MANUAL DE PLANES DE CONTINUIDAD DE LA OPERACIÓN TECNOLÓGICA Y DE RECUPERACIÓN ANTE DESASTRES

UTC-DAF-BCP-DRP

Junio 2022

APROBACIÓN DEL DOCUMENTO

ACUERDO **SAE/BCP-DRP/02/2022**, CON LA **UNIVERSIDAD TECNOLÓGICA DE CALVILLO**, POR EL QUE SE ESTABLECE EL PRESENTE MANUAL EN APEGO AL ARTICULO 33, FRACCIÓN XXIII DE LA LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA DEL ESTADO.

MANUAL DE PLANES DE CONTINUIDAD DE OPERACIÓN TECNOLÓGICA Y DE RECUPERACIÓN ANTE DESASTRES

Elaboración	Nombre y Puesto	Firma
Integró:	Ing. Oscar Moisés Alvarez Esparza Coordinador de Soporte Técnico Y Coordinador de BCP-DRP	
Validó:	C. Noé Rodríguez Martínez Director de Administración y Finanzas	
Autorizó:	Lic. Javier Valdivia Díaz Rector de la Universidad Tecnológica de Calvillo	
Liberó por la SAE:	Ing. Alejandro Viay Danielli Director General de Mejores Prácticas Gubernamentales	

CONTENIDO

1. INTRODUCCIÓN

Se establece el presente manual en apego al artículo 14 fracción III, inciso f) apartado c., del Acuerdo mediante el cual se establecen las Normas Generales de Control Interno para la Administración Pública Estatal, en el que se establece que a las dependencias y entidades se les requiere a través de los niveles operativos de control interno, el existir y operar los controles necesarios en materia de tecnologías de información y comunicaciones (TIC´s), para un plan de contingencias que dé continuidad a la operación de las TIC´s y de la institución.

A su vez, en cumplimiento a los artículos 2°, 5°, 84 y 209 del Manual de Lineamientos de la Dirección General de Mejores Prácticas Gubernamentales de la Secretaría de Administración del Estado (DGMPG), se conforma el presente manual como instrumento administrativo para la coordinación, dirección y control de los Planes de Continuidad de la Operación Tecnológica y de Recuperación ante Desastres (BCP-DRP mejor conocidos por sus siglas en ingles). Este manual permitirá asegurar una respuesta organizada por parte de las Unidades Administrativas involucradas ante un evento causado por fallas humanas de manera accidental o intencional o ante posibles desastres de carácter natural que provoquen daño o interrupción en los sistemas de información, la pérdida de la comunicación de datos y/o afecte la disponibilidad de la infraestructura tecnológica y como consecuencia la información almacenada en ella, así como responder adecuadamente a la emergencia para asegurar el regreso en el menor tiempo posible a la operación normal.

Los planes que conforman el presente manual han sido elaborados conforme al procedimiento para la Elaboración de Planes de Continuidad Tecnológica y de Recuperación ante Desastres proporcionado por la DGMPG, partiendo de la identificación de los servicios que proporciona cada Unidad Administrativa en congruencia con los sistemas asociados a su operación y los riesgos identificados por la Unidad de Control Interno de esta Institución, que se pudieran presentar ante una contingencia. Dichos servicios fueron analizados con base en su impacto en la operación tecnológica (BIA) y posteriormente con base en su riego ambiental (ERA). El resultado obtenido fue la calificación de criticidad y selección de los servicios que por su operación se consideran los más críticos y que requieren de contar con su plan de continuidad de operación tecnológica y de recuperación ante un desastre, mismos que a su vez contienen los activos tecnológicos asociados al sistema, así como las funciones, responsabilidades, equipos y actividades requeridas para la restauración de los sistemas.

Las pruebas anuales a los planes establecidos en el presente manual o la ejecución de los mismos ante un hecho real, quedarán registradas en los reportes correspondientes, de conformidad con las políticas establecidas en el Procedimiento para la Elaboración de los Planes de Continuidad Tecnológica y de Recuperación ante Desastres.

2. MARCO JURÍDICO – ADMINISTRATIVO

De manera enunciativa más no limitativa, se indican las siguientes disposiciones normativas que sustentan el presente documento:

a. LEYES

a.1. Ley Orgánica de la Administración Pública del Estado de Aguascalientes. POEA 27 de octubre de 2017, última reforma 28 de diciembre de 2020.

a.2. Ley de Responsabilidades Administrativas del Estado de Aguascalientes. POEA 01 de agosto de 2017, última reforma POEA 17 de septiembre de 2018.

a.3. Ley para el Control de las Entidades Paraestatales del Estado de Aguascalientes. POEA 20 de marzo de 1988, última reforma POEA 15 de junio de 2020.

b. ESTATUTOS

b.1. Ninguno aplicable

c. CÓDIGOS

c.1. Ninguno aplicable

d. REGLAMENTOS

d.1. Reglamento Interior de la Universidad tecnológica de Calvillo. POEA, Agosto de 2021.

e. DECRETOS

e.1. Ninguno aplicable

f. ACUERDOS

f.1. Acuerdo mediante el cual se aprueban, los Lineamientos para la Protección de Datos Personales del Estado de Aguascalientes y sus Municipios. POEA 04 de junio de 2018.

g. CONVENIOS

g.1. Ninguno aplicable

h. LINEAMIENTOS

h.1. Lineamientos para la Protección de Datos Personales del Estado de Aguascalientes y sus Municipios. POEA 28 de mayo de 2018.

i. MANUALES

i.1. Manual de Lineamientos de la Dirección General de Mejores Prácticas Gubernamentales de la Secretaría de Administración del Estado de Aguascalientes. POEA 24 de agosto de 2020.

i.2. Manual de procedimientos de la Universidad Tecnológica de Calvillo. Versión 1. Agosto 2021.

i.3. Manual de Políticas para la Elaboración de Documentos. SAE abril de 2018.

j. OTRAS DISPOSICIONES

j.1. Plan Estatal de Desarrollo 2016-2022. POEA 30 de mayo de 2017, última reforma POEA 16 de junio de 2020

j.2. Procedimiento para la Elaboración de los Planes de Continuidad de la Operación Tecnológica y de Recuperación ante Desastres. SAE. Versión 01. diciembre 2020.

j.3. Metodología COSO para la administración de riesgos.

j.4. ISO 27001 Gestión de la Seguridad de la Información

j.5. ISO 22301. Continuidad del negocio

j.6. ITIL v4: Service Continuity Management

j.7. EC0907 Elaboración de plan de Continuidad de Operaciones para Dependencias y Organizaciones.

3. GLOSARIO

Para los efectos del presente Manual, se entenderá por:

Activos informáticos. Cualquier componente que contribuya a la entrega de un servicio o producto de tecnologías de información.

Administradores del servicio informático. Especialistas técnicos designados por un responsable de servicio para administrar un recurso o conjunto de recursos necesarios para proporcionar un servicio informático determinado.

Amenaza. la causa potencial de un incidente que puede resultar en una violación de la seguridad de la información o comprometer las operaciones comerciales.

BCP-DRP. Planes de Continuidad de Operación Tecnológica y de Recuperación ante Desastres que contienen un conjunto de estrategias, acciones, roles y responsabilidades que se deben aplicar ante una contingencia para recuperar la operación de los servicios con base tecnológica, en el menor tiempo posible;

BIA. (*Business Impact Analisys*). Análisis de Impacto al Negocio y hace referencia a un documento que cuantifica la prioridad de un servicio, y su(s) plataforma(s) tecnológica(s) para soportar los servicios de la Dependencia o Entidad.

Contingencia. Hace referencia a los hechos o eventos no planeados que generan una interrupción de los servicios esenciales a la ciudadanía

Continuidad de la Operación o del negocio. Capacidad de la organización para restablecer la entrega de un servicio a niveles aceptables luego de un incidente disruptivo.

Dependencia (s). Las Unidades Administrativas adscritas a la Administración Pública Centralizada del Gobierno del Estado de Aguascalientes, señaladas en la Ley Orgánica de la Administración Pública del Estado de Aguascalientes.

Entidad (es). Las señaladas en la Ley para el Control de las Entidades Paraestatales del Estado de Aguascalientes.

ERA: (*Environment Risk Analisys*). Análisis de Riesgos Ambientales y hace referencia a un documento que cualifica y cuantifica los riesgos que pueden afectar la continuidad de la plataforma tecnológica de la entidad.

Matriz de Administración de Riesgos: la herramienta de control y gestión diseñada para identificar, analizar, evaluar y tratar los riesgos asociados a los objetivos estratégicos, operacionales o de información, que pudieran afectarlos.

Respaldo de la información y de las configuraciones: La copia digital realizada con frecuencia de los datos o de las configuraciones de los equipos que el responsable de los mismos considere relevantes y se encuentren almacenados en los medios que defina la Unidad de Informática.

Riesgo: Probabilidad de ocurrencia de un evento que afecte negativamente al logro de los objetivos o los intereses de la organización.

RPO: (*Recovery Point Objective).* Punto de recuperación objetivo de la información. Tiempo máximo que la Dependencia/Entidad puede permitirse perder información ante una interrupción en los sistemas de información producida por un desastre.

RTO: (*Recovery Time Objective*) Tiempo de recuperación objetivo. Tiempo que la Dependencia/Entidad necesita para recuperar sus servicios después de una inactividad producida por un desastre.

Servicios con base tecnológica: servicios o procesos que llevan a cabo las distintas Unidades Administrativas de la Dependencia o Entidad, incluyendo la información digital que contengan, y cuya operación depende de los servicios de TIC proporcionados internamente por el área informática o de forma transversal para todo gobierno por parte de la Secretaría de Administración.

Tecnologías de la información y comunicaciones o TIC: Conjunto de recursos como: computadoras, dispositivos y medios electrónicos, ópticos y magnéticos, programas informáticos y redes, necesarios para procesar, almacenar, administrar, acceder y transmitir información.

Unidad Administrativa: Cada una de las direcciones generales o áreas específicas definidas en el Manual de Organización de la Dependencia o Entidad.

UPS: Uninterruptable Power Supply, también llamado Sistema de Alimentación Ininterrumpida (SAI). Dicho dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.

4. OBJETIVO GENERAL

El presente manual tiene como objetivo establecer las acciones de mitigación a llevar a cabo ante una emergencia, asegurando la continuidad de la operación de los servicios críticos afectados, así como la recuperación de las infraestructuras relacionadas con las tecnologías de la información y comunicación.

5. ACTIVACIÓN DE LOS PLANES DE CONTINUIDAD TECNOLÓGICA PARA CADA SERVICIO CRÍTICO

Se establece un plan de continuidad tecnológica para cada servicio crítico resultante del análisis de impacto a la operación (BIA) y del análisis de riegos ambiental (ERA).

a. BCP-DRP PARA EL SERVICIO DE CONTROL DE CALIFICACIONES

a.1. OBJETIVO

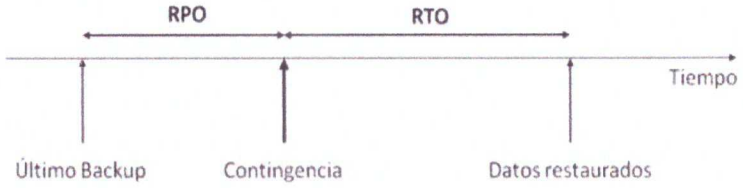
Mantener la continuidad del servicio de control de calificaciones mediante el sistema MIESCUELA, tanto para el registro de calificaciones por parte de los profesores de asignatura como la consulta de las calificaciones por parte de los alumnos.

a.2. ALCANCE

Las acciones de este plan están diseñadas para asegurar la continuidad de las operaciones así como recuperar los servicios en los tiempos planeados.

a.3. TIEMPO DE RECUPERACIÓN OBJETIVO (RTO): Hardware: 240hrs, Software: 12hrs.

a.4. PUNTO DE RECUPERACIÓN OBJETIVO DE LA INFORMACIÓN (RPO): 720 horas



a.5. SUPUESTOS

Los siguientes supuestos en relación al servicio crítico se han establecido como medida preventiva y punto de partida para asegurar el desarrollo del presente plan:

a.5.1. El equipo de respuesta para atender el servicio crítico, estará disponible en caso de emergencia.
a.5.2. Se cuenta con depuración programada de usuarios de sistema.
a.5.3. Se cuenta con respaldos disponibles e íntegros de los datos y sistemas tecnológicos implicados en el presente plan.
a.5.4. El personal relacionado con la operación del servicio crítico está identificado y capacitado en sus funciones de respuesta de recuperación y está disponible para actuar en la ejecución del presente Plan.
a.5.5. El personal informático aplica el procedimiento de respaldos y restauración de los sistemas y datos asociados al servicio crítico.
a.5.6. Se han identificado los activos informáticos críticos relacionados con el servicio a atender en este Plan.
a.5.7. Se cuenta con una planeación tecnológica que permite identificar el recurso económico que se pueda necesitar para asegurar la adquisición de infraestructura requerida para la operación eficiente de los servicios.
a.5.8. Se cuenta con contratos vigentes de mantenimiento a los sistemas, servicios o infraestructura aplicables en el presente plan.

a.5.9. Se cuenta con personal capacitado de servicios generales en el caso de ser necesario para la contingencia.

a.5.10. Los dueños del sistema crítico identifican la información que se tendría que recuperar y cómo recuperarla físicamente.

a.6. ESCENARIOS DE CONTINGENCIA

(En función de los eventos de mayor riesgo identificados en el análisis ERA).

ESCENARIOS DE CONTINGENCIA	ACTIVOS ASOCIADOS AL ESCENARIO
Ciberataque	Bases de dato, sistema (código), equipo
Internet	Sistema.
Incendios	Equipo (Servidores, equipos de red, equipo de respaldo), sistema, bases de dato.
Energía eléctrica	Sistema, Equipo, Base de Datos.

a.7. EQUIPO DE RESPUESTA PARA LA ACTIVACIÓN DEL PLAN

RESPONSABLE/ CARGO	TEL/EXT /CEL	CORREO	FIRMAS
Oscar Moises Alvarez Esparza Coordinador de Soporte Técnico	185	moises.alvarez@utcalvillo.edu.mx	
Noé Rodríguez Martínez Director de Administración y Finanzas	191	noe.rodriguez@utcalvillo.edu.mx	
José de Jesús Santana Loera Jefe del Departamento de Gestión Académica	204	jose.santana@utcalvillo.edu.mx	
Patricia Anahí García Martínez Coordinador de Servicios Escolares	193	anahi.garcia@utcalvillo.edu.mx	
Laura Lucía Serna Saucedo Coordinador de Servicios Generales	135	laura.serna@utcalvillo.edu.mx	
Daniel Rojas Salazar Coordinador de Adquisiciones	194	daniel.rojas@utcalvillo.edu.mx	
Angel Soriano ACNET	4491096985	asoriano@digitalags.net	*
Oficina CFE	071	n/a	*

Renato Noriega TECNOWARE	44915196 66	rnoriega@siexa.mx	*

* Ante la imposibilidad de recabar la firma de los proveedores, este documento se les enviará vía mail a los proveedores para su conocimiento.

a.8. MEDIDAS INICIALES DE CONTINUIDAD

a.8.1. Medidas iniciales ante un ciberataque:

1. Desconexión de servidor de servicio de la red exterior.
2. Desconexión de servidor de servicio de la red interna.
3. Limitar el acceso a los usuarios.
4. Cambios de contraseñas de administradores.
5. Identificar el estatus del antivirus.
6. Verificar la bitácora de actividad.
7. Identificar ataque y bloquear.

a.8.2. Medidas iniciales ante un corte de internet:

1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con el proveedor del servicio para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.

a.8.3. Medidas iniciales ante un incendio:

1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con servicios generales para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.

a.8.4. Medidas iniciales ante un corte de energía eléctrica:

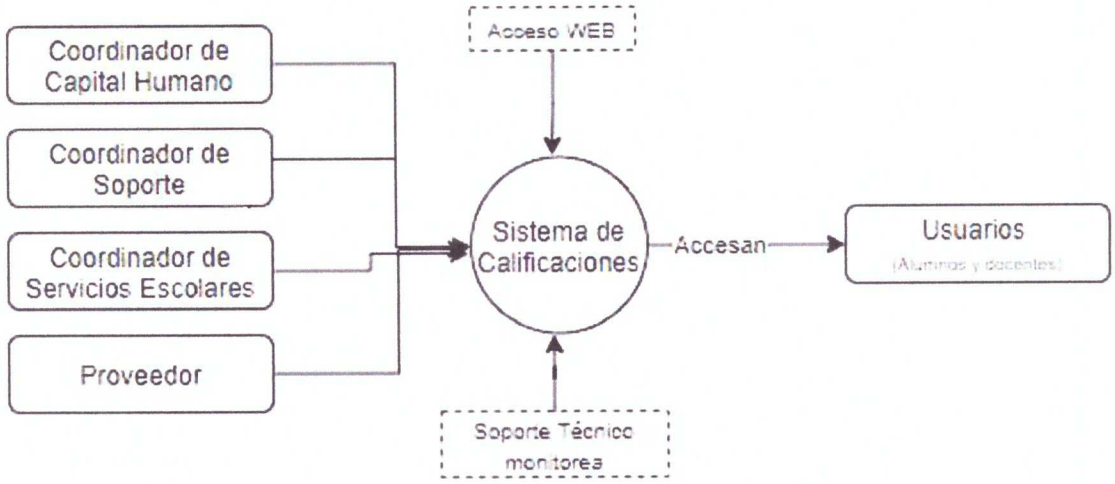
1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con servicios generales y CFE si es necesario para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia, los tiempos aproximados de recuperación y los tiempos aproximados de servicio del UPS.

a.9. BCP. ESTRATEGIAS DE CONTINUIDAD DE LA OPERACIÓN DEL SERVICIO

Las siguientes acciones se aplicarán como medidas de continuidad a ser adoptadas de forma temporal en caso de interrupción del servicio, para actuar de manera rápida y eficaz ante una eventualidad que ponga en riesgo la operación normal de las actividades.

1. Los docentes capturan calificaciones en un formato impreso determinado por el área académica.
2. En el caso de ser calificaciones finales, estos formatos son entregados al área de Servicios Escolares para cumplir con lo establecido en su procedimiento.
3. Los docentes pueden compartir a los alumnos mediante el formato impreso las calificaciones para su consulta.

a.10. ESQUEMA DE ARQUITECTURA DEL SERVICIO (diagrama a nivel 0).



a.11. DRP RECUPERACIÓN DE LOS ACTIVOS ASOCIADOS A CADA ESCENARIO DE CONTINGENCIA

Acciones para restablecer las funciones de los sistemas asociados al servicio crítico en función de cada escenario (sección.6):

a.11.1. Escenario de contingencia de Ciberataque.

a.11.1.1. Acciones a aplicar en los activos de Equipo:

1. Desconectar el equipo de la red.
2. Reiniciar el equipo.
3. Revisar el estatus de antivirus y software de protección.
4. Realizar limpieza física y lógica, además de correr un escaneo avanzado con el antivirus, para bloquear actividad sospechosa.
5. Realizar cambios de contraseñas de administrador.
6. Solicitar al área de adquisiciones con autorización de director de administración y finanzas o rector, la compra de equipo, parte del mismo o del antivirus, si fuera necesario.

7. Nuevamente escanear computadora para confirmar que ya no existen archivos o procesos sospechosos.

a.11.1.2. Acciones a aplicar en los activos de Sistema:

1. Verifica el acceso al sistema con el equipo desconectado de la red.
2. Verificar el acceso con las credenciales y cambiar contraseñas de administrador.
3. Verificar el funcionamiento del sistema en todos sus módulos.
4. Reestablecer el último respaldo si fuera necesario, y verificar el comportamiento.

a.11.1.3. Acciones a aplicar en los activos de Base de Datos:

1. Revisar la integridad de la información, generando reportes y registros actuales.
2. Restablecer el último respaldo si fuera necesario
3. Verificar las credenciales de conexión a la base de datos y si fuera necesario cambiar contraseña.
4. Recuperar los registros faltantes si hubiera el caso que se pudieran recuperar de otra fuente.

a.11.2. Escenario de contingencia de corte de Internet.

a.11.2.1. Acciones a aplicar en los activos de Sistema:

1. Verificar la disponibilidad de un posible proveedor de internet temporal con el área de adquisiciones.
2. Utilizar los sistemas de manera de red local.

a.11.3. Escenario de contingencia de Incendio.

a.11.3.1. Acciones a aplicar en los activos del Equipo:

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.
3. Realizar pruebas de estrés o de conexión, confirmando el funcionamiento correcto.

a.11.3.2. Acciones a aplicar en los activos del Sistema:

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.

3. Instalar sistema operativo y lo necesario para correr el sistema, en caso de que se haya reemplazado el equipo.
4. Revisión del funcionamiento del sistema, si hubiera algún problema con el mismo se recupera el último respaldo generado según el procedimiento de respaldos de sistemas.
5. Realizar pruebas de estrés del funcionamiento y operatividad local para corroborar el correcto funcionamiento.

a.11.3.3. Acciones a aplicar en los activos de la Base de Datos:

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.
3. Instalar sistema operativo y lo necesario para correr el sistema, en caso de que se haya reemplazado el equipo.
4. Revisar el funcionamiento de la base de datos, si hubiera algún problema con el mismo se recupera el último respaldo generado según el procedimiento de respaldos de sistemas.
5. Revisar pruebas de estrés del funcionamiento y operatividad local para corroborar el correcto funcionamiento.

a.11.4. Escenario de contingencia de corte de Energía Eléctrica.

a.11.4.1. Acciones a aplicar en los activos del Sistema:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS (soporte técnico) y notifica cuando esté en un 10% de batería a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.
3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.

a.11.4.2. Acciones a aplicar en los activos del Equipo:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS y notifica cuando esté en un 10% de batería, a los usuarios para que puedan guardar los

trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.

3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.

a.11.4.3. Acciones a aplicar en los activos de la Base de Datos:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS (Soporte técnico) y notifica cuando esté en un 10% de batería, a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.
3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.

a.12. RESTAURACIÓN DEL SERVICIO

Acciones a realizar una vez recuperado el servicio afectado para restablecer el servicio a su condición normal:

a.12.1. Habilitan las configuraciones iniciales en las cuentas y permisos de acceso de los usuarios.

a.12.2. Conectar el equipo a la red LAN y WAN para la activación del servicio, realizando pruebas de estrés del funcionamiento.

a.12.3. Solicitar a los usuarios utilizar el sistema de manera regular y reportar cualquier detalle de funcionamiento.

a.12.4. Probar y monitoreo de 7 días del funcionamiento del sistema, base de datos y equipo, para determinar si se realiza alguna otra actividad.

a.12.5. Solicitar a los usuarios hacer la recuperación de la información generada en formato impreso al sistema para tener la integridad de la información totalmente.

b. BCP-DRP PARA EL SERVICIO DE CURSOS EN LÍNEA

b.1. OBJETIVO

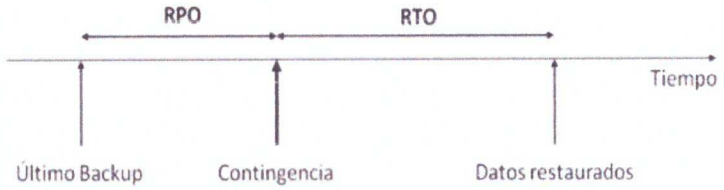
Mantener la continuidad del servicio para que los usuarios de los cursos virtuales sean accedidos en línea en el momento que lo requieran.

b.2. ALCANCE

Las acciones de este plan están diseñadas para asegurar la continuidad de las operaciones así como recuperar los servicios en los tiempos planeados.

b.3. TIEMPO DE RECUPERACIÓN OBJETIVO (RTO): Hardware: 240hrs, Software: 24hrs.

b.4. PUNTO DE RECUPERACIÓN OBJETIVO DE LA INFORMACIÓN (RPO): 360 horas



b.5. SUPUESTOS

Los siguientes supuestos en relación al servicio crítico se han establecido como medida preventiva y punto de partida para asegurar el desarrollo del presente plan:

b.5.1. El equipo de respuesta para atender el servicio crítico, estará disponible en caso de emergencia.

b.5.2. Se cuenta con depuración programada de usuarios de sistema.

b.5.3. Se cuenta con respaldos disponibles e íntegros de los datos y sistemas tecnológicos implicados en el presente plan.

b.5.4. El personal relacionado con la operación del servicio crítico está identificado y capacitado en sus funciones de respuesta de recuperación y está disponible para actuar en la ejecución del presente Plan.

b.5.5. El personal informático aplica el procedimiento de respaldos y restauración de los sistemas y datos asociados al servicio crítico.

b.5.6. Se han identificado los activos informáticos críticos relacionados con el servicio a atender en este Plan.

b.5.7. Se cuenta con una planeación tecnológica que permite identificar el recurso económico que se pueda necesitar para asegurar la adquisición de infraestructura requerida para la operación eficiente de los servicios.

b.5.8. Se cuenta con personal capacitado de servicios generales en el caso de ser necesario para la contingencia.

b.5.9. Los dueños del sistema crítico identifican la información que se tendría que recuperar y cómo recuperarla físicamente.

b.5.10. Se cuenta con respaldos actualizados y disponibles de los datos y softwares de los sistemas implicados en el presente plan.

b.6. ESCENARIOS DE CONTINGENCIA

(En función de los eventos de mayor riesgo identificados en el análisis ERA).

ESCENARIOS DE CONTINGENCIA	ACTIVOS ASOCIADOS AL ESCENARIO
Ciberataque	Bases de dato, sistema (código), equipo
Internet	Sistema.
Incendios	Equipo (Servidores, equipos de red, equipo de respaldo), sistema, base de datos.
Energía eléctrica	Sistema, Equipo, Base de Datos.

b.7. EQUIPO DE RESPUESTA PARA LA ACTIVACIÓN DEL PLAN

RESPONSABLE/ CARGO	TEL/ EXT / CEL	CORREO	FIRMA
Oscar Moises Alvarez Esparza Coordinador de Soporte Técnico	185	moises.alvarez@utcalvillo.edu.mx	
Hugo de Jesús Becerra Reyes Administrador de plataforma	106	hugo.becerra@utcalvillo.edu.mx	
Laura Lucía Serna Saucedo Coordinador de Servicios Generales.	135	laura.serna@utcalvillo.edu.mx	
Angel Soriano ACNET	4491096985	asoriano@digitalags.net	*
Oficina CFE	071	n/a	*
Noé Rodríguez Martínez Director de Administración y Finanzas	191	noe.rodriguez@utcalvillo.edu.mx	
José de Jesús Santana Loera Jefe del Departamento de Gestión Académica	204	jose.santana@utcalvillo.edu.mx	
Daniel Rojas Salazar	194	daniel.rojas@utcalvillo.edu.mx	

* Este documento se les enviará vía email para que los proveedores estén enterados, mientras se obtienen sus firmas.

b.8. MEDIDAS INICIALES DE CONTINUIDAD

b.8.1. Medidas iniciales ante un ciberataque:

1. Desconexión de servidor de servicio de la red exterior.
2. Desconexión de servidor de servicio de la red interna.
3. Limitar el acceso a los usuarios.
4. Cambios de contraseñas de administradores.
5. Identificar el estatus del antivirus.
6. Verificar la bitácora de actividad.
7. Identificar ataque y bloquear.

b.8.2. Medidas iniciales ante un corte de Internet:

1. Realizar las pruebas de conexión de internet para confirmar el corte del servicio del internet.
2. Revisar si el corte del servicio en interno o externo:
    a. Si es Interno, revisar el cableado, servidor y software su funcionamiento para tratar de resolver el fallo.
    b. Si es externo, contactar al proveedor del Servicio para reportar y a la vez, determinen el tiempo de restablecimiento.
3. Si se tuviera conexión de internet de respaldo se activaría para el servicio temporal.
4. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.

b.8.3. Medidas iniciales ante un incendio:

1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con servicios generales para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.

b.8.4. Medidas iniciales ante un corte de energía eléctrica:

1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con servicios generales y CFE si es necesario para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia, los tiempos aproximados de recuperación y los tiempos aproximados de servicio del UPS.

b.9. BCP. ESTRATEGIAS DE CONTINUIDAD DE LA OPERACIÓN DEL SERVICIO

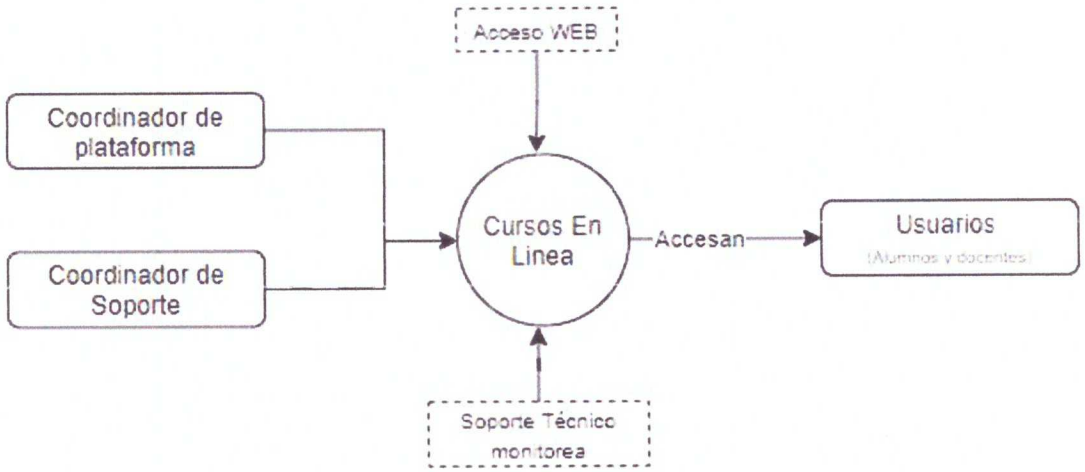
Las siguientes acciones se aplicarán como medidas de continuidad a ser adoptadas de forma temporal en caso de interrupción del servicio, para actuar de manera rápida y eficaz ante una eventualidad que ponga en riesgo la operación normal de las actividades.

b.9.1. Los docentes enviarán por correo electrónico la información del curso a los alumnos.

b.9.2. Los alumnos entregan vía correo electrónico los avances del curso.

b.9.3. El alumno será retroalimentado vía correo electrónico si es necesario.

b.10. ESQUEMA DE ARQUITECTURA DEL SERVICIO (diagrama a nivel 0).



b.11. DRP. RECUPERACIÓN DE LOS ACTIVOS ASOCIADOS A CADA ESCENARIO DE CONTINGENCIA

Acciones para restablecer las funciones de los sistemas asociados a los servicios críticos:

b.11.1. Escenario de contingencia de ciberataque:

b.11.1.1. Acciones a aplicar en los activos de Equipo:

1. Desconectar el equipo de la red.
2. Reiniciar el equipo.
3. Revisar el estatus de antivirus y software de protección.
4. Realizar limpieza física y lógica, además de correr un escaneo avanzado con el antivirus, para bloquear actividad sospechosa.
5. Realizar cambios de contraseñas de administrador.
6. Solicitar al área de adquisiciones con autorización de director de administración y finanzas o rector, la compra de equipo, parte del mismo o del antivirus, si fuera necesario.
7. Nuevamente escanear computadora para confirmar que ya no existen archivos o procesos sospechosos.

b.11.1.2. Acciones a aplicar en los activos de Sistema:

1. Verifica el acceso al sistema con el equipo desconectado de la red.
2. Verificar el acceso con las credenciales y cambiar contraseñas de administrador.
3. Verificar el funcionamiento del sistema en todos sus módulos.
4. Reestablecer el último respaldo si fuera necesario, y verificar el comportamiento.

b.11.1.3. Acciones a aplicar en los activos de Base de Datos:

1. Revisar la integridad de la información, generando reportes y registros actuales.
2. Restablecer el último respaldo si fuera necesario
3. Verificar las credenciales de conexión a la base de datos y si fuera necesario cambiar contraseña.
4. Recuperar los registros faltantes si hubiera el caso que se pudieran recuperar de otra fuente.

b.11.2. Escenario de contingencia de un corte de Internet:

b.11.2.1. Acciones a aplicar en los activos de Sistema:

1. Verificar la disponibilidad de un posible proveedor de internet como conexión de respaldo con el área de adquisiciones.
2. Utilizar el sistema de manera de red local.

b.11.3. Escenario de contingencia de Incendio:

b.11.3.1. Acciones a aplicar en los activos del Equipo

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.
3. Realizar pruebas de estrés o de conexión, confirmando el funcionamiento correcto.

b.11.3.2. Acciones a aplicar en los activos del Sistema:

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.
3. Instalar sistema operativo y lo necesario para correr el sistema, en caso de que se haya reemplazado el equipo.

4. Revisión del funcionamiento del sistema, si hubiera algún problema con el mismo se recupera el último respaldo generado según el procedimiento de respaldos de sistemas.
5. Realizar pruebas de estrés del funcionamiento y operatividad local para corroborar el correcto funcionamiento.

b.11.3.3. Acciones a aplicar en los activos de la Base de Datos:

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.
3. Instalar sistema operativo y lo necesario para correr el sistema, en caso de que se haya reemplazado el equipo.
4. Revisar el funcionamiento de la base de datos, si hubiera algún problema con el mismo se recupera el último respaldo generado según el procedimiento de respaldos de sistemas.
5. Revisar pruebas de estrés del funcionamiento y operatividad local para corroborar el correcto funcionamiento.

b.11.4. Escenario de contingencia de corte de Energía Eléctrica.

b.11.4.1. Acciones a aplicar en los activos del Sistema:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS (soporte técnico) y notifica cuando esté en un 10% de batería a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.
3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.

b.11.4.2. Acciones a aplicar en los activos del Equipo:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS y notifica cuando esté en un 10% de batería, a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.

3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.
4. Si hubiera algún daño en el equipo por el corte eléctrico, solicitar al área de adquisiciones la compra de la pieza o equipo para reactivar el servicio.

b.11.4.3. Acciones a aplicar en los activos de la Base de Datos:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS (Soporte técnico) y notifica cuando esté en un 10% de batería, a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.
3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.

b.12. RESTAURACIÓN DEL SERVICIO

Acciones a realizar una vez recuperado el servicio afectado para restablecer el servicio a su condición normal:

b.12.1. Habilitar las configuraciones iniciales en las cuentas y permisos de acceso de los usuarios.

b.12.2. Conectar el equipo a la red LAN y WAN para la activación del servicio, realizando pruebas de estrés del funcionamiento.

b.12.3. Solicitar a los usuarios utilizar el sistema de manera regular y reportar cualquier detalle de funcionamiento.

b.12.4. Probar y monitoreo de 7 días del funcionamiento del sistema, base de datos y equipo, para determinar si se realiza alguna otra actividad.

b.12.5. Solicitar a los usuarios hacer la recuperación de la información generada en formato impreso al sistema para tener la integridad de la información totalmente.

c. BCP-DRP PARA EL SISTEMA DE GESTIÓN DE CONEXIÓN DE INTERNET

c.1. OBJETIVO

Mantener la correcta gestión del servicio de internet para tener además de una conexión de internet, que ésta sea más eficiente y veloz para los usuarios y zonas de servicio de toda la comunidad universitaria.

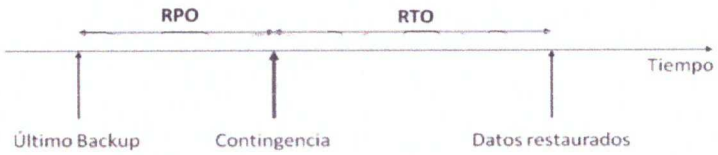
c.2. ALCANCE

Las acciones de este plan están diseñadas para asegurar la continuidad de las operaciones, así como recuperar los servicios en los tiempos planeados.

c.3. TIEMPO DE RECUPERACIÓN OBJETIVO (RTO): Hardware: 240hrs, Software: 2hrs.

c.4. PUNTO DE RECUPERACIÓN OBJETIVO DE LA INFORMACIÓN (RPO):

720 horas.



c.5. SUPUESTOS

Los siguientes supuestos en relación al servicio crítico se han establecido como medida preventiva y punto de partida para asegurar el desarrollo del presente plan:

c.5.1. El equipo de respuesta para atender el servicio crítico, estará disponible en caso de emergencia.

c.5.2. Se cuenta con depuración programada de usuarios de sistema.

c.5.3. Se cuenta con respaldos disponibles e íntegros de los datos y sistemas tecnológicos implicados en el presente plan.

c.5.4. El personal relacionado con la operación del servicio crítico está identificado y capacitado en sus funciones de respuesta de recuperación y está disponible para actuar en la ejecución del presente Plan.

c.5.5. Se han identificado los activos informáticos críticos relacionados con el servicio a atender en este Plan.

c.5.6. Se cuenta con una planeación tecnológica que permite identificar el recurso económico que se pueda necesitar para asegurar la adquisición de infraestructura requerida para la operación eficiente de los servicios.

c.5.7. Se cuenta con personal capacitado de servicios generales en el caso de ser necesario para la contingencia.

c.5.8. Los dueños del sistema crítico identifican la información que se tendría que recuperar y cómo recuperarla físicamente.

c.6. ESCENARIOS DE CONTINGENCIA

(En función de los eventos de mayor riesgo identificados en el análisis ERA).

ESCENARIOS DE CONTINGENCIA	ACTIVOS ASOCIADOS AL ESCENARIO
Ciberataque	Sistema (código), equipo
Internet	Sistema.
Incendio	Equipo (Servidores, equipos de red, equipo de respaldo), sistema.
Energía eléctrica	Sistema, Equipo.

c.7. EQUIPO DE RESPUESTA PARA LA ACTIVACIÓN DEL PLAN

RESPONSABLE/ CARGO	TEL/ EXT / CEL	CORREO	FIRMA
Oscar Moises Alvarez Esparza Coordinador de Soporte Técnico	185	moises.alvarez@utcalvillo.edu.mx	
Laura Lucía Serna Saucedo Coordinador de Servicios Generales	135	laura.serna@utcalvillo.edu.mx	
Angel Soriano ACNET	4491096985	asoriano@digitalags.net	*
Oficina CFE	071	n/a	*
Noé Rodríguez Martínez Director de Administración y Finanzas	191	noe.rodriguez@utcalvillo.edu.mx	
Daniel Rojas Salazar Coordinador de Adquisiciones	194	daniel.rojas@utcalvillo.edu.mx	

* Este documento se les enviará vía email para que los proveedores estén enterados, mientras se obtienen sus firmas.

c.8. BCP. MEDIDAS INICIALES DE CONTINUIDAD

c.8.1. Medidas iniciales ante un ciberataque:

1. Desconexión de servidor de servicio de la red exterior.
2. Desconexión de servidor de servicio de la red interna.
3. Limitar el acceso a los usuarios.
4. Cambios de contraseñas de administradores.
5. Identificar el estatus del antivirus.
6. Verificar la bitácora de actividad.
7. Identificar ataque y bloquear.

8. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.

c.8.2. Medidas iniciales ante un corte de Internet:

1. Realizar las pruebas de conexión de internet para confirmar el corte del servicio del internet.
2. Revisar si el corte del servicio en interno o externo:
   a. Si es Interno, revisar el cableado, servidor y software su funcionamiento para tratar de resolver el fallo.
   b. Si es externo, contactar al proveedor del Servicio para reportar y a la vez, determinen el tiempo de restablecimiento.
3. Si se tuviera conexión de internet de respaldo se activaría para el servicio temporal.
4. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.

c.8.3. Medidas iniciales ante un incendio:

1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con servicios generales para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia y los tiempos aproximados de recuperación.
4. Ver la posibilidad de utilizar otro espacio para el restablecimiento temporal.

c.8.4. Medidas iniciales ante un corte de energía eléctrica:

1. Identificar la magnitud de la contingencia y afección al servicio.
2. Trabajar con servicios generales y CFE si es necesario para determinar el tiempo de recuperación del servicio.
3. Comunicar a los usuarios sobre la contingencia, los tiempos aproximados de recuperación, así como los tiempos aproximados de respaldo eléctrico del UPS.
4. Ver la posibilidad con el área de adquisiciones la renta de una planta eléctrica.

c.9. MEDIDAS DE CONTINUIDAD DE LA OPERACIÓN DEL SERVICIO

Las siguientes acciones se aplicarán como medidas de continuidad a ser adoptadas de forma temporal en caso de interrupción del servicio, para actuar de manera rápida y eficaz ante una eventualidad que ponga en riesgo la operación normal de las actividades.

c.9.1. Los usuarios determinarían si pueden continuar actividades con otra alternativa, de lo contrario sería esperar a la reactivación del servicio.

c.9.2. Los usuarios pueden utilizar los datos de su celular si fuera urgente su uso.

c.9.3. Si hubiera conexión de internet de respaldo, se activa para su uso, de lo contrario sería esperar a la reactivación de la conexión principal.

c.10. ESQUEMA DE ARQUITECTURA DEL SERVICIO (diagrama a nivel 0).

c.11. DRP. RECUPERACIÓN DE LOS ACTIVOS ASOCIADOS A CADA ESCENARIO DE CONTINGENCIA

Acciones para restablecer las funciones de los sistemas asociados al servicio crítico en función de cada escenario (sección.6):

c.11.1. Escenario de contingencia de ciberataque:

c.11.1.1. Acciones a aplicar en los activos de Equipo:

1. Revisar el estatus de antivirus y software de protección.
2. Realizar limpieza física y lógica, además de correr un escaneo avanzado con el antivirus, para bloquear actividad sospechosa.
3. Realizar cambios de contraseñas de administrador.
4. Solicitar al área de adquisiciones con autorización de director de administración y finanzas o rector, la compra de equipo, parte del mismo o del antivirus, si fuera necesario.
5. Si fuera necesario, restablecer el último respaldo generado.
6. Nuevamente escanear computadora para confirmar que ya no existen archivos o procesos sospechosos.

c.11.1.2. Acciones a aplicar en los activos de Sistema:

1. Verifica el acceso al sistema con el equipo desconectado de la red.
2. Verificar el acceso con las credenciales y cambiar contraseñas de administrador.
3. Verificar configuraciones que sean correctas o ajustar las reglas de conexión.
4. Verificar el funcionamiento del sistema en todos sus módulos.
5. Reestablecer el último respaldo si fuera necesario, y verificar el comportamiento.

c.11.2. Escenario de contingencia de un corte de Internet:

c.11.2.1. Acciones a aplicar en los activos de Sistema:

1. Verificar la disponibilidad de un posible proveedor de internet como conexión de respaldo con el área de adquisiciones.
2. Utilizar el sistema de manera de red local.

c.11.3. Escenario de contingencia de Incendio:

c.11.3.1. Acciones a aplicar en los activos del Equipo:

1. Entrar a Site a realizar un levantamiento de daños ya que se declare el libre acceso a la zona por la brigada contra incendios.
2. Revisar el estatus de los equipos, encendido en otro lugar, revisar el funcionamiento y si hubiera problema con el equipo, se solicitará compra según la necesidad o reemplazo.

c.11.3.2. Acciones a aplicar en los activos del Sistema:

1. Instalar sistema operativo, sistema y configuraciones en caso de que se haya reemplazado el equipo o igual se restablece el último respaldo.
2. Realizar pruebas de estrés del funcionamiento y operatividad local para corroborar el correcto funcionamiento.

c.11.4. Escenario de contingencia de corte de Energía Eléctrica.

c.11.4.1. Acciones a aplicar en los activos del Sistema:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS (soporte técnico) y notifica cuando esté en un 10% de batería a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual

manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.

3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.

c.11.4.2. Acciones a aplicar en los activos del Equipo:

1. Confirmar el corte eléctrico por parte de Servicios Generales, si fuera necesario reportar a CFE sobre el mismo, e indica al área de soporte técnico los tiempos aproximados para su restablecimiento.
2. Monitorear el estatus de servicio del UPS y notifica cuando esté en un 10% de batería, a los usuarios para que puedan guardar los trabajos activos que tengan sobre sus equipos de oficina y de igual manera se hace el apagado correcto del servidor para evitar daños en los componentes del equipo.
3. Si el UPS llega a su fin y no se restableció la energía eléctrica, la actividad continua en los formatos impresos determinados si la actividad lo permite.
4. Si hubiera algún daño en el equipo por el corte eléctrico, solicitar al área de adquisiciones la compra de la pieza o equipo para reactivar el servicio.

c.12. RESTAURACIÓN DEL SERVICIO

Acciones a realizar una vez recuperado el servicio afectado para restablecer el servicio a su condición normal:

c.12.1. Se habilitan las cuentas y permisos de los usuarios.
c.12.2. Se conecta el equipo a la red local e Internet.
c.12.3. Se pide a los usuarios utilizar el sistema de manera regular y reportar cualquier detalle de funcionamiento.
c.12.4. Prueba y monitoreo de 7 días del funcionamiento del sistema y equipo.
c.12.5. Se realizan pruebas de estrés al sistema, verificando el comportamiento.
c.12.6. Se apaga servidor temporal en caso se haya habilitado alguno.

CONTROL DE CAMBIOS AL DOCUMENTO

N° de Revisión	Fecha de Revisión	Descripción del Cambio

AGUASCALIENTES

GOBIERNO DEL ESTADO

Contigo al 100