



UNIVERSIDAD  
POLITÉCNICA DE  
**BACALAR**

# Plan de Contingencia Informática y Recuperación

Handwritten blue ink marks are located in the bottom right corner of the page. They include a large, stylized letter 'A' and a signature that appears to be 'A. B. C.'.



## Introducción

Un plan de contingencia informática y recuperación es un conjunto de estrategias y procedimientos que permiten a una organización restaurar sus sistemas de tecnologías y datos después de un evento disruptivo.

Actualmente las instituciones públicas y privadas se han vuelto cada vez más dependientes de las computadoras y las redes de comunicación de datos para mejorar sus actividades, y mejorar su productividad.

A medida que la tecnología ha evolucionado, y la importancia de los sistemas de información con ella, la información se ha convertido en uno de los patrimonios principales de toda Institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

El presente documento está diseñado para identificar las actividades, los procesos y riesgos críticos de la Universidad Politécnica de Bacalar (UPB) ante cualquier evento de desastres (falla eléctrica grave, sismo, incendio, inundación), con la finalidad de determinar planes de acción que nos permitan encontrar soluciones que puedan ser utilizadas para una correcta recuperación, continuidad y reanudación eficiente y efectiva de los procesos y servicios vitales en el menor tiempo posible para reducir el impacto del desastre en el proceso de impartir educación superior en la UPB.

## Objetivo

Diseñar un plan para establecer los principios básicos, normas y procedimientos necesarios para enfrentar cualquier dificultad que pueda surgir en los equipos e instalaciones tecnológicas, aplicaciones informáticas, bases de datos y sistemas de información y comunicación así como los servicios administrados por el Departamento de Desarrollo de Sistemas (DDS) que permitan la recuperación de los mismos en forma rápida y oportuna en caso de algún siniestro o contingencia, con el fin de garantizar la operabilidad, continuidad, seguridad y confiabilidad de los procesos y servicios indispensables de mayor urgencia para el funcionamiento de la UPB.

## Alcance

El Plan de Contingencia Informática y Recuperación es un análisis que contiene los posibles riesgos y eventuales siniestros a los cuales pueden estar



expuestos los equipos e instalaciones tecnológicas, aplicaciones informáticas, bases de datos y sistemas de información y comunicación, así como componentes y recursos informáticos que son manejados en la UPB.

Este plan ha sido diseñado para utilizarse ante una situación de desastres que afecten las instalaciones y recursos informáticos con los que cuenta la UPB en materia de tecnología y está dirigido a minimizar eventuales riesgos ante situaciones adversas que atentan contra el funcionamiento normal de los procesos y servicios esenciales de la misma.

## Definiciones

**Acceso.** – Proceso mediante el cual se otorga permiso a un usuario o entidad para acceder a un sistema, recurso o información específica, basándose en su identidad y en políticas de seguridad predefinidas. Este permiso se otorga después de una autenticación exitosa y garantiza que solo las personas o sistemas con los privilegios necesarios puedan ver, usar o modificar los datos protegidos.

**Amenaza.** – Cualquier evento o acción que pueda causar daño o interferir con el funcionamiento de un sistema, red de datos y/o computadora que, al aprovechar una vulnerabilidad, accede de forma no autorizada, compromete su confidencialidad, integridad o disponibilidad. Ejemplo: fallas del suministro eléctrico, virus, saboteos o descuido del usuario.

**Aplicaciones.** – Son los archivos y programas desarrollados o adquiridos por una entidad u organización para realizar o agilizar una o varias tareas específicas.

**Ataque.** – Cualquier acción o evento que pretende acceder, dañar, interrumpir, robar información o interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a una computadora.

**Base de Datos.** – Es un conjunto de datos organizados, entre los cuales existe una correlación y que, también, están almacenados con criterios independientes de los programas que los utilizan. La base de datos también puede definirse como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:



- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

**Cortafuegos (Firewall).** – Es un sistema de seguridad de red, ya sea de hardware o software, que actúa como una barrera entre una red interna de confianza y una red externa no confiable, el cual está configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos, esto es, supervisa y controla el tráfico de red entrante y saliente, mediante el bloqueo del tráfico no autorizado y el acceso malintencionado con base en un conjunto de normas y otros criterios de seguridad predeterminados.

**Datos.** – En informática los datos son hechos y cifras que una computadora puede interpretar y almacenar y que, al ser procesados, constituyen una información. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, números, archivos y bases de datos, texto, hojas de cálculo, imágenes, vídeo, etc.

**Integridad.** – En informática se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema, es decir, que la información contenida en ellos sea precisa, completa y que estos no estén sujetos a modificaciones no autorizadas. Las técnicas de integridad buscan asegurar la exactitud de los datos y la fiabilidad de los sistemas al largo de su ciclo de vida, protegiéndolos de la corrupción, pérdida y manipulación, así como la discreción que se debe de tener con ellos.

**Incidente.** – Un incidente en informática es un evento no deseado que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o de los datos que se maneja; cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

**Privacidad.** – Es la protección de datos personales en el ámbito digital que otorga a los usuarios el control sobre su información al decidir quién accede a ella y cómo se utiliza.



**Seguridad.** – Es el conjunto de técnicas y prácticas que protegen sistemas, redes, programas y datos contra ataques, daños o accesos no autorizados que garantizan la confidencialidad, integridad y disponibilidad de la información. Se enfoca en prevenir ciberataques, asegurar la información personal y corporativa y mantener el funcionamiento continuo de los sistemas y abarca la seguridad de las redes de comunicación, la nube, los dispositivos y las aplicaciones. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

**Sistemas de Información.** – Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos, hardware y redes de comunicación. Estos ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada institución.

**Riesgo.** – Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de errores humanos, fallos de hardware, un fenómeno natural o artificial, que puedan causar un impacto negativo en la información tales como la pérdida de confidencialidad, integridad o disponibilidad de datos.

**Tecnología.** – Se refiere al conjunto de herramientas, equipos de cómputo, programas, redes de comunicación y sistemas de información que procesan y agilizan la creación, almacenamiento y gestión de información en una institución.

## Identificación de procesos y servicios sustantivos

Identificar los procesos y servicios sustantivos permite definir las actividades sustanciales y esenciales de la UPB, lo cual es de suma importancia ya que implica conocer los principales servicios y productos que serán reactivados en caso de que ocurra una contingencia. Tras un análisis detallado se han priorizado los siguientes procesos, servicios, softwares y sistemas de información.

- Principales procesos:
  - ✓ Control Escolar.





- ✓ Nómina.
- ✓ Contabilidad.
  
- Principales servicios que deberán ser restablecidos y/o recuperados:
  - ✓ Energía eléctrica.
  - ✓ Internet.
  - ✓ Correo electrónico.
  - ✓ Página institucional.
  - ✓ Herramientas de *Microsoft Office*.
  - ✓ Telefonía.
  
- Software Base:
  - ✓ Sistema de Servicios y Control Escolar.
  - ✓ Sistemas y plataformas de Nómina y Contabilidad.
  - ✓ Base de datos.
  - ✓ Respaldos de información.
  
- Respaldo de la información:
  - ✓ Respaldo de la base de datos.
  - ✓ Respaldo de la Plataforma de Aplicaciones (Sistemas).
  - ✓ Respaldo de sitios web.

## Identificación de Riesgos (Análisis y Valoración)

La pérdida total o parcial de los procesos y servicios puede ocurrir por las siguientes causas:

- Delitos informáticos: ocurren cuando son atacados los sistemas de información, datos o redes de comunicación a través de medios electrónicos mediante la utilización de una identidad falsa para acceder a plataformas, la alteración de datos y el bloqueo de servicios u operaciones esenciales.
- Vulnerabilidades y riesgos de seguridad en sistemas operativos o en aplicaciones que se encuentran alojadas en los equipos de cómputo.
- Problemas y exposiciones tales como fuga de datos o información de claves de usuarios, interceptación de líneas, fallas eléctricas, virus o código malicioso en el *software*, errores durante la generación y restauración de respaldos de información que detengan parcial o totalmente los servicios prestados por la institución.



- Exposición de acceso físico, como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copias, visualización o divulgación de información sensible.
- Problemas y exposiciones ambientales, como falla en la energía eléctrica interna o externa, voltaje severamente reducido, depresiones, picos y sobre voltajes o interferencia magnética.
- Falla en los servicios de internet por parte del proveedor.
- Sabotaje de los procesos y servicios de los sistemas de información a causa de chantaje, fraude, descontentos, amenazas (acción disciplinaria o con despido), directas o indirectamente involucradas con el personal.
- Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor o los medios empleados para extinguir y contener un incendio, ya sea por acción directa o indirecta.
- Combustión espontánea de algún elemento que forme parte de algún equipo de cómputo o dispositivo.

## Medidas preventivas

Medidas para controlar los diferentes accesos a los activos computacionales y restringirlos en caso de que se presenten.

- **Acceso físico de personas no autorizadas.** – Únicamente el usuario al que fue asignado el equipo de cómputo tendrá acceso total al mismo, salvo indicación directa y explícita de su jefe inmediato.
- **Acceso a plataformas o sistemas de información y correo institucional.** – Solo el personal del DDS será quien administre las cuentas de usuario y contraseñas de acceso para todos los sistemas de información, previa solicitud por parte de las áreas que requieran altas, bajas o modificaciones en estas plataformas. Al recibir el nombre de usuario y contraseña, el usuario final es y será el único responsable de salvaguardar sus datos.



- **Acceso a la Red Institucional.** – Sólo el personal autorizado podrá ingresar a los servicios de la red de internet institucional, la persona responsable del DDS es quien realizará la configuración necesaria para tal efecto. En caso de detectar conexiones no permitidas, se procederá a bloquear el acceso a los dispositivos.
- **Acceso al área de Servidores (SITE).** – Solo personal autorizado por el DDS tendrá acceso al área del SITE. Salvo alguna indicación por parte del personal directivo.
- **Acceso restringido a los sistemas información, aplicaciones informáticas y datos.** – Los departamentos y/o áreas que conforman la UPB cuentan con amplia información y sistemas diversos, para acceder a estos, se cuenta con credenciales de acceso, tales como usuarios y contraseñas; esta información será accesible por el titular del área y al menos un integrante del mismo, serán los únicos facultados para acceder a la totalidad de información de su departamento.
- **Uso de dispositivos de almacenamiento portátiles (Disco duro externo, memoria USB).** – Se utilizarán preferentemente para realizar respaldos de información de manera general, dichos respaldos no se compartirán para evitar cualquier posible propagación de virus o amenazas.

## Previsión ante siniestros y desastres naturales

Los desastres causados por un evento natural o humano pueden ocurrir en cualquier parte, hora y organización.

Existen distintos tipos de contingencias o riesgos, como:

**Riesgos naturales:** mal tiempo, inundaciones por exceso de lluvia, huracanes, terremotos, tsunamis, etc.

**Riesgos tecnológicos:** incendios por equipos electrónicos, fallas en el suministro de energía eléctrica, fallas en telecomunicaciones, falla total o parcial de cableado, fallas de hardware y software.

**Riesgos sociales:** actos vandálicos, desórdenes, bloqueo de acceso a instalaciones, actos terroristas y/o crimen común.



Con base en la identificación de riesgos o desastres efectuada previamente, a continuación, se presenta la jerarquización de los elementos que integran los sistemas de información, según su importancia, para definir la prioridad incluso antes de activar un plan de contingencia informática, esto implica intentar rescatar todo lo que podría generar una pérdida irreparable.

Nivel	Nombre	Descripción
1	Servidores	Contienen todos los sistemas de información que requieren de alta disponibilidad, referente a los servicios escolares, información del personal administrativo y docente, así como los servicios financieros y todas las bases de datos.
2	Respaldos de Información	Ante cualquier eventualidad se deben de realizar copias de seguridad periódicas de la información valiosa que se genera por las áreas que conforman la UPB, ya que son el medio de rescate, continuidad y recuperación para el correcto funcionamiento de la misma.
3	Equipo de las áreas que conforman la Institución	Contienen datos e información importante que generan en cada uno de los departamentos.
4	Dispositivos de Red (Routers, switches, acces point)	Indispensables para la reactivación del acceso y cobertura a internet en las instalaciones de la Institución.

## Plan de recuperación y respaldo.

La tarea más elemental e importante es y será la base de cualquier solución ante cualquier desastre en la UPB es el denominado "Respaldo de información". Esta actividad se realizará con base en las siguientes directivas:

- ❖ La persona servidora pública es y será la única responsable de salvaguardar su información, y deberá realizar su respaldo con una periodicidad semanal, quincenal o mensual.
- ❖ El respaldo de información realizado se mantendrá en un lugar seguro y fácilmente accesible. Tanto el personal, como su jefe inmediato deberán conocer la ubicación del respaldo.



- ❖ Los respaldos de información se podrán almacenar en dos formas o ubicaciones:
  - ✓ Dispositivos físicos. - como un disco duro externo, CD, DVD o memoria USB.
  - ✓ Servicio en la nube. - se recomienda el uso de "Google drive" y "Microsoft OneDrive", accesibles desde la cuenta de correo institucional para todo personal activo.
- ❖ Respecto a la plataformas y herramientas para la realización de clases en línea y presenciales, el personal académico y docente son los responsables de realizar el respaldo de sus cursos.
- ❖ El personal de la institución podrá solicitar asesoría respecto de la creación de sus respaldos de información al personal del Departamento de Desarrollo de Sistemas, misma que se otorgará oportunamente con base en la carga de trabajo del área.
- ❖ El resguardo del respaldo de información es responsabilidad del usuario.
- ❖ Los respaldos de cada sistema de información alojados en los servidores se realizarán semanal, quincenal o mensual debido a su importancia en la operación, por el Departamento de Desarrollo de Sistemas.



A continuación, se presenta el plan de recuperación que se aplicará ante cualquier contingencia dependiendo del tipo de siniestro, de acuerdo con la siguiente tabla:

Tipo	Clasificación	Consecuencias	Modo de recuperación	Prevención
Incendio	Grave	De acuerdo con la magnitud y la gravedad, puede ocurrir la pérdida total del inmueble y los equipos e instalaciones tecnológicas.	Adquisición: de equipo de cómputo nuevo (servidores o PC), utilizar el último respaldo de información para la restauración de procesos y servicios.	<ul style="list-style-type: none"> <li>• Uso de extintores correspondientes en zonas claves y capacitación para el personal en su uso.</li> <li>• Inspecciones eléctricas periódicas para prevenir cortocircuitos.</li> <li>• No sobrecargar tomas de corriente. Plan de evacuación y simulacros regulares</li> </ul>
Inundación (Huracanes)	Grave	Dependerá de la magnitud del fenómeno y esta se podrá clasificar en pérdida total o parcial de los equipos e instalaciones tecnológicas.	Adquisición: de equipo de cómputo nuevo (servidores o PC), utilizar el último respaldo de información para la restauración de procesos y servicios.	<ul style="list-style-type: none"> <li>• Instalación de equipos en zonas levantadas o seguras (alejadas de áreas inundables). Sellado de puertas, ventanas y drenaje en áreas críticas.</li> <li>• Uso de racks herméticos para servidores. Plan de contingencia para traslado de equipos a zonas seguras antes de un huracán.</li> <li>• Contratación de seguros contra desastres naturales</li> </ul>
Epidemia Viral humana	Alto	Impedir la interacción física entre los servidores públicos de la Institución.	Realizar actividades 100 % en línea, salvo algunas excepciones e indicaciones por parte del área directiva y garantizar el funcionamiento de servidores, para continuar con la operación normal de la institución.	<ul style="list-style-type: none"> <li>• Implementación de políticas de trabajo en casa y plataformas colaborativas en línea desde antes.</li> <li>• Capacitación del personal en herramientas digitales.</li> <li>• Disposición de protocolos sanitarios y monitoreo de salud del personal.</li> <li>• Uso de Redes Privadas Virtuales (VPNs) seguras y acceso remoto controlado a sistemas internos.</li> </ul>

Tipo		Clasificación	Consecuencias	Modo de Recuperación	Recomendaciones de Prevención
Virus Cibernético	Medio	Depende del área donde se filtre el virus, se determinan los daños que este pueda causar.	Uso de antivirus o <i>antimalware</i> , en caso de pérdida de información utilizar el último respaldo de información para la restauración de procesos y servicios.	<ul style="list-style-type: none"> <li>• Uso de antivirus/malware actualizados y con licencia.</li> <li>• Firewalls bien configurados.</li> <li>• Segmentación de redes críticas.</li> <li>• Políticas de contraseñas seguras.</li> <li>• Capacitación en ciberseguridad al personal.</li> <li>• Respaldos frecuentes fuera de línea o en la nube.</li> </ul>	
Robo	Bajo	Pérdida de equipos.	Adquisición de equipo de cómputo nuevo (servidores o PC), utilizar el último respaldo de información para la restauración de procesos y servicios.	<ul style="list-style-type: none"> <li>• Uso de cámaras de videovigilancia.</li> <li>• Control de acceso físico con credenciales.</li> <li>• Equipos anclados físicamente (cables de seguridad, racks cerrados).</li> <li>• Contratación de personal de seguridad o vigilancia.</li> <li>• Etiquetado y control de inventario de equipos.</li> </ul>	
Tembor	Bajo	Dependerá de la escala, existe la posibilidad de que algunos equipos soporten el siniestro, por lo tanto, los equipos e instalaciones tecnológicas, podrían no perderse en su totalidad.	Adquisición de equipo de cómputo nuevo (servidores o PC), utilizar el último respaldo de información para la restauración de procesos y servicios.	<ul style="list-style-type: none"> <li>• Ubicación de equipos alejados de ventanas o estantes altos.</li> <li>• Fijación de estanterías y muebles a muros.</li> <li>• Simulacros de evacuación periódicos.</li> <li>• Almacenamiento de respaldos en ubicaciones remotas.</li> </ul>	





## Recomendaciones.

Hacer de conocimiento general el contenido del presente Plan de Contingencia Informática y Recuperación, con la finalidad de instruir adecuadamente al personal de la UPB.

Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de seguro.

Cuando el personal administrador de la red se encuentre ausente se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para reanudar todos los procesos y servicios, a fin de que la operación básica de la institución no se vea interrumpida.

Adicionalmente al plan de contingencia se deben desarrollar acciones correctivas para minimizar los riesgos identificados (según el Programa Interno de Protección Civil de la Universidad Politécnica de Bacalar):

- ❖ Preparar extinguidores.
- ❖ Organizar señales de evacuación.
- ❖ Preparar bombas de extracción de agua.
- ❖ Generadores eléctricos, etc.

El presente plan se deberá aplicar a partir de su publicación en la página oficial de la Universidad Politécnica de Bacalar, para continuar y garantizar la operabilidad de esta.

Cualquier asunto no contemplado en el presente Plan de Contingencia Informática y Recuperación, será analizado y reformado por el Departamento de Desarrollo de Sistemas de la UPB.

Bacalar, Quintana Roo a 02 de diciembre de 2025.

**DRA. INGRID CITLALLI SUÁREZ MC LIBERTY**  
**RECTORA**