla 104. Mapa de Ambiente de Riesgos, Activo Sistema Integrado de Información del CEC-EPN - contenedor personas

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Personas	
PERSONAL INTERNO	
Nombre o Rol/Responsabilidad	**Área/ Departamento**
1. Ing. Ximena Uchupanta **Coordinadora de Tecnología CEC-EPN** Administra y gestiona los nuevos requerimientos del sistema.	Coordinación de Tecnología CEC-EPN
2. Ing. Bolívar Basantes **Desarrollador de la Coordinación de Tecnología CEC-EPN** Desarrollador del sistema, se encarga de realizar los cambios necesarios en base a las necesidades de los usuarios (tres unidades productivas).	Coordinación de Tecnología CEC-EPN
3. Ing. Christian Hidalgo **Jefe de Gestión UEV** Registra los cursos en el sistema y realiza consultas al sistema para realizar informes.	Área de Gestión - Coordinación Unidad de Educación Virtual
4. Sr. David Valencia **Asistente de Gestión UEV** Registra los datos personales y empresariales de los estudiantes de cursos y gestiona la entrega de certificados de aprobación.	Área de Gestión - Coordinación Unidad de Educación Virtual

5. Ing. Silvana Calderón **Tutora de Tutores UEV** Registra las notas de los estudiantes de los cursos virtuales.	Área Académica - Coordinación Unidad de Educación Virtual
6. Tlga. Andrea Conza **Jefe de Tecnologías de la Información UEV.** Accede a los datos de los estudiantes EPN para la matriculación en las aulas virtuales de Pregrado y Posgrado.	Área de TI - Coordinación Unidad de Educación Virtual
PERSONAL EXTERNO	
Contratista, Proveedor	**Organización**
No existe personal externo	N/A

Activo de Información Gestores de Cursos Virtuales CEC-EPN: El Área de TI de la Unidad de Educación Virtual, administra los gestores de aprendizaje.

Tabla 105. Mapa de Ambiente de Riesgos, Activo Gestores de Cursos Virtuales CEC-EPN - contenedor técnico

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Técnico	
INTERNO	
Descripción del Contenedor	**Propietario(s)**
2. *Plataforma Moodle CEC-EPN*, este sistema es desarrollado bajo licencia de código abierto en PHP y MySQL, utilizado para gestionar los cursos virtuales regulares CEC-EPN. Versión de **Moodle es 1.9.9**	Este contenedor es gestionado por el Área de TI UEV.
3. *Plataforma Moodle CEC-EPN V2*, este sistema es desarrollado bajo licencia de código abierto, en PHP y MySQL, utilizado para gestionar los nuevos cursos virtuales creados por la UEV. Versión de **Moodle es 2.5.4**	Este contenedor es gestionado por el Área de TI UEV.
4. *Plataforma Moodle CEC-INEPE,* este sistema es desarrollado bajo licencia de código abierto, en PHP y MySQL, utilizado para gestionar los cursos virtuales del programa Instituto de Investigación, Educación y Promoción Popular del Ecuador en conjunto con la UEV. Versión de **Moodle es 1.9.9**	Este contenedor es gestionado por el Área de TI UEV.
5. *Plataforma Moodle PREGRADO*, este sistema es desarrollado bajo licencia de código abierto, en PHP y MySQL, utilizado para gestionar los cursos virtuales como apoyo académico de Pregrado de la EPN. Versión de **Moodle es 1.9.9**	Este contenedor es gestionado por el Área de TI UEV.
6. *Plataforma Moodle POSGRADO*, este sistema es desarrollado bajo licencia de código abierto, en PHP y MySQL, utilizado para gestionar los cursos virtuales como apoyo académico de Posgrado de la EPN.	Este contenedor es gestionado por el Área de TI UEV.

	Versión de **Moodle es 1.9.9**	
7.	*Software* ***SSH Secure Shell for Workstations***, utilizado para transferir los archivos desde las estaciones de trabajo de TI hacia el Servidor Dedicado de la UEV.	Este contenedor es gestionado por el Área de TI UEV.
8.	**Estaciones de Trabajo de la UEV,** se utilizan para procesar la información que colocará en los Sitios Web del CEC-EPN. El sistema operativo de las Estaciones de Trabajo es Windows 7.	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
EXTERNO		
Descripción del Contenedor		**Propietario(s)**
1.	**Servidor dedicado de la UEV**, El sistema operativo del servidor es Centos 6. Únicamente se accede por SSH por el personal autorizado de TI de la UEV.	Proveedor del Servicio Servidor Dedicado.
2.	El **Internet** se utiliza en la mayoría de las actividades que realiza la UEV, este servicio es contratado por la EPN.	CEDIA

Tabla 106. Mapa de Ambiente de Riesgos, Activo Gestores de Cursos Virtuales CEC-EPN - contenedor físico

Hoja de trabajo Metodología OCTAVE Allegro		
Mapa de Ambiente de Riesgos de los Activos de Información - Físico		
INTERNO		
Descripción del Contenedor		**Propietario(s)**
1.	*Estaciones de Trabajo de la UEVI***:** la información es procesada en las estaciones de trabajo, las cuales se encuentran ubicadas en la **oficina de la Unidad de Educación Virtual.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
2.	*Red Interna:* la información que será subida a los Gestores de Cursos Virtuales CEC-EPN, son gestionados en la red interna, los cuales son almacenado en un Servidor de Archivos en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.
3.	*Respaldos de Cursos Virtuales*, son almacenados en: Un Disco Externo de la UEV ubicado en la oficina de la UEV en la **Estación de Trabajo del Jefe de TI.** En el Servidor Local ubicado en el **Data Center del CEC-EPN.** Las copias de los cursos de los Gestores de Cursos Virtuales: CEC-EPN, CEC-EPN V2, CEC-INEPE, se almacenan anualmente en **DVD's**	Este contenedor es gestionado por el Área de TI UEV.
4.	*Respaldos de la unidad de red:* es la información que se respalda de las distintas unidades de red del CEC-EPN, este activo es almacenado en cintas en el **Data Center del CEC-EPN.**	Este contenedor es gestionado por la Coordinación de Tecnología CEC-EPN.

EXTERNO	
Descripción del Contenedor	**Propietario(s)**
5. *Servidor dedicado de la UEV*: este servidor es contratado a una empresa en Ecuador que a su vez **se encuentra en un Data Center EEUU.** Únicamente se accede por SSH por el personal autorizado de TI de la UEV.	Proveedor del Servicio Servidor Dedicado.

Tabla 107. Mapa de Ambiente de Riesgos, Activo Gestores de Cursos Virtuales CEC-EPN - contenedor personas

Hoja de trabajo Metodología OCTAVE Allegro	
Mapa de Ambiente de Riesgos de los Activos de Información – Personas	
PERSONAL INTERNO	
Nombre o Rol/Responsabilidad	**Área/ Departamento**
1. Lic. Gabriela Martínez MgS. **Coordinadora de la Unidad de Educación Virtual**	Coordinación Unidad de Educación Virtual
2. Ing. Cristhian Castillo **Diseñador Instruccional**	Área Académica - Coordinación Unidad de Educación Virtual
3. Lic. Leticia Correa **Experta Pedagoga**	Área Académica - Coordinación Unidad de Educación Virtual
4. Ing. Silvana Calderón **Tutora de Tutores**	Área Académica - Coordinación Unidad de Educación Virtual
5. Ing. Christian Hidalgo **Jefe de Gestión**	Área de Gestión - Coordinación Unidad de Educación Virtual
6. Tlga. Andrea Conza **Jefe de Tecnologías de la Información.**	Área de TI - Coordinación Unidad de Educación Virtual
7. Sr. Iván Mullo **Asistente de Tecnologías de la Información**	Área de TI - Coordinación Unidad de Educación Virtual
8. Ing. Carla Gómez **Diseñadora Gráfica**	Área de Diseño Gráfico - Coordinación Unidad de Educación Virtual
PERSONAL EXTERNO	
Contratista, Proveedor	**Organización**
9. Proveedor del Servicio de Servidor Dedicado con la Unidad de Educación Virtual	Undermedia
10. Proveedor de Nombre de Dominio	NIC.ec
11. Proveedor de Servicio de Videoconferencia	Barrazueta & Asociados.
12. Proveedor de Internet	CEDIA

Anexo N° 4 Riesgos de Activos de Información

Escenarios de Amenazas para el activo: Sitios Web CEC-EPN - Consecuencias

- Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Tabla 108. Riesgos de Activos de Información - Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.		
(1) Actor	Personal interno y externo.		
(2) Medios	Ingresando al activo de información utilizando la clave de un usuario con privilegios elevados.		
(3) Motivo	Intereses personales, lucro.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Sólo el personal autorizado (personal administrativo y técnico del CEC-EPN) con un usuario y contraseña proporcionado por los responsables de tecnología, pueden realizar actividades dentro del activo de información.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no pueden acceder a los sitios web en tiempo de matrículas.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%,	Económica	Bajo	2
El personal del Área de Gestión deja de recibir y tramitar las matriculas debido a la interrupción del servicio, provocando el aumento de carga laboral al 1%	Productividad	Bajo	1

Puntuación del Riesgo Relativo		**6**

(9) Mitigación de Riesgo **Acciones a tomar**			
[x] Aceptar	[ ] Aplazar	[ ] Mitigar	[ ] Transferir

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Exposición de los activos de información, acceso no autorizado a la infraestructura física

Tabla 109. Riesgos de Activos de Información - Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Sitios Web CEC-EPN**			
Área de Preocupación	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
(1) Actor	Personal interno y externo.			
(2) Medios	Ingreso a las instalaciones físicas sin identificación y registro en los puntos de acceso (datacenter y oficinas).			
(3) Motivo	Intereses personales, lucro, robo			
(4) Resultado	[ ] Divulgación [ ] Modificación	[ ] Destrucción [X] Interrupción		
(5) Requisitos de seguridad	Sólo el personal autorizado (personal técnico del CEC-EPN), puede acceder al Datacenter de la organización, a través de una tarjeta de acceso.			
(6) Probabilidad	Alto [ ]	Medio [ ]	Bajo [X]	
(7) Consecuencias	**(8) Gravedad**			
	Área de Impacto		**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no pueden acceder a los sitios web en tiempo de matrículas.	Posición y Fidelización de los Clientes		Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%,	Económica		Bajo	2
El personal del Área de Gestión deja de recibir y tramitar las matriculas debido a la interrupción del servicio, provocando el aumento de carga laboral al 1%	Productividad		Bajo	1
Puntuación del Riesgo Relativo				6
(9) Mitigación de Riesgo **Acciones a tomar**				
[X] Aceptar	[ ] Aplazar	[ ] Mitigar	[ ] Transferir	

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Desconocimiento en el manejo de los sistemas o equipos informáticos.

Tabla 110. Riesgos de Activos de Información - Desconocimiento en el manejo de los sistemas o equipos informáticos.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Desconocimiento en el manejo de los sistemas o equipos informáticos.		
(1) Actor	Personal interno		
(2) Medios	Ingresando al activo utilizando el usuario y contraseña revelado por otra persona interna o externa a la organización.		
(3) Motivo	➢ Desconocimiento en el manejo del sistema. ➢ Falta de capacitación. ➢ Superar la ausencia de un compañero de trabajo brindando apoyo en la gestión de actividades ajena a su área de trabajo.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Solo el personal autorizado y capacitado (personal administrativo y técnico del CEC-EPN) que tenga un, usuario y contraseña proporcionado por los responsables de tecnología, podrá realizar actividades dentro del activo de información, sino se cumple esto la integridad de los datos se vería afectada.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque el personal no conoce cómo gestionar los sistemas de gestión de contenidos.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%	Económica	Bajo	2
Disminución de la productividad del personal por interrupción de los servicios necesarios para cumplir con las actividades diarias en el lugar de trabajo es menor al 1% provocando el aumento de carga de trabajo al 1%.	Productividad	Bajo	1

Puntuación del Riesgo Relativo		6
(9) Mitigación de Riesgo **Acciones a tomar**		
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología, responsable del área Ing. Ximena Uchupanta y Coordinadora de UEV Lic. Gabriela Martínez.		
Si se decide mitigar se realizará lo siguiente:		
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Interrupción en el servicio de energía eléctrica.

Tabla 111. Riesgos de Activos de Información - Interrupción en el servicio de energía eléctrica.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Interrupción en el servicio de energía eléctrica.		
(1) Actor	Agentes externos		
(2) Medios	➢ Descarga eléctrica. ➢ Falta de pago al proveedor del servicio. ➢ Falla de los equipos alternos.		
(3) Motivo	Causas naturales Falta de previsión y mantenimiento de los equipos alternos.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles sino se cuenta con equipos UPS y planta generadora de energía eléctrica.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no pueden acceder al correo y sitios web en tiempo de matrículas.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica	Bajo	2
El personal de la UEV disminuirá su trabajo 1% hasta que se restablezca la energía a través de la planta eléctrica de la organización, provocando un aumento de trabajo de 1%	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir

Observación: Se transfiere el riesgo al Administrador del Edificio Aulas y Relación con el Medio Externo EPN, cuyo responsable es Ing. Andrea Plaza.	
Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Problemas de conectividad en la red interna de la organización.

Tabla 112. Riesgos de Activos de Información - Problemas de conectividad en la red interna de la organización.

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Sitios Web CEC-EPN**			
Área de Preocupación	Problemas de conectividad en la red interna de la organización.			
(1) Actor	Personal interno y externo (cracker).			
(2) Medios	➢ Manipulación de los dispositivos de comunicación (switch, router). ➢ Saturación del canal de comunicación por implantación de virus o malware en la red. ➢ Configuración errónea de los dispositivos de comunicación.			
(3) Motivo	Lucro, entretenimiento, desconocimiento.			
(4) Resultado	☐ Divulgación ☐ Modificación		☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los dispositivos de comunicación contienen un control de acceso para proteger contra el uso no autorizado de los recursos de la red.			
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐	
(7) Consecuencias	**(8) Gravedad**			
	Área de Impacto		**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque los clientes no pueden revisar la información actualizada en los sitios web.	Posición y Fidelización de los Clientes		Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica		Bajo	2
El personal de la UEV no puede realizar su trabajo porque no cuenta con el acceso a los materiales colocados en las unidades de red. Se disminuiría la productividad en 2% provocando el aumento de carga laboral en 2%	Productividad		Moderado	2
Puntuación del Riesgo Relativo				7

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta**.**			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Interrupción en el servicio de internet

Tabla 113. Riesgos de Activos de Información - Riesgos de Activos de Información - Problemas de conectividad en la red interna de la organización.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Interrupción en el servicio de internet		
(1) Actor	Personal interno y externo.		
(2) Medios	➢ El proveedor del servicio de internet realiza mantenimiento de equipos de red. ➢ Falla de los equipos alternos. ➢ Falta de pago del servicio. ➢ El gestor del servicio no comunica el mantenimiento de los equipos de comunicación.		
(3) Motivo	➢ Falta de comunicación entre las partes (proveedor y cliente). ➢ Accidental		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles por la falta de conexión a internet y no proveer los servicios que se ofrecen en la web por parte del proveedor.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La confianza y credibilidad de la organización ser vería afectada, la matriculación se reduciría en un 2% al no recibir la notificación de matriculación y pago de los cursos virtuales de forma oportuna.	Posición y Fidelización de los Clientes	Moderado	6
Los ingresos por matriculación de cursos virtuales se reducirían en un 2%.	Económica	Moderado	4
El personal de la UEV disminuirá 1% su trabajo hasta que el servicio se restablezca. El personal deberá laborar horas extras hasta responder los correos electrónicos solicitando	Productividad	Moderado	2

<table>
<tr><td>información y notificación de pagos aumentando su carga de trabajo en 2%.</td><td colspan="2"></td><td></td></tr>
<tr><td>Puntuación del Riesgo Relativo</td><td colspan="2"></td><td>12</td></tr>
<tr><td colspan="4">(9) Mitigación de Riesgo
Acciones a tomar</td></tr>
<tr><td>☐ Aceptar</td><td>☐ Aplazar</td><td>☐ Mitigar</td><td>☒ Transferir</td></tr>
<tr><td colspan="4">Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.</td></tr>
<tr><td colspan="4">Si se decide mitigar se realizará lo siguiente:</td></tr>
<tr><td colspan="2">Contenedor</td><td colspan="2">Aplicación de Controles Técnicos / Administrativos / Físicos
Riesgo Residual</td></tr>
</table>

Cambio de Proveedor de Servicios.

Tabla 114. Riesgos de Activos de Información - Cambio de proveedor de servicios.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Cambio de proveedor de servicios		
(1) Actor	Personal interno y externo		
(2) Medios	La empresa que presta servicios (servidor dedicado, internet, software) termina el contrato ya sea por disolución o cambio de políticas.		
(3) Motivo	➢ Cambio de políticas internas en la organización. ➢ Mejoramiento de calidad. ➢ Finalización de contrato de servicios.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles durante el cambio y estabilización de los servicios con el nuevo proveedor.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque los clientes no pueden acceder a los sitios web, hasta actualizar los datos de DNS del servidor dedicado.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica	Bajo	2
El personal del Área de Gestión deja de recibir y tramitar las matriculas debido a la interrupción del servicio disminuyendo su trabajo en 1%.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

(9) Mitigación de Riesgo **Acciones a tomar**			
☒ Aceptar	☐ Aplazar	☐ Mitigar	☐ Transferir

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Falla en los componentes de hardware de los equipos informáticos.

Tabla 115. Riesgos de Activos de Información - Falla en los componentes de hardware de los equipos informáticos.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Falla en los componentes de hardware de los equipos informáticos.		
(1) Actor	Personal interno y externo.		
(2) Medios	➢ Conexión errónea de equipos informáticos. ➢ Uso inadecuado de los equipos informáticos. ➢ Falta de protección en las variaciones de voltaje. ➢ Falta de monitoreo de los componentes del equipo informático.		
(3) Motivo	Accidental, falla de fabricación.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles durante la reposición y configuración de los nuevos componentes de hardware de los equipos informáticos por parte del proveedor y tecnología de la organización.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 2%, porque no pueden acceder a los sitios web en tiempo de matrículas, por fallas en disco duro y tarjeta de red en los servidores dedicados.	Posición y Fidelización de los Clientes	Moderado	6
Los ingresos por matriculación de cursos virtuales se reducirían en un 2%, por no acceder a los sitios web.	Económica	Moderado	4
El personal de la UEV deja de laborar disminuyendo su trabajo en 1%.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			11
(9) Mitigación de Riesgo **Acciones a tomar**			

☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología, responsable Ing. Ximena Uchupanta y la Coordinadora de UEV Lic. Gabriela Martínez			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Desactualización de los sistemas

Tabla 116. Riesgos de Activos de Información - Desactualización de sistemas

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Sitios Web CEC-EPN**			
Área de Preocupación	Desactualización de sistemas			
(1) Actor	Personal interno y externo.			
(2) Medios	➢ El personal interno y externo no actualizan o colocan parches de seguridad a los sistemas operativos. ➢ El personal interno no actualizan los LMS y CMS Joomla.			
(3) Motivo	Falta de conocimiento, falta de presupuesto.			
(4) Resultado	[ ] Divulgación [ ] Modificación		[ ] Destrucción [X] Interrupción	
(5) Requisitos de seguridad	Al no realizar las actualizaciones a los diferentes sistemas y plataformas, se vulnera la integridad de los activos provocando la paralización temporal de los servicios de la UEV.			
(6) Probabilidad	Alto [X]	Medio [ ]	Bajo [ ]	

(7)Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los sitios web es mínimamente afectada debido a la funcionalidad de la interfaz de los sitios web.	Posición y Fidelización de los Clientes	Bajo	3
Existe un aumento de los costos de operación en 1% para actualizar los nuevos sitios web de la organización.	Económica	Bajo	2
El Área de Gestión debe invertir más horas de trabajo para confirmar la matriculación debido a que no existe el sistema de matriculación actualizado en línea.	Productividad	Moderado	2
Puntuación del Riesgo Relativo			7

(9) Mitigación de Riesgo **Acciones a tomar**			
[ ] Aceptar	[ ] Aplazar	[X] Mitigar	[ ] Transferir
Si se decide mitigar se realizará lo siguiente:			

Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**
➢ Servidor dedicado del CEC-EPN. ➢ Servidor dedicado de la UEV. ➢ Sistema de Gestión de Contenidos CEC-EPN. ➢ Sistema de Gestión de Contenidos UEV Joomla. ➢ Estaciones de Trabajo de TI	➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios en los servidores. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.

Alta Rotación de Personal

Tabla 117 Riesgos de Activos de Información - Alta Rotación de personal.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Alta Rotación de personal		
(1) Actor	Personal interno.		
(2) Medios	Al renunciar al cargo en la organización y llevar los conocimientos adquiridos del puesto de trabajo.		
(3) Motivo	➢ Inestabilidad laboral. ➢ Ambiente de trabajo. ➢ Intereses personales. ➢ Crecimiento profesional.		
(4) Resultado	[ ] Divulgación [ ] Modificación	[ ] Destrucción [x] Interrupción	
(5) Requisitos de seguridad	Los activos no estarían disponibles mientras se contrata a un nuevo empleado, la curva de aprendizaje sería mayor o menor dependiendo del nuevo personal contratado.		
(6) Probabilidad	Alto [X]	Medio [ ]	Bajo [ ]

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
Los clientes no confían en la organización por la imagen que presenta ante el cambio constante del personal.	Posición y Fidelización de los Clientes	Bajo	3
La matriculación en los cursos virtuales se reduciría en un 1%, porque no se atiende las inquietudes de posibles clientes en el tiempo esperado en el período de matrículas	Económica	Bajo	2
El personal deberá realizar actividades adicionales para superar un puesto de trabajo, el aumento de la carga laboral del personal es del 2 %	Productividad	Moderado	2
Puntuación del Riesgo Relativo			7

(9) Mitigación de Riesgo **Acciones a tomar**			
[ ] Aceptar	[ ] Aplazar	[x] Mitigar	[ ] Transferir
Si se decide mitigar se realizará lo siguiente:			

Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**
➢ Coordinadora de la Unidad de Educación Virtual ➢ Jefe de Gestión UEV ➢ Asistente de Gestión UEV ➢ Jefe de Tecnologías de la Información UEV ➢ Asistente de Tecnologías de la Información UEV ➢ Diseñadora Gráfica UEV ➢ Coordinadora de Tecnología CEC-EPN	➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral. ➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV

Desastres naturales

Tabla 118 Riesgos de Activos de Información - Desastres naturales.

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Sitios Web CEC-EPN**			
Área de Preocupación	Desastres naturales.			
(1) Actor	Fenómenos naturales.			
(2) Medios	Tormentas eléctricas, terremoto, incendios, maremotos.			
(3) Motivo	Calentamiento global, factores climatológicos.			
(4) Resultado	☐ Divulgación ☐ Modificación	☒ Destrucción ☐ Interrupción		
(5) Requisitos de seguridad	Los activos como infraestructura y recurso humano no estarán disponibles al producirse estos desastres mencionados.			
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒	

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 5%, porque no pueden acceder a los sitios web en tiempo de matrículas.	Posición y Fidelización de los Clientes	Alto	9
Los ingresos por matriculación de cursos virtuales se reducirían en un 5%.	Económica	Alto	6
El personal de la UEV disminuye su productividad debido a la pérdida del servicio.	Productividad	Alto	3
Puntuación del Riesgo Relativo			18

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Si se decide mitigar se realizará lo siguiente:			
Observación: Se transfiere a los proveedores de los distintos servicios Servidor Dedicado, responsables: Undermedia, Ecualinux y aseguradora de equipos.			
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos Riesgo Residual**		

Fallo o defecto de Software.

Tabla 119. Riesgos de Activos de Información - Fallo o defecto de Software.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sitios Web CEC-EPN**		
Área de Preocupación	Fallo o defecto de Software.		
(1) Actor	Personal interno y externo		
(2) Medios	➢ Instalación de software no licenciado. ➢ Instalación de software no compatible. ➢ Eliminación de archivos propios del sistema operativo. ➢ Error de código de programación al ejecutar nuevas actualizaciones en los sistemas informáticos.		
(3) Motivo	Desconocimiento, error, pruebas no controladas.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Afecta la disponibilidad de los activos de información, al interrumpir los servicios mientras se detecta el fallo en el software instalado.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en 2%, porque no pueden acceder a los sitios web en tiempo de matrículas, por fallas en software, sistema operativo en los servidores dedicados.	Posición y Fidelización de los Clientes	Moderado	6
Los ingresos por matriculación de cursos virtuales se reducirían en un 2%, por no acceder a los sitios web.	Económica	Moderado	4
El personal de la UEV deja de laborar disminuyendo la productividad en 1%.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			11

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☒ Mitigar	☐ Transferir

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**
➢ Servidor dedicado del CEC-EPN. ➢ Servidor dedicado de la UEV. ➢ Sistema de Gestión de Contenidos CEC-EPN. ➢ Sistema de Gestión de Contenidos UEV Joomla. ➢ Estaciones de Trabajo de TI	➢ Planificar configuración de Servidores. ➢ Instalar herramienta antivirus de acuerdo a las capacidades de los servidores y estaciones de trabajo de TI. ➢ Programar ejecución de herramienta antivirus para analizar de forma periódica a las aplicaciones y sistemas operativos huésped. ➢ Escoger un Sistema Operativo adecuado a los componentes instalados de los servidores. ➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios. ➢ Realizar pruebas de carga al sistema operativo. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.

Escenarios de Amenazas para el activo: Sistema Integrado de Información del CEC-EPN - Consecuencias

Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Tabla 120. Riesgos de Activos de Información - Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Hoja de trabajo Metodología OCTAVE Allegro					
Riesgos de Activos de Información					
Activos de Información	**Sistema Integrado de Información del CEC-EPN**				
Área de Preocupación	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.				
(1) Actor	Personal interno y externo.				
(2) Medios	Ingresando al activo de información utilizando la clave de un usuario con privilegios elevados.				
(3) Motivo	Intereses personales, lucro.				
(4) Resultado	[ ] Divulgación [x] Modificación		[ ] Destrucción [ ] Interrupción		
(5) Requisitos de seguridad	Sólo el personal autorizado con un usuario y contraseña proporcionado por los responsables de tecnología, pueden realizar actividades dentro del activo de información.				
(6) Probabilidad	Alto [ ]		Medio [ ]		Bajo [x]
(7) Consecuencias	**(8) Gravedad**				
	Área de Impacto		**Valor de Impacto**		**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no existe confianza en la información proporcionada a los estudiantes sobre las calificaciones obtenidas (registro académico). El posicionamiento es: Mínimamente afectado; poco o ningún esfuerzo o gasto es requerido para recuperarse.	Posición y Fidelización de los Clientes		Bajo		3
	Económica		Bajo		2
El personal de TI del CEC-EPN, tendrían que invertir varias horas de trabajo para regresar a la Base de Datos a su estado	Productividad		Moderado		2

anterior.			
Puntuación del Riesgo Relativo			7
(9)Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Si se decide mitigar se realizará lo siguiente:			
Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Tabla 121. Riesgos de Activos de Información - Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Exposición de los activos de información, acceso no autorizado a la infraestructura física.		
(1) Actor	Personal interno y externo.		
(2) Medios	Ingreso a las instalaciones físicas sin identificación y registro en los puntos de acceso (datacenter y oficinas).		
(3) Motivo	Intereses personales, lucro, robo		
(4) Resultado	[ ] Divulgación [ ] Modificación	[ ] Destrucción [X] Interrupción	
(5) Requisitos de seguridad	Sólo el personal autorizado (personal técnico del CEC-EPN), puede acceder al Datacenter de la organización, a través de una tarjeta de acceso.		
(6) Probabilidad	Alto [ ]	Medio [X]	Bajo [ ]

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en 1%, porque no se pudo registrar a las personas en el sistema.	Posición y Fidelización de los Clientes	Bajo	3
Pérdida de ingresos del 1% por no permitir el ingreso de datos para gestionar el proceso de cobro a los clientes en el sistema Olympo.	Económica	Bajo	2
El Área de Gestión, tendrían que invertir varias horas de trabajo para registrar los datos que no pudieron ser ingresados a tiempo en el sistema. Disminuiría la productividad en 1%.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

(9) Mitigación de Riesgo **Acciones a tomar**			
[ ] Aceptar	[ ] Aplazar	[ ] Mitigar	[X] Transferir

Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.	
Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Desconocimiento en el manejo de los sistemas o equipos informáticos.

Tabla 122. Riesgos de Activos de Información - Desconocimiento en el manejo de los sistemas o equipos informáticos.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Desconocimiento en el manejo de los sistemas o equipos informáticos.		
(1) Actor	Personal interno		
(2) Medios	Ingresando al activo utilizando el usuario y contraseña revelado por otra persona interna o externa a la organización.		
(3) Motivo	➢ Desconocimiento en el manejo del sistema. ➢ Falta de capacitación. ➢ Superar la ausencia de un compañero de trabajo brindando apoyo en la gestión de actividades ajena a su área de trabajo.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Solo el personal autorizado y capacitado (personal administrativo y técnico del CEC-EPN) que tenga un, usuario y contraseña proporcionado por los responsables de tecnología, podrá realizar actividades dentro del activo de información, sino se cumple esto la integridad de los datos se vería afectada.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en 1%, porque el personal no conoce cómo gestionar el sistema académico y el proceso en sí.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en 1% y existirían errores en los cobros por no conocer la política de cobros y descuentos.	Económica	Bajo	2
Disminución de la productividad del personal por interrupción de los servicios necesarios para cumplir con las actividades diarias en el lugar de trabajo es mayor al 5% provocando un aumento de carga laboral de 5%	Productividad	Alto	3

<table>
<tr><td colspan="2">Puntuación del Riesgo Relativo</td><td></td><td>8</td></tr>
<tr><td colspan="4">(9) Mitigación de Riesgo
Acciones a tomar</td></tr>
<tr><td>☐ Aceptar</td><td>☐ Aplazar</td><td>[x] Mitigar</td><td>☐ Transferir</td></tr>
<tr><td colspan="4">Si se decide mitigar se realizará lo siguiente:</td></tr>
<tr><td colspan="2">Contenedor</td><td colspan="2">Aplicación de Controles Técnicos / Administrativos / Físicos
Riesgo Residual</td></tr>
<tr><td colspan="2">➢ Coordinadora de la Unidad de Educación Virtual
➢ Jefe de Gestión UEV
➢ Asistente de Gestión UEV
➢ Jefe de Tecnologías de la Información UEV
➢ Asistente de Tecnologías de la Información UEV
➢ Diseñadora Gráfica UEV
➢ Coordinadora de Tecnología CEC-EPN</td><td colspan="2">➢ Elaborar diagramas y esquemas donde se pueda apreciar los procedimientos administrativos del área.
➢ Elaborar manual de manejo de los sistemas que utilice el área.
➢ Crear una base de conocimientos de los incidentes más conocidos para su posterior resolución.
➢ Realizar pruebas pilotos y entrevistas con el personal para obtener retroalimentación y realizar mejoras.
➢ Mantener actualizado los manuales y realiza capacitaciones a los nuevos elementos.</td></tr>
</table>

Interrupción en el servicio de energía eléctrica.

Tabla 123. Riesgos de Activos de Información - Interrupción en el servicio de energía eléctrica.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Interrupción en el servicio de energía eléctrica.		
(1) Actor	Agentes externos		
(2) Medios	➢ Descarga eléctrica. ➢ Falta de pago al proveedor del servicio. ➢ Falla de los equipos alternos.		
(3) Motivo	Causas naturales Falta de previsión y mantenimiento de los equipos alternos.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles sino se cuenta con equipos UPS y planta generadora de energía eléctrica.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no se puede registrar los datos de nuevos clientes en tiempo de matrículas.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica	Bajo	2
El personal de la UEV disminuirá su trabajo hasta que se restablezca la energía a través de la planta eléctrica de la organización.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo al Administrador del Edificio Aulas y Relación con el Medio Externo EPN, cuyo responsable es Ing. Andrea Plaza.			

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Problemas de conectividad en la red interna de la organización.

Tabla 124. Riesgos de Activos de Información - Problemas de conectividad en la red interna de la organización.

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Sistema Integrado de Información del CEC-EPN**			
Área de Preocupación	Problemas de conectividad en la red interna de la organización.			
(1) Actor	Personal interno y externo (cracker).			
(2) Medios	➢ Manipulación de los dispositivos de comunicación (switch, router). ➢ Saturación del canal de comunicación por implantación de virus o malware en la red. ➢ Configuración errónea de los dispositivos de comunicación.			
(3) Motivo	Lucro, entretenimiento, desconocimiento.			
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción		
(5) Requisitos de seguridad	Los dispositivos de comunicación contienen un control de acceso para proteger contra el uso no autorizado de los recursos de la red.			
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐	
(7) Consecuencias	**(8) Gravedad**			
	Área de Impacto		**Valor de Impacto**	**Puntaje**
La matriculación y confianza en los cursos virtuales se reduciría en 1%, porque no se puede ingresar los datos en el sistema y/o entregar certificados de aprobación.	Posición y Fidelización de los Clientes		Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1% y existirían errores en los cobros por no conocer la política de cobros y descuentos.	Económica		Bajo	2
El personal de la UEV no puede realizar su trabajo porque no cuenta con el acceso al sistema y así verificar la información de los clientes. Se disminuiría la productividad en 2% provocando el aumento de carga laboral en	Productividad		Moderado	2

2%			
Puntuación del Riesgo Relativo			7
(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta**.**			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Interrupción en el servicio de internet

Tabla 125. Riesgos de Activos de Información - Interrupción en el servicio de internet.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Interrupción en el servicio de internet		
(1) Actor	Personal interno y externo.		
(2) Medios	➢ El proveedor del servicio de internet realiza mantenimiento de equipos de red. ➢ Falla de los equipos alternos. ➢ Falta de pago del servicio. ➢ El gestor del servicio no comunica el mantenimiento de los equipos de comunicación.		
(3) Motivo	➢ Falta de comunicación entre las partes (proveedor y cliente). ➢ Accidental		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles por la falta de conexión a internet y no proveer los servicios que se ofrecen en la web.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La confianza y credibilidad de la organización ser vería afectada, la matriculación se reduciría en un 2% al no recibir la notificación de matriculación y pago de los cursos virtuales de forma oportuna.	Posición y Fidelización de los Clientes	Moderado	6
Los ingresos por matriculación de cursos virtuales se reducirían en un 2%.	Económica	Moderado	4
El personal de la UEV disminuirá 1% su trabajo hasta que el servicio se restablezca. El personal deberá laborar horas extras hasta responder los correos electrónicos solicitando información y notificación de	Productividad	Moderado	2

<table>
<tr><td colspan="2">pagos aumentando su carga de trabajo en 2%.</td><td></td><td></td></tr>
<tr><td colspan="2">Puntuación del Riesgo Relativo</td><td colspan="2">12</td></tr>
<tr><td colspan="4">(9) Mitigación de Riesgo
Acciones a tomar</td></tr>
<tr><td>☐ Aceptar</td><td>☐ Aplazar</td><td>☐ Mitigar</td><td>☒ Transferir</td></tr>
<tr><td colspan="4">Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.</td></tr>
<tr><td colspan="4">Si se decide mitigar se realizará lo siguiente:</td></tr>
<tr><td colspan="2">Contenedor</td><td colspan="2">Aplicación de Controles Técnicos / Administrativos / Físicos
Riesgo Residual</td></tr>
</table>

Cambio de Proveedor de Servicios.

Tabla 126. Riesgos de Activos de Información - Cambio de proveedor de servicios.

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Sistema Integrado de Información del CEC-EPN**			
Área de Preocupación	Cambio de proveedor de servicios			
(1) Actor	Personal interno y externo			
(2) Medios	La empresa que presta servicios (servidor dedicado, internet, software) termina el contrato ya sea por disolución o cambio de políticas.			
(3) Motivo	➢ Cambio de políticas internas en la organización. ➢ Mejoramiento de calidad. ➢ Finalización de contrato de servicios.			
(4) Resultado	☐ Divulgación ☐ Modificación		☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles durante el cambio y estabilización de los servicios con el nuevo proveedor.			
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒	
(7) Consecuencias	**(8) Gravedad**			
	Área de Impacto		**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque los clientes no pueden acceder a los sitios web, hasta actualizar los datos de DNS del servidor dedicado.	Posición y Fidelización de los Clientes		Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica		Bajo	2
El personal del Área de Gestión deja de recibir y tramitar las matriculas debido a la interrupción del servicio disminuyendo su trabajo en 1%.	Productividad		Bajo	1
Puntuación del Riesgo Relativo				6
(9) Mitigación de Riesgo **Acciones a tomar**				
☒ Aceptar	☐ Aplazar	☐ Mitigar	☐ Transferir	

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Falla en los componentes de hardware de los equipos informáticos.

Tabla 127. Riesgos de Activos de Información - Falla en los componentes de hardware de los equipos informáticos.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Falla en los componentes de hardware de los equipos informáticos.		
(1) Actor	Personal interno y externo.		
(2) Medios	➢ Conexión errónea de equipos informáticos. ➢ Uso inadecuado de los equipos informáticos. ➢ Falta de protección en las variaciones de voltaje. ➢ Falta de monitoreo de los componentes del equipo informático.		
(3) Motivo	Accidental, falla de fabricación.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles durante la reposición y configuración de los nuevos componentes de hardware de los equipos informáticos por parte del proveedor y tecnología de la organización.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no pueden acceder a al sistema en tiempo de matrículas, por fallas en disco duro y tarjeta de red en el servidor dedicado.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%, por no acceder al sistema.	Económica	Bajo	2
El personal de la UEV deja de laborar parcialmente si falla los componentes de hardware en el servidor dedicado que contiene el sistema SIICECW.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6
(9) Mitigación de Riesgo **Acciones a tomar**			

☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología, responsable Ing. Ximena Uchupanta y la Coordinadora de UEV Lic. Gabriela Martínez			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Desactualización de los sistemas.

Tabla 128. Riesgos de Activos de Información - Desactualización de sistemas.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Desactualización de sistemas		
(1) Actor	Personal interno y externo.		
(2) Medios	➢ El personal interno y externo no actualizan o colocan parches de seguridad a los sistemas operativos. ➢ El personal interno no actualizan los LMS y CMS Joomla.		
(3) Motivo	Falta de conocimiento, falta de presupuesto.		
(4) Resultado	[ ] Divulgación [ ] Modificación	[ ] Destrucción [X] Interrupción	
(5) Requisitos de seguridad	Al no realizar las actualizaciones a los diferentes sistemas y plataformas, se vulnera la integridad de los activos provocando la paralización temporal de los servicios de la UEV.		
(6) Probabilidad	Alto [ ]	Medio [ ]	Bajo [X]

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
El posicionamiento es afectado y algún esfuerzo y gasto es requerido para recuperarse.	Posición y Fidelización de los Clientes (3)	Moderado	6
Existe un aumento en los gastos de operación por no informar los cambios de parámetros en el sistema que afectan en el proceso de matriculación (valores de cobro y descuentos).	Económica (2)	Moderado	4
El Área de Gestión debe invertir más horas de trabajo para encontrar los inconvenientes y gestionar los cobros erróneos en el sistema y comunicarse con los clientes.	Productividad (1)	Moderado	2
Puntuación del Riesgo Relativo			12

Mitigación de Riesgo **Acciones a tomar**			
[ ] Aceptar	[ ] Aplazar	[ ] Mitigar	[X] Transferir

Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.	
Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Alta Rotación de Personal

Tabla 129. Riesgos de Activos de Información - Alta Rotación de personal.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Alta Rotación de personal		
(1) Actor	Personal interno.		
(2) Medios	Al renunciar al cargo en la organización y llevar los conocimientos adquiridos del puesto de trabajo.		
(3) Motivo	➢ Inestabilidad laboral. ➢ Ambiente de trabajo. ➢ Intereses personales. ➢ Crecimiento profesional.		
(4) Resultado	[ ] Divulgación [ ] Modificación	[ ] Destrucción [x] Interrupción	
(5) Requisitos de seguridad	Los activos no estarían disponibles mientras se contrata a un nuevo empleado, la curva de aprendizaje sería mayor o menor dependiendo del nuevo personal contratado.		
(6) Probabilidad	Alto [x]	Medio [ ]	Bajo [ ]

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
Los clientes no confían en la organización por la imagen que presenta ante el cambio constante del personal.	Posición y Fidelización de los Clientes	Bajo	3
La matriculación en los cursos virtuales se reduciría en un 1%, porque no se atiende las inquietudes de posibles clientes en el tiempo esperado en el período de matrículas.	Económica	Bajo	2
El personal deberá realizar actividades adicionales para superar un puesto de trabajo, el aumento de la carga laboral del personal es del 2%.	Productividad	Moderado	2
Puntuación del Riesgo Relativo			7

(9) Mitigación de Riesgo **Acciones a tomar**			
[ ] Aceptar	[ ] Aplazar	[x] Mitigar	[ ] Transferir
Si se decide mitigar se realizará lo siguiente:			

Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**
➢ Coordinadora de Tecnología CEC-EPN ➢ Desarrollador de la Coordinación de Tecnología CEC-EPN ➢ Jefe de Gestión UEV ➢ Asistente de Gestión UEV ➢ Tutora de Tutores UEV ➢ Jefe de Tecnologías de la Información UEV	➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral. ➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV.

Desastres naturales

Tabla 130. Riesgos de Activos de Información - Desastres naturales.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Desastres naturales.		
(1) Actor	Fenómenos naturales.		
(2) Medios	Tormentas eléctricas, terremoto, incendios, maremotos.		
(3) Motivo	Calentamiento global, factores climatológicos.		
(4) Resultado	☐ Divulgación ☐ Modificación	☒ Destrucción ☐ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles al producirse estos desastres mencionados.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 5%, porque no pueden acceder al sistema en tiempo de matrículas.	Posición y Fidelización de los Clientes	Alto	9
Los ingresos por matriculación de cursos virtuales se reducirían en un 5%.	Económica	Alto	6
El personal de la UEV disminuye su productividad debido a la pérdida del servicio.	Productividad	Alto	3
Puntuación del Riesgo Relativo			18

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere a los proveedores de los distintos servicios Servidor Dedicado, responsables: Undermedia, Ecualinux y aseguradora de equipos.			
Si se decide mitigar se realizará lo siguiente:			
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**		

Fallo o defecto de Software

Tabla 131. Riesgos de Activos de Información - Fallo o defecto de Software.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Sistema Integrado de Información del CEC-EPN**		
Área de Preocupación	Fallo o defecto de Software.		
(1) Actor	Personal interno y externo		
(2) Medios	➢ Instalación de software no licenciado. ➢ Instalación de software no compatible. ➢ Eliminación de archivos propios del sistema operativo. ➢ Error de código de programación al ejecutar nuevas actualizaciones en los sistemas informáticos.		
(3) Motivo	Desconocimiento, error, pruebas no controladas.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Afecta la disponibilidad de los activos de información, al interrumpir los servicios mientras se detecta el fallo en el software instalado.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no pueden acceder al sistema en tiempo de matrículas, por fallas en software, sistema operativo en el servidor dedicado.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%, por no acceder a dicho sistema.	Económica	Bajo	2
El personal de la UEV deja de laborar parcialmente si falla o existe incompatibilidad en el servidor dedicado que contiene el sistema SIICECW.	Productividad	Moderado	2
Puntuación del Riesgo Relativo			7

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir

Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.	
Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Escenarios de Amenazas para el activo: Gestores de Cursos Virtuales CEC-EPN y EPN - Consecuencias

Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Tabla 132. Riesgos de Activos de Información - Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Hoja de trabajo Metodología OCTAVE Allegro					
Riesgos de Activos de Información					
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**				
Área de Preocupación	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.				
(1) Actor	Personal interno y externo.				
(2) Medios	Ingresando al activo de información utilizando la clave de un usuario con privilegios elevados.				
(3) Motivo	Intereses personales, lucro.				
(4) Resultado	☐ Divulgación ☐ Modificación		☐ Destrucción ☒ Interrupción		
(5) Requisitos de seguridad	Sólo el personal autorizado (personal administrativo y técnico del CEC-EPN) con un usuario y contraseña proporcionado por los responsables de tecnología, pueden realizar actividades dentro del activo de información.				
(6) Probabilidad	Alto ☐		Medio ☐		Bajo ☒
(7) Consecuencias	**(8) Gravedad**				
	Área de Impacto		**Valor de Impacto**		**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 2%, porque no existe confianza en el sistema de aprendizaje. El posicionamiento es: Afectado y algún esfuerzo y gasto es requerido para recuperarse.	Posición y Fidelización de los Clientes		Moderado		6
Los ingresos por matriculación de cursos virtuales se reducirían en un 2%.	Económica		Moderado		4
El personal de TI de la UEV, tendrían que invertir varias horas de trabajo para regresar la Base de Datos a su estado anterior.	Productividad		Moderado		2
Puntuación del Riesgo Relativo					12

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinadora de la UEV cuyo responsable del área es Lic.Gabriela Martinez y al Proveedor Undermedia.			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Tabla 133. Riesgos de Activos de Información - Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Exposición de los activos de información, acceso no autorizado a la infraestructura física.		
(1) Actor	Personal interno y externo.		
(2) Medios	Ingreso a las instalaciones físicas sin identificación y registro en los puntos de acceso (datacenter y oficinas).		
(3) Motivo	Intereses personales, lucro, robo		
(4) Resultado	[ ] Divulgación [ ] Modificación	[ ] Destrucción [X] Interrupción	
(5) Requisitos de seguridad	Sólo el personal autorizado (personal técnico del CEC-EPN), puede acceder al Datacenter de la organización, a través de una tarjeta de acceso.		
(6) Probabilidad	Alto [ ]	Medio [X]	Bajo [ ]

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque no pueden acceder a los cursos virtuales en tiempo de matrículas.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica	Bajo	2
El personal de las áreas de TI y Académica de la UEV no ingresan a los gestores de contenido debido a la interrupción del servicio	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

Mitigación de Riesgo **Acciones a tomar**			
[ ] Aceptar	[ ] Aplazar	[ ] Mitigar	[X] Transferir
Observación: Se transfiere el riesgo al Proveedor Undermedia.			

Si se decide mitigar se realizará lo siguiente:	
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Desconocimiento en el manejo de los sistemas o equipos informáticos.

Tabla 134. Riesgos de Activos de Información - Desconocimiento en el manejo de los sistemas o equipos informáticos.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Desconocimiento en el manejo de los sistemas o equipos informáticos.		
(1) Actor	Personal interno		
(2) Medios	Ingresando al activo utilizando el usuario y contraseña revelado por otra persona interna o externa a la organización.		
(3) Motivo	➢ Desconocimiento en el manejo del sistema. ➢ Falta de capacitación. ➢ Superar la ausencia de un compañero de trabajo brindando apoyo en la gestión de actividades ajena a su área de trabajo.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Solo el personal autorizado y capacitado (personal administrativo y técnico del CEC-EPN) que tenga un, usuario y contraseña proporcionado por los responsables de tecnología, podrá realizar actividades dentro del activo de información, sino se cumple esto la integridad de los datos se vería afectada.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en 1%, porque un curso no cumplió con las expectativas, no hay buenos comentarios para una recompra de un curso virtual.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en 1% por malas referencias de un curso específico.	Económica	Bajo	2
Las Áreas Académicas y de TI disminuyen sus horas de trabajo para solventar los inconvenientes presentados, deja de realizar sus actividades diarias en un 2% provocando una carga de trabajo de 2%	Productividad	Moderado	2

Puntuación del Riesgo Relativo			7
Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☒ Mitigar	☐ Transferir
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	
➢ Coordinadora de la Unidad de Educación Virtual ➢ Diseñador Instruccional ➢ Experta Pedagoga ➢ Tutora de Tutores ➢ Jefe de Gestión ➢ Jefe de Tecnologías de la Información ➢ Asistente de Tecnologías de la Información ➢ Diseñadora Gráfica		➢ Elaborar diagramas y esquemas donde se pueda apreciar los procedimientos administrativos del área. ➢ Elaborar manual de manejo de los sistemas que utilice el área. ➢ Crear una base de conocimientos de los incidentes más conocidos para su posterior resolución. ➢ Realizar pruebas pilotos y entrevistas con el personal para obtener retroalimentación y realizar mejoras. ➢ Capacitar al personal.	

Interrupción en el servicio de energía eléctrica.

Tabla 135. Riesgos de Activos de Información – Interrupción en el servicio de energía eléctrica.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Interrupción en el servicio de energía eléctrica.		
(1) Actor	Agentes externos		
(2) Medios	➢ Descarga eléctrica. ➢ Falta de pago al proveedor del servicio. ➢ Falla de los equipos alternos.		
(3) Motivo	Causas naturales Falta de previsión y mantenimiento de los equipos alternos.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles sino se cuenta con equipos UPS y planta generadora de energía eléctrica.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 5%, porque no existe confianza en el sistema de aprendizaje.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 5%.	Económica	Bajo	2
El personal de la UEV disminuirá su trabajo hasta que se restablezca la energía a través de la planta eléctrica de la organización.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

(9) Mitigación de Riesgo **Acciones a tomar**			
☒ Aceptar	☐ Aplazar	☐ Mitigar	☐ Transferir
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos /**	

	Administrativos / Físicos **Riesgo Residual**

Problemas de conectividad en la red interna de la organización.

Tabla 136. Riesgos de Activos de Información - Problemas de conectividad en la red interna de la organización.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Problemas de conectividad en la red interna de la organización.		
(1) Actor	Personal interno y externo (cracker).		
(2) Medios	➢ Manipulación de los dispositivos de comunicación (switch, router). ➢ Saturación del canal de comunicación por implantación de virus o malware en la red. ➢ Configuración errónea de los dispositivos de comunicación.		
(3) Motivo	Lucro, entretenimiento, desconocimiento.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los dispositivos de comunicación contienen un control de acceso para proteger contra el uso no autorizado de los recursos de la red.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque los clientes no pueden revisar la información actualizada en los sitios web.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica	Bajo	2
El personal de la UEV no puede realizar su trabajo porque no cuenta con el acceso a los materiales colocados en las unidades de red	Productividad	Moderado	2
Puntuación del Riesgo Relativo			7
(9) Mitigación de Riesgo **Acciones a tomar**			

☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Interrupción en el servicio de internet

Tabla 137. Riesgos de Activos de Información - Interrupción en el servicio de internet.

Hoja de trabajo Metodología OCTAVE Allegro				
Riesgos de Activos de Información				
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**			
Área de Preocupación	Interrupción en el servicio de internet			
(1) Actor	Personal interno y externo.			
(2) Medios	➢ El proveedor del servicio de internet realiza mantenimiento de equipos de red. ➢ Falla de los equipos alternos. ➢ Falta de pago del servicio. ➢ El gestor del servicio no comunica el mantenimiento de los equipos de comunicación.			
(3) Motivo	➢ Falta de comunicación entre las partes (proveedor y cliente). ➢ Accidental			
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción		
(5) Requisitos de seguridad	Los activos no estarán disponibles por la falta de conexión a internet y no proveer los servicios que se ofrecen en la web.			
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐	
(7) Consecuencias	**(8) Gravedad**			
	Área de Impacto		**Valor de Impacto**	**Puntaje**
La confianza y credibilidad de la organización ser vería afectada, la matriculación se reduciría en 1% al no recibir el soporte técnico, envío de usuario y contraseña a tiempo.	Posición y Fidelización de los Clientes		Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en 1%, las personas solicitan la devolución de su dinero.	Económica		Bajo	2
El personal de la UEV disminuirá su trabajo hasta que el servicio se restablezca. El personal de la UEV deberá laborar horas extras para cumplir con las actividades diarias en los gestores de aprendizaje.	Productividad		Bajo	1

<table>
<tr><td colspan="2">Puntuación del Riesgo Relativo</td><td></td><td>6</td></tr>
<tr><td colspan="4">Mitigación de Riesgo
Acciones a tomar</td></tr>
<tr><td>☐ Aceptar</td><td>☐ Aplazar</td><td>☐ Mitigar</td><td>[X] Transferir</td></tr>
<tr><td colspan="4">Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta.</td></tr>
<tr><td colspan="4">Si se decide mitigar se realizará lo siguiente:</td></tr>
<tr><td colspan="2">Contenedor</td><td colspan="2">Aplicación de Controles Técnicos / Administrativos / Físicos
Riesgo Residual</td></tr>
</table>

Cambio de Proveedor de Servicios.

Tabla 138. Riesgos de Activos de Información - Cambio de proveedor de servicios.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Cambio de proveedor de servicios		
(1) Actor	Personal interno y externo		
(2) Medios	La empresa que presta servicios (servidor dedicado, internet, software) termina el contrato ya sea por disolución o cambio de políticas.		
(3) Motivo	➢ Cambio de políticas internas en la organización. ➢ Mejoramiento de calidad. ➢ Finalización de contrato de servicios.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles durante el cambio y estabilización de los servicios con el nuevo proveedor.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 1%, porque los clientes no pueden acceder a los gestores de aprendizaje, hasta actualizar los datos de DNS, IP's del servidor dedicado.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos por matriculación de cursos virtuales se reducirían en un 1%.	Económica	Bajo	2
El personal de la UEV no pude continuar con sus labores debido a la interrupción del servicio.	Productividad	Bajo	1
Puntuación del Riesgo Relativo			6

Mitigación de Riesgo **Acciones a tomar**			
☒ Aceptar	☐ Aplazar	☐ Mitigar	☐ Transferir
Si se decide mitigar se realizará lo siguiente:			

Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**

Falla en los componentes de hardware de los equipos informáticos.

Tabla 139. Riesgos de Activos de Información - Falla en los componentes de hardware de los equipos informáticos.

<table>
<tr><th colspan="5">Hoja de trabajo Metodología OCTAVE Allegro</th></tr>
<tr><th colspan="5">Riesgos de Activos de Información</th></tr>
<tr><td>Activos de Información</td><td colspan="4">Gestores de Cursos Virtuales CEC-EPN y EPN</td></tr>
<tr><td>Área de Preocupación</td><td colspan="4">Falla en los componentes de hardware de los equipos informáticos.</td></tr>
<tr><td>(1) Actor</td><td colspan="4">Personal interno y externo.</td></tr>
<tr><td>(2) Medios</td><td colspan="4">➢ Conexión errónea de equipos informáticos.
➢ Uso inadecuado de los equipos informáticos.
➢ Falta de protección en las variaciones de voltaje.
➢ Falta de monitoreo de los componentes del equipo informático.</td></tr>
<tr><td>(3) Motivo</td><td colspan="4">Accidental, falla de fabricación.</td></tr>
<tr><td>(4) Resultado</td><td colspan="2">☐ Divulgación
☐ Modificación</td><td colspan="2">☐ Destrucción
☒ Interrupción</td></tr>
<tr><td>(5) Requisitos de seguridad</td><td colspan="4">Los activos no estarán disponibles durante la reposición y configuración de los nuevos componentes de hardware de los equipos informáticos por parte del proveedor y tecnología de la organización.</td></tr>
<tr><td>(6) Probabilidad</td><td>Alto ☐</td><td>Medio ☒</td><td colspan="2">Bajo ☐</td></tr>
<tr><th rowspan="2">(7) Consecuencias</th><th colspan="3">(8) Gravedad</th></tr>
<tr><th>Área de Impacto</th><th>Valor de Impacto</th><th>Puntaje</th></tr>
<tr><td>La matriculación en los cursos virtuales se reduciría en 1%, porque no pueden acceder a los gestores de aprendizaje durante la capacitación, por fallas en disco duro y tarjeta de red en el servidor dedicado.</td><td>Posición y Fidelización de los Clientes</td><td>Moderado</td><td>6</td></tr>
<tr><td>Los ingresos por matriculación de cursos virtuales se reducirían en 1%, por no acceder a los gestores de aprendizaje.</td><td>Económica</td><td>Moderado</td><td>4</td></tr>
<tr><td>El personal de la UEV deja de laborar si falla los componentes de hardware en el servidor dedicado que contiene los gestores de cursos virtuales.</td><td>Productividad</td><td>Moderado</td><td>2</td></tr>
<tr><td>Puntuación del Riesgo Relativo</td><td colspan="2"></td><td>12</td></tr>
<tr><td colspan="4">(9) Mitigación de Riesgo</td></tr>
</table>

Acciones a tomar			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere el riesgo a la Coordinación de Tecnología cuyo responsable del área es Ing. Ximena Uchupanta y el Proveedor Undermedia.			
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**	

Desactualización de los sistemas.

Tabla 140. Riesgos de Activos de Información - Desactualización de sistemas.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Desactualización de sistemas		
(1) Actor	Personal interno y externo.		
(2) Medios	➢ El personal interno y externo no actualizan o colocan parches de seguridad a los sistemas operativos. ➢ El personal interno no actualizan los LMS y CMS Joomla.		
(3) Motivo	Falta de conocimiento, falta de presupuesto.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Al no realizar las actualizaciones a los diferentes sistemas y plataformas, se vulnera la integridad de los activos provocando la paralización temporal de los servicios de la UEV.		
(6) Probabilidad	Alto ☒	Medio ☐	Bajo ☐

Consecuencias	**Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 5%, porque el material de un curso virtual se encuentra desactualizado.	Posición y Fidelización de los Clientes	Bajo	3
Los ingresos se reducirían en un 5% debido a desactualización del material en un curso virtual.	Económica	Bajo	2
"El Área de Gestión y TI debe invertir más horas de trabajo para gestionar la matriculación en los gestores de aprendizaje.	Productividad	Moderado	2
Puntuación del Riesgo Relativo			7

Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☒ Mitigar	☐ Transferir
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos**	

	Riesgo Residual
➢ Servidor dedicado de la UEV ➢ Estaciones de Trabajo de la UEV ➢ Plataforma Moodle CEC-EPN ➢ Plataforma Moodle CEC-EPN V2 ➢ Plataforma Moodle CEC-INEPE ➢ Plataforma Moodle PREGRADO ➢ Plataforma Moodle POSGRADO	➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios en los servidores. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.

Alta Rotación de Personal.

Tabla 141. Riesgos de Activos de Información - Alta Rotación de personal.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Alta Rotación de personal		
(1) Actor	Personal interno.		
(2) Medios	Al renunciar al cargo en la organización y llevar los conocimientos adquiridos del puesto de trabajo.		
(3) Motivo	➢ Inestabilidad laboral. ➢ Ambiente de trabajo. ➢ Intereses personales. ➢ Crecimiento profesional.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Los activos no estarían disponibles mientras se contrata a un nuevo empleado, la curva de aprendizaje sería mayor o menor dependiendo del nuevo personal contratado.		
(6) Probabilidad	Alto ☒	Medio ☐	Bajo ☐

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
El posicionamiento se ve afectado por la falta de personal especializado.	Posición y Fidelización de los Clientes	Moderado	6
Los ingresos se reducirían en un 2% debido a la pérdida de proyectos por la falta de personal	Económica	Moderado	4
El personal deberá realizar actividades extras para superar un puesto de trabajo, el aumento de la carga laboral del personal es del 2%	Productividad	Moderado	2
Puntuación del Riesgo Relativo			12

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☒ Mitigar	☐ Transferir
Si se decide mitigar se realizará lo siguiente:			
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos**		

	Riesgo Residual
➢ Coordinadora de la Unidad de Educación Virtual ➢ Diseñador Instruccional ➢ Experta Pedagoga ➢ Tutora de Tutores ➢ Jefe de Gestión ➢ Jefe de Tecnologías de la Información ➢ Asistente de Tecnologías de la Información ➢ Diseñadora Gráfica	➢ Generar manuales e instructivos de procedimientos técnicos, creados por los expertos de las áreas de Tecnologías de la Información. ➢ Crear grupos de trabajo y capacitar al personal en el manejo del sistema. ➢ Mejorar el clima laboral. ➢ Motivar al personal continuamente. ➢ Generar la transferencia de conocimiento entre el personal de la UEV.

Desastres naturales.

Tabla 142. Riesgos de Activos de Información - Desastres naturales.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Desastres naturales.		
(1) Actor	Fenómenos naturales.		
(2) Medios	Tormentas eléctricas, terremoto, incendios, maremotos.		
(3) Motivo	Calentamiento global, factores climatológicos.		
(4) Resultado	☐ Divulgación ☐ Modificación	☒ Destrucción ☐ Interrupción	
(5) Requisitos de seguridad	Los activos no estarán disponibles al producirse estos desastres mencionados.		
(6) Probabilidad	Alto ☐	Medio ☐	Bajo ☒

(7) Consecuencias	**(8) Gravedad**		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
Los estudiantes no pueden acceder a los gestores de cursos, la posición y fidelidad de los clientes se vería afectada.	Posición y Fidelización de los Clientes	Alto	9
Los ingresos por matriculación de cursos virtuales se reducirían en un 5%.	Económica	Alto	6
El personal de la UEV disminuye su productividad debido a la pérdida del servicio.	Productividad	Alto	3
Puntuación del Riesgo Relativo			18

(9) Mitigación de Riesgo **Acciones a tomar**			
☐ Aceptar	☐ Aplazar	☐ Mitigar	☒ Transferir
Observación: Se transfiere a los proveedores de los distintos servicios Servidor Dedicado, responsables: Undermedia, Ecualinux y aseguradora de equipos.			
Si se decide mitigar se realizará lo siguiente:			
Contenedor	**Aplicación de Controles Técnicos / Administrativos / Físicos** **Riesgo Residual**		

Fallo o defecto de Software.

Tabla 143. Riesgos de Activos de Información - Fallo o defecto de Software.

Hoja de trabajo Metodología OCTAVE Allegro			
Riesgos de Activos de Información			
Activos de Información	**Gestores de Cursos Virtuales CEC-EPN y EPN**		
Área de Preocupación	Fallo o defecto de Software.		
(1) Actor	Personal interno y externo		
(2) Medios	➢ Instalación de software no licenciado. ➢ Instalación de software no compatible. ➢ Eliminación de archivos propios del sistema operativo. ➢ Error de código de programación al ejecutar nuevas actualizaciones en los sistemas informáticos.		
(3) Motivo	Desconocimiento, error, pruebas no controladas.		
(4) Resultado	☐ Divulgación ☐ Modificación	☐ Destrucción ☒ Interrupción	
(5) Requisitos de seguridad	Afecta la disponibilidad de los activos de información, al interrumpir los servicios mientras se detecta el fallo en el software instalado.		
(6) Probabilidad	Alto ☐	Medio ☒	Bajo ☐

(7) Consecuencias	(8) Gravedad		
	Área de Impacto	**Valor de Impacto**	**Puntaje**
La matriculación en los cursos virtuales se reduciría en un 2%, porque no pueden acceder a los gestores en tiempo de ejecución de los cursos virtuales por fallas en software, sistema operativo en el servidor dedicado.	Posición y Fidelización de los Clientes	Moderado	6
Los ingresos por matriculación de cursos virtuales se reducirían en un 2%, por no acceder a los gestores de aprendizaje.	Económica	Moderado	4
El personal de la UEV deja de laborar si falla o existe incompatibilidad en el servidor dedicado que contiene los gestores de aprendizaje.	Productividad	Alto	3
Puntuación del Riesgo Relativo			13
Mitigación de Riesgo **Acciones a tomar**			

☐ Aceptar	☐ Aplazar	☒ Mitigar	☐ Transferir
Si se decide mitigar se realizará lo siguiente:			
Contenedor		**Aplicación de Controles Técnicos / Administrativos / Físicos Riesgo Residual**	
➢ Servidor dedicado de la UEV ➢ Estaciones de Trabajo de la UEV ➢ Plataforma Moodle CEC-EPN ➢ Plataforma Moodle CEC-EPN V2 ➢ Plataforma Moodle CEC-INEPE ➢ Plataforma Moodle PREGRADO ➢ Plataforma Moodle POSGRADO		➢ Planificar configuración de Servidores. ➢ Instalar herramienta antivirus de acuerdo a las capacidades de los servidores y estaciones de trabajo de TI. ➢ Programar ejecución de herramienta antivirus para analizar de forma periódica a las aplicaciones y sistemas operativos huésped. ➢ Escoger un Sistema Operativo adecuado a los componentes instalados de los servidores. ➢ Instalar actualizaciones y parches de seguridad en los servidores. ➢ Desinstalar y deshabilitar servicios y programas innecesarios. ➢ Realizar pruebas de carga al sistema operativo. ➢ El ingreso y actualizaciones remotas se realizan a través de protocolos seguros. Ejemplo SSH. ➢ Antes de instalar actualizaciones de nuevas versiones para los gestores de contenidos se realizará pruebas y estudios de compatibilidad y carga.	

Anexo N° 5 Cuestionarios

Sitios Web CEC-EPN

Cuestionario 1: Contenedor Técnico

Considerando la siguiente abreviatura para los contenedores:

- Sistema de Gestión de Contenidos CEC-EPN: SGC-CEC
- Sistema de Gestión de Contenidos UEV: SGC-UEV
- Servidor dedicado CEC-EPN: SCEC
- Servidor dedicado de la UEV: SUEV
- Correo electrónico: CE
- Estaciones Trabajo: ET
- Internet: I

Tabla 144.Escenario de Amenaza – Contenedor Técnico – Sitios Web CEC-EPN

Cuestionario 1: Escenario de Amenazas Contenedor Técnico			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información en los contenedores técnicos donde reside. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidentalmente o intencionalmente, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado puede acceder a uno o más contenedores técnicos, de manera accidental o intencional, la causa de su activo de información puede ser:			
¿Se divulga a personas no autorizadas?	**No**	**Sí (accidentalmente)**	**Si (intencionalmente)**
		SGC-CEC, SGC-UEV, ET, CE, I	SCEC, SUEV
¿Por modificación de manera que no sea utilizable para fines previstos?	CE, I	SGC-CEC, SGC-UEV, SCEC, SUEV, ET	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?	SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño podía acceder a uno o más contenedores técnicos, accidental o intencionalmente, la causa de su activo de información puede ser:			
¿Se expone a las personas no autorizadas?	ET, I	SGC-CEC, SGC-UEV, CE	SUEV, SCEC
¿Por modificación de manera	SGC-CEC,	SUEV, SCEC	

que no sea utilizable para fines previstos?	SGC-UEV, ET, CE,I		
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	SGC-CEC, SGC-UEV, ET, CE,I	SUEV, SCEC	
Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines.	SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I		

Escenario 3:

En este escenario, considere las situaciones que puedan afectar a su activo de información sobre cualquier contenedor técnico que ha identificado. Determinar si alguno de los siguientes podría ocurrir, y en caso afirmativo, determinar si estas situaciones provocarían una o más de los siguientes resultados:

La divulgación no intencional de sus activos de información.

Modificación no deseada de sus activos de información.

Interrupción involuntaria de la disponibilidad de sus activos de información.

Destrucción permanente inesperada o la pérdida temporal de su activo de información.

	No	Si (revelado)	Si (modificación)	Si (interrupción)	Si (perdido)
Por producto de un defecto de software	ET, I, CE		SGC-CEC, SGC-UEV, SCEC,SUEV,	SCEC,SUEV	SCEC, SUEV
Producido por un fallo del sistema de origen conocido o desconocido	ET, I, CE		SGC-CEC, SGC-UEV, SCEC,SUEV	SGC-CEC, SGC-UEV, SCEC,SUEV	
Por producto de un defecto de hardware			ET	SGC-CEC, SGC-UEV, SCEC,SUEV	SUEV, SCEC
Se ejecuta el código malicioso (por ejemplo, virus, gusano, troyano o puerta trasera).	I		ET	SUEV,SCEC	
Se interrumpe el suministro de energía a los contenedores técnicos				SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I	
Problemas con las telecomunicaciones				SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I	
Otros problemas o sistemas de terceros			SCEC, SUEV	SGC-CEC, SGC-UEV,ET, I, CE	

Las catástrofes naturales o de origen humano (inundaciones, incendios, tornados, explosión, o huracanes) se producen.	I			SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I	SUEV, SCEC, I,ET

Cuestionario 2: Contenedor Físico

Considerando la siguiente abreviatura para los contenedores:

- Data Center del CEC-EPN: DCCEC
- Data Center EEUU CEC: DCEU-CEC
- Oficina de la UEV: OUEV
- Data Center EEUU UEV:DCE-UEV

Tabla 145. Escenario de Amenaza – Contenedor Físico – Sitios Web CEC-EPN

Cuestionario 2: Escenario de Amenazas Contenedor Físico			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información en los contenedores físicos donde reside. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidentalmente o intencionalmente, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado puede acceder a uno o más contenedores físico, de manera accidental o intencional, la causa de su activo de información puede será:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?	DCCEC, DCEU-CEC, DCEU-UEV	OUEV	
¿Por modificación de manera que no sea utilizable para fines previstos?	DCCEC, DCEU-CEC, DCEU-UEV	OUEV	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	DCCEC, OUEV, DCEU-CEC, DCEU-UEV		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?	DCCEC, OUEV, DCEU-CEC, DCEU-UEV		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño podía acceder a uno o más contenedores físicos, accidental o intencional, la causa de su activo de información será:			
¿Se expone a las personas no autorizadas?		DCCEC, OUEV, DCEU-CEC, DCEU-UEV	
¿Por modificación de manera que no sea utilizable para fines previstos?		DCCEC, OUEV, DCEU-CEC, DCEU-UEV	

¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	DEUEV, DCCEC, OUEV	DCEU-CEC, DCEU.UEV	
Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines	DCCEC, OUEV, DCEU-CEC, DCEU-UEV		

Escenario 3:					
En este escenario, considere las situaciones que puedan afectar a sus contenedores físicos y por defecto afectar su activo de información. Determinar si alguno de los siguientes podría ocurrir, y en caso afirmativo, determinar si estas situaciones provocarían una o más de los siguientes resultados:					
La divulgación no intencional de sus activos de información.					
Modificación no deseada de sus activos de información.					
Interrupción involuntaria de la disponibilidad de sus activos de información.					
Destrucción permanente inesperada o la pérdida temporal de su activo de información.					
	No	**Si (revelado)**	**Si (modificación)**	**Si (interrupción)**	**Si (perdido)**
Otros problemas o sistemas de terceros				DCCEC, OUEV, DCEU-CEC, DCEU-UEV	
Las catástrofes naturales o de origen humano (inundaciones, incendios, tornados, explosión, o huracanes) se producen.					DCCEC, OUEV, DCEU-CEC, DCEU-UEV

Cuestionario 3: Contenedor Personas

Considerando la siguiente abreviatura para los contenedores:

CEC-EPN
- Coordinadora de Tecnología CEC-EPN: CTCEC

UEV
- Coordinadora de la Unidad de Educación Virtual: CUEV
- Jefe de Gestión UEV: JGUEV
- Jefe de Tecnologías de la Información UEV: JTIUEV
- Diseñadora Gráfica UEV: DGUEV
- Asistente de Gestión UEV: AGUEV
- Asistente de Tecnologías de la Información UEV: ATIUEV

Proveedores
- Proveedor de Nombre de Dominio: PD
- Proveedor del Servidor Dedicado CEC-EPN
- Proveedor del Servidor Dedicado UEV
- Proveedor de Internet: PI
- Proveedor de Correo electrónico: PCE

Tabla 146. Escenario de Amenaza – Contenedor Personas – Sitios Web CEC-EPN

Cuestionario 3 Escenario de Amenazas Personas			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información ya que es conocido por el personal clave de la organización. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidental o intencional, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado tiene el conocimiento detallado de sus activos de información accidental o intencional, la causa de su activo de información será:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?	CEC-EPN, UEV		
¿Por modificación de manera que no sea utilizable para fines previstos?[1]	CEC-EPN, UEV		

[1] El caso es poco probable, pero si una persona clave en su organización tiene conocimiento de un activo de información y comunica esta información de una manera alterada que afecta a la organización, podría dar como resultado un riesgo.

¿De manera Interrumpida de modo que no se puede acceder para fines previstos?[2]	CEC-EPN, UEV		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?[3]		UEV	

Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño conoce su activo de información accidental o intencional, la causa de su activo de información puede ser:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?		Proveedores	

[2] Este caso es acerca de la disponibilidad de la información. Si una persona clave en la organización tiene conocimiento de que es vital para un proceso de negocio y no es accesible o disponible, la información no puede ser utilizable para los fines previstos, en última instancia, afectan la organización.

[3] Si una persona clave en la organización conoce el activo de información y deja la organización, y la información no está documentada o en otros lugares, podría suponer un riesgo para la organización.

Sistema Integrado de Información del CEC-EPN

Cuestionario 1: Contenedor Técnico

Considerando la siguiente abreviatura para los contenedores:

- Servidor de Aplicaciones CEC-EPN: SA-CEC
- Internet: I
- Servidor de Base de Datos CEC-EPN: SBDCEC
- Framework para aplicaciones web CodeIgniter: MVC
- Estaciones Trabajo: ET
- Servidor de Versiones CEC-EPN: SVCEC

Tabla 147. Escenario de Amenaza – Contenedor Técnico – Sistema Integrado de Información del CEC-EPN

Cuestionario 1 Escenario de Amenazas Contenedor Técnico			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información en los contenedores técnicos donde reside. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidentalmente o intencionalmente, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado puede acceder a uno o más contenedores técnicos, de manera accidental o intencional, la causa de su activo de información puede ser:			
	No	**Sí (accidentalmente)**	**Si (intencionalmente)**
¿Se divulga a personas no autorizadas?	SA-CEC, SBDCEC, MVC, SVCEC	I, ET	
¿Por modificación de manera que no sea utilizable para fines previstos?	SA-CEC, I, SBDCEC, MVC, ET, SVCEC		
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	SA-CEC, I, SBDCEC, MVC, ET, SVCEC		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?	SA-CEC, I, SBDCEC, MVC, ET, SVCEC		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño podía acceder a uno o más contenedores técnicos, accidental o intencionalmente, la causa de su activo de información puede ser:			
¿Se expone a las personas no autorizadas?	SA-CEC, I, SBDCEC, MVC, ET, SVCEC		
¿Por modificación de manera que no sea utilizable para fines previstos?	SA-CEC, I, SBDCEC, MVC, ET, SVCEC		
¿De manera Interrumpida de			

modo que no se puede acceder para fines previstos?			
Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines	SA-CEC, I, SBDCEC, MVC, ET, SVCEC		

Escenario 3:
En este escenario, considere las situaciones que puedan afectar a su activo de información sobre cualquier contenedor técnico que ha identificado. Determinar si alguno de los siguientes podría ocurrir, y en caso afirmativo, determinar si estas situaciones provocarían una o más de los siguientes resultados:
La divulgación no intencional de sus activos de información
Modificación no deseada de sus activos de información
Interrupción involuntaria de la disponibilidad de sus activos de información
Destrucción permanente inesperado o la pérdida temporal de su activo de información

	No	**Si (revelado)**	**Si (modificación)**	**Si (interrupción)**	**Si (perdido)**
Por producto de un defecto de software	ET, I		SA-CEC, SBDCEC, MVC, SVCEC	SA-CEC, SBDCEC, MVC, SVCEC	
Producido por un fallo del sistema de origen conocido o desconocido	ET, I		SA-CEC, SBDCEC, MVC, SVCEC	SA-CEC, SBDCEC, MVC, SVCEC	
Por producto de un defecto de hardware	I			SA-CEC, SBDCEC, MVC, SVCEC, ET	
Se ejecuta el código malicioso (por ejemplo, virus, gusano, troyano o puerta trasera)	I			SA-CEC, SBDCEC, MVC, SVCEC, ET	
Se interrumpe el suministro de energía a los contenedores técnicos				SA-CEC, SBDCEC, MVC, SVCEC, ET, I	
Problemas con las telecomunicaciones				SA-CEC, SBDCEC, MVC, SVCEC, ET, I	
Otros problemas o sistemas de terceros				SGC-CEC, SGC-UEV,ET, I, CE	

Las catástrofes naturales o de origen humano (inundaciones, incendios, tornados, explosión, o huracanes) se producen.				SGC-CEC, SGC-UEV,ET, I, CE	SGC-CEC, SGC-UEV,ET, I, CE

Cuestionario 2: Contenedor Físico

Considerando las siguientes abreviaturas para los contenedores:

- Data Center del CEC-EPN: DCCEC
- Oficina de la UEV: OUEV
- Red interna: RI
- Archivador ventanilla UEV: VUEV
- Archivador oficina UEV: VOUEV

Tabla 148. Escenario de Amenaza – Contenedor Físico – Sistema Integrado de Información del CEC-EPN

Cuestionario 2: Escenario de Amenazas Contenedor Físico			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información en los contenedores físicos donde reside. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidentalmente o intencionalmente, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado puede acceder a uno o más contenedores físico, de manera accidental o intencional, la causa de su activo de información puede será:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?	DCCEC, RI	OUEV, VUEV, VOUEV	
¿Por modificación de manera que no sea utilizable para fines previstos?		DCCEC, RI, OUEV, VUEV, VOUEV	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?		DCCEC, RI, OUEV, VUEV, VOUEV	
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?	DCCEC, RI, OUEV, VUEV, VOUEV		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño podía acceder a uno o más contenedores físicos, accidental o intencional, la causa de su activo de información será:			
¿Se expone a las personas no autorizadas?	DCCEC, RI	DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV	
¿Por modificación de manera que	DCCEC, RI	OUEV, VUEV,	

no sea utilizable para fines previstos?		VOUEV	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	DCCEC, RI, OUEV, VUEV, VOUEV		
Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines	DCCEC, RI, OUEV, VUEV, VOUEV		

Escenario 3:

En este escenario, considere las situaciones que puedan afectar a sus contenedores físicos y por defecto afectar su activo de información. Determinar si alguno de los siguientes podría ocurrir, y en caso afirmativo, determinar si estas situaciones provocarían una o más de los siguientes resultados:

La divulgación no intencional de sus activos de información

Modificación no deseada de sus activos de información

Interrupción involuntaria de la disponibilidad de sus activos de información

Destrucción permanente inesperado o la pérdida temporal de su activo de información

	No	Si (revelado)	Si (modificación)	Si (interrupción)	Si (perdido)
Otros problemas o sistemas de terceros				DCCEC, RI, OUEV, VUEV, VOUEV	
Las catástrofes naturales o de origen humano (inundaciones, incendios, tornados, explosión, o huracanes) se producen				DCCEC, RI, OUEV, VUEV, VOUEV	

Cuestionario 3: Contenedor Personas

Considerando que:

- Coordinadora de Tecnología CEC-EPN: CTCEC
- Desarrollador de Tecnología CEC-EPN: DCT
- Jefe de Gestión UEV: JGUEV
- Tutora de Tutores UEV: TTUEV

Tabla 149. Escenario de Amenaza – Contenedor Personas – Sistema Integrado de Información del CEC-EPN

Cuestionario 3 Escenario de Amenazas Personas			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información ya que es conocido por el personal clave de la organización. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidental o intencional, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado tiene el conocimiento detallado de sus activos de información accidental o intencional, la causa de su activo de información será:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?		UEV, CEC-EPN	
¿Por modificación de manera que no sea utilizable para fines previstos?[4]		UEV, CEC-EPN	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?[5]	UEV, CEC-EPN		

[4] El caso es poco probable, pero si una persona clave en su organización tiene conocimiento de un activo de información y comunica esta información de una manera alterada que afecta a la organización, podría dar como resultado un riesgo.

[5] Este caso es acerca de la disponibilidad de la información. Si una persona clave en la organización tiene conocimiento de que es vital para un proceso de negocio y no es accesible o disponible, la información no puede ser utilizable para los fines previstos, en última instancia, afectan la organización.

¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?[6]	UEV, CEC-EPN		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño conoce su activo de información accidental o intencional, la causa de su activo de información puede ser:			
	No	Si (accidentalmente)	Si (intencionalmente)
¿Se expone a las personas no autorizadas?	UEV, CEC-EPN		

[6] Si una persona clave en la organización conoce el activo de información y deja la organización, y la información no está documentada o en otros lugares, podría suponer un riesgo para la organización.

Gestores de Cursos Virtuales CEC-EPN y EPN

Cuestionario 1: Contenedor Técnico:

Considerando que:

- Plataformas Moodle UEV: Moodle
- Estaciones Trabajo: ET
- Sistemas SSH: SSH
- Servidor dedicado de la UEV: SUEV
- Internet: I

Tabla 150. Escenario de Amenaza – Contenedor Técnico – Gestores de Cursos Virtuales CEC-EPN y EPN

Cuestionario 1 Escenario de Amenazas Contenedor Técnico			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información en los contenedores técnicos donde reside. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidentalmente o intencionalmente, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado puede acceder a uno o más contenedores técnicos, de manera accidental o intencional, la causa de su activo de información puede ser:			
¿Se divulga a personas no autorizadas?	**No**	**Sí (accidentalmente)**	**Si (intencionalmente)**
		Moodle, ET, SSH, I, SUEV	Moodle
¿Por modificación de manera que no sea utilizable para fines previstos?		Moodle, ET, SSH, I, SUEV	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	Moodle, ET, SSH, I, SUEV		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?	Moodle, ET, SSH, I, SUEV		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño podía acceder a uno o más contenedores técnicos, accidental o intencionalmente, la causa de su activo de información puede ser:			
¿Se expone a las personas no autorizadas?	ET, SSH, I	Moodle, SUEV	
¿Por modificación de manera que no sea utilizable para fines previstos?	ET, SSH, I	Moodle, SUEV	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	Moodle, ET, SSH, I	SUEV	
Permanentemente destruido o	Moodle, ET,		

perdido temporalmente de modo que no se puede utilizar para fines	SSH, I, SUEV		

Escenario 3:					
En este escenario, considere las situaciones que puedan afectar a su activo de información sobre cualquier contenedor técnico que ha identificado. Determinar si alguno de los siguientes podría ocurrir, y en caso afirmativo, determinar si estas situaciones provocarían una o más de los siguientes resultados:					
La divulgación no intencional de sus activos de información					
Modificación no deseada de sus activos de información					
Interrupción involuntaria de la disponibilidad de sus activos de información					
Destrucción permanente inesperado o la pérdida temporal de su activo de información					
	No	**Si (revelado)**	**Si (modificación)**	**Si (interrupción)**	**Si (perdido)**
Por producto de un defecto de software	ET, I, CE, SSH		Moodle, SUEV		SCEC,SUEV
Producido por un fallo del sistema de origen conocido o desconocido	ET, I, CE		SGC-CEC, SGC-UEV, SCEC,SUEV	SGC-CEC, SGC-UEV, SCEC,SUEV	
Por producto de un defecto de hardware			ET	SGC-CEC, SGC-UEV, SCEC,SUEV	SUEV, SCEC
Se ejecuta el código malicioso (por ejemplo, virus, gusano, troyano o puerta trasera)	I		ET	SUEV,SCEC	
Se interrumpe el suministro de energía a los contenedores técnicos				SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I	
Problemas con las telecomunicaciones				SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I	
Otros problemas o sistemas de terceros			SCEC, SUEV	SGC-CEC, SGC-UEV,ET, I, CE	
Las catástrofes naturales o de origen humano (inundaciones, incendios, tornados, explosión, o huracanes) se producen	I			SGC-CEC, SGC-UEV, ET, SCEC,SUEV, CE,I	SUEV, SCEC, I,ET

Cuestionario 2: Contenedor Físico

Considerando que:

- Data Center EEUU CEC:DCEU-CEC
- Data Center del CEC-EPN: DCCEC
- Oficina de la UEV: OUEV
- Data Center EEUU UEV:DCEU

Tabla 151. Escenario de Amenaza – Contenedor Físico – Gestores de Cursos Virtuales CEC-EPN y EPN

Cuestionario 2: Escenario de Amenazas Contenedor Físico			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información en los contenedores físicos donde reside. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidentalmente o intencionalmente, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado puede acceder a uno o más contenedores físico, de manera accidental o intencional, la causa de su activo de información puede será:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?	DEUEV, DCCEC, DCEU-CEC, DCEU.UEV	OUEV	
¿Por modificación de manera que no sea utilizable para fines previstos?	DEUEV, DCCEC, DCEU-CEC, DCEU.UEV	OUEV	
¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?	DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV		
Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño podía acceder a uno o más contenedores físicos, accidental o intencional, la causa de su activo de información será:			
¿Se expone a las personas no autorizadas?		DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV	
¿Por modificación de manera que no sea utilizable para fines previstos?		DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV	

¿De manera Interrumpida de modo que no se puede acceder para fines previstos?	DEUEV, DCCEC, OUEV	DCEU-CEC, DCEU.UEV	
Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines	DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV		

Escenario 3:					
En este escenario, considere las situaciones que puedan afectar a sus contenedores físicos y por defecto afectar su activo de información. Determinar si alguno de los siguientes podría ocurrir, y en caso afirmativo, determinar si estas situaciones provocarían una o más de los siguientes resultados:					
La divulgación no intencional de sus activos de información					
Modificación no deseada de sus activos de información					
Interrupción involuntaria de la disponibilidad de sus activos de información					
Destrucción permanente inesperado o la pérdida temporal de su activo de información					
	No	**Si (revelado)**	**Si (modificación)**	**Si (interrupción)**	**Si (perdido)**
Otros problemas o sistemas de terceros				DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV	
Las catástrofes naturales o de origen humano (inundaciones, incendios, tornados, explosión, o huracanes) se producen.					DEUEV, DCCEC, OUEV, DCEU-CEC, DCEU.UEV

Cuestionario 3: Contenedor Personas

Considerando que:

- Coordinadora de la Unidad de Educación Virtual: CUEV
- Coordinadora de Tecnología CEC-EPN: CCEC
- Jefe de Gestión UEV: JGUEV
- Jefe de Tecnologías de la Información UEV: JTIUEV
- Diseñadora Gráfica UEV: DGUEV
- Asistente de Gestión UEV: AGUEV
- Asistente de Tecnologías de la Información UEV: ATIUEV
- Proveedor de Nombre de Dominio: PD
- Proveedor del Servidor Dedicado CEC-EPN
- Proveedor del Servidor Dedicado UEV
- Proveedor de Internet: PIData
- Proveedor de Correo electrónico: PCE

Tabla 152. Escenario de Amenaza – Contenedor Personas – Gestores de Cursos Virtuales CEC-EPN y EPN

Cuestionario 3 Escenario de Amenazas Personas			
Este cuestionario ayudará a pensar acerca de los escenarios que podrían afectar el activo de información ya que es conocido por el personal clave de la organización. Estos escenarios pueden plantear riesgos que se necesiten hacer frente. Hay que considerar cada escenario y escoger la respuesta apropiada. Si la respuesta es "sí" hay que considerar si el escenario podría ocurrir accidental o intencional, o ambos.			
Escenario 1:			
Piense en las personas que trabajan en su organización. ¿Hay una situación en la que un empleado tiene el conocimiento detallado de sus activos de información accidental o intencional, la causa de su activo de información será:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?	CEC-EPN		
¿Por modificación de manera que no sea utilizable para fines previstos?[7]	CEC-EPN		

[7] El caso es poco probable, pero si una persona clave en su organización tiene conocimiento de un activo de información y comunica esta información de una manera alterada que afecta a la organización, podría dar como resultado un riesgo.

¿De manera Interrumpida de modo que no se puede acceder para fines previstos?[8]	CEC-EPN		
¿Permanentemente destruido o perdido temporalmente de modo que no se puede utilizar para fines previstos?[9]		UEV	

Escenario 2:			
Piense en las personas que son externos a su organización. Esto podría incluir a las personas que pueden tener una relación comercial legítima con su organización o no. ¿Hay una situación en la que un extraño conoce su activo de información accidental o intencional, la causa de su activo de información puede ser:			
	No	**Si (accidentalmente)**	**Si (intencionalmente)**
¿Se expone a las personas no autorizadas?		Proveedores	

[8] Este caso es acerca de la disponibilidad de la información. Si una persona clave en la organización tiene conocimiento de que es vital para un proceso de negocio y no es accesible o disponible, la información no puede ser utilizable para los fines previstos, en última instancia, afectan la organización.

[9] Si una persona clave en la organización conoce el activo de información y deja la organización, y la información no está documentada o en otros lugares, podría suponer un riesgo para la organización.

Anexo N° 6 Información de contactos del BCP

Tabla 181. Formato para recopilar información de contactos del plan de continuidad.

Información de contacto para el plan de continuidad		
Última actualización (dd/mm/aaaa): 27/09/2014		**Versión: BCP-UEV-001**
Tipo de contacto:	Personal CEC-EPN ☐	Proveedor ☐
Unidad o empresa:		
Nombre del funcionario:		
Cargo:		
Rol (es) desempeñado(s) en el BCP:	Líder Ejecutivo ☐ Oficial de Seguridad ☐ Líder de proceso ☐	Coordinador del BCP ☐ Jefe de Información ☐ Proveedor ☐
Correo electrónico:		
Número de teléfono:	Oficina y extensión:	Teléfono celular:
Dirección de domicilio:		
Persona de reemplazo en caso de ausencia:		

Anexo N° 7 Glosario de Términos

A

AAA: Asociación de Contadores Americanos.

Acción: es el efecto que causa un objeto o agente sobre algo.

Análisis: estudio minucioso de un asunto, noticia, suceso, etc.

AS/NZS: Estándar de Australia / Nueva Zelanda.

B

BCI: Business Continuity Institute.

BCM: Business Continuity Management.

BCP: Business Continuity Plan.

BIA: Business Impact Analisys.

C

CEC: Centro de Educación Continua.

CEC-EPN: Centro de Educación Continua de la Escuela Politécnica Nacional.

COBIT: Control Objetives for Information and Related Technology.

Contenedor: lugar donde los activos se almacenan, transportan o procesan.

Contingencia: posibilidad o riesgo de que suceda una cosa.

Continuidad: duración o permanencia de una cosa sin interrupción.

Control: comprobación o inspección de una cosa.

COSO: Committee of Sponsoring Organizations.

CRAMM: CCTA Risk Analysis and Management Method.

D

DELPHI: entorno de desarrollo de software.

DRII: Disaster Recovery Institute International.

DRP: Disaster Recovery Plan.

E

EARME: Edificio Aulas y Relación con el Medio Externo.

EPN: Escuela Politécnica Nacional.

E-learning: se denomina a la capacitación o aprendizaje a través del internet.

Estándar: es un patrón, modelo o punto de referencia para medir o valorar objetos de la misma clase.

Estrategia: plan que especifica una serie de pasos que tienen como fin la consecución de un determinado objetivo.

Entregable: es el resultado de un proyecto o cualquier parte de un proyecto.

I

Incidente: circunstancia o suceso que pasa de manera inesperada y que puede afectar al desarrollo de un asunto o negocio, aunque no forme parte de él.

INTECO: Instituto Nacional de Tecnologías de la Comunicación.

ISACA: Information Systems Audit and Control Association.

ISO: International Organization for Standardization.

ITGI: Instituto de Administración de las Tecnologías de la Información.

ITIL: Information Technology Infrastructure Library

ITSCM: IT Service Continuity Management, Gestión de la Continuidad del Servicio de TI.

L

LMS: Learning Management System.

M

MAGERIT: Metodología de Análisis y Gestión de Riesgos IT

MEHARI: Método Armonizado de Análisis de Riesgos.

Metodología: conjunto de métodos que se siguen en una investigación científica, un estudio o una exposición doctrinal.

Misión: es la razón de ser de una empresa.

Mitigación: reducción de la vulnerabilidad, atenuación de los daños potenciales sobre la vida o los bienes causados por un evento.

MTD: Maxium Tolerable Downtimes.

MOODLE: Modular Objet-Oriented Dynamic Learning Enviroment, es un sistema de gestión aprendizaje de distribución libre, que ayuda a los educadores a crear comunidades de aprendizaje en línea.

N

NIST: National Institute of Standardas and Technology.

O

OCTAVE: Operationally Critical Threat Asset and Vulnerability Evaluation.

OCTAVE-S: Operationally Critical Threat Asset and Vulnerability Evaluation Small.

OCTAVE-Allegro: Operationally Critical Threat Asset and Vulnerability Evaluation Allegro.

P

PILAR II: Proceso Informático-Lógico para el Análisis y Gestión de Riesgos.

Plataforma: es un sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Posicionamiento: es el arte de diseñar la oferta y la imagen de la empresa de modo que ocupen un lugar distintivo en el mercado.

R

Resiliencia: es la capacidad que tiene una persona o un grupo de recuperarse frente a la adversidad para seguir proyectando el futuro.

RPO: (Recovery Point Objetive), es la cantidad aceptable de pérdida de datos en base a la última copia de respaldo en el momento del desastre.

RTO: (Recovery Time Objetive), es el tiempo que puede permanecer una empresa sin ejecutar una actividad o proceso, también puede ser el tiempo máximo de inactividad.

S

Salvaguarda: custodia, amparo, garantía.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SIICEC: Sistema Integrado de Información del CEC-EPN.

SSH: Secure SHell, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

T

TI: Tecnología de la Información.

TIC: Tecnología de la Información y la Comunicación.

U

UEV: Unidad de Educación Virtual.

V

Visión: define las metas que se pretenden conseguir en el futuro dentro de una empresa.

W

WRT: Work Recovery Time.