Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información

PLAN DE CONTINGENCIA INFORMATICO

ENERO 2020

PLAN DE CONTINGENCIA INFORMATICO

La protección de la información vital de una entidad ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático.

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un Plan de Contingencia adecuado, de tal forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal.

INTRODUCCION

Para realizar el Plan de contingencia informático del Hospital San José de la Palma Cundinamarca se tiene en cuenta la información como uno de los activos más importantes de la Organización, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Entidad.

Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Es importante resaltar que para que este Ente de Control logre sus objetivos es indispensable el manejo de información, por tanto necesita garantizar tiempos de indisponibilidad mínimos para no originar distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación, ya que de continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones por falta de información para el control y toma de decisiones de la entidad. De acuerdo a lo anterior es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

OBJETIVOS

Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.

Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

IDENTIFICACION DE PROCESOS Y SERVICIOS

Principales Procesos de Software Identificados

Software

- Presupuesto.
- Contabilidad.
- Tesorería.
- Suministros
- Facturación
- Manejo de Historia Clínica
- Citas
- Nomina
- Contabilidad
- Cartera

Principales servicios que deberán ser restablecidos Y/O recuperados Windows

– Correo Electrónico.
– Internet.
– Antivirus.
– Herramientas de Microsoft Office.

Software Base

– Base de Datos CITISALUD
– Backup de la Información.
– Ejecutables de las aplicaciones.

Respaldo de la Información.

– Backup de la Base de Datos CITISALUD.
– Backup Documentos Usuario.

ANALISIS DE EVALUACION DE RIESGOS Y ESTRATEGIAS

Metodología aplicada
Para la clasificación de los activos de las Tecnologías de Información del Hospital San José de la Palma Cundinamarca se han considerado tres criterios:

Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).

Frecuencia del Evento: Puede ser (Nunca, aleatoria, Periódico y continuo).

Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de Contingencia: Son procedimientos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

Leves (Caídas de energía de corta duración, fallas en disco duro, etc.)

Severas (Destrucción de equipos, incendios, etc.)

Riesgo: Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño. Existen distintos tipos de riesgo:

Riesgos Naturales: tales como mal tiempo, terremotos, etc.

Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.

Riesgos Sociales: como actos terroristas y desordenes.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la entidad iniciaremos describiendo los activos que se pueden encontrar dentro de las tecnologías de información de la entidad:

ACTIVOS SUSCEPTIBLES DE DAÑO

- Personal
- Hardware
- Software y utilitarios

 Datos e información
 Documentación
 Suministro de energía eléctrica
 Suministro de telecomunicaciones

POSIBLES DAÑOS

 Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

 Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

 Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

FUENTES DE DAÑO

 Acceso no autorizado.

 Ruptura de las claves de acceso a los sistemas computacionales.

 Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario.

 Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).

 Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red Switch, cableado de la Red, Router, FireWall).

CLASES DE RIESGOS

 Incendio o Fuego

 Robo común de equipos y archivos.

 Falla en los equipos

 Equivocaciones

 Acción virus informático

 Fenómenos naturales

 Accesos no autorizados

 Ausencia del personal de sistemas.

MINIMIZACION DEL RIESGO

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo. Es de tener en cuenta que en lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en las instalaciones del Hospital desechos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

INCENDIO O FUEGO
Grado de Negatividad: Muy Severo
Frecuencia de Evento: Aleatorio

Grado de Impacto: Alto **SITUACIÓN ACTUAL**	**ACCIÓN CORRECTIVA**
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma cada piso cuenta con un extintor debidamente cargado.	No se Cumple
No se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios nuevos, lo que no es eficaz para enfrentar un incendio y sus efectos	Realizar capacitación para el manejo de extintores y primeros auxilios.
El servidor realiza backups de la información diariamente, pero no existe ninguna otra copia de respaldo.	Realizar backups del servidor de forma mensual, almacenada en DVD y ubicarlos estratégicamente cerca a la salida principal de la Entidad.