UNIVERSIDAD VERACRUZANA FACULTAD DE INFORMÁTICA

TITULO:

Plan de contingencia

**PRESENTA:**

Equipo 1

**DOCENTE:**

Mtro. Millán Martínez Max William

**FECHA:**

xx-12-2023

Contenido

[**1.** **Descripción de eventualidad** 3](#_Toc152676569)

[**3.** **Acciones inmediatas que tomar** 7](#_Toc152676570)

[**4.** **Pasos para resolver el problema** 10](#_Toc152676571)

[**5.** **Rol de cada miembro del equipo de contingencia** 13](#_Toc152676572)

[**6.** **Recursos necesarios para la implementación del plan.** 14](#_Toc152676573)

[**7.** **Comunicación interna y externa durante la crisis** 16](#_Toc152676574)

[**8.** **Estrategias para la prevención y la mitigación futura** 18](#_Toc152676575)

# **Descripción de eventualidad**

|  |  |  |
| --- | --- | --- |
| Vulnerabilidad | Descripción | Clasificación |
| Pérdida de energía eléctrica | Interrupciones eléctricas inesperadas que pueden resultar en la indisponibilidad del sistema y pérdida de datos. | **Infraestructura Física** |
| Fallo en el hardware del servidor | Problemas en el hardware, como fallas de discos duros o de memoria RAM, que pueden afectar la disponibilidad del sistema. | **Infraestructura Física** |
| Ataques cibernéticos | Intentos de acceso no autorizado, malware o ransomware que pueden comprometer la seguridad de la base de datos. | **Seguridad Informática** |
| Errores humanos en la manipulación de datos | Acciones accidentales o malintencionadas por parte de usuarios que pueden resultar en pérdida o corrupción de datos. | **Factores Humanos** |
| Pérdida de conexión con la API | Interrupciones en la conexión con la API que pueden afectar la comunicación entre el sistema y otros componentes. | **Infraestructura de Red** |
| Incapacidad de recuperar datos del respaldo | Problemas en los procedimientos de respaldo que pueden dificultar la recuperación de datos en caso de pérdida. | **Proceso y Procedimientos** |
| Desastres naturales o eventos catastróficos | Eventos como terremotos, inundaciones o incendios que pueden afectar la infraestructura física y la disponibilidad del sistema. | **Desastres Naturales** |
| Malfuncionamiento del software | Errores en el código o problemas de compatibilidad que pueden afectar el rendimiento y la estabilidad del sistema. | **Desarrollo de Software** |
| Falta de actualizaciones de seguridad | No aplicar actualizaciones de seguridad podría dejar al sistema vulnerable a brechas de seguridad y ataques. | **Seguridad Informática** |
| Pérdida de datos durante la migración | Problemas durante la migración de datos que podrían resultar en pérdida o corrupción de información crítica. | **Proceso y Procedimientos** |
| Conflictos de versión del sistema | Incompatibilidades entre diferentes versiones de software o componentes que pueden afectar la operación del sistema. | **Desarrollo de Software** |
| Fallos en la conexión a la base de datos | Interrupciones o problemas en la conectividad a la base de datos que pueden afectar la disponibilidad del sistema. | **Infraestructura de Red** |

* 1. **Impacto en el servicio y en los clientes**

1. **Pérdida de energía eléctrica:**
   * **Impacto para el cliente:** Incapacidad para realizar pedidos y transacciones en el comedor universitario. Posible frustración debido a la falta de acceso a servicios alimentarios.
   * **Impacto en el servicio:** Indisponibilidad temporal del sistema, interrupción en las operaciones diarias del comedor.
2. **Fallo en el hardware del servidor:**
   * **Impacto para el cliente:** Imposibilidad de acceder a menús, realizar pedidos o revisar transacciones pasadas.
   * **Impacto en el servicio:** Pérdida temporal de acceso a la base de datos, interrupción en la prestación de servicios.
3. **Ataques cibernéticos:**
   * **Impacto para el cliente:** Riesgo de pérdida de datos personales, contraseñas u otra información confidencial.
   * **Impacto en el servicio:** Compromiso de la integridad y confidencialidad de la información del comedor, posible interrupción del servicio.
4. **Errores humanos en la manipulación de datos:**
   * **Impacto para el cliente:** Posible pérdida de historial de transacciones o datos personales.
   * **Impacto en el servicio:** Corrupción o pérdida de datos críticos, afectando la calidad del servicio.
5. **Pérdida de conexión con la API:**
   * **Impacto para el cliente:** Dificultad para realizar transacciones y acceder a información actualizada.
   * **Impacto en el servicio:** Interrupción en la comunicación con otros sistemas, posiblemente afectando la operación normal del comedor.
6. **Incapacidad de recuperar datos del respaldo:**
   * **Impacto para el cliente:** Pérdida potencial de historial de transacciones y preferencias de usuarios.
   * **Impacto en el servicio:** Dificultades para restaurar el sistema a un estado funcional, posible interrupción prolongada del servicio.
7. **Desastres naturales o eventos catastróficos:**
   * **Impacto para el cliente:** Interrupción completa de los servicios alimentarios durante un período prolongado.
   * **Impacto en el servicio:** Daño físico a la infraestructura, pérdida de datos y posible cese temporal de las operaciones.
8. **Malfuncionamiento del software:**
   * **Impacto para el cliente:** Experimentar errores al realizar pedidos o acceder a menús.
   * **Impacto en el servicio:** Interrupciones temporales debido a problemas de software, afectando la experiencia del usuario.
9. **Falta de actualizaciones de seguridad:**
   * **Impacto para el cliente:** Vulnerabilidad a posibles ataques, riesgo de pérdida de datos personales.
   * **Impacto en el servicio:** Posible compromiso de la seguridad de la base de datos y pérdida de confianza del cliente.
10. **Pérdida de datos durante la migración:**
    * **Impacto para el cliente:** Pérdida de historial de transacciones y preferencias almacenadas.
    * **Impacto en el servicio:** Retraso en la migración de datos, posible interrupción temporal del servicio.

# **Acciones inmediatas que tomar**

1. **Pérdida de energía eléctrica:**
   * + Implementar un sistema de alimentación ininterrumpida (UPS) para asegurar una transición suave durante cortes de energía.
     + Desarrollar un procedimiento para salvar automáticamente los datos críticos en caso de una interrupción eléctrica.
2. **Fallo en el hardware del servidor:**
   * + Monitorizar la salud del hardware y establecer alertas para identificar problemas antes de que afecten el servicio.
     + Mantener una lista de repuestos críticos y un plan para la rápida sustitución en caso de fallo.
3. **Ataques cibernéticos:**
   * + Reforzar la seguridad mediante firewalls, antivirus y sistemas de detección de intrusiones.
     + Actualizar regularmente los parches de seguridad y realizar auditorías de seguridad.
4. **Errores humanos en la manipulación de datos:**
   * + Implementar niveles de autorización y validar los cambios críticos antes de su ejecución.
     + Realizar copias de seguridad antes de realizar cambios significativos en los datos.
5. **Pérdida de conexión con la API:**
   * + Implementar mecanismos de reintento y recuperación para garantizar la continuidad del servicio.
     + Establecer un sistema de monitoreo para detectar y abordar rápidamente problemas de conectividad.
6. **Incapacidad de recuperar datos del respaldo:**
   * + Realizar pruebas regulares de recuperación para verificar la eficacia de los procedimientos de respaldo.
     + Establecer alertas automáticas para notificar cualquier fallo en los procedimientos de respaldo.
7. **Desastres naturales o eventos catastróficos:**
   * + Crear un plan de evacuación y asegurar la integridad física del personal.
     + Implementar sistemas de respaldo en ubicaciones geográficamente separadas.
8. **Malfuncionamiento del software:**
   * + Realizar una revisión del código para identificar y corregir errores críticos.
     + Mantener un entorno de prueba para validar nuevas versiones antes de implementarlas.
9. **Falta de actualizaciones de seguridad:**
   * + Establecer un calendario de actualizaciones regulares para todos los componentes del sistema.
     + Monitorear las alertas de seguridad y aplicar parches críticos de inmediato.
10. **Pérdida de datos durante la migración:**
    * + Realizar una revisión completa del proceso de migración para identificar y corregir posibles problemas.
      + Implementar una estrategia de respaldo adicional durante el proceso de migración.

# **Pasos para resolver el problema**

1. **Pérdida de energía eléctrica:**

* Coordinar la activación de generadores de respaldo.
* Notificar al personal clave y a los usuarios sobre la interrupción y las medidas tomadas.

1. **Fallo en el hardware del servidor:**

* Identificar la causa del fallo y aislar el hardware afectado.
* Notificar a los usuarios sobre posibles interrupciones y proporcionar el tiempo estimado de resolución.

1. **Ataques cibernéticos:**

* Activar medidas de bloqueo para prevenir la propagación del ataque.
* Coordinar con equipos de seguridad para mitigar el impacto.
* Informar a los usuarios sobre la situación y las medidas tomadas.

1. **Errores humanos en la manipulación de datos:**

* Identificar y revertir cambios no autorizados.
* Implementar correcciones y restaurar desde copias de seguridad si es necesario.
* Notificar a los usuarios afectados sobre cualquier impacto y las acciones tomadas.

1. **Pérdida de conexión con la API:**

* Coordinar con el equipo de desarrollo para identificar y resolver el problema.
* Notificar a los usuarios sobre la interrupción temporal.

1. **Incapacidad de recuperar datos del respaldo:**

* Identificar la causa de la incapacidad para recuperar datos.
* Corregir problemas en los procedimientos de respaldo.
* Informar a los usuarios clave sobre cualquier impacto y las soluciones implementadas.

1. **Desastres naturales o eventos catastróficos:**

* Activar el plan de evacuación y respaldo en ubicaciones separadas.
* Notificar a todo el personal y usuarios sobre las acciones tomadas.
* Coordinar con las autoridades locales y servicios de emergencia.

1. **Malfuncionamiento del software:**

* Acciones cuando se presente el problema:
* Revertir a la versión anterior del software si es posible.
* Implementar correcciones y parches según sea necesario.
* Informar a los usuarios sobre el problema y las acciones correctivas.

1. **Falta de actualizaciones de seguridad:**

* Aplicar parches críticos de seguridad de inmediato.
* Realizar una revisión de seguridad para identificar posibles vulnerabilidades.
* Notificar a los usuarios clave sobre las actualizaciones y la seguridad mejorada.

1. **Pérdida de datos durante la migración:**

* Identificar la causa de la pérdida de datos y corregir el proceso de migración.
* Implementar medidas correctivas y realizar pruebas exhaustivas antes de futuras migraciones.
* Notificar a los usuarios afectados sobre la situación y las acciones correctivas.

# **Rol de cada miembro del equipo de contingencia**

|  |  |
| --- | --- |
| Eventualidad | Persona Encargada |
| Pérdida de energía eléctrica | Jefe de Infraestructura |
| Fallo en el hardware del servidor | Administrador de Sistemas |
| Ataques cibernéticos | Responsable de Seguridad Informática |
| Errores humanos en la manipulación de datos | Administrador de Bases de Datos |
| Pérdida de conexión con la API | Desarrollador de API |
| Incapacidad de recuperar datos del respaldo | Administrador de Bases de Datos |
| Desastres naturales o eventos catastróficos | Coordinador de Emergencias |
| Malfuncionamiento del software | Desarrollador de Software |
| Falta de actualizaciones de seguridad | Responsable de Seguridad Informática |
| Pérdida de datos durante la migración | Coordinador de Migraciones |

# **Recursos necesarios para la implementación del plan.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Eventualidad | Recursos Necesarios | Personal Responsable | Herramientas y Tecnologías | Equipamiento | Otros Recursos |
| Pérdida de energía eléctrica | Generadores, UPS, Baterías de respaldo | Jefe de Infraestructura | Generadores, UPS, Sistema de Monitoreo de Energía | Generadores, Baterías de Respaldo | Combustible para generadores |
| Fallo en el hardware del servidor | Inventario de repuestos, Herramientas de diagnóstico | Administrador de Sistemas | Herramientas de Diagnóstico, Monitoreo de Hardware | Repuestos de Hardware | Contratos de mantenimiento |
| Ataques cibernéticos | Firewall, Software Antivirus, IDS/IPS | Responsable de Seguridad Informática | Software de Seguridad, Herramientas de Detección | Equipamiento de Red | Servicios de Auditoría |
| Errores humanos en la manipulación de datos | Sistema de Control de Versiones, Procesos de Aprobación | Administrador de Bases de Datos | Herramientas de Control de Versiones, Sistemas de Aprobación | Equipamiento de Desarrollo | Materiales de Capacitación |
| Pérdida de conexión con la API | Redundancia de Conexión, Mecanismos de Reintento | Desarrollador de API | Herramientas de Monitoreo de Conexión, Sistemas de Respaldo | Equipamiento de Red | Contratos de Proveedor de Internet |
| Incapacidad de recuperar datos del respaldo | Procedimientos de Pruebas, Sistemas de Respaldos | Administrador de Bases de Datos | Herramientas de Pruebas de Respaldos, Almacenamiento Redundante | Equipamiento de Almacenamiento | Espacio de Almacenamiento Redundante |
| Desastres naturales o eventos catastróficos | Plan de Evacuación, Centros de Datos Secundarios | Coordinador de Emergencias | Herramientas de Comunicación de Emergencia, Equipamiento de Respuesta a Desastres | Equipamiento de Respuesta a Desastres | Acuerdos con Centros de Datos Secundarios |
| Malfuncionamiento del software | Sistemas de Retroalimentación de Usuarios | Desarrollador de Software | Herramientas de Monitoreo de Código, Sistemas de Retroalimentación | Equipamiento de Desarrollo | Sistemas de Retroalimentación de Usuarios |
| Falta de actualizaciones de seguridad | Programa de Actualizaciones, Auditorías Regulares | Responsable de Seguridad Informática | Herramientas de Monitoreo de Actualizaciones, Sistemas de Auditoría | Equipamiento de Seguridad | Contratos con Proveedores de Seguridad |
| Pérdida de datos durante la migración | Procedimientos de Migración, Pruebas Exhaustivas | Coordinador de Migraciones | Herramientas de Migración de Datos, Sistemas de Pruebas | Equipamiento de Desarrollo | Espacio de Almacenamiento para Pruebas |

# **Comunicación interna y externa durante la crisis**

|  |  |  |
| --- | --- | --- |
| Eventualidad | Comunicación Interna | Comunicación Externa |
| Pérdida de Energía Eléctrica | - Responsable de la Situación: Notificar al personal clave sobre la pérdida de energía y las medidas inmediatas. Coordinar la activación de generadores y baterías de respaldo. | - Usuarios Afectados: Enviar alertas a través de medios electrónicos informando sobre la interrupción y proporcionar actualizaciones. - Proveedores de Servicios: Notificar sobre posibles interrupciones y establecer comunicación para coordinar acciones de respuesta. |
| Fallo en el Hardware del Servidor | - Administrador de Sistemas: Identificar la causa del fallo y aislar el hardware afectado. Notificar al personal sobre posibles interrupciones y proporcionar el tiempo estimado de resolución. | - Usuarios Afectados: Informar sobre la situación y las acciones tomadas. |
| Ataques Cibernéticos | - Equipo de Respuesta a Incidentes: Activar un canal de comunicación seguro para el equipo. Coordinar acciones para contener y mitigar el ataque. | - Usuarios y Stakeholders: Emitir comunicados sobre la situación y las acciones tomadas. Proporcionar orientación sobre medidas de seguridad. |
| Errores Humanos en la Manipulación de Datos | - Administrador de Bases de Datos: Identificar y revertir cambios no autorizados. Implementar correcciones y restaurar desde copias de seguridad si es necesario. Notificar a los usuarios afectados. | - Usuarios Afectados: Notificar sobre cualquier impacto y las acciones tomadas. |
| Pérdida de Conexión con la API | - Desarrollador de API: Coordinar con el equipo de desarrollo para identificar y resolver el problema. Configurar sistemas para intentar restablecer la conexión. | - Usuarios Afectados: Notificar sobre la interrupción temporal. |
| Incapacidad de Recuperar Datos del Respaldo | - Administrador de Bases de Datos: Identificar la causa y corregir problemas en los procedimientos de respaldo. Informar a los usuarios clave sobre cualquier impacto y las soluciones implementadas. | - Usuarios Clave: Notificar sobre cualquier impacto y las soluciones implementadas. |
| Desastres Naturales o Eventos Catastróficos | - Coordinador de Emergencias: Activar el plan de comunicación de emergencia y coordinar la evacuación si es necesario. | - Autoridades y Servicios de Emergencia: Establecer contacto y proporcionar actualizaciones sobre la situación. |
| Malfuncionamiento del Software | - Desarrolladores y Equipo de TI: Activar un canal de comunicación. Coordinar acciones para revertir cambios o implementar soluciones temporales. | - Usuarios Afectados: Emitir comunicados sobre el problema y proporcionar orientación. |
| Falta de Actualizaciones de Seguridad | - Responsable de Seguridad Informática: Aplicar parches críticos de seguridad y realizar una revisión de seguridad. Notificar a los usuarios clave. | - Usuarios Clave: Notificar sobre las actualizaciones y la seguridad mejorada. |
| Pérdida de Datos durante la Migración | - Coordinador de Migraciones: Notificar al equipo y detener la migración. Coordinar acciones para identificar y corregir la causa del problema. | - Usuarios Afectados: Informar sobre la situación y proporcionar líneas de contacto para consultas y soporte. |

# **Estrategias para la prevención y la mitigación futura**

**1. Pérdida de Energía Eléctrica:**

**Prevención:**

* + Instalar generadores y baterías de respaldo con capacidad suficiente para mantener operativos los sistemas críticos durante cortes de energía.
  + Implementar sistemas de monitoreo de energía para detectar fluctuaciones y prevenir sobrecargas.

**Mitigación Futura:**

* + Realizar pruebas regulares de los generadores y sistemas de respaldo.
  + Mantener inventarios actualizados de combustible y realizar mantenimiento preventivo en generadores.

**2. Fallo en el Hardware del Servidor:**

**Prevención:**

* + Establecer una política de mantenimiento preventivo para revisar y reemplazar hardware obsoleto.
  + Configurar sistemas de monitoreo para detectar signos tempranos de fallos.

**Mitigación Futura:**

* + Implementar redundancia en servidores críticos.
  + Mantener contratos de servicio y repuestos con proveedores.

**3. Ataques Cibernéticos:**

**Prevención:**

* + Actualizar regularmente software y sistemas de seguridad.
  + Educación continua para empleados sobre prácticas seguras en línea.

**Mitigación Futura:**

* + Implementar sistemas de detección y respuesta ante amenazas.
  + Realizar auditorías de seguridad regulares.

**4. Errores Humanos en la Manipulación de Datos:**

**Prevención:**

* + Establecer procesos de aprobación para cambios en la base de datos.
  + Capacitación regular sobre mejores prácticas de manipulación de datos.

**Mitigación Futura:**

* + Implementar sistemas de control de versiones robustos.
  + Realizar auditorías periódicas de cambios en la base de datos.

**5. Pérdida de Conexión con la API:**

**Prevención:**

* + Configurar redundancia en conexiones y servidores de la API.
  + Monitorear continuamente la salud de la conexión.

**Mitigación Futura:**

* + Implementar sistemas de reintento automático de conexión.
  + Establecer acuerdos de nivel de servicio (SLA) con proveedores de servicios de red.

**6. Incapacidad de Recuperar Datos del Respaldo:**

**Prevención:**

* + Realizar pruebas regulares de recuperación de datos.
  + Validar la integridad de los respaldos periódicamente.

**Mitigación Futura:**

* + Automatizar y programar pruebas regulares de recuperación.
  + Mantener documentación detallada de los procedimientos de respaldo.

**7. Desastres Naturales o Eventos Catastróficos:**

**Prevención:**

* + Identificar ubicaciones seguras y alternativas para centros de datos.
  + Desarrollar e implementar planes de evacuación y respuesta a desastres.

**Mitigación Futura:**

* + Realizar simulacros de evacuación y respuesta a desastres.
  + Mantener acuerdos con centros de datos secundarios para la continuidad del servicio.

**8. Malfuncionamiento del Software:**

**Prevención:**

* + Implementar prácticas sólidas de desarrollo de software.
  + Utilizar sistemas de retroalimentación de usuarios para identificar problemas temprano.

**Mitigación Futura:**

* + Desarrollar e implementar planes de reversión rápida a versiones anteriores.
  + Realizar auditorías de código regulares.

**9. Falta de Actualizaciones de Seguridad:**

**Prevención:**

* + Establecer procesos automáticos para la aplicación de parches.
  + Monitorear activamente las actualizaciones de seguridad.

**Mitigación Futura:**

* + Implementar un programa de gestión proactiva de vulnerabilidades.
  + Realizar auditorías de seguridad periódicas.

**10. Pérdida de Datos durante la Migración:**

**Prevención:**

* + Realizar análisis exhaustivos de los requisitos y riesgos antes de las migraciones.
  + Establecer procedimientos de respaldo antes de cualquier migración importante.

**Mitigación Futura:**

* + Realizar pruebas exhaustivas antes de cada migración.
  + Mantener comunicación abierta con usuarios afectados y proporcionar canales de soporte durante el proceso.