ESE SAN VICENTE DE PAUL

Lorica – Córdoba

2026

PLAN DE CONTINGENCIA INFORMATICO

Tabla de Contenido

CAPITULO I: ANALISIS DE LA SITUACION ACTUAL INFORMATICA EN LA ESE HOSPITAL SAN VICENTE DE PAUL

1.1. Introducción.

Los sistemas y redes de información de la **ESE Hospital San Vicente de Paúl** están expuestos a diversos factores de riesgo, tanto de origen humano como físico. Ante cualquier adversidad, la capacidad de respuesta y la mitigación del impacto dependen directamente de un plan estructurado que permita identificar con exactitud la gravedad y las características de la falla.

La vulnerabilidad de componentes críticos puede derivar en pérdidas catastróficas de información o daños irreparables en la infraestructura, ya sea por incidentes técnicos o desastres naturales. En este sentido, el presente plan busca minimizar las consecuencias de dichos fallos y, en la medida de lo posible, prevenir su ocurrencia. Para ello, se establece un marco de acción basado en el análisis de riesgos, el respaldo sistemático de la información y protocolos definidos para la recuperación de datos, garantizando así la seguridad física y lógica de los activos digitales de la institución.

1.2. Objetivos e Importancia del Plan de Contingencia.

Garantizar la continuidad operativa de los procesos y activos críticos que integran los sistemas de información institucionales, minimizando el impacto de cualquier interrupción.

Establecer protocolos y procedimientos de respuesta inmediata ante fallas técnicas o desastres que afecten la infraestructura tecnológica y la disponibilidad de los datos.

Optimizar la gestión de recursos y esfuerzos para una atención de contingencias oportuna, mediante la asignación clara de roles y responsabilidades en las fases de prevención, respuesta y recuperación.

1.3. Sistema de Red de Computadoras en la Ese Hospital San Vicente de Paul.

La infraestructura de red de la **ESE Hospital San Vicente de Paúl de Lorica** presenta una arquitectura de red local (LAN) basada en la interconexión de estaciones de trabajo mediante switches, sin una segmentación avanzada bajo estándares de TI.

El ecosistema de aplicaciones está encabezado por el sistema integral **SaludSystem**, el cual centraliza la gestión asistencial y financiera desde un servidor institucional físico. Este se complementa con **GoTelemedicina** para imágenes diagnósticas y el software de gestión documental **ORFEO**. Asimismo, la entidad ha modernizado sus comunicaciones mediante la implementación de **Telefonía IP 3CX**, una solución alojada en la nube que garantiza alta disponibilidad y cuenta con soporte técnico a nivel local para asegurar la continuidad del servicio telefónico ante cualquier incidencia.

1.4. Sistemas de Información de la Ese Hospital San Vicente de Paul.

La **ESE Hospital San Vicente de Paúl de Lorica** centraliza su operación en el sistema de información integral **SaludSystem**, desarrollado por la firma INFOTEC. Esta plataforma es el núcleo tecnológico de la institución, permitiendo la gestión transversal de los procesos asistenciales y administrativos. Entre sus funciones críticas se encuentran la administración de historias clínicas, laboratorio clínico, admisiones y nómina, así como los módulos financieros de contabilidad, presupuesto, cartera, almacén y el sistema de facturación electrónica.

CAPITULO 2: PLAN DE REDUCCIÓN DE RIESGOS

El objetivo de este capítulo es realizar un diagnóstico integral de las causas que pueden comprometer la integridad de la infraestructura tecnológica de la **ESE Hospital San Vicente de Paúl**. Este análisis abarca tanto los equipos de cómputo y activos de red como la información crítica almacenada en los diversos medios digitales de la entidad.

A través de un detallado **Análisis de Riesgos**, se establecen las pautas de actuación y los protocolos necesarios para mitigar el impacto de posibles incidentes, garantizando la continuidad de los servicios asistenciales y administrativos.

2.1. Análisis de Riesgos

Mediante este estudio, se desglosan las amenazas que podrían afectar el normal funcionamiento de los sistemas y la seguridad de la información procesada diariamente en la institución.

Tabla de Análisis de Riesgos Actualizada

Bienes Susceptibles	Daño Potencial	Fuentes de Daño
Personal	Imposibilidad de acceso a recursos por incidentes físicos, naturales o humanos.	Acceso no autorizado, enfermedad, accidentes o abandono de cargo.
Hardware y Redes	Inoperatividad del sistema, daño físico de componentes o ruptura de seguridad perimetral.	Fallas en el servidor local, averías en switches/routers o fallas en el cableado.
Software y Utilitarios	Pérdida de acceso, cambios no autorizados, eliminación de bases de datos o cifrado de información.	Ataques cibernéticos, cambios involuntarios de claves o errores de configuración.
Datos e Información	Divulgación no autorizada (fuga de datos), robo de identidad o pérdida de	Infidencia, robo físico de medios de almacenamiento o acceso lógico no

	integridad patrimonial.	autorizado.
Suministro Eléctrico	**Interrupción de la operación asistencial, daño en fuentes de poder y pérdida de datos en tránsito.**	**Cortes de fluido eléctrico, picos de voltaje o fallas en la planta de emergencia / UPS.**
Telecomunicaciones	Aislamiento digital, caída del sistema SaludSystem (nube) y pérdida de telefonía IP 3CX.	Fallas del proveedor de internet (ISP), daños en fibra óptica o incendios.
Infraestructura	Destrucción física de los centros de datos o estaciones de trabajo.	Desastres naturales (sismos, inundaciones) o incendios en las instalaciones.

2.1.1. Valoración de los Riesgos

2.1.1. Valoración de Riesgos

La institución llevará a cabo una evaluación cualitativa de cada riesgo identificado, clasificándolos en cuatro niveles: **Alto, Medio, Bajo y Muy Bajo**. Este proceso permite priorizar los activos y aplicaciones críticas que presentan una mayor vulnerabilidad ante amenazas internas o externas.

El objetivo de esta valoración es determinar la factibilidad de las estrategias de mitigación para cada riesgo. Aquellos que, por limitaciones técnicas o económicas, no puedan ser eliminados o reducidos, se considerarán **riesgos residuales**, los cuales deberán ser asumidos por la entidad bajo una supervisión constante. La nomenclatura para la medición será la siguiente:

- **Alto**
- **Medio**
- **Bajo**
- **Muy Bajo**

2.1.2. Riesgos

Para que un sistema se defina como seguro, debe garantizar el cumplimiento de la **Tríada de la Seguridad (CID)**:

- **Confidencialidad:** Garantizar que la información sea accesible únicamente para el personal autorizado.
- **Integridad:** Salvaguardar la exactitud y completitud de los datos, evitando modificaciones no autorizadas.
- **Disponibilidad:** Asegurar que los sistemas y la información estén operativos y accesibles cada vez que la institución lo requiera.

A pesar de las soluciones tecnológicas globales, las amenazas evolucionan constantemente. En la **ESE Hospital San Vicente de Paúl de Lorica**, la seguridad de la información enfrenta retos críticos debido a la obsolescencia de la infraestructura física y lógica, lo que incrementa la probabilidad de incidentes con consecuencias desastrosas.

Principales Riesgos Identificados y Situación Actual

1. **Fallas Críticas en la Infraestructura de Red:**
    - **Situación:** La red presenta una topología deficiente con **conexiones en cascada**, lo cual es fatal para el rendimiento, y presencia de **loops (bucles)** generados por malas conexiones físicas. Los **equipos de red son obsoletos y carecen de administración** (switches no gestionables), lo que impide segmentar el tráfico o detectar fallas proactivamente. Esto deriva en una **baja velocidad de transmisión de datos**, afectando la agilidad de la atención médica.
2. **Inestabilidad del Fluido Eléctrico y Soporte de Energía:**
    - **Situación:** Existen fallas recurrentes en el fluido eléctrico y el cableado es antiguo. La ausencia de **Sistemas de Alimentación Ininterrumpida (UPS)** robustos y la falta de un control centralizado

dejan a los equipos vulnerables a daños por picos de voltaje y pérdida de datos en tránsito.

3. **Vulnerabilidad en las Telecomunicaciones:**
   - **Situación:** La dependencia de un **canal dedicado de internet** es alta. Un corte en este servicio paraliza tanto el acceso a la nube como la telefonía IP 3CX, aislando digitalmente a la entidad.
4. **Accesos no Autorizados y Debilidad en Políticas:**
   - **Situación:** Existe una práctica común de compartir contraseñas entre personal de la misma dependencia. No se cuenta con un registro automatizado de altas/bajas de usuarios, lo que facilita el acceso de personal no autorizado a información sensible.

Tabla de Clasificación de Riesgos Actualizada

He incluido los nuevos riesgos técnicos solicitados para reflejar con exactitud la vulnerabilidad de la red:

Tipo de Riesgo	Probabilidad de Ocurrencia	Causa Controlable	Intensidad del Daño (1-10)
Fallas de fluido eléctrico	Muy Alta	No	10
Equipos de red obsoletos y sin administración	Permanente	Sí	9
Conexiones en cascada y presencia de Loops	Permanente	Sí	9

Baja velocidad de transmisión de datos	Alta	Sí	7
Corte de servicio de canal dedicado (Internet)	Mediana	No	10
Virus e Infecciones Informáticas	Mediana	Sí	8
Robo de Hardware e Información	Mediana	Sí	8
Accesos lógicos no autorizados	Alta	Sí	8
Vandalismo	Muy Baja	Sí	10
Fuego / Incendio	Muy Baja	Sí	10
Fenómenos Naturales (Terremotos)	Baja	No	10

2.2. Análisis de Fallas en la Seguridad

La gestión de la infraestructura tecnológica y la seguridad de la información en la entidad es liderada por un **Ingeniero de Sistemas**, quien define la estrategia y los protocolos de seguridad, sistemas de información. Este liderazgo cuenta con el soporte operativo de un **Especialista de Soporte en redes y plataformas tecnológicas,** dedicado a la administración de redes (voz y datos) internet, telecomunicaciones y servidores de producción y un **Técnico en Sistemas**, conformando un equipo técnico encargado de la ejecución de mantenimientos,

resolución de incidencias y resguardo de la plataforma digital.

A pesar de contar con este equipo profesional, la seguridad se ve condicionada por una red de datos que presenta **conexiones en cascada** y equipos obsoletos que generan una **baja velocidad de transmisión**. El equipo técnico trabaja en la mitigación de estos riesgos, enfocándose en eliminar los **loops** de red, duplicidad de ips y en asegurar la continuidad de los servicios críticos ante los constantes **cortes de fluido eléctrico**.

Actualización de la Tabla: Responsables en Caso de Desastre

Se ha distribuido las cargas para que se vea el flujo de trabajo entre los tres niveles:

Tipo de Riesgo	Medida a Tomar	Responsable
Fallas Críticas de Red (Loops/Cascadas)	Rediseño de la topología y supervisión de la reestructuración física.	**Ingeniero de Sistemas y Especialista de Soporte en redes.**
Fallas en Equipos (Hardware)	Diagnóstico técnico, reparación básica o trámite de reposición.	**Técnico en Sistemas**
Incidencias de Usuario y Soporte	Atención inmediata a fallas en estaciones de trabajo y periféricos.	**Técnico en Sistemas**
Cortes de Fluido Eléctrico	Verificación de UPS por área y coordinación con mantenimiento para la planta.	**Especialista de Soporte**
Corte de Internet / Telefonía 3CX	Gestión de escalamiento con proveedores (ISP) y monitoreo de enlace dedicado.	**Especialista de Soporte / Ingeniero**
Virus e Incidentes de Seguridad	Análisis de brechas, restauración de backups y despliegue de antivirus.	**Ingeniero de Sistemas**

2.1.2. Prevención de Contingencias (Infraestructura Técnica)

En este apartado, se detalla cómo el equipo aborda los problemas específicos de la ESE:

- **Optimización de Conectividad:** El **Ingeniero de Sistemas** proyecta la eliminación de las conexiones en cascada. El **Especialista** y el **Técnico** ejecutan el despliegue del cableado estructurado para eliminar la baja velocidad y los loops que afectan la operación asistencial.
- **Gestión de Energía:** El **Técnico en Sistemas** realizará un censo y revisión mensual de las UPS, asegurando que cada equipo crítico esté protegido ante las fallas de fluido eléctrico, mientras que el **Especialista** supervisará que la planta eléctrica responda en los tiempos establecidos (10 min).
- **Soporte a Telecomunicaciones:** Ante un corte del canal dedicado de internet, el equipo técnico activará el protocolo de trabajo manual para las áreas de urgencias y administración, garantizando que el hospital no se detenga.

CAPITULO III: PLAN DE RESPALDO DE LA INFORMACIÓN

3.1. Actividades Previas al Desastre

3.1. Actividades Previas al Desastre (Fase de Preparación)

En esta etapa se definen las acciones de planeación, capacitación y ejecución necesarias para salvaguardar los activos de información de la entidad.

Estrategia de Acción:

- **Gestión de Sistemas de Información:** La ESE Hospital San Vicente de Paúl prioriza la operatividad de sus plataformas críticas (*SaludSystem,*

GoTelemedicina, ORFEO y *3CX*). El **Especialista de Soporte** supervisará que estos sistemas cuenten con las licencias y configuraciones de seguridad actualizadas.

- **Protocolos de Respaldo (Backup):** La recuperación de datos se fundamenta en copias de seguridad periódicas. El **Ingeniero de Sistemas** será responsable de almacenar estos backups en dispositivos externos y servidores seguros, asegurando su correcta clasificación para una recuperación inmediata.
- **Políticas de Seguridad y Mantenimiento:** El **Técnico en Sistemas** ejecutará rutinas de limpieza y cuidado del hardware. La reposición de equipos se activará bajo tres criterios: cumplimiento del ciclo de vida útil, falla crítica del hardware o pérdida física.

3.2. Actividades Durante el Desastre (Fase de Respuesta)

Ante un siniestro, la prioridad es la seguridad humana, seguida de la protección de los activos tecnológicos.

1. **Coordinación:** El **Ingeniero de Sistemas** evaluará la magnitud del evento y coordinará la salvaguarda de servidores y backups físicos.
2. **Mitigación:** Si las condiciones lo permiten, el **Especialista de Soporte** y el **Técnico** procederán al apagado preventivo de equipos y resguardo de hardware crítico.
3. **Comunicación:** Se dispondrá de un directorio de emergencia visible con contactos de organismos de socorro (Bomberos, Policía) y proveedores de servicios críticos.

3.3. Actividades Después del Desastre (Fase de Recuperación)

Una vez controlada la situación, se procederá a la evaluación de daños y restablecimiento del servicio según la siguiente tabla:

Tipo de Riesgo	Medida de Recuperación	Responsable
Robo / Vandalismo	Diagnóstico de activos faltantes, informe técnico y denuncia ante las autoridades pertinentes.	Empresa de Vigilancia / **Ingeniero de Sistemas**
Fallas en los Equipos	Diagnóstico técnico detallado; ejecución de mantenimiento correctivo o trámite de reposición de hardware.	**Técnico en Sistemas**
Virus / Ciberataques	Aislamiento de red, desinfección mediante consola corporativa y restauración de backups inalterados.	**Ingeniero de Sistemas**
Corte de Fluido Eléctrico	Verificación de carga en UPS y supervisión de la transferencia de energía de la planta eléctrica. Si persiste la falla, apagado seguro de servidores.	**Especialista de Soporte** / Mantenimiento
Caída de Internet / Telefonía 3CX	Verificación del enlace dedicado, gestión con el ISP y activación del **Plan de Operación Manual** en Urgencias y Administración.	**Ingeniero de Sistemas / Especialista**
Equivocaciones / Error Humano	Evaluación de impacto en la base de datos por el Coordinador Asistencial y corrección técnica de registros en el sistema.	Coord. Asistencial / **Ingeniero de Sistemas**

Fuego / Desastre Natural	Evaluación de integridad de la infraestructura de red, corte preventivo de energía y recuperación de equipos resguardados.	Brigadistas / **Equipo de Sistemas**

Disposiciones Finales de Mejora

Para garantizar el éxito de este plan, la ESE Hospital San Vicente de Paúl establece las siguientes directrices:

1. **Diagnóstico de Daños:** Tras cualquier incidente, se debe emitir un informe técnico que defina los puntos críticos a recuperar y el tiempo estimado de restauración (RTO).
2. **Registro Documental:** Cada siniestro debe quedar consignado en un archivo histórico de ejecución del Plan de Contingencia. Esto permitirá realizar análisis de causa raíz y retroalimentar la matriz de riesgos.
3. **Optimización Continua:** El plan será revisado trimestralmente por el **Ingeniero de Sistemas** y la gerencia para adaptarlo a nuevos cambios tecnológicos, como la eliminación de conexiones en cascada y la mejora de la velocidad de transmisión de

3.4 Fortalecimiento en Ciberseguridad (Ataques Cibernéticos)

Actualmente, el plan se centra en virus comunes y accesos físicos. Se deben incluir medidas específicas contra **Ransomware** y **Phishing**:

- **Protocolo Anti-Ransomware:** * **Aislamiento Inmediato:** En caso de detectar archivos cifrados o mensajes de rescate, el personal debe desconectar el equipo de la red eléctrica y de datos (cable LAN) para evitar la propagación.

- **Inmutabilidad de Backups:** Implementar la regla **3-2-1** (3 copias, 2 medios diferentes, 1 fuera de línea/nube). Las copias de seguridad deben ser inalterables para que un atacante no pueda borrarlas.

- **Seguridad de Identidad:**

  - **Autenticación de Dos Factores (2FA):** Obligatorio para el acceso al sistema **SaludSystem** y correos institucionales, eliminando la práctica de compartir contraseñas.

  - **Gestión de Privilegios Mínimos:** Los usuarios solo tendrán acceso a las carpetas y funciones estrictamente necesarias para su cargo.

3.5 Plan de Trabajo Manual por Caída de Internet/Sistema

Cuando el sistema **SaludSystem** o el internet no estén disponibles, se activará el **Modo de Operación Manual**:

Área de Urgencias (Prioridad Crítica)

- **Kit de Contingencia Física:** Cada estación de enfermería y consultorio debe tener una carpeta física con:

  - Formatos de Historia Clínica en papel (clones del sistema digital).

  - Recetarios y órdenes de exámenes manuales con papel químico (copia).

  - Hojas de signos vitales y control de líquidos.

- **Triaje y Admisiones:** Se utilizará un libro de registro manual (Libro de Folios) para anotar el ingreso, documento de identidad y hora de llegada de cada paciente.

- **Identificación Temporal:** Uso de manillas escritas a mano para asegurar la correcta administración de medicamentos sin el apoyo del visor digital.

Oficinas Administrativas

- **Facturación y Cartera:** Registro en plantillas locales de Excel (si hay energía) o formularios de contingencia pre-impresos para su posterior digitación cuando el servicio retorne.
- **Gestión Documental:** Uso temporal de archivos locales o carpetas físicas para correspondencia recibida, aplicando el software **Alfresco** solo cuando se restablezca el servidor local.

3.6 Matriz de Riesgos Actualizada (Nuevas Amenazas)

Añadir estos ítems a la tabla de riesgos existente:

Tipo de Riesgo	Probabilidad	Causa Controlable	Impacto (1-10)	Medida Preventiva
Secuestro de Datos (Ransomware)	Alta	Sí	10	Backups desconectados y firewall avanzado.
Caída Total de Internet/Red	Mediana	No	9	Switch a formatos físicos y kit de urgencias.
Suplantación (Phishing)	Alta	Sí	7	