Aprobado por:	**Dr. Silvio Enrique Farfán Benavente**	**Fecha:**
Revisado por:	**Jorge Antonio Huamani Infantes**	**Fecha: 04/07/2024**
Elaborado por:	**Elvis Joel Carrillo Montalvo**	**Fecha: 04/07/2024**

DOCUMENTO TÉCNICO:

“PLAN DE CONTINGENCIA INFORMÁTICO”

CARMEN DE LA LEGUA REYNOSO - CALLAO

PERU-2024

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:35:17 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:31:14 -05:00

INDICE

1. Introducción 3
2. Finalidad 3
3. Objetivo 3
3.1. General 3
3.2. Específicos 3
4. Ámbito de Aplicación 4
5. Base Legal 4
6. Contenidos 5
6.1. Aspectos técnicos conceptuales 5
6.2. Análisis de la Situación Actual 6
6.2.1. Antecedentes: 6
6.2.2. Problema: 6
6.2.3. Causas del Problema: 6
6.2.4. Población objetivo: 6
6.2.5. Alternativas de solución: 6
6.3. Articulación Estratégica con los Objetivos y Acciones del PEI y Actividades Operativas del POI 7
7. Metodología de Trabajo 7
7.1. Fase 1: Planificación 8
7.2. Fase 2: Determinación de Vulnerabilidades 13
7.3. Fase 3: Estrategias del Plan de Contingencias 19
7.4. Fase 4. Elaboración del Plan de Contingencia 24
7.5. Fase 5. Implementación del Plan de Contingencia 25
7.6. Fase 6: Ejecución del plan de Pruebas 25
7.7. Fase 7: Monitoreo. 25
8. Responsables del Plan de Contingencia Informático 25
9. Presupuesto 25
10. Anexos. 26

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:35:40 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:31:26 -05:00

1. Introducción

El Hospital San José es un establecimiento del sector salud con nivel de complejidad II-2, que brinda atenciones preventivas promocionales, recuperativas y de rehabilitación a las personas, familia y la población en un ambiente saludable contribuyendo al desarrollo del país.

El Hospital San José cuenta con procesos administrativos y asistenciales que se encuentran apoyados en las tecnologías de la información y comunicaciones, en tal sentido, es susceptible a enfrentarse a eventos desfavorables que puedan originar efectos adversos dentro del hospital. Por ello, el tiempo y la capacidad resolutiva con que se enfrente y controle cualquier evento desfavorable resulta ser de vital importancia para nuestra institución.

El área de Informática, como buena práctica de TI, ha elaborado el Plan de Contingencia, dado que la institución es vulnerable a eventos adversos que pueden interrumpir o dañar los servicios informáticos, lo que no solo afecta a usuarios internos sino también a usuarios externos. Asimismo, este plan de contingencia está encargado de velar por la confidencialidad, integridad y disponibilidad de la información necesarios para el correcto funcionamiento de los servicios informáticos dentro de la institución.

Así, en el presente plan se establece el ámbito de aplicación, los objetivos y metodología del plan, con la finalidad de lograr reducir el impacto negativo ante cualquier interrupción de los servicios informáticos, contribuyendo a que el Hospital San José se encuentre preparado ante cualquier situación de contingencia a nivel de tecnologías de la información.

2. Finalidad

Garantizar la continuidad de los servicios informáticos que brinda el Hospital San José para la atención del público ante una falla, en el menor tiempo posible.

3. Objetivo

3.1. General

Establecer los procedimientos y acciones necesarias en caso de una contingencia para proteger y asegurar el funcionamiento de las Tecnologías de Información utilizadas para la atención del público en la adquisición de algún servicio dentro del Hospital. Esto incluye establecer una capacidad operativa para reanudar aplicaciones críticas identificadas previamente, recuperación de datos y restaurar los sistemas afectados al estado operativo normal.

3.2. Específicos

- Definir los activos más importantes a proteger para la continuidad en los procesos de los sistemas de información ante un evento.
- Identificar y definir los riesgos potenciales que afectarían la continuidad de los procesos y servicios informáticos brindados por el Hospital San José.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:35:50 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:31:35 -05:00

- Definir actividades y procedimientos necesarios para recuperar las operaciones de los sistemas de Información en los plazos definidos.
- Organizar y capacitar al personal para afrontar adecuadamente la contingencia ante un evento grave.
- Establecer acciones que permitan evaluar los resultados y retroalimentación del presente plan.

4. Ámbito de Aplicación

El Plan de Contingencia Informático del Hospital San José del Callao abarca todos los sistemas de información que alojan los servidores, los mismos que son gestionados por la Unidad de Estadística, Informática y Comunicaciones.

5. Base Legal

- Ley N°28716, Ley de Control Interno de las Entidades del Estado
- Ley Nº28551, Ley que establece la obligación de elaborar y presentar planes de contingencia.
- Resolución Ministerial N° 028-2015-PCM, aprobación de los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Resolución Ejecutiva Regional N°316 que aprueba las Políticas del Gobierno Regional del Callao sobre Seguridad de la Información.
- Decreto Supremo N° 034-2014-PCM que aprueba el Plan Nacional de Gestión del Riesgo de Desastres — PLANAGERD 2014-2021.
- Decreto Supremo N° 118-2018-PCM, que declara de interés nacional el desarrollo del gobierno digital, la innovación y la economía digital con enfoque territorial y se crea el Comité de Alto Nivel por un Perú digital, Innovador y Competitivo.
- Decreto Legislativo N° 1412-2018, que aprueba la Ley de Gobierno Digital.
- Resolución Ministerial N° 188-2015-PCM, que aprueba los Lineamientos para la Formulación y Aprobación de Planes de Contingencia
- Resolución Directoral 090-2022/MINSA, Directiva Administrativa para la Formulación, Seguimiento y Evaluación de los Planes Específicos en el Ministerio de Salud.
- Resolución de Contraloría General N° 320-2006-CG, que aprueba la Norma de Control Interno del Sector Público.
- Resolución de Contraloría N° 146-2019-CG, que aprueba la Directiva N° 006-2019- CG/INTEG "Implementación del Sistema de Control Interno en las Entidades del Estado".
- Resolución Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial 166- 2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP¬ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Jefatural N° 386-2002-INEI, del 31 de diciembre de 2002, que aprueba la Directiva N°016-2002-INEI/DTNP, "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Públicas".
- Resolución Jefatural N° 347-2001-INEI, que aprueba la Directiva N° 018- 2001. INEI/DTNP, "Normas y Procedimientos Técnicos para Garantizar la Seguridad de la Información Publicada por las Entidades de la Administración Pública".

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:36:05 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:31:45 -05:00

- Guía Práctica para el Desarrollo de Planes de Contingencia de Información del INEI (Instituto Nacional de Estadística e Informática de Perú).

6. Contenidos

6.1. Aspectos técnicos conceptuales

Para la mejor comprensión de los términos y contenido del presente Plan, se detallan las siguientes definiciones:

- **Programa de Ofimática:** Programa que permite procesamiento de texto, hojas de cálculo y realizar presentaciones en la computadora.
- **Archivo de Copia de Seguridad:** Copiar el esquema y datos de una base de datos o un conjunto de archivos almacenados dentro de un disco duro hacia otra unidad de disco duro.
- **LAN:** Una LAN consiste en computadoras personales que están conectadas entre sí a través de varios medios, para que puedan comunicarse entre sí. Una red de computadoras, dentro de un área limitada como una empresa. Equipos informáticos, muy próximos entre sí, conectados a un servidor que alberga software al que pueden acceder los usuarios. Este método no utiliza internet.
- **Sistema operativo:** El programa principal que administra las funciones internas de una computadora y proporciona un medio para instalar software y agregar archivos a la computadora.
- **Switch:** Un dispositivo que controla el flujo de tráfico entre múltiples equipos informáticos dentro de una red.
- **Router:** Un dispositivo electrónico que conecta dos o más redes y enruta los paquetes de datos entrantes a la red adecuada.
- **Servidor:** Una computadora de altas prestaciones que almacena aplicaciones y archivos de datos para todas las estaciones de trabajo en una red.
- **Ticketera:** Impresora utilizada por un Sistema de Información para emitir tickets que den constancia de adquisición de algún servicio por parte de una persona.
- **Virus:** una aplicación informática que se almacena en la computadora que impide su correcto funcionamiento o permite el robo de datos.
- **Software de detección de virus:** software para escanear el sistema de archivos dentro de una computadora para detectar y/o eliminar virus.
- **Probabilidad:** Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado.
- **Amenaza:** Causa potencial de un incidente de seguridad de la información no deseado, que puede resultar en un daño para la organización o el sistema.
- **Riesgo:** Posibilidad de que suceda algún evento adverso que tendrá un impacto sobre el cumplimiento de los objetivos institucionales o de los procesos para la presentación de servicios al ciudadano. Se expresa en términos de probabilidad y consecuencias.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos o controles, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.
- **Sistema de Información:** Es un conjunto de elementos organizados a fin de administrar datos e información necesarios para lograr un objetivo. Dichos sistemas están formados por personas, equipos y procedimientos.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:36:22 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:33:10 -05:00

6.2. Análisis de la Situación Actual

6.2.1. Antecedentes:

- Las Normas de Control Interno, aprobado con Resolución de Contraloría N° 320-2006-CG (30OCT2006), en el numeral *3.10 Controles para las tecnologías de la información y comunicaciones*, comentario 07, enuncia que se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado; esto con el fin de garantizar el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad.
- La Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", aprobado mediante Resolución Ministerial N° 246-2007-PCM (22AGO2007), en la cláusula 14, *Gestión de continuidad del negocio*, enuncia que se deberá desarrollar e implantar planes de contingencia para asegurar que en los procesos del negocio se puedan restaurar las operaciones esenciales en los plazos requeridos a causa de interrupciones como la de falla de equipos.
- La Norma Técnica Peruana "NTP-ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la información. Requisitos. 2ª Edición", aprobado a través de la Resolución Ministerial N° 004-2016-PCM (08ENE2016), establece en su Anexo "A" como uno de sus controles el de la *Planificación de continuidad de la seguridad de la información* en situaciones adversas (A.17.1.1), sabiéndose que la seguridad de la información busca preservar, entre otros aspectos, la disponibilidad de la misma.

6.2.2. Problema:

- Interrupción en la continuidad de los procesos de TI

6.2.3. Causas del Problema:

- Fallo en el Hardware.
- Fallo en la energía eléctrica.
- Falta de mantenimiento preventivo y Correctivo.

6.2.4. Población objetivo:

- Cantidad de trabajadores del Hospital San José.
- Cantidad de pacientes concurrentes al Hospital San José.

6.2.5. Alternativas de solución:

Analizar los riesgos posibles que afectarían la continuidad de los procesos de TI con el objetivo de reducir los daños.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:36:37 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:33:25 -05:00

6.3. Articulación Estratégica con los Objetivos y Acciones del PEI y Actividades Operativas del POI

VINCULACIÓN CON LA POLÍTICA GENERAL DE GOBIERNO (PGG)		
EJE 8	**Gobierno y transformación digital con equidad**	
LIN. 8.1	**Garantizar el acceso inclusivo, seguro y de calidad al entorno digital y el aprovechamiento de las tecnologías digitales en todas las regiones del país para consolidar la ciudadanía digital considerando sus condiciones de vulnerabilidad y diversidad cultural**	
Plan Estratégico Institucional (PEI)		
OBJETIVO ESTRATÉGICO	**DESCRIPCIÓN DEL OBJETIVO ESTRATÉGICO**	**INDICADOR**
OEI.08	Fortalecer la Gestión Institucional	Porcentaje de cumplimiento anual del Plan Estratégico Institucional
ACCIÓN ESTRATEGICA	**DESCRIPCIÓN DE LA ACCIÓN ESTRATÉGICA**	**INDICADOR**
AEI.08.05	Proceso de modernización de la gestión pública implementada en el Gobierno Regional del Callao	Número de ubicación en el ranking de institucionalidad regional
Plan Operativo Institucional (POI)		
CÓDIGO DE AOI	**DESCRIPCIÓN DE LA ACTIVIDAD OPERATIVA INSTITUCIONAL (AOI)**	
AOI00131800482	ATENCION DE SOPORTE DE TECNOLOGIA DE INFORMACION Y COMUNICACION	
AOI00131800484	SOPORTE INFORMATICO PARA LOS APLICATIVOS INFORMATICOS	
AOI00131800487	DESARROLLO Y MANTENIMIENTO DE LOS APLICATIVOS INFORMATICOS	

7. Metodología de Trabajo

La metodología de Trabajo estará dividida siguientes siete (7) fases:

Fase 1: Planificación.

Fase 2: Determinación de Vulnerabilidades.

Fase 3: Estrategias del Plan de Contingencia.

Fase 4: Elaboración del Plan de Contingencia.

Fase 5: Implementación del Plan de Contingencia.

Fase 6: Ejecución del plan de Pruebas.

Fase 7: Monitoreo.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:36:54 -05:00

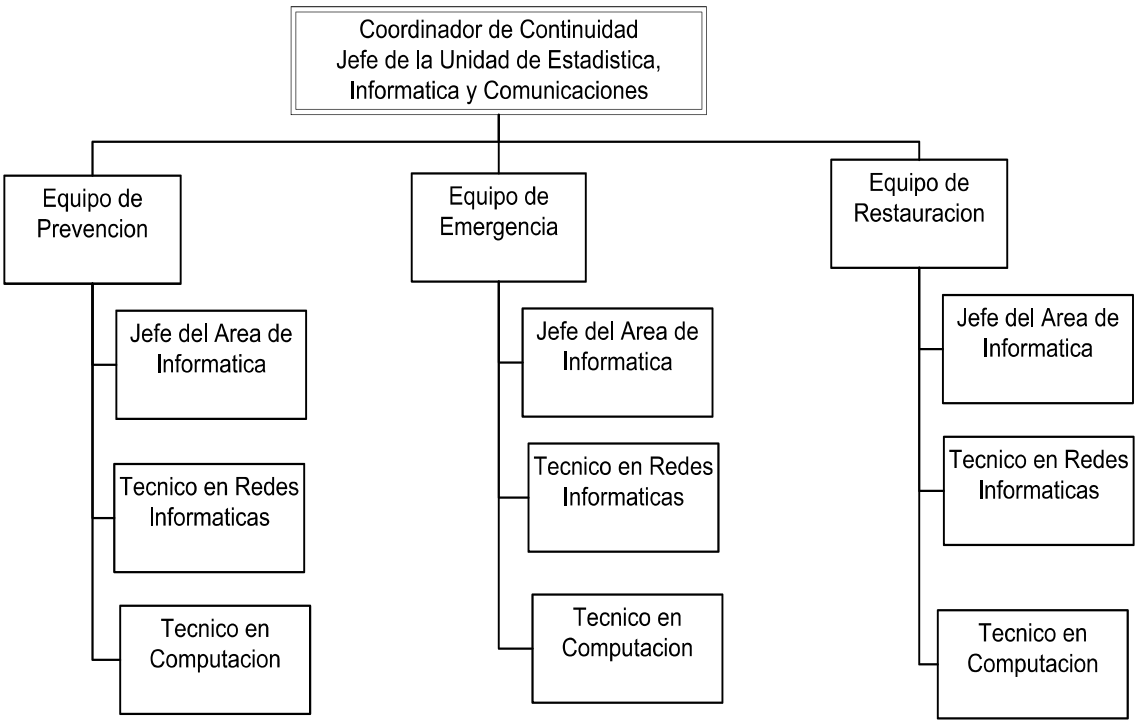
Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:33:39 -05:00

7.1. Fase 1: Planificación

En esta etapa se identifican los problemas específicos que se pueden enfrentar en la ejecución del plan, los recursos que se utilizarán, que están disponibles y cuales tendrán que ser solicitados, los requisitos de las partes interesadas, las condiciones de ejecución, y los objetivos finales del plan.

Fase 1.1: Organización del Área de Informática

El área de Informática depende de la Unidad de Estadística, Informática y Comunicaciones, la labor que desempeña es administrar, brindar soluciones informáticas y soporte técnico en materia de tecnologías de la Información, dando prioridad a todas las áreas que tengan servicios de atención al paciente. Así como, realizar el soporte tecnológico y seguridad de información para la operatividad de la red informática interna dentro del Hospital.



Fase 1.2: Roles, funciones y responsabilidades dentro del Plan

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia de Tecnologías de la Información:

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:37:19 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:36:16 -05:00

Coordinador de Continuidad

Sera representado por el jefe de la Unidad de Estadística, Informática y Comunicaciones que tiene las siguientes funciones:

- Coordinar, dirigir y activar el Plan de Contingencia según una contingencia dada.
- Monitorear, supervisar y vigilar la recuperación de los Sistemas Informáticos de atención al público administrados por el Área de Informática.
- Declarar el fin de la ejecución del Plan de Contingencia.

EQUIPO DE PREVENCIÓN:

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre, con el fin de evitar se concrete el siniestro o desastre y en caso ocurriese, tener todas las herramientas o medios necesario para realizar la recuperación de los servicios de tecnologías de la información, en el menor tiempo posible.

El responsable del Personal de Prevención es el *Administrador de Seguridad de Redes Informáticas*. A continuación, se detalla las funciones por cada miembro del equipo de prevención:

Administrador de Seguridad de Redes Informáticas:

- Supervisar el tráfico de red, perfiles de seguridad de información digital compartida entre los usuarios y uso indebido de los recursos de internet del personal.
- Supervisar el uso de licencias de software.
- Supervisar la actualización de las aplicaciones informáticas.
- Velar por la continuidad de los servicios externos (Hosting, Central Virtual, Telefonía Móvil, Internet)
- Realizar el requerimiento de equipos o repuestos necesarios para la continuidad de los procesos informáticos.

Técnico en Redes Informáticas:

- Monitorear la performance de la red de datos.
- Verificar el adecuado flujo eléctrico en los equipos de Redes Informáticas
- Realizar el mantenimiento preventivo y correctivo de los equipos de red y conectividad de red (cableado, radio enlaces y APs)
- Realizar el mantenimiento preventivo y correctivo de los servidores.
- Mantener actualizado el inventario de hardware de los equipos de cómputo y red.
- Mantener actualizado la documentación de configuración de los equipos de comunicaciones y servidores.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:37:31 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:36:28 -05:00

Técnico en mantenimiento de Equipos de Cómputo:

- Realizar mantenimiento preventivo y correctivo de los equipos de cómputo (PC, impresoras, etc.).
- Revisar el correcto funcionamiento de los equipos de cómputo.
- Mantener el abastecimiento oportuno de los insumos de impresión y de contómetros (papel térmico).
- Verificar el flujo eléctrico en los equipos de cómputo.
- Mantener actualizado el inventario de hardware de los equipos de cómputo.
- Monitorear el software antivirus.

Administrador de Copias de Respaldo:

- Verificar los archivos de copia de seguridad de los Sistemas de Información de atención al público.
- Verificar las copias de archivos y carpetas compartidas del personal que guarda información en los servidores.
- Realizar pruebas previas de recuperación de las copias de seguridad.
- Mantener un control actualizado de las versiones de las fuentes de los sistemas de información y de los portales web de la entidad.
- Coordinar periódicamente las pruebas de restauración de las fuentes de los sistemas informáticos de la entidad.

Electricista del Área de Mantenimiento y Servicios Generales

- Personal técnico encargado de subsanar los problemas de fluido eléctrico notificados por los *Técnicos en mantenimiento de Equipos de Redes Informáticas y Equipos de cómputo de Escritorio.*

PERSONAL DE EMERGENCIA:

Es el equipo encargado de ejecutar todas las acciones durante la ejecución del siniestro o desastre, con la finalidad de mitigar su impacto sobre la operatividad de los equipos tecnológicos y los servicios informáticos de atención al público administrado por el Área de Informática. El responsable del Equipo de emergencia es el *Administrador de Seguridad de Redes Informáticas*. A continuación, se detalla las funciones por cada miembro del equipo de emergencia:

Administrador de Seguridad de Redes Informáticas:

- Notificar el desastre o incidencia al coordinador de contingencia informática.
- Apoyar en las acciones que se requieran.
- Comunicar al Coordinador de contingencia informática las acciones de emergencia ejecutadas.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:37:43 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:36:40 -05:00

Técnico en Redes Informáticas

- Ejecutar las actividades de emergencia detalladas en el Plan de Contingencia de acuerdo con el escenario de riesgo presentado.
- Realizar la evaluación de condiciones de los servidores y equipos de redes y comunicación del centro de datos durante la emergencia.
- Apoyar en las acciones que se requieran.
- Comunicar al Coordinador de contingencia informática las acciones de emergencia ejecutadas.

Técnico en mantenimiento de Equipos de Cómputo:

- Ejecutar las actividades de emergencia detalladas en el Plan de Contingencia de acuerdo con el escenario de riesgo presentado.
- Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios.
- Apoyar en las acciones que se requieran.
- Comunicar al Coordinador de contingencia informática las acciones de emergencia ejecutadas.

Administrador de Copias de Respaldo:

- Ejecutar las actividades de emergencia detalladas en el Plan de Contingencia de acuerdo con el escenario de riesgo presentado.
- Realizar la evaluación de las condiciones de la información almacenada en los diferentes sistemas y bases de datos durante la emergencia.
- Apoyar en las acciones que se requieran.
- Comunicar al Coordinador de contingencia informática las acciones de emergencia ejecutadas.

Electricista del Área de Mantenimiento y Servicios Generales

- Encargado de velar por el funcionamiento del grupo electrógeno en caso de falla de pérdida de fluido para las áreas de atención a usuarios externos.

PERSONAL DE RESTAURACIÓN:

Es el equipo encargado de ejecutar todas las acciones después de haber ocurrido el siniestro, con el fin de restituir en el menor tiempo posible la operatividad de los equipos tecnológicos y recuperar el servicio informático de atención al público administrado por el Área de Informática. El responsable del Equipo de restauración es el

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:38:04 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:36:57 -05:00

Administrador de Seguridad de Redes Informáticas. A continuación, se detalla las funciones por cada miembro del equipo de restauración:

***Administrador de Seguridad de Redes Informáticas*:**

- Iniciar el proceso de recuperación de los servicios de TI, realizando pruebas de funcionamiento en los equipos afectados de la Sala de Servidores.
- Supervisar la recuperación de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los equipos componentes del Centro de Datos.
- Coordinar y monitorear la restauración de los sistemas de información y ejecución de pruebas para la verificación de su funcionalidad.
- Notificar al Coordinador de Continuidad, las acciones de recuperación ejecutadas.
- Apoyar en las acciones que se requieran.

Técnico en Equipos de Cómputo de Redes Informáticas

- Iniciar el proceso de recuperación de los equipos de red afectados, realizando las pruebas de funcionamiento en el centro de datos.
- Restaurar la conectividad de red entre los equipos de comunicación, servidores y equipos de cómputo realizando las acciones necesarias.
- Restaurar los servicios de servidores de aplicaciones alojados en los servidores y Sistemas de Información.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los servidores, equipos de red y conectividad afectados en el proceso de recuperación.
- Apoyar en las acciones que se requieran.

Técnico en Equipos de Cómputo Personal

Corregir la conectividad de equipos de cómputo de manera presencial los equipos de redes informáticas que se encuentran dentro del ambiente del personal que usa los sistemas de información.

- Corregir la conectividad de equipos a dispositivos de salida de impresión.
- Reemplazar o revisar equipos de cómputo informático que no funcionen.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos de cómputo afectados en el proceso de recuperación.
- Apoyar en las acciones que se requieran.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:38:20 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:37:12 -05:00

Administrador de Copias de Respaldo:

- Restaurar las copias de respaldo de carpetas compartidas, base de datos que usan los sistemas de información de atención a usuarios externos según las acciones de restauración.
- Comunicar las acciones realizadas al Administrador de Seguridad de Redes informáticas.
- Elaborar un informe técnico que incluya la evaluación de las copias de respaldo de base de datos, archivos y las fuentes de las aplicaciones.
- Apoyar en las acciones que se requieran.

Electricista del Área de Mantenimiento y Servicios Generales

- Encargado de velar por el funcionamiento del grupo electrógeno en caso de falla de pérdida de fluido para las áreas de atención a usuarios externos.

7.2. Fase 2: Determinación de Vulnerabilidades

En esta etapa se identifican las aplicaciones críticas y los recursos que puedan ser susceptibles de provocar eventos que afecten el normal funcionamiento de los Sistemas de Información y Comunicaciones afectando a procesos críticos de nuestra Institución y que conlleven a activar la contingencia.

Fase 2.1: Procesos y recursos críticos

En esta etapa se describen las aplicaciones y recursos críticos con su expectativa en tiempo de recuperación:

Tabla Nº 1. Procesos y recursos críticos de TI

N°	Recursos Críticos	Descripción
1	Servidores	Directorio Activo, DNS, Base de Datos, Archivos, Aplicaciones
2	Equipos de red	Switch, Punto de Accesos, Router
3	Seguridad perimetral	Equipo cortafuego
4	Central Telefónica	Equipo encargado de gestionar las llamadas internas y externas.
5	Sistema de aire acondicionado	Equipo encargado de mantener la temperatura adecuada en el centro de datos.
6	Sistemas de Información	Aplicaciones disponibles para acceso al usuario interno y externo
7	Equipo de respaldo de energía eléctrica	Equipo UPS para respaldo de energía continua.
8	Equipos de computo	Equipamiento de cómputo para el procesamiento de información

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:38:37 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:37:29 -05:00

N°	Recursos Críticos	Descripción
9	Conectividad de Red	Equipos o accesorios que posibilitan la conexión de una oficina y/o equipo con la red institucional
10	Personal critico de procesos de TI	Servicios profesionales críticos encargados de procesos de TI.
11	Servicio de Telefónica Móvil	Servicio de comunicación telefónica
12	Servicio de Telefonía Fija	Servicio de telefónica fija para la central
13	Servicio de Internet Corporativo	Servicio de Internet dedicado
14	Servicio de Hosting	Servicio web y correo electrónico.
15	Servicio de Central Telefónica Virtual	Servicio de telefonía exclusivo para brindar las citas por teléfono.
16	Servicio de Facturación Electrónica	Solución informática que proporciona todo lo necesario para envió de los comprobantes electrónicos a SUNAT.

Fase 2.2: Identificación de amenazas

En esta etapa se identificarán las amenazas que puedan vulnerar los recursos y sistemas de TI, considerando su ubicación actual y contexto.

Tabla Nº 2. Tipos de Amenazas a los servicios de TI

Nº	Amenaza	Tipo
1	Falla de software	Interno
2	Falla de hardware	
3	Ausencia o no disponibilidad del personal	
4	Acceso no autorizado	
5	Terremoto	Externo
6	Inundación o aniegos	
7	Incendio	
8	Caída de servicios externos en TI	
9	Virus informáticos o ataques maliciosos	
10	Robo o vandalismo	
11	Caída o interrupción del suministro eléctrico	

Una vez identificadas las amenazas que pueden afectar los recursos y sistemas críticos de TI, calculamos el nivel de probabilidad de ocurrencia, para lo cual nos guiamos de los valores definidos en la metodología de Gestión de riesgos que se encuentra en la siguiente tabla:

Tabla Nº 3. Determinación de la Probabilidad

Probabilidad	Valor	Frecuencia
Bajo	1	Al menos una vez en los últimos 5 años o mas
Medio	2	Al menos una vez en 3 años

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:38:51 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 11:37:44 -05:00

Alto	3	Al menos una vez al año.
Muy Alto	4	Más de una vez al año.

Tabla N° 4. Probabilidad estimada de las amenazas a los servicios de TI

A continuación, se detalla el resultado obtenido, en base a la metodología de gestión de riesgos, mediante la cual se ha obtenido el valor de probabilidad por cada amenaza:

Nº	Amenaza	Nivel de Probabilidad de ocurrencia	Nivel de Probabilidad estimada
1	Falla de software	4	Muy Alto
2	Falla de hardware	4	Muy Alto
3	Ausencia o no disponibilidad del personal	2	Medio
4	Acceso no autorizado	2	Medio
5	Terremoto	1	Bajo
6	Inundación o aniegos	1	Bajo
7	Incendio	1	Bajo
8	Caída de servicios externos en TI	3	Alto
9	Virus informáticos o ataques maliciosos	2	Medio
10	Robo o vandalismo	1	Bajo
11	Caída o interrupción del suministro eléctrico	4	Muy Alto

Fase 2.3: Identificación de controles existentes

La identificación de controles existentes, nos permiten conocer que tan protegidos están nuestros recursos informáticos frente a cada amenaza. Los controles existentes son los siguientes:

- Grupo electrógeno para el centro de datos operativo.
- Mantenimiento para equipos de aire acondicionado del Centro de Datos.
- Extintor en el Centro de Datos.
- Respaldo de información en medios de respaldo.

Fase 2.4: Evaluación del Nivel de Riesgo

En esta etapa se determina el nivel de riesgo de un recurso crítico de TI, consideramos el valor del nivel de probabilidad de ocurrencia identificado (Tabla Nº 3), probabilidad estimada de las amenazas a los servicios de TI (Tabla Nº 4), determinación del impacto (Tabla Nº 5) y el cálculo del nivel de riesgo (Tabla Nº 6).

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:39:03 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:02:34 -05:00

Para obtener el valor del impacto, se consideró el nivel del impacto, definido en la aplicación de la metodología de Gestión de Riesgos, como se muestra en la siguiente tabla:

Tabla Nº 5. Niveles de impacto

El valor obtenido ha sido en base a la metodología de Gestión de Riesgos (Tabla Nº 5) que ha determinado el impacto por cada amenaza, obteniendo el siguiente resultado:

Impacto	Valor	Descripción
Bajo	1	Si la amenaza llega a concretarse, el impacto sería leve y se puede prescindir del servicio por un tiempo limitado.
Medio	2	Si la amenaza llega a concretarse, tendría un impacto moderado, que se puede llegar a controlar mediante un proceso de soporte en un corto plazo.
Alto	3	Si la amenaza llegara a concretarse, el impacto sería alto y podría comprometer recursos del hospital o información clasificada como confidencial o importante, llegando a un retraso o paralización de labores en el hospital por un tiempo considerable.
Muy Alto	4	Si la amenaza llegara a concretarse, el impacto sería severo y comprometería la integridad, confidencialidad y disponibilidad de la información crítica del hospital o la paralización de las labores por un tiempo no tolerable por el hospital.

Cálculo del Nivel de Riesgo: Se desarrolla considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Tabla Nº 6. Matriz del Nivel de Riesgo

Nivel de Riesgo (probabilidad de ocurrencia x impacto			Impacto			
			Bajo	Medio	Alto	Muy Alto
			1	2	3	4
Probabilidad de ocurrencia	Bajo	1	1 (Bajo)	2 (Bajo)	3 (Medio)	4 (Medio)
	Medio	2	2 (Bajo)	4 (Medio)	6 (Alto)	8 (Alto)
	Alto	3	3 (Medio)	6 (Alto)	9 (Alto)	12 (Muy Alto)
	Muy Alto	4	4 (Medio)	8 (Alto)	12 (Muy Alto)	16 (Muy Alto)

La interpretación de la Matriz de nivel de riesgo (Tabla N° 7) de la amenaza se detalla en Tabla N°7

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:39:15 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:02:56 -05:00

Tabla N° 7. Interpretación del nivel de riesgo

Nivel de Riesgo	Descripción
Bajo	Riesgo aceptable, sin revisión y no se requieren acciones
Medio	Riesgo aceptable con revisión de la dirección, y se evalúa tomar acciones.
Alto	Riesgo no aceptable, se requiere de una acción correctiva, pero se permite planificar plazos y compromisos.
Muy Alto	Riesgo no aceptable, acción correctiva inmediata.

Seguidamente, obtenemos la Tabla N° 8, los resultados de la evaluación del riesgo de los servicios de TI:

Tabla Nº 8. Resultado de la evaluación de riesgos de los servicios de TI

N°	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de Riesgo
1	Falla de software	Daño en base de datos	4	3	Muy Alto
		Insuficiente espacio en discos de servidores	4	3	Muy Alto
		Actualización errónea de software de producción	2	2	Medio
2	Falla de hardware	Fallo de servidor	3	4	Muy Alto
		Fallo del aire acondicionado	3	3	Alto
		Fallo en Switch	3	4	Muy Alto
		Fallo en radioenlace	2	4	Alto
		Fallo en equipo de computo	2	2	Medio
3	Ausencia o no disponibilidad del personal	Renuncia o Ausencia de personal	3	3	Alto
4	Acceso no autorizado	Usuario ingresa con otras credenciales	4	2	Alto
5	Terremoto	Centro de datos inoperativo	1	4	Medio
6	Inundación o aniegos	Centro de datos inaccesible	1	4	Medio
7	Incendio	Centro de datos inaccesible	1	4	Medio
8	Caída de servicios externos en TI	Inaccesibilidad al servicio de Internet	2	3	Alto
		Caída del servicio de Hosting y Correo	2	2	Medio
		Caída del servicio de Central IP	2	3	Alto
		Caída del servicio de facturación electrónica	2	4	Alto
		Falta de renovación de licencias	1	2	Bajo
9	Virus informáticos o ataques maliciosos	Ataque por virus informático producido por el mal uso del internet	2	4	Alto
10	Robo o vandalismo	Robo de servidores	1	4	Medio
11	Caída o interrupción del suministro eléctrico	Corte del servicio de energía eléctrica no programado	3	4	Muy Alto

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:03:22 -05:00

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:39:26 -05:00

Fase 2.5: Escenarios de Riesgo

De acuerdo a los resultados de la evaluación de riesgos de los servicios de TI (Tabla Nº 8), se han establecido los siguientes escenarios que corresponden a amenazas con probabilidad de nivel alto o muy alto:

1. Daño en base de datos.
2. Insuficiente espacio en discos de servidores.
3. Fallo en el servidor.
4. Fallo en Switch.
5. Corte del servicio de energía eléctrica no programado.
6. Fallo del aire acondicionado.
7. Fallo en radioenlace
8. Renuncia o ausencia de personal.
9. Usuario ingresa con otras credenciales.
10. Inaccesibilidad al servicio de Internet.
11. Caída del servicio del Hosting y Correo.
12. Caída del servicio de Central IP.
13. Caída del servicio de Facturación electrónica.
14. Ataque por virus informático.

Tabla Nº 9. Escenario de Riesgos

Los riesgos que se tomaran en cuenta serán los de impacto MUY ALTO para este plan de contingencia de TI, es decir aquellos que afectaran la perdida de información, la suspensión de manera parcial o total de los sistemas informáticos.

N°	Escenario de Riesgo	Descripción	Impacto
1	Daño en base de datos	Este escenario hace referencia a la falla lógica en las tablas de archivos planos (carpeta DATA) que maneja el SIAF, generando la inaccesibilidad a los diferentes modulo del sistema.	Muy Alto
2	Insuficiente espacio en discos de servidores	Hace referencia al fallo de los sistemas informáticos alojados en el servidor por motivos de insuficiencia de espacio en los discos.	Muy Alto
3	Fallo de servidor	Este escenario hace referencia al fallo físico en los servidores, lo cual generará una corte en el servicio en el funcionamiento de los sistemas de información.	Muy Alto
4	Fallo en Switch	Este escenario hace referencia al fallo físico o lógico en los Switch o conmutadores, con el cual una sección de la red o toda la red dejaría de estar interconectada.	Muy Alto
5	Corte del servicio de energía eléctrica no programado	Este escenario hace referencia a la interrupción o corte del servicio de energía eléctrica, lo cual produce una indisponibilidad de los servicios	Muy Alto

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:39:40 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:03:38 -05:00

N°	Escenario de Riesgo	Descripción	Impacto
		informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	
6	Fallo del aire acondicionado	Escenario en el cual hay un fallo físico en el equipo, de tal forma que no cumpla su función de regular la temperatura, con lo cual ocasionaría que los servidores de apagaran.	Alto
7	Fallo en radioenlace	Este escenario hace referencia al fallo físico o lógico en los Switch o conmutadores, con el cual una sección de la red o toda la red dejaría de estar interconectada.	Alto
8	Renuncia o Ausencia de personal	Este escenario hace referencia a la renuncia o ausencia de un personal clave de manera fortuita.	Alto
9	Usuario ingresa con otras credenciales	Este escenario hace referencia al uso de credenciales de personal que ya no labora en la entidad.	Alto
10	Inaccesibilidad al servicio de Internet	Hace referencia a la caída o corte del servicio de Internet, ocasionando la inaccesibilidad a las consultas de servicios web.	Alto
11	Caída del servicio de Central IP	Hacer referencia a la caída o corte del servicio de la Central IP, ocasionando el corte en las comunicaciones para el servicio de atención de citas por teléfono.	Alto
12	Caída del servicio de facturación electrónica	Este escenario hace referencia al corte o caída del servicio de generación, envió y validación de los comprobantes electrónicos, ocasionando retraso en los plazos establecidos de envió a la SUNAT.	Alto
13	Ataque por virus informático producido por el mal uso del internet	Este escenario hace referencia a la infección de virus informático en los equipos de cómputo mediante el uso del internet, ocasionando perdida de información en el equipo y propagándose por toda la red hacia las demás estaciones de trabajo.	Alto

7.3. Fase 3: Estrategias del Plan de Contingencias

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre:

Estrategias de prevención de tecnologías de la información

a) Almacenamiento y respaldo

- Realización de copias de respaldo de la información almacenada (archivo y base de datos) en distintos servidores, para luego ser copiadas a un medio externo y resguardadas en un lugar diferente al centro de datos.
- Las copias de base de datos son diarias, se comprimen, y luego de son extraídas a los 4 días posteriores a un medio externo.
- Responsables: Administrador de Copias de Respaldo y Administrador de Seguridad de Redes Informáticas.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:39:56 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:03:47 -05:00

b) Verificación de las copias de respaldo.

- Se realiza pruebas de restauración de copias de respaldo para evaluar el tiempo y la integridad de los Backups.
- Periodicidad: Trimestral.
- Responsables: Administrador de Copias de Respaldo y Administrador de Seguridad de Redes Informáticas.

c) Entrenamiento y personal de reemplazo.

- Todo el personal del área de Informática, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.
- Se debe contemplar un personal de reemplazo para el caso de vacaciones.
- Periodicidad: Semestral
- Responsables: Coordinador *de Continuidad* y *Administrador de Seguridad de Redes Informáticas*.

d) Evaluación y gestión de proveedores.

- Actualizar el listado de proveedores claves que brindan servicios y recursos de TI.
- Periodicidad: Trimestral.
- Responsables: Administrador de Seguridad de Redes Informáticas

e) Definir periodo de vacaciones que permita la continuidad de los servicios de TI

- Al final de cada año se debe realizar un programa de vacaciones del siguiente año que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos tales como soporte técnico, redes, sistemas de información y bases de datos, así como seguridad de la información.
- Periodicidad: Anual.
- Responsables: *Coordinador de Continuidad* y *Administrador de Seguridad de Redes Informáticas*

f) Renovación tecnológica.

- A final del año se desarrolla la programación de Requerimientos del Área de Informática que incluye acciones de renovación tecnológica para el siguiente año.
- Periodicidad: Anual.
- Responsables: Administrador de Seguridad de Redes Informáticas

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:40:42 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:03:57 -05:00

Estrategia frente a emergencias en tecnologías de la información

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información respaldada y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre.

A continuación, se citan las acciones que se realizarán durante una contingencia:

Acciones durante la emergencia:

- El Coordinador *de Continuidad* notifica y reúne a todos los integrantes del equipo de emergencia.
- El *Administrador de Seguridad de Redes Informáticas* informa al *Coordinador de Continuidad* sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y evaluar la dimensión de los daños a los equipos, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitarse una emergencia o desastre, a fin de recuperar la información y los servicios informáticos para estabilizar la infraestructura tecnológica luego del evento suscitado.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

Tabla Nº 10. Prioridad de atención durante la restauración de TI

Detalle de los equipos de la sala de servidores, equipos de red y de escritorio clasificado por la prioridad de atención para la recuperación:

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los pacientes y manejen alto volumen de información como son los servidores de bases de datos, aplicaciones y web.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:40:52 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:04:06 -05:00

2	Atención normal: Sistemas de información y equipos no relacionados con la atención a pacientes y manejen información administrativa.
3	Atención baja: Sistemas de información y equipos de uso interno con poco volumen de transacciones, así como recursos compartidos.

Tabla Nº 11. Prioridad de equipos de TI

N°	Equipos de Red	Función	Descripción	Prioridad
1	Servidor	Controlador de Dominio	Servidor de dominio de red. (Directorio Activo, DNS).	1
2	Servidor	Base de datos	Base de Datos Microsoft SQL	1
3	Servidor	Aplicaciones	Sistemas de Información	1
4	Switch	Comunicaciones	Core	1
5	Switch	Comunicaciones	Distribución	1
6	Firewall	Seguridad	UTM	1
7	UPS	Energía	Equipo de suministro eléctrico para Servidores, Equipos de comunicaciones y Seguridad Core	1
8	Servidor	Repositorio de Información	Servidor de archivos, donde se encuentra la información de las carpetas compartidas de red de atención al paciente.	1
9	Aire acondicionado	Acondicionamiento	Aire acondicionado para la Sala de Servidores	1
10	Servicio de Internet	Seguridad	Atención por central telefónica, administrar contenido web institucional y usar páginas de registro de información web externas	1
11	Equipos de Red	Comunicaciones	Switch de acceso	1
12	Computadoras	Cliente de Escritorio	Equipos de cómputo de Escritorio que usan sistemas de información de atención al paciente externo	1
13	Impresoras	Impresoras de Escritorio	Impresoras de Escritorio que usan sistemas de información de atención al usuario externo	1
14	Servidor	Web	Sistema de trámite documentario	1
15	Servidor	Aplicaciones	Servidor SIGA, SIAF (SIGA-MEF)	2
16	Servidor	Base de datos	Servidor SIGA (SIGA-MEF)	2

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:04:18 -05:00

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:41:07 -05:00

N°	Equipos de Red	Función	Descripción	Prioridad
18	Servidor	Repositorio de Información	Servidor de archivos, donde se encuentra la información de las carpetas compartidas de red que se guardan de manera semanal	3
19	Servidor	Web	Sistema de trámite documentario	3

Listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación:

Tabla Nº 12. Prioridad de Sistemas de Información

N°	Nombre del Sistema de Información	Función del Sistema de Información	Tipo de Aplicación	Prioridad
1	Sistema SIHCE	Sistema que permite la creación de Historia Clínica con validación de DNI por servicio web, registro de citas de consulta médica y cobro de las mismas de los pacientes SIS y pagantes.	Escritorio y Servicios Web	1
2	Sistema de Fichas de Emergencia	Permite el registro de fichas de atención del paciente de emergencia.	Escritorio	1
3	Sistema de Recaudación	Sistema que permite el cobro de servicios de procedimientos y medicamentos de farmacia, así como la distribución de medicamentos, registro de atención de pacientes SIS y su consumo, creación de cuentas corrientes y el cobro de las mismas.	Escritorio	1
4	Sistema de Facturación Electrónica	Sistema que permite el envío diario de las boletas, facturas, comunicados de baja y retenciones electrónicas de los sistemas anteriores hacia la SUNAT, usa servicio web y firma digital.	Escritorio y Servicios Web	1
5	Sistema de Diagnóstico por Imágenes	Sistema que permite agendar las citas para la toma de placas de rayos x y ecografías de los pacientes pagantes y SIS.	Escritorio	1
6	Sistema de Anatomía Patológica	Sistema que permite resultados de Análisis de Anatomía Patológica	Escritorio	1
7	Sistema HAE	Sistema que permite registrar la atención de diagnósticos de los pacientes Hospitalizados	Escritorio	1
8	Sistema Integrado de Gestión Administrativa (SIGA)	Soporta la gestión de procesos administrativos. El proceso de Selección en sus distintas etapas, seguimiento de ejecución de contratos.	Escritorio	2
9	SIAF	Sistema que permite la gestión de datos relacionados a los procesos de gasto e ingreso a nivel administrativo.	Escritorio	2

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:04:29 -05:00

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:41:23 -05:00

10	Sistema de Tramite Documentario	Sistema que permite crear Hojas de Trámite y darle seguimiento dentro de las Áreas del Hospital y recepción de documentos de usuarios de otras entidades y dentro del mismo Hospital	Web	3
11	Carpetas compartidas	Sistema de archivos para el intercambio de información interna	Escritorio	3
12	Libro de Reclamaciones	Permite registrar en línea los reclamos de los usuarios por la atención de los servicios de la Entidad.	Web	3

7.4. Fase 4. Elaboración del Plan de Contingencia

Una vez que se ha logrado identificar nuestras amenazas y los eventos de contingencia, se procede con la metodología del plan de contingencia que contempla los eventos que tengan mayor impacto (muy alto), identificado en la matriz de riesgos de contingencia y serán abordados tal como se indica en la siguiente tabla:

Tabla Nº 13. Eventos de mayor impacto

Nº	Amenaza	Exposición al riesgo	Formato del Plan de Contingencia
01	Daño en base de datos	Muy Alto	FPC-01
02	Insuficiente espacio en servidores	Muy Alto	FPC-02
03	Fallo en servidor	Muy Alto	FPC-03
04	Fallo en Switch	Muy Alto	FPC-04
05	Corte del servicio de energía eléctrica no programado	Muy Alto	FPC-05

7.5. Fase 5. Implementación del Plan de Contingencia

La implementación del presente plan iniciará en un plazo no mayor de 60 días calendarios después de su aprobación, con el objetivo de reducir la probabilidad de riesgos, asegurando el adecuado funcionamiento de los servicios informáticos. Por ello, se realizarán las siguientes funciones:

- Supervisión de las actividades de copias de respaldo y restauración.
- Realizar pruebas de restauración de software y hardware.
- Participar en las pruebas y simulacros de desastres.
- Pruebas de suministro de energía eléctrica con UPS y Grupo Electrógeno.

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:04:42 -05:00

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:41:39 -05:00

7.6. Fase 6: Ejecución del plan de Pruebas

Una vez que se tenga la documentación requerida del Plan de Contingencia, que nos servirá para la recuperación de los servicios informáticos ante un desastre o evento adverso, se deberá realizar pruebas que evidencien el correcto funcionamiento de este plan, y a su vez, permitirá:

- Verificar la eficacia y eficiencia de los procedimientos ante un evento adverso o desfavorable.
- Contar con un Plan de Contingencia acorde a los requerimientos actuales.
- Evidenciar la capacidad de los responsables en la ejecución del plan de contingencia.
- Identificar procedimientos o actividades que necesitan ser optimizadas.
- Medir el desempeño de los sistemas informáticos y computacionales.
- Validar la capacidad de recuperación de información y restauración de servicios.
- Las pruebas deberán ser realizadas en un escenario real, sin que afecte el correcto funcionamiento de los sistemas informáticos o que tenga un impacto mínimo.

7.7. Fase 7: Monitoreo.

La Fase de Monitoreo brinda la tranquilidad de poder responder en el momento adecuado y con las medidas apropiadas. Esta fase se centra principalmente en el mantenimiento. Cada vez que se produce una modificación en la infraestructura, es esencial llevar a cabo los ajustes correspondientes. A continuación, se detallan las principales actividades a realizar:

- Actualizar la documentación técnica de operación de los servicios de TI.
- Evaluación constante de las aplicaciones, sistemas de información y sitios web.
- Examinar regularmente el sistema de respaldo de datos.
- Revisión periódica de los UPS y sistemas de soporte eléctrico del Centro de Datos

8. Responsables del Plan de Contingencia Informático

El jefe de la Unidad de Estadística, Informática y Comunicaciones es responsable de la aprobación del presente documento.

La responsabilidad de la aplicación del plan de contingencia recae en el encargado del Área de Informática.

9. Presupuesto

El presente Plan de Contingencia Informático no requiere de presupuesto y/o financiamiento para su desarrollo, debido a que son acciones que forman parte

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:41:57 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:04:56 -05:00

de la Unidad de Estadística Informática y Comunicación del Hospital San José del Callao

10. Anexos.

Anexo 1: Formatos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones por evento de riesgo.

Anexo 2: Formato de control y certificación de las pruebas.

Anexo 3: Formato de registro del Plan de Contingencias TI.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:42:12 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:05:23 -05:00

ANEXO Nº 1

FORMATO DE PROCEDIMIENTOS DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS INFORMÁTICOS

	Riesgo: Daño en base de datos	**Código: PCI-01**

1. PROCEDIMIENTO DE PREVENCIÓN

A. Situación actual

- El Centro de Datos aloja al servidor donde se encuentra instalado la aplicación SIAF, con su respectiva base de datos relacional visual fox pro.
- Debido a la arquitectura cliente / servidor, y su base de datos basada en archivos dbf, y a la cantidad de conexiones a través de una carpeta compartida, corre el riesgo que los archivos se dañen.
- Las fallas eléctricas o de conectividad (cableado o radioenlace) producen que varios archivos queden abiertos produciendo errores al momento de grabar o trasmitir ocasionando problemas en la data.

B. Objetivo

Garantizar la continuidad del aplicativo SIAF.

C. Personal encargado

El Equipo de Prevención es el encargado del correcto funcionamiento de los aplicativos informáticos.

D. Condiciones de Prevención de Riesgo

- Realizar como mínimo backups diarios de la carpeta DATA del SIAF y semanalmente de toda la carpeta del SIAF, para posteriormente extraerlos a un disco externo.
- Revisión periódica de los backups, para prevenir mal funcionamiento de los mismos.
- Tener un equipo dedicado para la transmisión de datos.

E. Acciones del Equipo de Prevención

- Realización de copias de respaldo de la información almacenada (archivo y base de datos) en distintos servidores, para luego ser copiadas a un medio externo y resguardadas en un lugar diferente al centro de datos.
- Las copias de base de datos son diarias, se comprimen, y luego de son extraídas a los 4 días posteriores a un medio externo.
- Se realiza pruebas de restauración de copias de respaldo para evaluar el tiempo y la integridad de los backups.
- A final del año se desarrolla la programación de Requerimientos del Área de Informática que incluye acciones de renovación tecnológica para el siguiente año.
- Mantener actualizado el inventario de hardware y software.

2. PROCEDIMIENTO DE EJECUCIÓN

A. Eventos que activan la contingencia

- Problemas para ingresar a la aplicación SIAF.
- Indisponibilidad para acceder a algún modulo del SIAF.

B. Personal que autoriza la contingencia informática

El/La Coordinador/a de continuidad.

C. Personal encargado

Equipo de Emergencia

D. Acciones que se deben realizar a corto plazo

- Tener disponible el personal capacitado para la restauración de la DATA.
- Contar con accesibilidad a los backups para la restauración de la información.
- Revisar y diagnosticar el estado del servidor que aloja al SIAF.
- Tener registro de los daños ocasionados y sus posibles causas para que se puedan establecer mecanismos de prevención.

E. Duración

En el caso que se confirme un fallo de software, el tiempo máximo para esta contingencia no deberá sobrepasar las 8 horas.

3. PROCEDIMIENTO DE RECUPERACIÓN

A. Personal encargado

El personal encargado es el Equipo de Restauración.

B. Actividades a realizar

- Comunicar a los usuarios cerrar sus conexiones al SIAF.
- Realizar un mantenimiento en las tablas del SIAF.
- Si fuese necesario coordinar con el sectorista del SIAF para cargar una copia de la data o para su revisión que el SIAF este operativo.
- Validar con los usuarios que la información se haya restaurado correctamente.
- Realizar pruebas de conexión al SIAF
- Comunicar a los usuarios la reanudación del SIAF

C. Mecanismos de comprobación

El equipo responsable de la restauración, deberá presentar un informe al coordinador de Continuidad, explicando detalladamente las actividades realizadas.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:42:26 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:05:37 -05:00

	Riesgo: Insuficiente espacio en discos en servidores	**Código: PCI-02**

1. PROCEDIMIENTO DE PREVENCIÓN

A. Situación actual

- Los servidores cuentan con espacio suficiente para el correcto funcionamiento del sistema operativo.
- Cada servidor aloja copias de respaldo de diferentes sistemas alojado en diferentes servidores.
- Debido que los servidores alojan copias de respaldo, están propensos a saturar su almacenamiento destinado a la ejecución de sus aplicaciones ocasionando un bajo rendimiento.

B. Objetivo

Garantizar la continuidad en los servicios informáticos y el buen funcionamiento de los servidores.

C. Personal encargado

El Equipo de Prevención es el encargado del correcto funcionamiento de los servidores y aplicaciones informáticas.

D. Condiciones de Prevención de Riesgo

- Revisión periódica del espacio de almacenamiento de los servidores.
- Realizar el desplazamiento de las copias de respaldo a un medio externo de tal forma que se libera el espacio en los discos de los servidores.
- Proponer un sistema de almacenamiento.

E. Acciones del Equipo de Prevención

- Realizar el mantenimiento preventivo y correctivo de los servidores.
- Mantener actualizado la documentación de configuración de los equipos de comunicaciones y servidores.
- Solicitar la adquisición de equipos y repuestos con la finalidad de mejorar o mantener la continuidad de los procesos informáticos.

2. PROCEDIMIENTO DE EJECUCIÓN

A. Eventos que activan la contingencia

- Falla o indisponibilidad de los servidores o sistemas de información.
- Problemas con la conexión.
- Problemas para acceder a recursos compartidos del servidor.

B. Personal que autoriza la contingencia informática

El/La Coordinador/a de continuidad.

C. Personal encargado

Equipo de Emergencia

D. Acciones que se deben realizar a corto plazo

- Verificar espacio en discos de los servidores.
- Liberar el espacio suficiente para que las aplicaciones funcionen correctamente.

E. Duración

El tiempo máximo para esta contingencia no deberá sobrepasar las 2 horas.

3. PROCEDIMIENTO DE RECUPERACIÓN

A. Personal encargado

El personal encargado es el Equipo de Restauración, que deberá restaurar el correcto funcionamiento de los sistemas de información afectados, realizarán las coordinaciones correspondientes con el usuario responsable e informarán las soluciones o medidas que se tomaron para el caso.

B. Actividades a realizar

- Revisar y diagnosticar los procesos de respaldos, copias y desplazamientos de los archivos que hubieran acarreado el espacio insuficiente.
- Realizar pruebas de conexión a los sistemas de información de la Institución.
- Comunicar a los usuarios la reanudación de los servicios.
- Realizar el informe sobre las acciones realizadas.

C. Mecanismos de comprobación

Se tendrá un registro de la avería de manera detallada, precisando todas las acciones que se realizaron, informando los servidores y sistemas de información que presentaron fallos y cuáles fueron las soluciones que se brindaron.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:42:41 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:05:48 -05:00

	Riesgo: Falla de servidor	Código: PCI-03

1. PROCEDIMIENTO DE PREVENCIÓN

A. Situación actual

- Los servidores se encuentran conectado a una red eléctrica estabilizada y conectado a UPS.
- Los servidores tienen un mantenimiento preventivo anual

B. Objetivo

Garantizar el funcionamiento de los servidores.

C. Personal encargado

El Equipo de Prevención es el encargado del correcto funcionamiento de los servidores y recursos informáticos.

D. Condiciones de Prevención de Riesgo

- Realizar copias de respaldo del sistema.
- Realizar pedidos de repuestos con mayor antigüedad y mayor probabilidad de fallo (discos, fuente, ventiladores).
- Monitorear el funcionamiento de los servidores.

E. Acciones del Equipo de Prevención

- Ejecutar, supervisar y organizar procesos de respaldo y restauración de información
- Planificar y supervisar el mantenimiento preventivo y correctivo de los servidores.
- Mantener actualizado el inventario de hardware y software.
- Evidenciar el correcto funcionamiento de los servidores del centro de datos mediante un monitoreo.
- Indicar la necesidad de adquisición de nuevos equipos evaluando el tiempo de vida de estos mismos y el impacto que puede causar su mal funcionamiento.

2. PROCEDIMIENTO DE EJECUCIÓN

A. Eventos que activan la contingencia

- Falla o indisponibilidad de los servidores o sistemas de información.
- Problemas con la conexión a carpetas compartidas
- Reinicio o apagado de servidores

B. Personal que autoriza la contingencia informática

El/La Coordinador/a de continuidad.

C. Personal encargado

Equipo de Emergencia

D. Acciones que se deben realizar a corto plazo

- Tener disponible el personal para la evaluación del equipo.
- Contar con accesibilidad a los backups para la restauración de la información.
- Revisar y diagnosticar el estado del equipo que presenta fallos.
- Tener registro de los daños ocasionados y sus posibles causas para que se puedan

E. Duración

La duración del evento dependerá de la magnitud de la avería, los componentes y los servicios informáticos afectados.

3. PROCEDIMIENTO DE RECUPERACIÓN

A. Personal encargado

El personal encargado es el Equipo de Restauración, que deberá reparar o reemplazar los componentes afectados en los servidores, como también poner en funcionamiento los sistemas de información afectados, realizarán las coordinaciones correspondientes con el usuario responsable e informarán las soluciones o medidas que se tomaron para el caso.

B. Actividades a realizar

- Reparar o reemplazar los componentes afectados.
- Si fuese el caso configurar el servidor con el nuevo componente. En caso sea necesario, se deberá utilizar los backups más recientes que se tengan para realizar la restauración de la información.
- Restaurar los sistemas informáticos, carpetas compartidas si fuese el caso y validar que la información y los sistemas se hayan restaurado correctamente.
- Realizar pruebas de conexión a los sistemas de información afectados.
- Comunicar a los usuarios la reanudación de los servicios.

C. Mecanismos de comprobación

Se tendrá un registro de la avería de manera detallada, precisando todas las acciones que se realizaron, informando los equipos o sistemas de información que presentaron fallos y cuáles fueron las soluciones que se brindaron.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:42:57 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:05:59 -05:00

	Riesgo: Falla de Switch	**Código: PCI-04**

1. PROCEDIMIENTO DE PREVENCIÓN

A. Situación actual

- Los Switch del centro de datos se encuentran conectado a una red eléctrica estabilizada y conectado a UPS.
- Cada Switch tiene una copia de seguridad de su configuración.

B. Objetivo

Garantizar la continuidad de funcionamiento de los switchs.

C. Personal encargado

El Equipo de Prevención es el encargado del correcto funcionamiento de los switch y radio enlaces.

D. Condiciones de Prevención de Riesgo

- Realizar copias actualizadas de respaldo de la configuración de cada switch.
- Realizar pedidos de equipamiento por renovación o para contingencia.
- Monitorear el funcionamiento de los switch.
- Realizar mantenimiento preventivo y correctivos de los switch y radio enlace.

E. Acciones del Equipo de Prevención

- Ejecutar, supervisar y organizar procesos de respaldo y restauración de la copia de seguridad de los switch y radioenlace.
- Planificar y supervisar el mantenimiento preventivo y correctivo de los switch y radio enlaces.
- Mantener actualizado el inventario de hardware y software.
- Evidenciar el correcto funcionamiento de los switchs y radio enlaces mediante un monitoreo.
- Indicar la necesidad de adquisición de nuevos equipos evaluando el tiempo de vida de estos mismos y el impacto que puede causar su mal funcionamiento.

2. PROCEDIMIENTO DE EJECUCIÓN

A. Eventos que activan la contingencia

- Falla o indisponibilidad de los sistemas de información.
- Fallas en la conexión de red de datos.
- Problemas con la conexión a carpetas compartidas
- Reinicio o apagado de switch.
- Corte de energía eléctrica.

B. Personal que autoriza la contingencia informática

El/La Coordinador/a de continuidad.

C. Personal encargado

Equipo de Emergencia

D. Acciones que se deben realizar a corto plazo

- Disponer del personal para la evaluación del equipo.
- Revisar y diagnosticar el estado del equipo que presenta fallas.
- Revisar las conexiones eléctricas y de red.

E. Duración

La duración del evento dependerá de la magnitud de la avería.

3. PROCEDIMIENTO DE RECUPERACIÓN

A. Personal encargado

El personal encargado es el Equipo de Restauración, que deberá reparar o reemplazar el equipo afectado, y realizarán las coordinaciones correspondientes con las oficinas afectadas por el corte del servicio.

B. Actividades a realizar

- Reparar o reemplazar el equipo de red.
- Si fuese el caso configurar la copia de seguridad del equipo de red.
- En caso sea necesario, reemplazar el equipo, se deberá configurar las conexiones de red según la documentación de cada switch.
- Revisar que las conexiones estén correctas, actualizar la documentación y generar nueva copia de seguridad.
- Comunicar a los usuarios la reanudación de los servicios.

C. Mecanismos de comprobación

El personal encargado de la seguridad presentara un informe al coordinador de la contingencia con las acciones realizadas y recomendaciones. Con este documento se determinará si se realiza un cambio en el plan de contingencia.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:43:24 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:06:11 -05:00

	Riesgo: Corte del servicio de energía eléctrica no programado	**Código: PCI-05**

1. PROCEDIMIENTO DE PREVENCIÓN

A. Situación actual

- El Centro de datos se encuentra soportado en 1 UPS, que garantizarán la continuidad del fluido eléctrico por un tiempo promedio de 15 minutos, mientras que se realiza la activación del grupo electrógeno que brindará suministro eléctrico a toda la Institución.
- Es importante entender lo relevante que son los UPS, el personal debe gestionar de manera adecuada los tiempos que brindan los UPS, a fin de que puedan evitar apagados imprevistos que puedan dañar equipos o información.
- No existen procedimientos formales que se deban seguir para un correcto apagado y encendido del Centro de Datos.
- No se ejecutan ensayos de corte ni interrupción del suministro eléctrico.

B. Objetivo

Restaurar los servicios informáticos que se consideren importantes dentro de la Institución.

C. Personal encargado

- El/la Coordinador/a de Continuidad, será el responsable de atender y supervisar las respuestas ante el incidente.

D. Condiciones de Prevención de Riesgo

- Para garantizar el suministro eléctrico en los equipos considerados como críticos se dispone de un grupo electrógeno y equipos UPS, que nos ayudarán a mantener continuidad en los servicios informáticos.
- El equipo UPS podrá soportar la continuidad de las operaciones por un mínimo de 15 minutos, este tiempo podría variar según los dispositivos que tenga que alimentar de energía eléctrica.
- El grupo electrógeno podrá proporcionar energía eléctrica para la continuidad de las operaciones por un tiempo mínimo de 8 horas, este tiempo podría variar según los dispositivos que tenga que alimentar de energía eléctrica.
- La autonomía del equipo UPS no deberá ser menor a 15 minutos.

E. Acciones del Equipo de Prevención

- Revisar, en forma conjunta con el personal pertinente, de manera periódica las instalaciones eléctricas del Centro de Datos y organizar, coordinar y supervisar el mantenimiento preventivo y correctivo a los equipos componentes del Centro de Datos.
- Organizar, revisar y supervisar el mantenimiento preventivo de aire acondicionado del Centro de Datos, UPS, grupo electrógeno, transformadores.
- Contar con un UPS de respaldo ante cualquier falla imprevista.

2. PROCEDIMIENTO DE EJECUCIÓN

A. Eventos que activan la contingencia

- Interrupción en el suministro de energía eléctrica.
- Indisponibilidad de los servicios informáticos
- Fallas en la conexión o identificación de fallas en estaciones de trabajo y/o Centro de Datos.

B. Personal que autoriza la contingencia informática

El/La Coordinador/a de continuidad.

C. Personal encargado

Equipo de Emergencia

D. Acciones que se deben realizar a corto plazo

- Comunicar a las diferentes áreas de la Institución algún corte del suministro eléctrico programado, previamente informado y advertido por el proveedor de energía.
- Si el corte del suministro de energía eléctrica fuera de manera imprevista, se deberá comunicar a la Unidad de Servicios Generales para que realice las coordinaciones con el proveedor de energía para averiguar el motivo y la hora de restauración del suministro eléctrico, así como resolver la incidencia.

E. Duración

En el caso que se confirme un fallo en la central eléctrica, el tiempo máximo para esta contingencia no deberá sobrepasar las 6 horas.

3. PROCEDIMIENTO DE RECUPERACIÓN

A. Personal encargado

El personal encargado es el Equipo de Restauración,

B. Actividades a realizar

- Una vez restablecido el suministro eléctrico se deberá verificar por los primeros 15 a 30 minutos si existen interrupciones o fluctuaciones de energía.
- La contingencia finaliza cuando los servicios informáticos se encuentren operativos y se haya verificado que no existen fluctuaciones o interrupciones en el suministro eléctrico.

C. Mecanismos de comprobación

El equipo de Restauración deberá presentar un informe al Coordinador de la contingencia, en el cual deberá informar si hubo servicios o equipos informáticos que fallaron durante la contingencia, y las medidas correctivas que se deberán realizar.

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:43:57 -05:00

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:06:24 -05:00

ANEXO Nº 2

FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA				
PRUEBA N°				
Escenario de Prueba:	(Descripción del escenario a probar/certificar)			
Área Responsable:	(Área responsable del escenario de prueba a probar/certificar)			
INFORMACION DEL PROCESO				
Metodología:	(Detallar lo que se va a hacer en la prueba)			
Alcance:	(Definir hasta donde va a abarcar)			
Condiciones de Ejecución:	Equipo:		Aplicación/Software:	
	Ubicación:		Fecha de Backup:	
RESULTADO DE LA PRUEBA				
Resultado:	Satisfactorio:			
	Satisfactorio con Observaciones:			
	Deficiente:			
Observaciones:	(En el caso de haber observaciones o que la prueba haya sido deficiente, se indicarán los motivos, y resultados)			
ACTUALIZACION EN EL PLAN DE CONTINGENCIA				
Cambios o actualizaciones en el Plan de Contingencia:	**(Se indicarán los cambios que se deben realizar al Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)**			

ACTUALIZACION PARTICIPANTES

Participante	Cargo	Firma

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:06:35 -05:00

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:44:11 -05:00

ANEXO 3

FORMATO DE REGISTRO DEL PLAN DE CONTINGENCIAS TI

REGISTRO DE ACTIVACION DEL PLAN DE CONTINGENCIAS TI					
N°:		FECHA:	____/_____/_____	HORA:	____:____
DATOS DEL COLABORADOR QUE INFORMA:					
Unidad:	(Unidad)		(Área)		
Nombre completo:	(Nombre completo)				
DESCRIPCION DE LA CONTINGENCIA					
Descripción:					
Firma de quien autoriza la Activación:		Hora Finalización:			
Firma de quien Autoriza el cierre		**OBSERVACIONES**			

Firmado digitalmente por CARRILLO MONTALVO Elvis Joel FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 04.07.2024 12:06:45 -05:00

Firmado digitalmente por HUAMANI INFANTES Jorge Antonio FAU 20380486351 soft
Motivo: Doy V° B°
Fecha: 05.07.2024 14:44:31 -05:00