UNIVERSIDAD DON BOSCO

VICERRECTORIA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

CONTINUIDAD DEL NEGOCIO EN LA RECUPERACIÓN DE DESASTRES PARA EL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN. CASO PRÁCTICO: UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR

MG. RENÉ ARTURO ANGULO ARRIAZA

PRESENTADO POR

KYRNA MARGARITA QUINTANILLA MACHADO
OSCAR ERNESTO RODRIGUEZ ALFARO
SALVADOR ALCIDES FRANCO SANCHEZ

ANTIGUO CUSCATLÁN, LA LIBERTAD, EL SALVADOR, CENTROAMERICA.

MARZO 2016

Contenido

1. Introducción

a. Antecedentes institucionales

La UTEC (Universidad Tecnológica de El Salvador) es una institución de educación superior fundada en el año 1979. La misión de la UTEC es proponer las soluciones pertinentes a las necesidades de amplios sectores de la sociedad, por ello cuenta con una oferta académica distribuida en cinco facultades: Maestrías y Estudios de Postgrados, Ciencias Sociales, Derecho, Ciencias Empresariales e Informática y Ciencias Aplicadas. Es la universidad privada más grande de El Salvador con un estimado 23,000 estudiantes de carreras presenciales y virtuales. Actualmente la UTEC posee un eslogan que le permite la identificación con la comunidad educativa y con la sociedad en general "Actitud Positiva", la idean con el eslogan es que la sociedad sea consiente que lo que cuenta es la actitud para lograr el éxito. También es importante mencionar algunas de las ventajas competitivas que le ha permitido llegar a ser la universidad privada más grande del país, su ubicación geográfica, ya que se encuentra en el centro de San Salvador permitiendo el fácil acceso desde cualquier lugar, la facilidad de horarios, ya que los estudiantes pueden optar por turnos matutinos, media mañana, nocturnos o fines de semana, y la tercera ventaja competitiva pero no menos importante la innovación, la UTEC se preocupa por mantener a la vanguardia de la tecnología su laboratorios especializados, bibliotecas especializadas, clínicas psicológicas, clínicas médicas, museo universitario de antropología, entre otros. Ya son 36 años de su existencia formando profesionales en las distintas áreas del conocimiento, formándolos con un compromiso ético y con un sentido de pertenencia hacia el legado cultural. **[1]**

También la UTEC busca vincularse con su entorno y los diferentes sectores que lo integran a través del desarrollo de investigaciones pertinentes y proyección social, permitiendo que la comunidad educativa el desarrollo de proyectos alineados a la responsabilidad social universitaria que benefician a sectores vulnerables de la sociedad en general. La UTEC cuenta con sistemas de información que le permiten procesar las operaciones del negocio, tales como: registro académico, recursos humanos y finanzas, también cuenta con una serie de portales web que permiten la interacción entre el docente y el alumno, posee una infraestructura de red en forma de anillo en todo el campus que conecta los edificios de forma física y así poder acceder a los servicios centralizados en el centro de datos, también posee una extensión del campus ubicada a dos cuadras del monumento salvador del mundo donde se imparten estudios de maestrías y post grados. **[2] [3]**

Para la UTEC es de vital importancia contar con una solución que defina las acciones a seguir cuando se presente un desastre natural o un incidente de seguridad ocasionado por ataques intencionados o no intencionados, actualmente no existe la suficiente documentación que contenga las personas responsables, roles, funciones y las diferentes actividades que se deben llevar a cabo al momento de un percance, tampoco se cuenta con la guía de procedimientos técnicos de recuperación y las prioridades de la recuperación de los activos de información de la UTEC, de tal forma que al momento de responder ante un evento de este tipo, será necesario que se tomen las decisiones en tiempo real, esto podría ocasionar largos tiempos para la recuperación, seleccionar de forma inadecuada las prioridades de recuperación y en el peor de los casos que la recuperación no pueda llevarse a cabo por las malas decisiones tomadas en el momento del incidente.

Otro aspecto importante es la poca visibilidad que tiene el departamento de TI a la hora de definir los tiempos para las recuperaciones de los sistemas de información, bases de datos o la infraestructura de red, si en este momento ocurriera un incidente los tiempos para la recuperación serían entregados a la alta gerencia a partir de la información que pueda ser proporcionada por el Jefe de TI, quien está a cargo de toda la infraestructura de red, servidores y sistemas de información, el agravante es que este tipo de información no está disponible y las respuestas son bien subjetivas.

b. Eventos de seguridad

Las empresas son cada vez más conscientes de la necesidad de estar preparadas para responder ante todo tipo de desastres y situaciones catastróficas, como podrían ser los incendios, inundaciones, terremotos, consecuencias de huracanes, entre otros. Sin embargo, estas situaciones también se podrían producir debido a los daños ocasionados por sabotajes, robos o, incluso, por atentados terroristas.

Para la continuidad del negocio se debe definir un plan que especifique los objetivos y las prioridades a tener en cuenta por la organización en caso de un desastre que pueda afectar a la continuidad del negocio. Para ello, es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento del sistema informático de la organización, así como recuperar los datos, aplicaciones y servicios básicos que se utilizan como soporte al negocio de la organización:

- Disponibilidad de un Centro Alternativo o Centro de Reserva para ubicación de los principales recursos informáticos (servidores y bases de datos corporativas).
- Existencia de líneas de respaldo para las comunicaciones.
- Sistema de almacenamiento RAID en los servidores.
- Implantación de clusters de servidores con balanceo de carga.
- Herramientas para llevar a cabo la replicación de los documentos y las bases de datos, que puedan ser síncrona, asíncrona o periódica.

Asimismo, se tiene que definir un Plan de Recuperación de Negocio cuál va a ser la composición de un equipo de dirección que se encarga de coordinar todas las tareas de recuperación frente a un desastre, realizando esta labor desde un determinado centro de control, cuya ubicación también tiene que haber sido previamente especificada en el Plan de Recuperación.

Un elemento fundamental en la continuidad del negocio es la existencia de un centro alternativo, también conocido como centro de respaldo o centro de backup, si bien en la práctica sólo las grandes empresas podrán disponer de un local o edificio dedicado exclusivamente a esta misión. Este centro tendría que estar equipado con los equipos informáticos adecuados y contar con copias de seguridad de los datos más críticos para el negocio suficientemente actualizadas.

Las organizaciones pueden adoptar distintas estrategias a la hora de implantar un centro alternativo:

a. No se dispone de un centro alternativo y no existen copias de seguridad externas. En esta situación la recuperación puede ser impredecible e, incluso, dependiendo de la gravedad del desastre, es posible que nunca se pueda llegar a recuperar totalmente los datos, programas y la documentación del sistema afectado. Debemos señalar que un importante porcentaje de empresas y organizaciones de todo tipo (sobre todo de menor tamaño) todavía se encuentran en esta situación. De las empresas que tenían una perdida principal de registros automatizados el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años, y solo el 6 % sobrevivirá el largo plazo. [4]
b. Transporte periódico de copias de seguridad a un almacén. En ese caso podemos considerar que ya existe un plan de recuperación del negocio, gracias a la existencia de copias de seguridad más o menos actualizadas en otra ubicación física. No obstante, el tiempo de recuperación puede ser alto, posiblemente superior a una semana, ya que no se dispone de un centro alternativo con equipos adecuados para volver a poner en marcha las aplicaciones y servicios informáticos de la organización.
c. Centro Alternativo “Frio”: se trata de un centro alternativo que cuenta con un equipamiento suficiente de hardware, software y de comunicaciones para mantener los servicios críticos de la organización. Asimismo, en este centro se guardan copias de seguridad de los datos y aplicaciones de la organización. El tiempo de recuperación puede ser de uno a varios días, ya que es necesario

restaurar los datos y las aplicaciones desde las copias de seguridad, poniendo en funcionamiento los distintos equipos del centro alternativo.

d. Centro Alternativo "Caliente": se trata de un centro alternativo que cuenta con el equipamiento de hardware, software y comunicaciones necesario para mantener los servicios críticos de la organización, y en el que además estos equipos se encuentran en funcionamiento y disponen de una réplica de todos los datos y aplicaciones del sistema informático, que se realizan de forma diaria o incluso cada hora. De este modo, el tiempo de recuperación es de unas pocas horas, inferior a un día.
e. Centro Alternativo "Caliente" en una configuración en "espejo": Se trata de un centro alternativo con el mismo equipamiento que el centro principal y que trabaja de un modo paralelo a éste, pudiendo entrar en acción inmediatamente a la caída del centro principal. Se trata, por tanto, de un sistema redundante, adecuado para situaciones que requieran de una alta disponibilidad.

Por otra parte, se debe destacar la importancia de documentar el sistema informático al mayor nivel de detalle posible, ya que en caso de desastre no siempre se podrá disponer de las personas clave para poder disponer de esta información.

2. Metodología de trabajo

a. Planteamiento del problema

Una de las grandes preocupaciones de la alta gerencia es la continuidad del negocio en aspectos informáticos, debido a que no se cuenta con las líneas claras sobre la forma de reaccionar ante un evento de desastres naturales, amenazas que pongan en riesgo la seguridad de las bases de datos y los sistemas de información, para ello es de vital importancia contar con un plan respuesta ante incidentes que le permita a la universidad seguir brindando los servicios a la comunidad educativa. **[5]**

b. Hipótesis

La implementación de un plan de recuperación ante desastres, contribuye para asegurar la continuidad de los servicios críticos de Tecnologías de Información del área de informática de la Universidad Tecnológica de el Salvador.

c. Formas de trabajo

La metodología para la presente investigación consistirá en identificar los principales recursos de los sistemas de información que la Universidad Tecnológica necesita para continuar operando de forma esencial pero efectiva. Estos sistemas de información serán analizados para ser categorizados por su importancia, impacto, orden de recuperación, tiempos y puntos esperados de recuperación, entre otros, para elaborar el Plan de Recuperación de desastres también conocido por sus siglas en inglés DRP (Desaster Recovery Plan).

También como parte de la metodología se elaborarán el documento de análisis del impacto del negocio (Bussiness Impact Analysis, BIA) para el área de Tecnologías de la información, identificando los procesos críticos y sus impactos en la UTEC. Se identificarán los proveedores internos y externos, sitios alternos, responsables y responsabilidades, todo para la definición de la estrategia de continuidad para el área de Tecnologías de la Información.

Otro aspecto que será utilizado para la definición de la estrategia de recuperación de desastres, será la descripción de posibles escenarios que impacten total o parcialmente en los servicios de información proporcionados por la UTEC, y los lineamientos que cada área o responsable debe seguir ante estos casos particulares.

3. Marco conceptual

a. La seguridad de la información

Muchas de las actividades que se realizan de forma cotidiana en los países desarrollados dependen en mayor o menor medida de sistemas y de redes informáticas. El espectacular crecimiento de Internet y los servicios telemáticos como el comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la video conferencia, ha contribuido a popularizar aún más, si cabe, el uso de la informática y las redes de ordenadores, hasta el punto de que en la actualidad no se circunscriben al ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y ocio de los ciudadanos.

Por otra parte, servicios críticos para una sociedad moderna, como podrían ser los servicios financieros, en control de la producción y suministro eléctrico (centrales eléctricas, redes de distribución y transformación), los medios de transporte (control de tráfico aéreo, control de vías terrestres y marítimas), la sanidad (historial clínico informatizado, telemedicina), las redes de abastecimientos (agua, gas y saneamiento), la propia administración pública y el sistema educativo están soportados en su práctica totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se ha eliminado o reducido de forma drástica los papeles y los procesos manuales.

En propias empresas, la creciente complejidad de las relaciones con el entono y el elevado número de transacciones realizadas como parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP (Enterprise Resource Planning), o paquetes software de gestión integral.

Por ello, en la actualidad las actividades cotidianas de las empresas y de las distintas administraciones públicas e, incluso, las muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan, y en especial, de su seguridad

De ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad en la información en una organización. La proliferación de los virus y código malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidente de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión.

Se puede definir la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Desde un punto de vista más amplio, en la norma ISO/IEC 17799 se define la Seguridad de la Información como la preservación de su confidencialidad, integridad y su disponibilidad (medidas conocidas por su acrónimo “CIA” en inglés “Confidentiality, Integrity, Availability”)

Figura 1: Seguridad de la Información según la norma ISO/IEC 17799

Dependiendo de tipo de información manejada y los procesos realizados por la organización, ésta podrá conceder más importancia a garantizar la confidencialidad, la integridad o la disponibilidad de los activos de información.

Entre los principales objetivos de la Seguridad Informática podríamos destacar los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos

Para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación: [6]

Plano Humano

- Sensibilización y formación.
- Funciones, obligaciones y responsabilidades del personal.
- Control y supervisión de los empleados.

Plano Técnico

- Selección, instalación, configuración y actualización de soluciones HW (Hardware) y SW (Software)
- Criptografía.
- Estandarización de productos.
- Desarrollo seguro de aplicaciones.

Organización

- Políticas, Normas y Procedimientos.
- Planes de Contingencia y respuestas a Incidentes.
- Relaciones con terceros (clientes, proveedores)

Legislación

Cumplimiento y adaptación a la legislación vigente

- LOPD (Ley Orgánica de Protección de Datos), LSSI (Ley de Servicios de Sociedad de Información), LGT (Ley General de Telecomunicaciones), Firma Electrónica, Código Penal, Propiedad Intelectual

Consecuencias de la falta de seguridad

En la actualidad el negocio y el desarrollo de las actividades de muchas organizaciones dependen de los datos e informaciones registradas en sus sistemas informáticos, así como el soporte adecuado de las Tecnologías de Información y las Comunicaciones para facilitar su almacenamiento, procesamiento, análisis y distribución. La eliminación de todas las transacciones de un día a una empresa podría ocasionarle más pérdidas económicas que sufrir un robo o un acto de sabotaje contra alguna de sus instalaciones, y por ello es necesario trasladar a los directivos la importancia de valorar y proteger la información de sus empresas.

A la hora de analizar las posibles consecuencias de la ausencia o de unas deficientes medidas de seguridad informática, el impacto total para la organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red, deberíamos tener en cuenta otros importantes perjuicios para la organización:

- Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos y redes
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos: costo de oportunidad por no poder utilizar estos recursos.
- Robo de información confidencial y su posible revelación a terceros no autorizados: fórmulas, diseños de productos, estrategias comerciales, programas informáticos, entre otros.
- Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes proveedores, contactos comerciales o candidatos de empleo, con las consecuencias que se derivan del incumplimiento de la legislación en materia de protección de datos.
- Posible impacto en la imagen de la empresa ante terceros: pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores.
- Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del servicio, perdida de oportunidad del negocio.
- Posibles daños a la salud de las personas, con pérdidas de vidas humanas en los casos más graves.
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar además posibles responsabilidades legales y la imposición de sanciones administrativas.

b. La continuidad del negocio

Las empresas son cada vez más conscientes de la necesidad de estar preparadas para responder ante todo tipo de desastres y situaciones catastróficas, como podrían ser los incendios, inundaciones, terremotos, consecuencias de huracanes, entre otros. Sin embargo, estas situaciones también se podrían producir debido a los daños ocasionados por sabotajes, robos o, incluso, por atentados terroristas.

Para la continuidad del negocio se debe definir un plan que especifique los objetivos y las prioridades a tener en cuenta por la organización en caso de un desastre que pueda afectar a la continuidad del negocio. Para ello, es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento del sistema informático de la organización, así como recuperar los datos, aplicaciones y servicios básicos que se utilizan como soporte al negocio de la organización:

- Disponibilidad de un Centro Alternativo o Centro de Reserva para ubicación de los principales recursos informáticos (servidores y bases de datos corporativas).
- Existencia de líneas de respaldo para las comunicaciones.
- Sistema de almacenamiento RAID en los servidores.
- Implantación de clusters de servidores con balanceo de carga.
- Herramientas para llevar a cabo la replicación de los documentos y las bases de datos, que puedan ser síncrona, asíncrona o periódica.

Asimismo, se tiene que definir un Plan de Recuperación de Negocio cuál va a ser la composición de un equipo de dirección que se encarga de coordinar todas las tareas de recuperación frente a un desastre, realizando esta labor desde un determinado centro de control, cuya ubicación también tiene que haber sido previamente especificada en el Plan de Recuperación.

Un elemento fundamental en la continuidad del negocio es la existencia de un centro alternativo, también conocido como centro de respaldo o centro de backup, si bien en la práctica sólo las grandes empresas podrán disponer de un local o edificio dedicado exclusivamente a esta misión. Este centro tendría que estar equipado con los equipos informáticos adecuados y contar con copias de seguridad de los datos más críticos para el negocio suficientemente actualizadas.

c. BCP y DRP

El Plan de recuperación ante desastres (DRP - Disaster Recovery Plan) y el Plan de continuidad del negocio (BCP - Business Continuity Plan) están diseñados ante un eventual desastre con el sistema informático. Ante una contingencia con el sistema informático, es necesario garantizar la protección de los datos. El desarrollo de este plan, le permitirá anticipar los riesgos a los que está expuesto su sistema informático en caso de desastres.

El plan de recuperación le permite conocer el equipo y el rol de cada uno de los que están a cargo del plan de recuperación, así como la lista de procedimientos a seguir.

El Plan de continuidad del negocio (BCP) es el último eslabón de la cadena y se aplica únicamente para proteger las aplicaciones que son vitales para la actividad de la empresa.
Los beneficios que trae consigo un BCP en una organización son:

- Minimiza las potenciales perdida económicas que pueden derivar de un Incidente de Seguridad no analizado.
- Reduce los riesgos potenciales de la Organización, a través del análisis de impacto.
- Claramente reduce significativamente las interrupciones de los Servicios.
- Por consecuencia asegura la estabilidad de la Organización y sus clientes
- Protege los activos de Información
- Minimiza el riesgo de tomas de decisiones erradas durante el acontecimiento de un evento
- Minimiza las responsabilidades legales

Algunos de los beneficios que podrá gozar una organización al hacer un “DRP”, a parte de los ahorros del esfuerzo, tiempo y dinero:

- Mantener la continuidad de los servicios relacionados con la TIC del negocio:
- Proteger al negocio de fallas generales en los servicios informáticos.
- Minimizar los riesgos generados por la falta de servicios.

- Garantizar el acceso de la información empresarial.
- Mantener la disponibilidad de los recursos informáticos.
- Minimizar la toma de decisiones erróneas al presentarse algún desastre.
- Dar atención continua a los clientes, proveedores, accionistas, colaboradores.
- Tener capacidad de recuperación exitosa.

La recuperación ante desastres se enfoca en el restablecimiento de los sistemas e infraestructura de TI que soportan los procesos de negocio críticos después de eventos de interrupción, mientras que la continuidad del negocio está orientada a la recuperación de los procesos de negocio críticos que son necesarios para la operación, por lo que no solo incluye lo anterior, sino también todos los demás aspectos operativos necesarios dentro de la organización. El DRP es un eslabón importante dentro del plan de continuidad del negocio, tal como se muestra en la siguiente figura:

Figura 2: Plan de continuidad del negocio

4. Desarrollo del trabajo

a. Investigación

I. Identificación del Negocio

Nombre de la empresa: Universidad Tecnológica de El Salvador

Misión:

La Universidad Tecnológica de El Salvador existe para brindar a amplios sectores poblacionales, innovadores servicios educativos, promoviendo su capacidad crítica y su responsabilidad social; utilizando metodologías y recursos académicos apropiados, desarrollando institucionalmente: investigación pertinente y proyección social, todo consecuente con su filosofía y su legado cultural.

Visión:

Ser reconocida como una de las mejores universidades privadas de la región, a través de sus egresados y de sus esmerados procesos institucionales de construcción y aplicación del conocimiento, proponiendo soluciones pertinentes a las necesidades de amplios sectores de la sociedad.

Valores:

- Compromiso agresivo
- Innovación permanente
- Respecto y pensamiento positivo
- Liderazgo institucional
- Solidaridad y transcendencia cultural
- Integridad

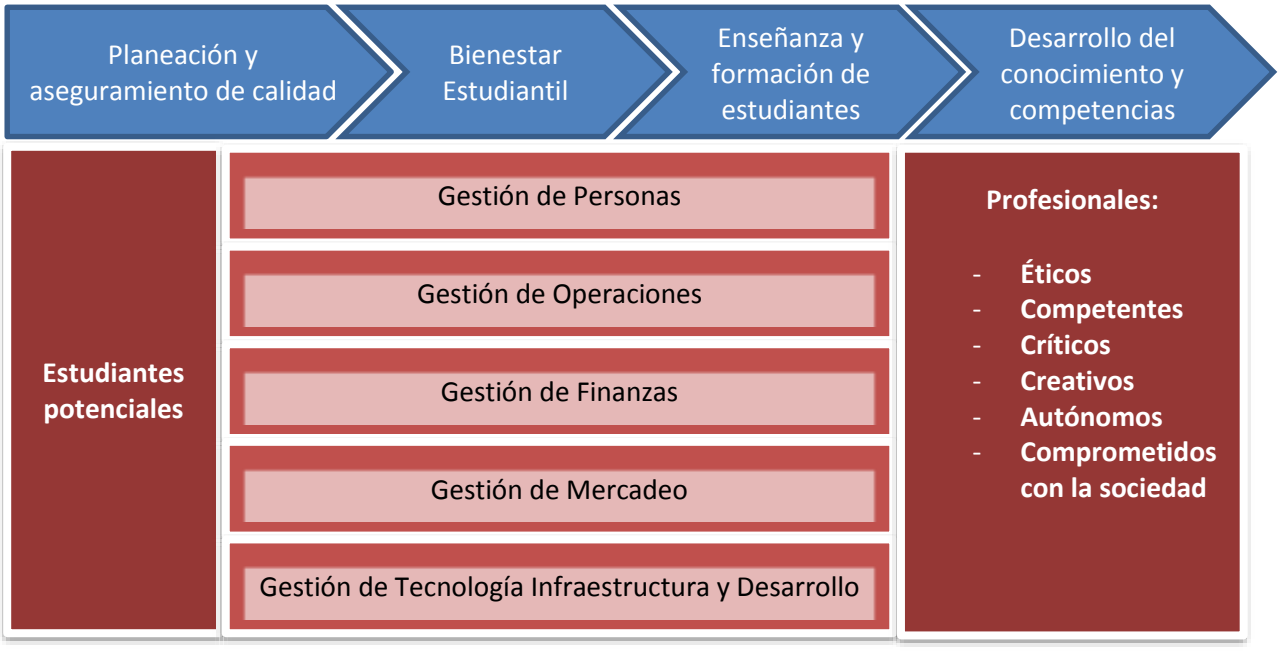
Política de calidad:

La política de calidad del Servicio de Calidad se orienta a conseguir la máxima satisfacción de los usuarios aplicando para ello los siguientes principios:

1. Planificar adecuadamente los procesos clave con el fin de conseguir su eficiente y eficaz realización.
2. Potenciar el desarrollo personal y profesional de las personas que constituyen el Servicio, como principal motor de excelencia de la Universidad en los servicios que presta.
3. Medir periódicamente los niveles de calidad percibidos por nuestros usuarios para mejorar continuamente nuestros servicios.

Nota: En este momento la UTEC está en proceso de redefinición de la política de calidad con la ayuda de la Universidad de Alicante, para someterse a una certificación de ANECA (Agencia Nacional de Evaluación de la Calidad y Acreditación). Para ello se ha conformado el SGCI (Sistema Gestión de la Calidad Interna)

Cadena de valor:



Principales partes interesadas (mencionando cuáles son sus intereses):

- Estudiantes : Empleabilidad
- Docentes : Experiencia y Empleabilidad
- Universidad : Reconocimiento internacional

FODA

II.

Fortalezas	Oportunidades
• Infraestructura física • Infraestructura tecnológica • Unidad de desarrollo educativo • Oferta académica definida • Modelo de proceso de enseñanza aprendizajes por competencias	• Educación virtual • Estudios de postgrados • Relación empresa universidad • Ubicación física
Debilidades	**Amenazas**
• Programas de retención de talentos • Internacionalización de programas de estudio • Certificación de la calidad de enseñanza aprendizaje	• Situación económica de país • Gobierno con la implementación de la Universidad Virtual • Huelgas • Obsolescencia de la infraestructura tecnológica

III. Lista de requisitos legales, normativos, contractuales y de otra índole

Requisito	Ley	Normativa	Convenios
Ministerio de Educación el Salvador	Educación superior	Acreditación de nivel superior	
Centro Nacional de Registros	Registro de comercio		
Ministerio de Hacienda	Tributación		
INCAE (Instituto Centroamericano de Administración de Empresas)			Marco de cooperación
Red latinoamericana			Cooperación universitaria
AUPRIDES			Carta entendimiento entre facultades
ITCR Costa Rica (Instituto Tecnológico de Costa Rica)			Transferencia de conocimiento
Universidad de Castilla la Mancha			Fomentar la investigación, la formación y estimular

			una colaboración internacional, basada en la igualdad y asistencia mutua
Universidad de Granada España			Intercambio de experiencias y conocimientos culturales, científicos y técnicos con intereses comunes
Universal Holding			Desarrollo de portal universitarios
Contrato Apha III – UTEC Universidad de Alicante			Promoción de internalización de Centroamérica
UTEC Panamericana			Cooperación para el fomento de la docencia, la investigación, la extensión universidad y la movilidad docente y estudiantil
Software Legal	Ley de propiedad intelectual		
Proveedores de Servicios		Contratos definiendo SLA – Service Leven Agreement	

IV. Lista de actividades

Esta lista incluye todas las actividades a ser consideradas en el Plan de Continuidad del Negocio:

1. **Infraestructura de Red (Habilitar el servidor en línea)**
    a. Encender el servidor de respaldo
    b. Instalación y configuración del Rol de Hyper-V
    c. Configuración de la infraestructura de red virtual
    d. Pruebas de conectividad
2. **Recuperación de virtuales**
    1. Creación de máquinas virtuales a partir de discos duros virtuales respaldados
    2. Verificación de conectividad en la red
    3. Verificación de servicios de red de la máquina virtual
    4. Verificación de los sistemas en producción Base de Datos y Servicios WEB
3. **Monitoreo y pruebas**
    1. Pruebas de acceso a los sistemas desde la LAN (Local Area Network)
    2. Pruebas de acceso a los sistemas desde la WAN (Wide Area Network) e Internet
    3. Anunciar que los sistemas están disponibles

4. **Restauración de Bases de Datos (aplica si el entorno virtual no se puede recuperar)**
    1. Ejecutar el software DPM (Data Protection Manager) para la recuperación de las bases de datos
    2. Seleccionar el destino de la recuperación de los datos
    3. Recuperar los datos
    4. Preparar la configuración de la base de datos para acceder a los datos recuperados
    5. Realizar pruebas de acceso a la información
    6. Configurar el servidor WEB para publicación de los sistemas
    7. Verificar que los usuarios pueden acceder a la información

V. Prioridades de recuperación para las actividades

Esta lista define los períodos máximos tolerables de interrupción (interrupciones máximas aceptables) para cada actividad y establece prioridades en consecuencia.

Actividad	Interrupción Máxima	Prioridades en Consecuencia
Habilitar el servidor en línea	20 Min	Encender Servidor Instalación y configuración del Rol de Hyper-V Configuración de la infraestructura de red virtual Pruebas de conectividad
Recuperación de virtuales	25 min	Creación de máquinas virtuales a partir de discos duros virtuales respaldados Verificación de conectividad en la red Verificación de servicios de red de la máquina virtual Verificación de los sistemas en producción Base de Datos y Servicios WEB
Monitoreo y pruebas	30 min	Pruebas de acceso a los sistemas desde la LAN Pruebas de acceso a los sistemas desde la WAN e Internet Anunciar que los sistemas están disponibles
Restauración de la Base de Datos	60 min	Ejecutar el software DPM para la recuperación de las bases de datos

		Seleccionar el destino de la recuperación de los datos Recuperar los datos Preparar la configuración de la base de datos para acceder a los datos recuperados Realizar pruebas de acceso a la información Configurar el servidor WEB para publicación de los sistemas Verificar que los usuarios pueden acceder a la información

VI. Objetivos de tiempo de recuperación

Esta lista define los objetivos de tiempo de recuperación para cada actividad en Universidad Tecnológica de El Salvador:

Actividad	Objetivos
Habilitar el servidor en línea	Encender, instalar, configurar la infraestructura de red, junto a las pruebas de conectividad que permitan tener una infraestructura lista para instalar las aplicaciones.
Recuperación de virtuales	Tener los ambientes productivos con las aplicaciones funcionando correctamente.
Monitoreo y pruebas	Realizar pruebas de acceso a los sistemas desde la LAN, pruebas de acceso a los sistemas desde la WAN e Internet para anunciar que los sistemas están disponibles.
Restauración de la Base de Datos	Preparar la configuración de la base de datos para acceder a los datos recuperados, dejando la información accesible para las aplicaciones.

VII. Análisis del Impacto en el Negocio

Proceso crítico del negocio	Responsable								
	IP	Descripción	Tipo	Aplicativo	Infraestructura	RTO	Comentario RTO	RPO	Criticidad
Base de datos	192.168.1.7	Base de datos de Finanzas, RRHH, repositorio central	APP	propio	Propio	1 día	Es el más crítico, por tanto, únicamente se pueden perder 4 horas de información. Recuperación automática.	3 horas	Alto
Sistema Empresarial	192.168.1.5	Sistema WEB para acceso a los sistemas empresariales	APP	propio	Propio	1 día	Es el más crítico, alimenta el BD empresarial, por tanto, únicamente se pueden perder 4 horas de información. Recuperación manual.	3 horas	Alto
Navegación en Internet	190.45.24.0 /27	Habilita las conexiones y accesos en línea	TCO	Outsourcing	Outsourcing	1 día	Es crítico para habilitar los servicios externos. Recuperación automática.	3 horas	Mediano
Pagos en línea	192.168.1.8	Pago puntoxpress, pago en línea	APP	propio	Propio	1 día	Luego de levantar las aplicaciones y la conexión a internet se procede a levantar el servicio de pagos en línea. Recuperación manual	3 horas	Mediano
Cortafuegos	192.168.1.1	Firewall que controla el tráfico de Internet entrante y saliente	TCO	Outsourcing	Outsourcing	1 día	Permite la navegación de Internet a los usuarios y servidores por lo tanto los servicios deben estar	4 horas	Mediano

Proceso crítico del negocio	Responsable								
	IP	Descripción	Tipo	Aplicativo	Infraestructura	RTO	Comentario RTO	RPO	Criticidad
							disponible al usuario interno y externo		
Equipos de la red cableada (router, switch, etc.)	192.168.10.1 -20	Componentes que habilitan la interconexión entre los equipos	TCO	propio	Propio	1 día	Infraestructura critica que permite brindar la conectividad de loa servicios y aplicaciones	8 horas	Alto
Sistema académico	192.168.1.6	Sistema WEB para acceso de aplicaciones estudiantil	APP	propio	Propio	2 días	Es crítico, por tanto, únicamente se pueden perder 8 horas de información. Recuperación manual.	8 horas	Mediano
Respaldos	192.168.1.4	Bases de datos de respaldo, aplicaciones	APP	propio	Propio	2 días	Es critico debido a que los respaldos deben están disponibles cuando se necesitan	8 horas	Alto
Servicios bancarios (Prestamos, Estados de Cuentas, TC)	192.168.1.3	Sistema que contiene los servicios bancarios de la universidad	APP	propio	Propio	2 días	Es critico debido a que los servicios bancarios permiten tener el estado actual de los préstamos y servicios de la UTEC	8 horas	Mediano

Proceso crítico del negocio	Responsable								
	IP	Descripción	Tipo	Aplicativo	Infraestructura	RTO	Comentario RTO	RPO	Criticidad
Servidores (Base de Datos, WEB, Active Directory, DNS)	192.168.1.2 – 10	Granja de Servidores donde se almacenan los servicios más críticos	SER	propio	Propio	3 días	Todos los servidores son críticos por que desempeñan una función fundamental en cada sistema	8 horas	Alto
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, Convenios)	192.168.1.110	Documentos relacionados a los proyectos, planes y nuevas ideas	REP	propio	Propio	3 días	Documentación sensible para la organización que debe estar disponible cuando se necesite	24 horas	Mediano
Servicio de Internet	181.54.88.0 /28	Habilita las conexiones y accesos en línea	TCO	Outsourcing	Outsourcing	1 día	Es crítico para habilitar el servicio de Internet a los Servidores de contingencia	3 horas	Mediano
Servidor HP NAS (Network Access Server)	192.168.2.3	Servidor de almacenamiento que contiene los respaldos de las máquinas virtuales	SER	propio	Propio	1 día	Es critico debido a que contiene los respaldos de las máquinas virtuales, base de datos y servidores web	3 horas	Alto
Servidor DELL	192.168.2.4	Servidor implementado para correr las máquinas virtuales críticas	SER	propio	Propio	1 día	Es crítico debido a que se utiliza para hacer funcionar las máquinas virtuales	3 horas	Alto

Proceso crítico del negocio	Responsable								
	IP	Descripción	Tipo	Aplicativo	Infraestructura	RTO	Comentario RTO	RPO	Criticidad
Servidor DNS (Domain Name Service)	192.168.2.2	Servidor utilizado para realizar la publicación de los sitios si el principal falla	SER	propio	Propio	1 día	Es crítico para publicar los servicios hacia el exterior de la LAN	3 horas	Mediano
WEB Services Virtual Private Network	192.168.2.5	Servidor WEB habilitados para configurar los pagos automáticos de puntoxpress	APP	propio	Propio	1 día	Es critico por qué se necesita para reactivar los pagos en línea de los alumnos	3 horas	Mediano
Cortafuegos VPN	192.168.2.1	Configuración en el cortafuegos para los pagos en línea a través de una nueva VPN	TCO	Outsourcing	Outsourcing	1 día	Es crítico porque permite la configuración del canal seguro para los pagos	3 horas	Mediano
Servidor TAPE Backup	192.168.2.7	Servidor utilizado para realizar respaldos a cinta	SER	propio	Propio	1 día	Es critico por que sobre este servidor se encuentra la plataforma de respaldos	8 horas	Alto
Software Veem Backup	192.168.2.6	Software utilizado para hacer respaldos a NAS y Cinta	SER	propio	Propio	1 día	Es critico porque es utilizado para realizar los respaldos de las máquinas virtuales	8 horas	Alto
Cintas de Respaldo (LTO4)		Contiene el respaldo de las máquinas virtuales, base de datos y servidores Web	INT	propio	Propio	2 días	Es crítico para la recuperación de los respaldos, si en todo caso fallan los respaldos almacenados en la NAS	24 horas	Alto

VIII. Resultados

a) Análisis de factores de riesgo

Se ha realizado un análisis de riesgo en base a la categorización de activos de información relacionado con Datos, Sistemas y Personal, en cada una de ella se detalla una serie de amenazas que pueden impactar en el negocio y los servicios de TI.

Las tres categorías de activos de información son evaluadas a partir de los siguientes tipos de amenazas

1. Actos originados por la criminalidad común y motivación política
    a. Allanamiento (ilegal, legal)
    b. Persecución (civil, fiscal, penal)
    c. Orden de secuestro / detención
    d. Sabotaje (ataque físico y electrónico)
    e. Daños por vandalismo
    f. Extorsión
    g. Fraude / Estafa
    h. Robo / Hurto (físico)
    i. Robo / Hurto de información electrónica
    j. Intrusión a la red interna
    k. Infiltración
    l. Virus / Ejecución no autorizada de programas
    m. Violación de derechos de autor

2. Sucesos de Origen físico
    a. Incendio
    b. Inundación / Deslave
    c. Sismo
    d. Polvo
    e. Falta de ventilación
    f. Electromagnetismo
    g. Sobrecarga eléctrica
    h. Falla de corriente (apagones)
    i. Falla de sistemas / Daños disco duro

3. Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
    a. Falta de inducción, capacitación y sensibilización sobre riesgos
    b. Mal manejo de sistemas y herramientas
    c. Utilización de programas no autorizados / software 'pirateado'
    d. Falta de pruebas de software nuevo con datos productivos
    e. Perdida de datos
    f. Infección de sistemas a través de unidades portables sin escaneo
    g. Manejo inadecuado de datos críticos (codificar, borrar, etc.)
    h. Unidades portables con información sin cifrado
    i. Transmisión no cifrada de datos críticos
    j. Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
    k. Compartir contraseñas o permisos a terceros no autorizados

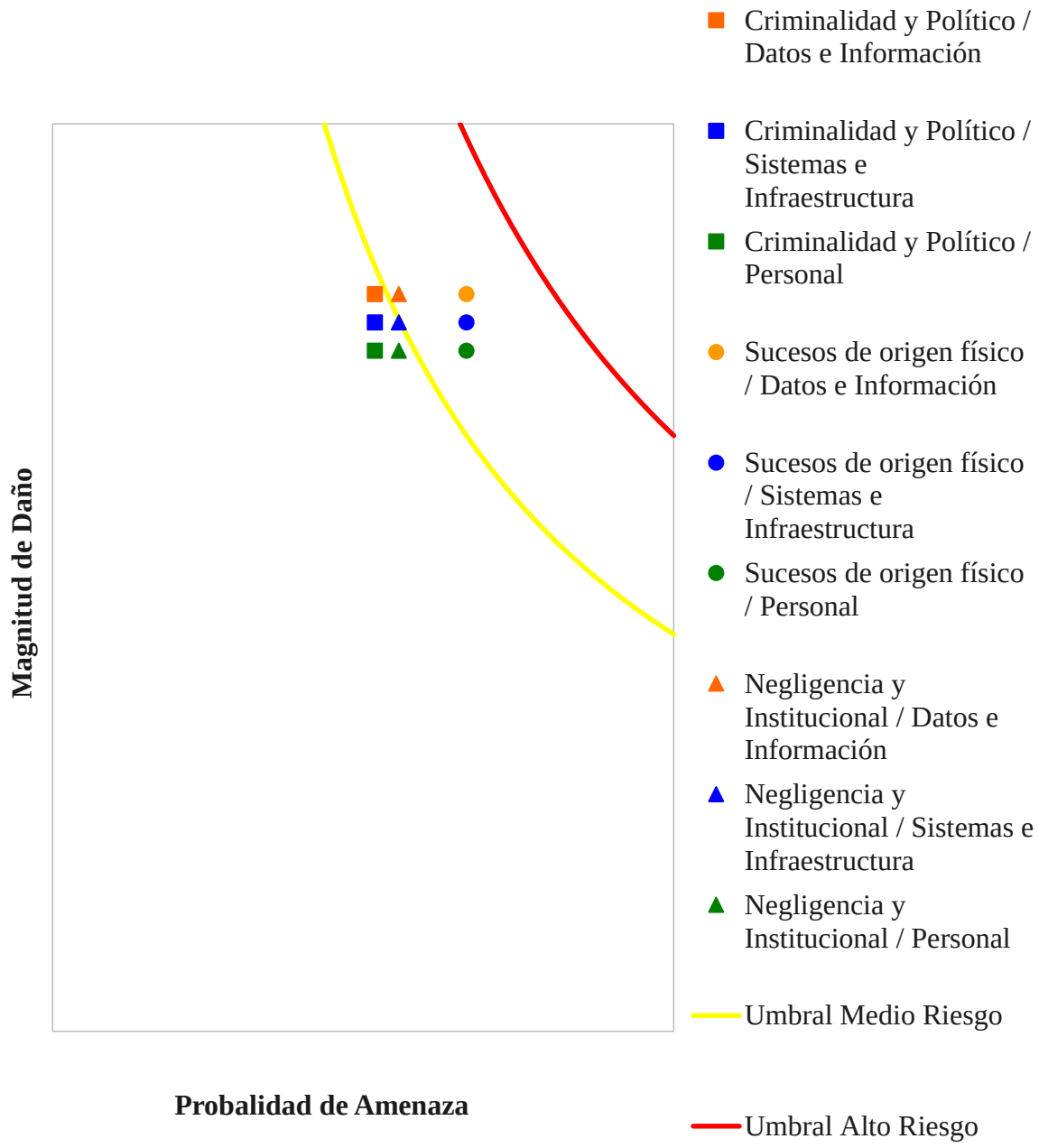
l. Transmisión de contraseñas por teléfono
m. Exposición o extravío de equipo, unidades de almacenamiento, etc.
n. Sobrepasar autoridades
o. Falta de definición de perfil, privilegios y restricciones del personal
p. Falta de mantenimiento físico (proceso, repuestos e insumos)
q. Falta de actualización de software (proceso y recursos)
r. Fallas en permisos de usuarios (acceso a archivos)
s. Acceso electrónico no autorizado a sistemas externos
t. Acceso electrónico no autorizado a sistemas internos
u. Red cableada expuesta para el acceso no autorizado
v. Red inalámbrica expuesta al acceso no autorizado
w. Dependencia a servicio técnico externo
x. Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
y. Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
z. Ausencia de documentación

La UTEC establece cuatro categorías de impacto. 1=Insignificante, 2= Bajo, 3= Mediano, 4= Alto, y establece un valor mínimo y un valor máximo para determinar la categoría del riesgo.

Valoración	Escala	Valor_min	Valor_max	Líneas	Umbral Medio Riesgo	Umbral Alto Riesgo
Ninguna	1	1	3		**7**	**10.5**
Baja	2	4	6	**x**	**y**	**Y**
Mediana	3	8	9	1.0	7.0	10.5
Alta	4	12	16	1.1	6.4	9.5
				1.2	5.8	8.8
				1.3	5.4	8.1
				1.4	5.0	7.5
				1.5	4.7	7.0
				1.6	4.4	6.6
				1.8	4.0	6.0
				1.8	3.9	5.8
				1.9	3.7	5.5
				2.0	3.5	5.3
				2.1	3.3	5.0
				2.2	3.2	4.8
				2.3	3.0	4.6
				2.4	2.9	4.4
				2.5	2.8	4.2
				2.6	2.7	4.0
				2.7	2.6	3.9
				2.8	2.5	3.8
				2.9	2.4	3.6
				3.0	2.3	3.5
				3.1	2.3	3.4

				3.2	2.2	3.3
				3.3	2.1	3.2
				3.4	2.1	3.1
				3.5	2.0	3.0
				3.6	1.9	2.9
				3.7	1.9	2.8
				3.8	1.8	2.8
				3.9	1.8	2.7
				4.0	1.8	2.6

Factor	X	Y
Criminalidad y Político / Datos e Información	2.076923077	3.25
Criminalidad y Político / Sistemas e Infraestructura	2.076923077	3.125
Criminalidad y Politico / Personal	2.076923077	3
Sucesos de origen físico / Datos e Información	2.666666667	3.25
Sucesos de origen físico / Sistemas e Infraestructura	2.666666667	3.125
Sucesos de origen físico / Personal	2.666666667	3
Negligencia e Institucional / Datos e Información	2.230769231	3.25
Negligencia e Institucional / Sistemas e Infraestructura	2.230769231	3.125
Negligencia y Institucional / Personal	2.230769231	3



b) Análisis de Riesgo promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia e Institucional
Magnitud de Daño	Datos e Información	6.8	8.7	7.3
	Sistemas e Infraestructura	6.5	8.3	7.0
	Personal	6.2	8.0	6.7

Para este análisis luego de tabular la información recopilada en el Reporte de Evaluación y Análisis de Riesgo [7], se obtuvieron los resultados mostrados en los cuadros anteriores.

Al graficar los valores resultantes para medir la probabilidad de que las amenazas asociadas como criminalidad y político, Sucesos de origen físico y negligencia e Institucional puedan ocurrir asociados a la magnitud del daño sobre datos de información, sistemas e infraestructura y personal. De los datos evaluados estadísticamente aplicando valores a los factores de riesgo asociados a las amenazas se obtiene el umbral de riesgo medio y alto, lo que establece la frontera entre lo menos probable, lo medianamente probable y lo más probable.

Al graficar la magnitud del daño contra la probabilidad de amenazas se obtiene que los sucesos de origen físico asociados al daño relacionado con datos e información, infraestructura y personal, son los que tienen la mayor probabilidad de que esa amenaza se concrete, convirtiéndose en un riesgo potencialmente alto.

Por otro lado la negligencia institucional asociada a su afectación sobre los datos e información, sistemas e infraestructura y personal, son los que tienen una probabilidad media al encontrarse sobre el umbral medio del riesgo. La probabilidad de que la criminalidad y el entorno político puedan ocasionar un daño a los datos e información, sistemas e infraestructura y personal son prácticamente medio pero en una mínima diferencia menor al anteriormente descrito.

IX. Alcance del proyecto

El presente proyecto esta enfocado en la definición e implantación de un plan de recuperación ante desastres enfocado al departamento de TI, la idea fundamental de esta invesitgación es:

- Identificar los activos de información críticos para TI
- Definir estrategias de recuperación alineados a la evaluación de impacto del negocio
- Definir claramente las prioridades de recuperación ante un incidente de seguridad
- Definir un equipo de recuperación ante desastres que permita tomar el mando de las operaciones ante un incidente de seguridad
- Documentar los canales de comunicación involucrados en un evento de seguridad
- Definir los roles y funciones del personal técnico, áreas administrativas y proveedores, acciones a seguir en una situación que comprometa la disponibilidad de servicios y sistemas información

X. Conclusiones

Corroborando lo anterior, el análisis de impacto del negocio - BIA, podrán ayudar a identificar dentro del marco de la seguridad de la información, las vulnerabilidades potenciales de la UTEC, podrá delimitar las actividades críticas que afectan el negocio y ayudará a las entidades a definir los planes adecuados de recuperación de los servicios que afectan el objeto del negocio; de otro lado las entidades podrán tener

mayor información sobre el estado de los procesos contribuyendo favorablemente a mejorar la competitividad y proyectar estrategias adecuadas para una recuperación exitosa de la información.

b. Planteamiento del plan de continuidad

Plan de recuperación de desastres

1.0 Generalidades

El presente Plan de Recuperación de Desastres de TI será desarrollado con base en los siguientes supuestos:

La recuperación se realizará en el Centro de Datos alterno a ser definido por la UTEC.
La infraestructura de contingencia debe encontrase operativa para lo cual el centro de datos alterno debe encontrase en línea y operando adecuadamente, lo cual debe ser controlado a través del monitoreo continuo.

El Plan de Recuperación de Desastres no cubre ningún acontecimiento que deje inoperable simultáneamente tanto al centro de datos primario como al alterno.

Al momento del desastre todos los participantes del Equipo de Recuperación de Desastres se encontrarán disponibles para las tareas encomendadas.

La documentación técnica se encontrará actualizada y disponible.

El plan ha sido distribuido, mantenido y actualizado; y el personal se encuentra capacitado para su uso.

El tipo de contingencia considerado para el presente trabajo es la destrucción total del Centro de Datos de la sede central de la UTEC ubicado en Calle Arce, casa 455, San Salvador.

El evento de desastre puede referirse a desastres naturales (mal tiempo, terremoto, etc.), por fallas tecnológicas (incendios, fallas eléctricas, inundaciones, entre otros) o por acontecimientos sociales tales como sabotaje o huelgas.

Los equipos de comunicación y los equipos de procesamiento de información ubicados en el Centro de Datos de la sede central quedan inhabilitados para realizar sus funciones normales.

Las operaciones deben ser restablecidas en un Centro de Datos alterno a ser definido por la UTEC.

1.1 Equipos de recuperación de desastres

Esta sección identifica a los equipos de personas involucradas en el esfuerzo de recuperación del evento de desastre y sus responsabilidades asociadas. Las pautas consideradas para la conformación de estos equipos han sido los siguientes:

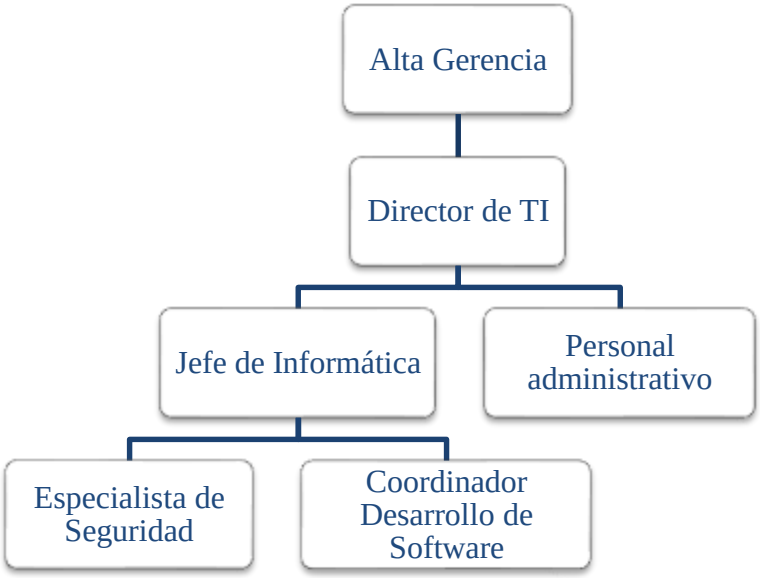
- Todo equipo debe estar conformado por un líder y un alterno.

- Ninguna persona debe estar participando en más de un equipo cuyas tareas, durante la recuperación de un desastre, sean concurrentes.

- Todas las personas identificadas en el Equipo de Recuperación de Desastres, deben conocer las responsabilidades que tienen que asumir. De esta manera se minimiza las posibilidades de

inoperatividad de los equipos debido a la ausencia de sus integrantes y/o al desconocimiento de sus responsabilidades.

Se ha conformado el siguiente Equipo de Recuperación de Desastres TI:



Coordinador de Recuperación de TI (Director de TI)
Implementación de las Normas y Gestión de Seguridad de Información en el Centro de Datos de la UTEC.

Tiene asignado las siguientes responsabilidades:

1. Encargado de coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
2. Tomar la decisión de activar el Plan de Recuperación de Desastres TI.
3. Proveer liderazgo general a los equipos de personas involucrados en el proceso de recuperación.
4. Guiar al personal necesario durante la situación de contingencia y supervisar sus actividades.
5. Evaluar la extensión del desastre y sus consecuencias potenciales sobre la infraestructura tecnológica.
6. Notificar, y mantener enterados, a la Alta Dirección acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
7. Documentar los eventos de desastres y las actividades realizadas para lograr la recuperación de las operaciones.
8. Monitorear la ejecución de los procedimientos de recuperación y asegurar que el cronograma y las prioridades establecidas se cumplan.
9. Supervisar / vigilar la recuperación de infraestructura de TI en el Centro de Datos alterno.
10. Contactar a los proveedores para el hardware de reemplazo para sistemas afectados.
11. Asistir a las reuniones del estado de la recuperación y comunicar al personal las necesidades y prioridades.
12. Declarar el evento de término de la ejecución de las operaciones del Plan de Recuperación de Desastres, cuando las operaciones del Centro de Datos primario hayan sido restablecidas.

Coordinador de Infraestructura Tecnológica (Jefe de Informática)

Tiene asignado las siguientes responsabilidades:

4. Evaluar el daño en la plataforma tecnológica básica de la UTEC, coordinar y dirigir las acciones necesarias para su recuperación en el Centro de Datos alterno y su restauración a condiciones normales.
5. Recuperar la plataforma base de los sistemas críticos de la UTEC de acuerdo a la prioridad de recuperación definida.
6. Asegurar que toda la documentación relacionada a estándares, operaciones, registros vitales, programas de aplicación, etc., se encuentren almacenados en un ambiente seguro.
7. Mantener los procedimientos de operaciones actualizados para soportar cualquier sistema (aplicativo) fuera de la UTEC.
8. Mantener actualizado y en un lugar seguro la configuración del sistema alterno.
9. Supervisar la instalación del hardware y software base, así como configurar las últimas versiones de los sistemas operativos, en los ambientes del Centro de Datos alterno.
10. Recuperar las cintas de respaldo del almacenaje externo y entregarlas al sitio de recuperación.
11. Habilitar los procedimientos de backup y restablecer los controles normales de operación en el Centro de Datos primario luego de restablecidos los servicios en dicho ambiente.
12. Mantener, recuperar y/o restaurar los enlaces de red y comunicaciones entre la sede principal de la UTEC y el Centro de Datos alterno.
13. Mantener actualizado el diagrama actual de conexiones de dispositivos, el diagrama alterno y el inventario de equipos de telecomunicaciones a ser usado en caso de emergencia.
14. Evaluar el daño en las redes de comunicación de datos y coordinar las estrategias de recuperación con los proveedores de servicios.

Coordinador de Sistemas de Información (Coordinador Desarrollo de Software)

Tiene asignado las siguientes responsabilidades:

1. Levantar los servicios de Base de Datos, con la data restaurada, válida, íntegra, probada y disponible para los usuarios, en el Centro de Datos alterno.
2. Informar a los usuarios hasta qué momento se tienen datos confiables.
3. Velar por el funcionamiento adecuado de las Bases de Datos.
4. Supervisar el correcto funcionamiento de los diferentes sistemas de aplicación.
5. Asegurar que la documentación de los aplicativos en producción se mantenga actualizada y que la documentación de operaciones contemple las actividades de respaldo de los aplicativos
6. Definir las actividades de recuperación para los casos de pérdida de información y/o contingencia.
7. Establecer los requerimientos de sistema operativo, archivos utilitarios, librerías y documentación indispensable para la operatividad de los aplicativos.
8. Mantener informados a los usuarios clave del negocio acerca del avance de las actividades de recuperación y el restablecimiento de cada uno de los procesos críticos que son de su responsabilidad.
9. Validar con el usuario del negocio acerca del adecuado desempeño de las aplicaciones posterior al restablecimiento de las operaciones en el Centro de Datos alterno.

Coordinador de Seguridad de Información (Especialista de Seguridad)

Tiene asignado las siguientes responsabilidades:

1. Supervisar el cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de contingencia.
2. Coordinar con los encargados de Seguridad Física, la evaluación del daño en la sede del Centro de Datos primario.

1.2 Administración del plan de recuperación de desastres.

a. Coordinador de Administración

Tiene asignado las siguientes responsabilidades:

1. Encargado de supervisar y dar a apoyo al desarrollo de las distintas tareas ejecutadas por los comités que conforman al equipo de administración.
2. Supervisar y colaborar en la ejecución del Plan de Distribución.

b. Comité de distribución

Tiene asignado las siguientes responsabilidades:

1. Garantizar la difusión del plan entre los miembros del equipo y mantener vigente el Plan de Distribución.
2. Asegurar que los miembros del equipo de recuperación de desastres siempre dispongan de, como mínimo, dos copias actualizadas del plan, una de las cuales debe mantenerse en el lugar del trabajo, siendo las demás almacenadas en algún otro lugar seguro externo a la UTEC.

   El objetivo del Plan de Distribución es entregar a la Universidad Tecnológica de El Salvador una estructura, dedicada a difundir y mantener vigente las medidas a considerar en caso de desastres. Este plan considera las siguientes acciones:

   - Elaborar y mantener actualizada la lista de los integrantes que deben poseer un ejemplar del Plan de Recuperación de Desastres TI.
   - Distribuir el ejemplar del Plan de Recuperación de Desastres TI.
   - Llevar un control de los ejemplares distribuidos y la versión de los mismos.
   - Entregar las nuevas modificaciones al momento de ser aprobadas, de tal forma que el Plan de Recuperación de Desastres TI se mantenga actualizado y se encuentre vigente para su aplicación.

   Las normas y políticas definidas por el Comité de Distribución deberán ser aprobadas por el Coordinador de Recuperación de TI antes de ser ejecutadas.

c. Comité de Entrenamiento

Tiene asignado las siguientes responsabilidades:

1. Velar por la definición y cumplimiento oportuno del Plan de Entrenamiento y Capacitación de los procedimientos de recuperación de TI.
2. Efectuar la planificación de los entrenamientos y asimismo, notificar a los participantes e instructores, acerca de los cronogramas y alcance de las pruebas establecidas.

   Plan de Entrenamiento:
   Está compuesto por un conjunto de actividades orientadas a entrenar al personal de la UTEC sobre cómo actuar frente a la presencia de una contingencia informática. Este plan se compone de las siguientes partes:

   1. Preparación de los instructores.

2. Definición del lugar, calendario y temario de entrenamiento.
3. Diseño de la lista de participantes.
4. Determinación de los requerimientos sobre el material para el entrenamiento.
5. Ejecución del entrenamiento supervisado por los instructores.
6. Evaluación de los participantes.

d. Comité de Pruebas (Especialista de Seguridad)

Tiene asignado las siguientes responsabilidades:

1. Supervisar y dar apoyo durante la ejecución de las pruebas, garantizando la ejecución de las mismas en los tiempos planeados.
2. Registrar los resultados de las pruebas y participar activamente en las pruebas a los sistemas de aplicación críticos.
3. Apoyar al personal de las líneas de negocio involucradas en la ejecución de las pruebas.

No importa cuán bien diseñado y planificado parezca estar el Plan de Recuperación de Desastres TI, una prueba realista puede revelar las áreas que requieren mayor atención. Si los resultados de la prueba resultan sin defectos, se debe examinar la adecuación y realismo de las pruebas. La mayoría de los componentes del plan deben ser probados y actualizados basándose en los resultados de cada prueba. Es importante que cada componente sea probado individualmente. Las pruebas pueden ser disruptivas, por tanto, se requiere el apoyo por parte de la Alta Dirección para asegurar la disponibilidad de una cantidad suficiente de recursos. No se recomienda probar el plan en conjunto debido a la necesidad intensiva de recursos, lo cual puede afectar las operaciones normales de la UTEC

e. Plan de pruebas

Este plan está compuesto, de una serie de actividades orientadas a mantener actualizado y vigente el Plan de Recuperación de Desastres TI. Estas pruebas están enmarcadas dentro de un calendario de pruebas, y se compone de las siguientes partes:

1. Definir el propósito de la prueba.
2. Definir la prueba.
3. Designar el equipo de prueba.
4. Estructurar los aspectos a probar.
5. Ejecutar las pruebas.
6. Analizar los resultados y modificar el Plan de Recuperación de Desastres TI, si fuese necesario.

f. Estrategias de la prueba

Existen varias estrategias que pueden ser adoptadas para probar el plan:

Tipo de prueba	Descripción
Prueba de Recorrido	El objetivo de esta prueba es hacer seguimiento a los documentos del plan disponibles para validar su adecuada definición y factibilidad de aplicación en la UTEC.

Verificación Manual	El objetivo de esta prueba es asegurar la disponibilidad de los materiales de recuperación requeridos según se estableció en el plan. Esta prueba requiere revisar toda la data requerida, suministros y/u otras copias impresas de documentos que se encuentran actualmente respaldados y correctamente resguardados externamente.
Ensayo Estructurado	El objetivo de esta prueba es liderar el equipo hacia una recuperación simulada a fin de determinar la suficiencia del plan. La prueba se debe conducir como sigue: Todos los líderes de equipo se reúnen en una habitación donde se les hará entrega del escenario a probar. Cada uno debe trabajar sus procedimientos de recuperación prestando particular atención en la interacción con los otros equipos. Los puntos identificados se anotarán y se les hará seguimiento.
Convocatoria no anunciada del Equipo de Recuperación TI	El objetivo de esta prueba es asegurar que la lista de equipos de movilización de recuperación se encuentre al día y que los equipos puedan ser movilizados en el momento requerido. Esta prueba debe ser conducida en tiempos diferentes (fuera y durante horas de trabajo) a manera de identificar cualquier defecto en el plan.
Prueba Paralela	El objetivo de la prueba paralela es verificar el correcto funcionamiento del Centro de Datos alterno, validando que los equipos y aplicaciones funcionen correctamente, soporten la carga de trabajo estimada en contingencia y que se cumpla con los tiempos estimados de recuperación. Esta prueba se realiza solo en el Centro de Datos alterno sin afectar las operaciones del Centro de Datos primario. Al igual que en las otras pruebas se deben tomar notas de fallas y posibles mejoras identificadas para poder actualizar y mejorar el plan. Se debe involucrar a personal de las áreas de negocio para que las pruebas incluyan la aprobación y observaciones de los mismos con respecto a sus expectativas de funcionalidad y rendimiento.
Prueba Total	Al igual que en la prueba paralela, se busca verificar el correcto funcionamiento del Centro de Datos alterno, sin embargo, la prueba total es más completa, e incluye la desactivación del Centro de Datos primario para mayor realismo de la prueba. Este tipo de pruebas deben realizarse en momentos de carga de trabajo baja para el negocio y de preferencia en fines de semana largos, del mismo modo se debe involucrar al personal de TI y personal vital involucrado de las áreas de negocio.

g. Comité de Mantenimiento

Tiene asignado las siguientes responsabilidades:

1. Considerar un conjunto de procedimientos de mantenimiento debidamente formalizados y documentados.
2. Analizar el impacto que tiene cualquier cambio en el ambiente informático sobre el Plan de Recuperación de Desastres TI y proceder a su actualización.

3. Coordinar con el Comité de Distribución y Comité de Pruebas para la actualización de sus respectivos procedimientos, de manera que tengan en cuentan los cambios realizados al Plan de Recuperación de Desastres TI.
4. Un Plan de Recuperación de Desastres TI se mantiene con mayor facilidad si los cambios en el negocio y/o en el ambiente de procesamiento de datos se registran y actualizan inmediatamente en el plan. Es esencial una revisión del plan para asegurar que refleje los objetivos de la organización, las funciones clave del negocio, los procesos y recursos correspondientes.
5. El mantenimiento del plan es de gran importancia para cubrir el alcance de lo que se va a restaurar y de las aplicaciones críticas que intervienen en los procesos de recuperación. Esto quiere decir que se debe tener actualizado y sincronizado el plan de prueba y de implantación de acuerdo con los cambios que surjan en el ambiente de sistemas.

h. Plan de Mantenimiento:

Las actividades contempladas en el Plan de Mantenimiento son las siguientes:

1. Notificar el cambio al Coordinador de Recuperación de TI.
2. Analizar la infraestructura tecnológica de la UTEC, contemplando los siguientes aspectos:
   - Desarrollo e implantación de nuevas aplicaciones.
   - Migración de sistemas.
   - Incorporación de nuevas plataformas tecnológicas.
3. Evaluación de los mecanismos de seguridad física y lógica. De esta forma, se estará verificando el normal funcionamiento de los instrumentos que controlan estos accesos.
4. Evaluar permanentemente mecanismos alternativos e incorporar nuevas tecnologías, para así incrementar la seguridad física y lógica.
5. En caso de existir algún cambio físico en las instalaciones de la UTEC, este cambio debe ser evaluado y analizado antes de realizar el traslado, se tiene que considerar si el nuevo ambiente reúne los mecanismos de control de seguridad física y ambiental.
6. Si producto de estas revisiones y cambios, resultan en adecuaciones al plan, se tiene que considerar los siguientes puntos:
   - Modificar el Plan de Recuperación de Desastres TI.
   - Coordinar con los responsables del Comité de Distribución y Comité de Pruebas.
   - Llevar a cabo el Plan de Pruebas de las modificaciones del Plan de Recuperación de Desastres TI.
   - Distribuir las nuevas modificaciones del Plan de Recuperación de Desastres TI.

i. Metodología

El Análisis de Impacto en el Negocio (BIA) es un proceso que tiene por objetivo determinar, de acuerdo con la misión de la UTEC, las funciones críticas del negocio y sus recursos críticos asociados.

Esto se logra al:

- Identificar todos los procesos de negocio de la UTEC.
- Identificar todas las aplicaciones que soportan esos procesos.
- Determinar el tiempo de recuperación objetivo en el ciclo de vida de cada proceso.
- Determinar si el proceso es crítico para el negocio.
- Estimar la pérdida potencial y el tiempo de recuperación.
- Determinar los niveles de importancia de los procesos vitales para el negocio.

El desarrollo del Análisis de Impacto en el Negocio (BIA) se describe en las siguientes fases:

Fase 1: Inicio del Proyecto
Durante esta fase se definieron las estrategias de recopilación, análisis y consolidación de datos, definiendo para ello lo siguiente:

- Se estableció responsable de indagación, revisión y validación de los datos a recopilar.
- Se identificó a los propietarios de información con quienes se debía realizar la indagación.
- Se preparó un cronograma de entrevistas para recopilar los datos necesarios para el BIA.
- Se solicitó a la Oficina de Informática el apoyo necesario para la regulación y coordinación con las áreas usuarias.

Fase 2: Recopilación de Datos
Durante esta fase se realizaron entrevistas con los usuarios responsables de cada uno de los procesos de Negocio (o con el adjunto que ellos delegaron), apoyados en el desarrollo de un Cuestionario BIA, el cual fue completado por el usuario contando con la asesoría del equipo de indagación. Dicho cuestionario contiene la siguiente información:
Introducción, la cual presenta al cuestionario indicando los objetivos del mismo, la metodología a utilizar, el escenario de desastre propuesto y el glosario de términos claves, que se muestran en el documento.

- Identificación de la Encuesta, donde se indica la ficha técnica del BIA, indicando al proceso de negocio involucrado, usuario responsable y fecha de entrevista.
- Información del proceso de Negocio, la cual presenta la descripción del proceso, características del proceso, personal involucrado en el proceso y usuarios del mismo.
- Impacto Financiero asociado a factores.
- Impacto Operacional asociado a factores.
- Períodos del año críticos.
- Definición del Tiempo de Recuperación Objetivo (RTO).
- Definición del Punto de Recuperación Objetivo (RPO).
- Definición y requerimientos de recuperación de información.
- Activos de información asociados al proceso.
- Comentarios adicionales del entrevistado.

Fase 3: Análisis de Datos
Durante esta fase se realizó la tabulación de los resultados, desarrollando las siguientes actividades:

- Identificar los valores de RTO y RPO por cada uno de los procesos de negocios.
- Identificar y tabular los resultados del impacto financiero y operacional.
- Priorizar los procesos de negocio de acerado al RTO obtenido.
- Presentar los resultados a la Oficina de Informática.
- Obtener la aprobación de los resultados por parte de las áreas usuarias y la Oficina de Informática. Los Documentos BIA, debidamente firmados por las áreas usuarias, se encuentran en poder de la oficina de informática.

Fase 4: Consolidación y Análisis de Datos a nivel Empresa
Durante esta fase se consolidó los resultados obtenidos en la fase anterior, presentando a manera de gráfico el resultado del Análisis de Impacto de Negocio, definiendo luego las estrategias de recuperación y respaldo para cada uno de los activos de información asociados.

j. Prioridad de Recuperación

La prioridad está definida en el documento de *bussiness Impact análisis (BIA)*, donde se establece la prioridad, y están identificados los procesos críticos, cuya recuperación debe realizarse de acuerdo a la prioridad indicada (RTO).

k. Aplicaciones Asociadas a los Procesos

El detalle de las aplicaciones asociados a los procesos, su orden de recuperación e importancia, se encuentran establecidos en el apéndice 2: *prioridades de recuperación para las actividades*.

l. Estrategias posibles de recuperación Contingencia – Análisis de la Arquitectura de la Plataforma

Como parte del plan de recuperación de desastres es necesario definir una estrategia para desplegar la infraestructura tecnológica que entrará en operación ante un escenario de contingencia. En tal sentido, analizando los RTOs (Recovery Time Objetive) establecidos en el BIA, se plantean las siguientes estrategias para las aplicaciones asociadas a cada actividad, tanto en la capa de base de datos como en la de aplicación.

Cod.	Actividad	Servidor de BD	Servidor de aplicaciones
1	Base de datos	REL	
2	Sistema Empresarial	REL	REL
3	Pagos en línea	CEE	CEE
4	Sistema academic		CEE
5	Respaldos		REL
6	Servicios bancarios (Prestamos, Estados de Cuentas, TC)	CEE	CEE
7	Servidores (Base de Datos, WEB, Active Directory, DNS)		CEE
8	Servicio de Internet		CLT
9	Servidor HP NAS		CLT
10	Servidor DELL		CLT
11	Servidor DNS		CLT
12	WEB Services VPN		CLT
13	Servidor TAPE Backup		CEE
14	Software Veem Backup		CEE
15	Cintas de Respaldo (LTO4)		CEE

A continuación, se detalla la definición de cada configuración:

Servidor de Base de Datos
REL = Replicación en línea: Indica que la base de datos es replicada hacia el servidor de contingencia cada cierta cantidad de minutos; manteniendo la base de datos primaria y de contingencia del aplicativo casi sincronizadas. **CEE = Contingencia en espera**: Indica que la base de datos de contingencia se encuentra instalada en el servidor de contingencia, pero no actualizada. Se debe restaurar el último respaldo de información en la misma y poner la base de datos en línea. **CLT = Clúster**: Indica que la base de datos primaria y de contingencia comparte una misma unidad lógica por lo que las instrucciones de escritura y actualización son replicadas a las dos. Si la base de datos primaria fallara la de contingencia ingresaría a atender de manera automática.

Servidor de aplicaciones
REL = Replicación en línea: Indica que la capa de aplicación (programas, ejecutables, componentes, entre otros) es replicada hacia el servidor de contingencia cada cierta cantidad de minutos; manteniendo la capa de aplicación primaria y de contingencia del sistema casi sincronizadas. **CEE = Contingencia en espera**: Indica que la capa de aplicación se encuentra instalada en el servidor de contingencia pero no actualizada. Se debe restaurar el último respaldo de información de la misma y poner el aplicativo en línea. **CLT = Clúster**: Indica que la capa de aplicación primaria y de contingencia comparte una misma unidad lógica por lo que la interacción del usuario contra la aplicación es replicada hacia ambos servidores. En caso fallara el primario, la contingencia atendería las solicitudes.

m. Procedimientos de Activación del Plan

Este procedimiento tiene como objetivo evaluar el desastre al cual se ve enfrentado el Centro de Datos primario de la UTEC, tomando las acciones correspondientes en caso de una situación de emergencia.
Equipo de Evaluación del Desastre, se encuentra conformado por:

- Coordinador de Recuperación de TI.
- Coordinador de Infraestructura Tecnológica.
- Coordinador de Sistemas de Información.

El siguiente diagrama muestra los criterios que deberán ser usados para activar el Plan de Recuperación de Desastres TI:

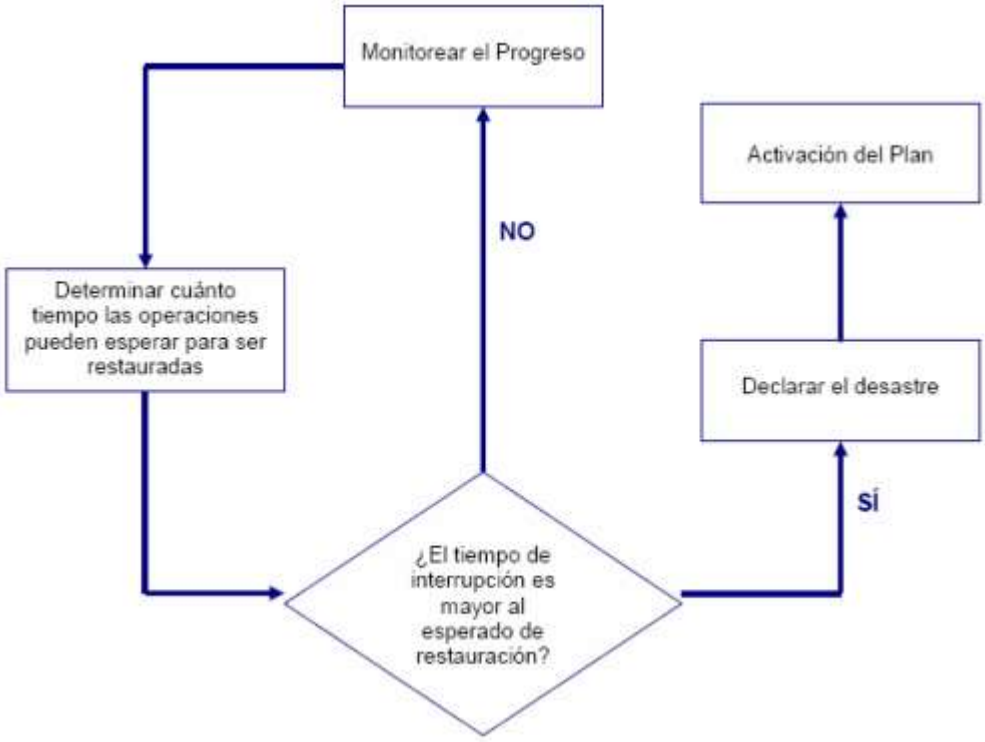


Figura 2: Diagrama representativo de criterios para TI

Debe notarse que una interrupción no es solamente un evento que reduce la efectividad de los sistemas, es un evento extraordinario que causa una pérdida de procesos de negocio clave y tiene un impacto alto en la UTEC.
Situaciones que pueden convertirse en una emergencia:

- Incendios
- Terremoto
- Sobre carga / falta de energía
- Inundaciones
- Huelgas
- Falla en los sistemas ambientales
- Mal tiempo

En una situación de emergencia, se deberá proceder de la siguiente manera:

#	Acción	Descripción	Responsabilidad	Referencia
1	Recibir Notificación	Cuando se presente una situación de emergencia, ésta deberá ser notificada al Coordinador de Recuperación de TI. Si la persona que detecta la emergencia no puede contactarse con el	Empleado de la UTEC	ANEXO A - Directorio del Equipo de Recuperación de Desastres

		responsable, entonces deberá notificar uno a uno a los miembros del Equipo de Recuperación hasta poder contactarse con alguno de ellos.		
2	Confirmar Notificación	Cuando la notificación de una contingencia potencial es recibida, se debe obtener una descripción breve de la naturaleza del incidente y cualquier tipo de daño. Si es necesario, se debe confirmar que la notificación es verídica a través de un medio secundario. El medio secundario puede ser otra persona que presenció el	Director de TI.	N/A
3	Contactar Servicios de Emergencia	Si la situación lo amerita, se deberá efectuar el contacto con los servicios de emergencia. Situaciones que pueden ser consideradas de emergencia son mencionadas anteriormente.	Director de Informática	ANEXO B – Directorio de Servicios de Emergencia
4	Notificar a la seguridad del Ministerios	Notificar inmediatamente al personal de seguridad de la UTEC: **Central Telefónica**: 2275-8888 / 2275-8892 Se debe regularizar esta notificación por medio de un documento formal al jefe de seguridad de la UTEC.	Director de Informática	N/A
5	Reunión de coordinación	Coordinar una reunión a la brevedad posible con el Equipo de Recuperación, con la finalidad de hacer una evaluación preliminar de los daños. Dependiendo de la criticidad del desastre, esta reunión se puede realizar en el local del Centro de Datos primario o en un lugar cercano al mismo.	Director de TI	N/A

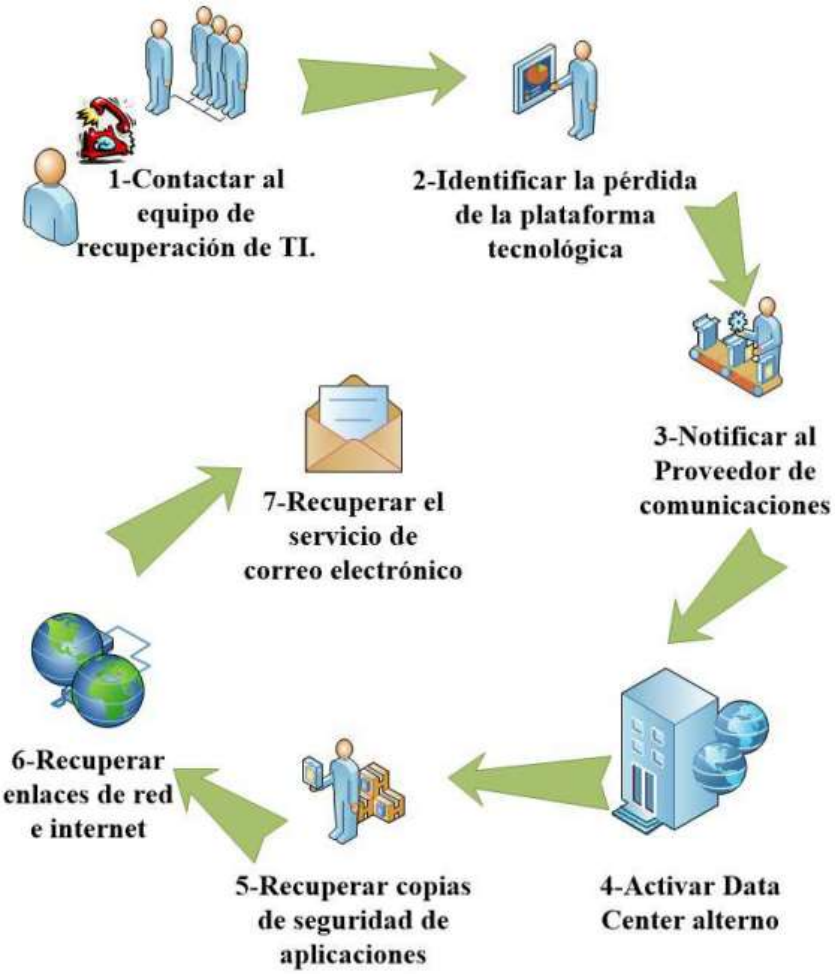
		Notificar a personal de seguridad de la UTEC.		
6	Reunión de coordinación	Coordinar una reunión a la brevedad posible con el Equipo de Recuperación, con la finalidad de hacer una evaluación preliminar de los daños. Dependiendo de la criticidad del desastre, esta reunión se puede realizar en el local del Centro de Datos primario o en un lugar cercano al mismo. Notificar a personal de seguridad de la UTEC.	Director de TI	N/A
7	Declarar la Contingencia	En caso que el tiempo requerido para completar la reparación de los daños sea mayor al tiempo de recuperación requerido por el negocio, se declara la situación de emergencia y se da por activado el Plan de Recuperación de Desastres.	Equipo de Evaluación del Desastre	N/A
8	Alistar los recursos requeridos para el Centro de Datos alterno	Proveer transporte para el equipo de recuperación, personas y suministros requeridos para el restablecimiento de las operaciones en el Centro de Datos alterno.	Director de TI	N/A
9	Alertar personal involucrado	Se debe alertar a todos los miembros del Equipo de Recuperación que no se encuentren presentes al momento de la declaración de la situación de emergencia. Progresivamente avisar y orientar al resto del personal de la empresa.	Director de TI	ANEXO A - Directorio del Equipo de Recuperación de Desastres
10	Ejecutar el Procedimiento General de Recuperación	Iniciar las actividades de recuperación en el Centro de Datos alterno de acuerdo a los procedimientos de recuperación definidos más	Director de TI	N/A

adelante. Este incidente debe ser registrado dentro del procedimiento de administración de incidentes.

n. Procedimientos generales de recuperación

Este procedimiento general tiene como objetivo la activación del Centro de Datos alterno para el restablecimiento de la totalidad de operaciones tecnológicas requeridas para garantizar la continuidad de los procesos críticos de la UTEC, identificados en el BIA. Es importante mencionar que existen procesos como la recuperación de Internet, que forman parte de las acciones a realizar y han sido colocados de acuerdo a su dependencia con el resto de procesos del negocio.

En la siguiente figura se aprecian los pasos generales en la recuperación de los servicios:



A continuación se detallan las acciones que conforman el procedimiento general de recuperación aquí graficado:

#	Acción	Descripción	Responsabilidad	Referencia
1	Contactar al Equipo de Recuperación de TI	El Equipo de Recuperación debe ser notificado y movilizado a las instalaciones del Centro de Datos alterno.	Director de TI	ANEXO A - Directorio del Equipo de Recuperación de Desastres
2	Identificar la pérdida de plataforma tecnológica	Utilizar el inventario de HW y SW, para identificar la Infraestructura tecnológica perdida en el Centro de datos primario y generar informe.	Jefe de informática	ANEXO A - Directorio del Equipo de Recuperación de Desastres
3	Notificar al proveedor de comunicaciones	Notificar al proveedor de comunicaciones acerca de la situación de desastre e indicar que puede haber cambios en la configuración. Detallar la información que se ha perdido y debe ser recuperada. Dejar constancia de la notificación.	Jefe de informática	ANEXO C – Directorio de Proveedores
4	Activar el Centro de Datos alterno	Declarar el Centro de Datos alterno como Centro de Datos de contingencia. Se debe revisar el checklist de los Requisitos en el Centro de Datos Alterno. Adicionalmente, se deberá tener en cuenta los insumos, adicionales al HW y SW críticos, para el correcto funcionamiento del mismo.	Director de TI	Requisitos en el Centro de Datos Alterno
5	Recuperar copias de seguridad de aplicaciones	(Documento de entrada: informes de los puntos 5 y 6). Recuperar, de ser necesarias las copias de seguridad, ya sean del Centro de Datos o en su defecto del almacenamiento externo y restaurarla información.	Jefe de informática	N/A
6	Recuperar los Enlaces de Red e Internet	Ejecutar el procedimiento de recuperación de los enlaces de red y comunicaciones; así como Internet.	Especialista de red	ANEXO C – Directorio de Proveedores

7	Recuperar el servicio de Correo Electrónico	Ejecutar el procedimiento de recuperación del Correo Electrónico	Especialista de red	Procedimiento de Correo Electrónico

Procedimiento para la recuperación

1. Procedimiento de recuperación de enlace de red e internet

i. Descripción del escenario

La Universidad Tecnológica de El Salvador pierde la disponibilidad de los servicios de enlaces de red e internet para sus servicios críticos, con los cuales no es posible entrar a los aplicativos como el Sistema Empresarial, Pago en Línea, Servicios Académicos y Servicios Bancarios. En este punto aseguramos que servidores de base de datos y de servicios se encuentran funcionando normalmente.

ii. Equipo participante

- Jefe de Informática
- Jefe de Desarrollo de Software
- Especialista de Seguridad
- Especialista de Redes

iii. Detalle del procedimiento

#	Acción	Descripción	Rol	Responsabilidad
1	Determinar Funcionalidad de Servidores de BD y Aplicaciones.	Se deberá determinar el grado de funcionamiento de los servidores. Esto con el fin de determinar que la caída en los sistemas se deberá en base a los enlaces de internet u otros enlaces.	-Coordinados desarrollo de software	Dueños de los servidores de BD y Aplicativos.
2	Inspección de la red de cableado estructurado.	-Se verificará el estado de los routers, switches que componen los dispositivos de networking. -Determinar por pruebas de ping, traceroute entre otros para la conectividad entre cada punto de red interna de la universidad. (Incluyendo también los cortafuegos)	-Jefe de Informática -Especialista de red -Especialista de servidores -Especialista de seguridad	Coordinador y Departamento de Infraestructura de Servicios.
3	Inspección de Enlaces Externos.	Esta acción se deberá hacer al mismo tiempo con la inspección de la red de cableado estructurado.	-Jefe de Informática -Especialista de red	Coordinador y Departamento de Infraestructura de Servicios.
4	Reparación de enlaces internos y externos en la	-En el caso de la infraestructura interna la reparación se realizará	-Jefe de Informática	Coordinador y Departamento de

	red de infraestructura.	tomando dándole prioridad a los servicios que posean un RTO bajo, en caso de haber 2 o más servicios críticos, y en base a ese tiempo estipulado. -En caso de los enlaces externos se deberá hacer las reparaciones tomando en cuenta el tiempo de recuperación establecido en el SLA.	-Especialista de red	Infraestructura de Servicios.
5	Realización de Pruebas de sistemas.	Se deberá hacer las pruebas respectivas sobre la funcionalidad de los sistemas críticos.	-Coordinador desarrollo de software	Dueños de los servidores de BD y Aplicativos.
6	Documentación de los puntos encontrados.	Se deberá de documentar la información sobre el desarrollo del incidente, para futuras procesos similares.	-Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	Coordinador y Departamento de Infraestructura de Servicios.

iv. Matriz RACI

ID	ACTIVIDAD	ROLES/RESPONSABILIDADES			
		Jefe de Informática	Jefe de Desarrollo de software	Especialista de seguridad	Especialista de Redes
1	Determinar Funcionalidad de Servidores de BD y Aplicaciones.	C	R	A	I

2	Inspección de la red de cableado estructurado.	R/A		I	C
3	Inspección de Enlaces Externos.	R/A	I	C	I
4	Reparación de enlaces internos y externos en la red de infraestructura.	R	I	C	A
5	Realización de Pruebas de sistemas.	A	R	I	C
6	Documentación de los puntos encontrados.	R	I	C	A

2. Procedimiento de recuperación luego de interrupción prolongada de electricidad

i. Descripción del escenario

La Universidad Tecnológica de El Salvador pierde la disponibilidad de los servicios debido al corte de energía eléctrica en un periodo prolongado de tiempo. Esto produce una baja en los servicios en línea como el Sistema Empresarial, Pago en Línea, Servicios Académicos y Servicios Bancarios.

ii. Equipo participante

- Director de TI
- Jefe de Informática
- Jefe de Desarrollo de Software
- Especialista de Seguridad
- Especialista de Redes
- Áreas Administrativas

iii. Detalle del procedimiento

#	Acción	Descripción	Rol	Responsabilidad
1	Activación de Dispositivos alternos	Se deberá activar los dispositivos alternos de generación de electricidad ya sea UPS u otros.	-Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	Coordinador y Departamento de Infraestructura de Servicios.

2	Verificación del funcionamiento de los sistemas con los métodos eléctricos alternos.	Se verificara los servidores, cortafuegos, y programas con el fin de determinar si existió una falla en los funcionamientos de los sistemas críticos del negocio.	-Jefe de Informática -Coordinador desarrollo de software	-Coordinador del departamento de infraestructura. -Dueños de los servidores de BD y Aplicativos.
3	Monitoreo de la reposición de los sistemas eléctricos.	Este proceso se tendrá que realizar en coordinación con el director de tecnología, donde buscara verificar la reposición de los servicios eléctricos de parte de los grupos externos que brindan este servicio.	- Director de TI	-Director de tecnología
4	Intercambio del sistema alterno al sistema principal de electricidad.	Al reponerse el sistema eléctrico principal se tendrá que hacer el cambio por parte del personal del departamento sin que esto emita una caída de los sistemas. Apagando cada UPS o método alterno.	-Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Departamento de infraestructura.
5	Verificación de Data.	En esta actividad se monitoreará con las áreas administrativas que hayan manejado información para ver si existe una posible pérdida de la misma.	-Coordinador desarrollo de software -Áreas Administrativas.	-Dueños de los servidores. -Áreas Administrativas.
6	Documentación de los puntos encontrados.	Se deberá de documentar la información sobre el desarrollo del incidente, para futuras procesos similares.	--Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	Coordinador y Departamento de Infraestructura de Servicios.

iv. Matriz RACI

ID	ACTIVIDAD	ROLES/RESPONSABILIDADES					
		Director de TI	Jefe de Informática	Jefe de Desarrollo de Software	Especialista de seguridad	Especialista de redes	Áreas de admón.
1	Activación de los dispositivos alternos	I	R/A	I	C	C	I
2	Verificación del funcionamiento de los sistemas con los métodos eléctricos alternos	I	R/A	R	C	C	I
3	Monitoreo de la reposición de los sistemas eléctricos	R/A	R	I	C	C	I
4	Intercambio del sistema alterno al sistema principal de electricidad	I	R	I	C	A	I
5	Verificación de la data	I	C	R/A	I	C	I
6	Documentación de los puntos encontrados	I	R/A	C	C	C	I

3. Procedimiento de recuperación luego de un terremoto

i. Descripción del escenario

La Universidad Tecnológica de El Salvador pierde la disponibilidad de los servicios críticos debido a un movimiento telúrico que imposibilita dicho manejo.

ii. Equipo participante

- Alta Gerencia.
- Director de TI.
- Jefe de Informática
- Coordinador desarrollo de software
- Especialista de red
- Especialista de seguridad
- Áreas administrativas
- Outsourcing para Nube

iii. Detalle del procedimiento

#	Acción	Descripción	Rol	Responsabilidad
1	Verificación del funcionamiento de los sistemas.	Este es el primer proceso crítico que se llevara a cabo, en donde se verificaran primero los servicios disponibles por medio de los servidores.	-Jefe de Informática	-Dueños de los servidores.
2	Determinar los servicios caídos más críticos del negocio para su envió al centro alterno.	Esto se verificara tomando la información del punto anterior contra el análisis de impacto del negocio de cada servicio (BIA)	-Alta Gerencia. -Director de TI.	-Alta Gerencia. -Director de tecnología.
3	Envió de Información a centro alterno.	En este punto se deberá hacer de acuerdo a las posibilidades de traslado: -Vía Terrestre: Se deberá enviar la información necesaria por medio de respaldos por esta vía al centro alterno de datos. -Nube: Este método de envió se deberá activar si por vía terrestre no es posible. En dicho método existirá un retraso de 4 horas con las actualizaciones. Y de este punto se deberá enviar la información al centro alterno de datos.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad -Outsourcing para Nube.	-Director de tecnología. -Departamento de infraestructura. -Outsourcing para Nube.
4	Activación de centro alterno de datos.	En este punto el centro alterno guardara la información. Pero en caso de un daño de gran magnitud a dicho lugar, la nube deberá quedar funcionando con los servicios más críticos hasta la recuperación de los sistemas.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Director de tecnología. -Departamento de infraestructura.
5	Verificación de Data y de los servicios.	Se buscará verificar primeramente el buen funcionamiento de los sistemas en el sitio alterno de recuperación.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software	-Director de tecnología. -Departamento de infraestructura.

		Además, en esta actividad se monitoreará con las áreas administrativas que hayan manejado información para ver si existe una posible pérdida de la misma.	-Especialista de red -Especialista de seguridad -Áreas Administrativas.	-Áreas Administrativas.
6	Restablecer los sistemas funcionales en el sitio principal.	Con el apoyo de la alta dirección por medio de del director de TI se deberá hacer las gestiones necesarias para la recuperación del data center en la parte principal de la universidad.	-Alta Gerencia. -Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Alta Gerencia. -Director de tecnología. -Departamento de infraestructura.
7	Restablecimiento de la data en el sitio principal.	Este método se podrá y deberá hacer en horas no hábiles para no afectar los procesos diurnos de la institución, por medio de backups o la clúster con respecto a la nube.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Director de tecnología. -Departamento de infraestructura.
8	Cierre de Sitio Alterno de Datos	En caso del sitio alterno físico se deberá eliminar la información con el fin de mantener los niveles de seguridad de la data. En el caso de los servicios de nube deberá devolver el control de estos al data center principal de la institución.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Director de tecnología. -Departamento de infraestructura.

iv. Matriz RACI

ID	ACTIVIDAD	ROLES/RESPONSABILIDADES							
		Alta Gerencia	Director de TI	Jefe de Informática	Jefe de Desarrollo de Software	Especialista de seguridad	Especialista de redes	Áreas de admón.	Outsourcing Nube
1	Verificación del funcionamiento de los sistemas		I	R/A	I	C	C	C	
2	Determinar los servicios caídos más críticos del negocio para su envió al centro alterno	I	R/A	C	I	I	C	I	
3	Envío de información al centro alterno		R/A	R	R	C	C	I	A
4	Activación del centro alterno		R	R/A	C	C	C	I	
5	Verificación de la data y los servicios		I	R/A	R	C	C	I	
6	Restablecer los sistemas funcionales		I	R/A	R	C	C	I	
7	Restablecimiento de la data en el sitio principal		R	R	R	C	C	I	I
8	Cierre del sitio alterno		R	R	C	R	C	I	I

4. Procedimiento de recuperación luego de un incendio

i. Descripción del escenario

La Universidad Tecnológica de El Salvador pierde la disponibilidad de los servicios debido a un incendio generado dentro de las instalaciones del Departamento de TI.

ii. Equipo participante

- Alta Gerencia
- Director de TI
- Jefe de Informática
- Coordinador desarrollo de software
- Especialista de red
- Especialista de seguridad
- Outsourcing para Nube
- Cuerpo de Bomberos

iii. Detalle del procedimiento

#	Acción	Descripción	Rol	Responsabilidad
1	Activación de centro alterno de datos.	Como primer punto se buscara la activación del sitio alterno de forma automática para el recibimiento de la información.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Director de tecnología. -Departamento de infraestructura.
2	Envió de Información a centro alterno.	En este punto se deberá hacer de acuerdo a las posibilidades de traslado: -Vía Terrestre: Se deberá enviar la información necesaria por medio de respaldos por esta vía al centro alterno de datos. -Nube: En dicho método existirá un retraso de 4 horas con las actualizaciones. El resto de data deberá enviarse por medio terrestre.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad -Outsourcing para Nube.	-Director de tecnología. -Departamento de infraestructura. -Outsourcing para Nube.
3	Controlar el incendio generado dentro del Departamento de TI.	Usar los dispositivos para el control de un incendio dentro del departamento de TI. Haciendo uso de extinguidores de acuerdo al tipo de generación de incendio. Hacer llamado al cuerpo de bomberos que puedan ayudarnos a mitigar dicho incidente.	-Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad -Cuerpo de Bomberos.	-Departamento de infraestructura. -Cuerpo de Bomberos.

4	Realizar un análisis de los servicios perdidos.	Se deberá realizar un análisis de los servicios perdidos producidos en el incendio, esto por medio del uso del BIA.	-Director de TI -Jefe de Informática	-Director de tecnología. -Departamento de infraestructura.
5	Restablecer los sistemas funcionales en el sitio principal.	Con el apoyo de la alta dirección por medio de del director de TI se deberá hacer las gestiones necesarias para la recuperación del data center en la parte principal de la universidad.	-Alta Gerencia -Director de TI -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Alta Gerencia. -Director de tecnología. -Departamento de infraestructura.
6	Restablecimiento de la data en el sitio principal.	Este método se podrá y deberá hacer en horas no hábiles para no afectar los procesos diurnos de la institución, por medio de backups o la cluster con respecto a la nube.	-Director de TI -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Director de tecnología. -Departamento de infraestructura.
7	Cierre de Sitio Alterno de Datos	En caso del sitio alterno físico se deberá eliminar la información con el fin de mantener los niveles de seguridad de la data. En el caso de los servicios de nube deberá devolver el control de estos al data center principal de la institución.	-Director de TI. -Jefe de Informática -Coordinador desarrollo de software -Especialista de red -Especialista de seguridad	-Director de tecnología. -Departamento de infraestructura.

iv. Matriz RACI

ID	ACTIVIDAD	ROLES/RESPONSABILIDADES							
		Alta Gerencia	Director de TI	Jefe de Informática	Jefe de Desarrollo de Software	Especialista de seguridad	Especialista de redes	Áreas de admón.	Outsourcing Nube
1	Activación del centro alternos		R	R/A	I	C	C		
2	Envió de información al centro alterno		R	R/A	C	I	I		C

3	Controlar el incendio generado en TI		I	R/A	C	I	I	I	
4	Realizar un análisis de los servicios perdidos		R	R/A	I	C	C		
5	Restablecer los sistemas funcionales en el sitio principal	I	R	R	I	C	C		
6	Restablecimiento de la data en el sitio principal		R	R/A	R	C	C		
7	Cierre del sitio alterno		R	R	I	C	C		

Beneficios

- La Universidad Tecnológica del El Salvador cuenta con una serie acciones a seguir ante incidente de seguridad ocurrido dentro de las instalaciones del departamento de TI.
- Se cuenta con una guía de procedimientos a seguir ante un evento en particular y se han definido los roles y funciones del personal a cargo.
- La definición de un equipo de trabajo para las respuestas ante incidentes permite a la Universidad Tecnológica gestionar adecuadamente los recursos
- El departamento de TI cuenta con un plan de recuperación que permite identificar las prioridades a la hora de realizar una recuperación de los sistemas de información

Conclusiones

Una vez finalizado el trabajo de investigación se concluye que:

- El análisis de impacto del negocio, hace parte importante del plan de continuidad del negocio y a su vez presenta consideraciones importantes para la gestión del riesgo dentro de las organizaciones, que establecen un marco de políticas, procedimientos y estrategias que permiten asegurar que las operaciones de carácter critico puedan ser mantenidas y recuperadas a la mayor brevedad posible, en caso de fallas graves dentro de los sistemas de información y las comunicaciones.
- El BIA es un instrumento operacional muy importante que permite la toma de decisiones en momentos críticos de la organización en virtud del cese de operaciones debido a una situación anómala presentada.
- De esta manera dicho instrumento, contribuye a identificar las operaciones y servicios considerados críticos dentro de la entidad, que contribuyen a restablecer en el menor tiempo posible los servicios y operaciones con el apoyo de un plan de continuidad del negocio de las entidades.
- Actualmente, la UTEC dispone de una plataforma tecnológica que le permite atender sus operaciones y brindar un servicio a sus usuarios en tiempos razonables para el negocio. Sin embargo, ante un evento de desastre total del Data Center no se estaría en la posibilidad de seguir brindando este servicio.

Recomendaciones

Como resultado del BIA de los procesos críticos de la UTEC de El Salvador y la elaboración de los procedimientos de recuperación para dichos procesos de acuerdo a la arquitectura y plataforma con la que cuenta actualmente la institución, se recomienda lo siguiente:

- La UTEC debe considerar la implementación de un Data Center alterno en cualquiera de las modalidades descritas en el presente análisis como algo prioritario. La mejor opción sería desplegar, con un tercero, un sitio de contingencia alterno fuera de las instalaciones de la UTEC (housing y hosting) el cual ayudará a
    - Contar con una distancia adecuada entre el Centro de Datos primario y el de alterno.
    - Contar con niveles de servicio con el proveedor que preste el servicio.
    - Trasladar los riesgos asociados al control de acceso y control ambiental al proveedor, ayudando a que la UTEC se concentre en recuperar las operaciones lo antes posible.

    - Tener una opción para renovación tecnológica de manera más dinámica ya que puede ser parte del contrato que el proveedor acepte una renovación tecnológica de los equipos de acuerdo a un periodo definido.
- Se recomienda mantener los intervalos actuales de respaldo de información para las distintas aplicaciones, siempre y cuando esto no degrade la performance del sistema de respaldo y restauración de información.
- Finalmente, es responsabilidad de las empresas disponer de un recurso humano suficientemente capacitado y especializado, capaz de enfrentarse a los eventos inesperados que atentan con la operatividad, seguridad y disponibilidad de los sistemas de información y las comunicaciones.

Referencias

[1] U. T. d. E. Salvador, «www.utec.edu.sv,» [En línea]. Available: http//www.utec.edu.sv.

[2] U. T. d. E. Salvador, «Portal UTEC,» [En línea]. Available: http://portal.utec.edu.sv.

[3] U. T. d. E. Salvador, «Portal Empresarial UTEC,» [En línea]. Available: https://portalempresarial.utec.edu.sv/uonline.

[4] J. Hoffer, Backing Up Business - Industry Trend or Event, Health Management Technology, Enero 2001.

[5] I. T. d. C. Rica, «Diagnóstico y plan de mejoras de la infraestructura de la UTEC,» Noviembre 2010.

[6] Á. G. Vieites, Enciclopedia de la Seguridad Informática, Segunda edición, 22011.

[7] J. A. O. Sánchez, «Reporte de Evaluación y Análisis de Riesgos,» Mayo 2011.

[8] Cacheda Fidel, Seijo; Fernández Luna, Juan Manuel; Huete Guadix, Juan Francisco, Recuperación de información: un enfoque práctico y multidisciplinar, 2011

[9] ISACA, COBIT 5, 2012

[10] Norma ISO/IEC 17799

Anexos

ANEXO A – DIRECTORIO DEL EQUIPO DE RECUPERACION DE DESASTRES

Nombre	Área de especialidad	Dirección	Teléfonos
Lic. Jorge Alberto Portillo Chávez	Director de TI	Col. Costa Rica, Av. San José 426, San Salvador	Tel. Oficina: 2275-8962 Tel. Casa: 2557-5205 Tel. Celular: 7101-5811
Ing. Salvador Alcides Franco Sanchez	Jefe de Informática	Res. Jardines del Valle, Senda 3, Polígono C, Casa #5, Quezaltepeque	Tel. Oficina: 2275-8726 Tel. Casa: Tel. Celular: 6180-8472
Ing. Juan Carlos Campos Rivera	Coordinador de Desarrollo de Sistemas	Carretera Troncal del norte, Km 5 1/2, Col El Mirador, Block “E” Numero 4, Ciudad Delgado	Tel. Oficina: 2275-8731 Tel. Casa: 2562-3494 Tel. Celular: 7915-0860
Ing. Dany Salvador Chacón Orellana	Especialista de Seguridad	Col. Guayacán pasaje lolotique casa N° 56-11B Soyapango	Tel. Oficina: 2275-8823 Tel. Casa: Tel. Celular: 7612-6706 Tel. Celular: 7909-9818
Tec. William Enrique García Arias	Especialista de Infraestructura de Red	Col. Jardines del Pepeto 1. Pasaje. 3 Casa 28 B. Soyapango	Tel. Oficina: 2275-8732 Tel. Casa: Tel. Celular: 7306-4014

ANEXO B – DIRECTORIO DE SERVICIOS DE EMERGENCIA

No	EMPRESA	TELEFONOS
1	COMPAÑIA DE BOMBEROS	2222-2222
2	POLICIA NACIONAL CIVIL	2121-2121
3	AMBULANCIA	2323-2323

ANEXO C – DIRECTORIO DE PROVEEDORES

EMPRESA	SERVICIO	CONTACTO	TELEFONO
COLUMBUS NETWORK	INTERNET	Fernando Miranda	2280-9425 / 7946-4146
TELEFONICA	INTERNET	Ada Samara Gochez	2257-4213 / 7833-0112
ORBITAL	SERVIDORES	Ingrid Granadino	2204-4704 / 7695 6806
AEEGLE	SERVIDORES	Carlos Campos	2564-6680 / 7850-5077
GMB	REDES	Cristina Cáceres	2250-5600
SSASIS	REDES	Patrick Cisneros	2263-5686 / 7861-4895
SEFISA	SEGURIDAD	Roxana Rivas	2528-1013 / 7856-9861