PLAN DE CONTINGENCIA DE LOS SISTEMAS DE LA INFORMACIÓN.

E.S.E.
CAMU
Santa Teresita
¡MAS cerca de Ti

PLANES DE CONTINGENCIA EN SISTEMAS DE INFORMACIÓN: TU MEJOR DEFENSA ANTE LO INESPERADO

En un mundo digital donde los sistemas operan 24/7, una falla técnica, un ciberataque o incluso un simple corte de energía pueden convertirse en una amenaza real para la continuidad de tu negocio. ¿Está tu organización preparada para reaccionar sin perder tiempo, dinero ni datos valiosos? La respuesta está en contar con un Plan de Contingencia bien estructurado.

Los planes de contingencia en sistemas de información son estrategias diseñadas para garantizar que, ante cualquier interrupción tecnológica, tu empresa pueda seguir operando de forma segura y eficiente. No se trata solo de tener respaldos, sino de contar con procedimientos claros, personal capacitado y soluciones tecnológicas listas para activarse en cuestión de minutos.

Un buen plan de contingencia no solo previene el caos; también protege la reputación de tu empresa, mejora la confianza de tus clientes y asegura la continuidad de tus operaciones en todo momento. ¡Recuerda! La verdadera ciberseguridad no está en evitar lo inevitable, sino en saber cómo actuar cuando lo inevitable sucede.

¿QUÉ INCLUYE UN PLAN DE CONTINGENCIA EN SISTEMAS DE INFORMACIÓN?

Un buen plan de contingencia no es un simple documento olvidado en una carpeta: es una guía viva, actualizada y diseñada para activarse con rapidez cuando más se necesita. Su estructura debe cubrir todos los aspectos críticos de los sistemas de información, asegurando una respuesta rápida, organizada y efectiva ante cualquier tipo de incidente.

Entre sus componentes principales se encuentran:

- **Análisis de riesgos y vulnerabilidades:** Identifica qué puede fallar y cómo afectaría a la operación.
- **Estrategias de recuperación:** Define las acciones para restaurar servicios, datos y operaciones en el menor tiempo posible.
- **Copias de seguridad y restauración de datos:** Establece procedimientos seguros y automáticos de respaldo, junto con pruebas periódicas de recuperación.
- **Roles y responsabilidades claras:** Determina quién hace qué, cuándo y cómo en caso de emergencia.
- **Protocolos de comunicación:** Asegura que el personal, los clientes y los proveedores estén informados durante cualquier eventualidad.
- **Simulacros y pruebas periódicas:** Garantizan que el plan realmente funcione y que todos estén preparados.

Diseñar e implementar un plan de contingencia es una inversión estratégica. No solo minimiza pérdidas económicas, sino que también demuestra responsabilidad, compromiso con la seguridad digital y visión a largo plazo.

Plan de contingencia de los sistemas de información

E.S.E. CAMU SANTA TERESITA

¿CUÁL ES EL OBJETIVO DEL PLAN?

Garantizar la continuidad de los sistemas de información, comunicación y servicios electrónicos ante cualquier interrupción, minimizando el impacto en la atención al paciente y operaciones administrativas.

¿A QUIÉN APLICA?

A todas las áreas que dependen del sistema informático:

- Facturación
- Personal médico y asistencial
- Odontología
- Laboratorio clínico
- Área administrativa

ETAPAS DEL PLAN DE CONTINGENCIA

1. **Notificación inmediata**
   - Grupo de WhatsApp oficial
   - Responsable: Coordinador de Sistemas
2. **Tiempo de reacción**
   - Máximo 15 minutos para evaluar la causa.
   - Si no hay respuesta en ese lapso, los usuarios deben reportar nuevamente la falla.
3. **Solución Manual**
   - Si no es posible restaurar el sistema rápidamente, se activa el plan de trabajo manual:
   - Formularios físicos
   - Registro en papel
4. **Activación de servidor alterno**
   - En caso de falla grave, se instala un servidor espejo para recuperar la información.
5. **Reactivación gradual del sistema**
   - Se avisa por bloques de usuarios para evitar sobrecarga del sistema.

¿QUÉ HACER SI SE CAE EL SISTEMA?

- Mantén la calma.
- Usa los formatos manuales.
- Notifica al área de sistemas si no se ha informado la falla.
- Espera instrucciones de reactivación.

RESPONSABLE DEL PROCEDIMIENTO

Coordinador de Sistemas

RECOMENDACIONES

- No intentes reiniciar los equipos por cuenta propia.
- Guarda frecuentemente tu trabajo si estás conectado al sistema.
- Participa en simulacros del plan de contingencia.

IMPORTANCIA DEL PLAN

Un fallo no planificado puede:

- Afectar la atención médica.
- Retrasar servicios esenciales.
- Generar pérdida de datos.
- Dañar la imagen institucional.