Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

MODELO INTEGRADO DE PLANEACION Y GESTION MIPG

DIMENSIÓN
5. DIMENCION INFORMACIÓN Y COMUNICACIÓN
5.3 PLAN DE CONTIGENCIA INFORMATICO

Aprobado por:
Dr. Amaury López Garcés
Gerente

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

PLAN DE CONTINGENCIA INFORMATICO

ESE HOSPITAL SAN JOSÉ DE SAN BERNARDO DEL VIENTO

"NUESTRO COMPROMISO ES SU BIENESTAR"

VIGENCIA

2019

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

OBJETIVO

Proporcionar a la ESE Hospital San José de San Bernardo del Viento, un Plan de Contingencia Informático, que contenga los procedimientos e instructivos necesarios para poder continuar con las operaciones, procesos y servicios informáticos críticos, en caso de que se llegara a presentar algún siniestro o contingencia. Así como minimizar el impacto que dichos daños pudieran causar.

PRESENTACIÓN

Ante la necesidad imperante del día a día con relación al uso de tecnologías de la información y la comunicación, y atendiendo las directrices indicadas en el MECI, se hace necesaria la ad opción de un Plan de Contingencia Informático, que proporcione instrucciones necesarias a seguir. Es por esto que se ha adoptado el presente Plan de contingencia Informático, que se adapta a todas las posibles ocurrencias en el área de sistemas, en nuestra región. Cabe resaltar que se han rescatado aquellas condiciones comunes con nuestra región y se ha adaptado a los posibles sucesos que pueden ocurrir en la ESE. Con base en esta guía cada una de las áreas que componen la ESE, deberán perseguir los siguientes fines:

1. Establecer mecanismo y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.
2. Estimular la creación de una cultura de seguridad en Informática, así como fomentar la ética entre sus miembros.
3. Definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese: confidencial, restringida, de uso

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

interno, general o público, estableciendo los procedimientos para identificación y uso de cada categoría de información.

4. Promover el establecimiento de procedimientos alternos en previsión a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar las contingencias que se presenten.

PLAN DE ACCION

1. Realizar un levantamiento de los servicios informáticos.
2. Llevar a cabo un Inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, Internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.
3. Identificar un conjunto de amenazas.
4. Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc.
5. Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.
6. Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Definición de Roles Presidente del Grupo de Trabajo. Es el responsable de aprobar la realización del Plan de Contingencia Informático, dirigir los comunicados de concientización y solicitud de apoyo a los jefes y/o gerentes de las diferentes áreas involucradas y aprobar su terminación.

Una vez concluida la realización del Plan de Contingencia, el presidente tendrá como función principal, verificar que se realicen reuniones periódicas, cuando menos cada seis meses, en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correcto funcionamiento del Plan de Contingencia Informático, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten. Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alterno y autorizará las inversiones a realizar, así como el fondo de efectivo a asignarse para los gastos necesarios iniciales. El presidente se mantendrá permanentemente informado respecto de la activación del Plan hasta la declaración de conclusión.

Coordinador General Tendrá como función principal asegurar que se lleven a cabo todas las fases para la realización del Plan de Contingencia, registrará las reuniones que se realicen, a manera de minutas, aprobará los procesos críticos y tipo de evento que abarcará el Plan de Contingencia y aprobará junto con el presidente del Comité la terminación de cada una de las fases y la conclusión del proyecto.

1. Establecer un Grupo de Trabajo y definir roles

Durante la realización del plan, una de sus actividades principales será la coordinación de la realización de las pruebas del Plan de Contingencia, la aprobación de las ubicaciones alternas que sea necesario definir, la aceptación de

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la realización del plan. Al término de la realización de las pruebas, será el Gerente quién de su Vo. Bo. De la conclusión de éstas y de sus resultados, rindiendo un informe a todos los coordinadores involucrados y en general al personal involucrado, y en caso necesario, convocar a la realización de una segunda prueba, corrigiendo previamente las fallas que se hubieran presentado. Una vez que se encuentre aprobado el Plan de Contingencia, será el Gerente quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal de la aplicación del Plan de Contingencia, cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades; será el responsable de dar por concluida la declaración de contingencia. Coordinador de Redes y Comunicaciones. Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, Servicios de Internet, Intranet, correo electrónico, mantener actualizados dichos procedimientos en el Plan de Contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switchs, antenas etc). Asimismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar a cabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de que se llegara a presentar alguna contingencia, ya sea parcial, grave o crítica.

El Coordinador de Comunicaciones es el responsable de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan de Contingencia

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Informático. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total. Coordinador de Soporte Técnico. Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, CD Writer, escáners, faxes, copiadoras, etc.; mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones; es responsable de elaborar o coordinar con los usuarios los respaldos de información. Deberá realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos en donde se procese lo enunciado en el párrafo anterior, efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia Informático.

En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores.

Para tal efecto debe participar en pruebas del Plan de Contingencia en conjunto con los demás participantes, con el objeto de estar permanentemente preparado para actuar en caso de contingencia. Ingeniero de Sistemas. Será el responsable de determinar los sistemas Críticos de la ESE Hospital San José de San Bernardo del Viento, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas críticos. En caso de cambiar a otras instalaciones alternas, el Coordinador de Programación deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los Manuales Técnicos y de Usuario, resguardándolos fuera de las instalaciones para su consulta y utilización al momento de requerirse. Personal involucrado (usuarios).

El personal usuario en general, al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo, cuando la situación que se estuviera presentado sea grave (incendio, temblor, etc.); posteriormente, y en la medida en que la situación lo permita, deberá coadyuvar a salvaguardar los bienes de la ESE (el propio inmueble, equipos, documentación importante, etc.).

Con posterioridad a la crisis inicial, deberá apoyar a solicitud del Coordinador de su área y/o del personal clave del Plan de Contingencia, en la toma del inventario de daños, para lo cual deberá seguir las instrucciones generales que indique el propio Plan. En forma alterna, deberá dar cumplimiento a las instrucciones que se incluyan en el Plan de Contingencia Informático para darle continuidad a las funciones informáticas críticas, siguiendo los procedimientos establecido, con la salvedad de que deberá, en forma creativa y responsable, adaptarlos a las circunstancias de limitación que represente el cambio de ubicación de las diferentes áreas

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

involucradas en los procesos y la utilización de recursos de cómputo, mensajería, comunicaciones, etc., limitados.

Al declararse concluida la contingencia, deberá participar activamente en la restauración de las actividades normales de la Administración, esto es, apoyar en la movilización de documentación, mobiliario, etc., a las instalaciones originales o al lugar que le sea indicado, hasta la estabilización de las actividades.

Cuando sea necesario, deberá participar en la capacitación del nuevo personal o del personal eventual que hubiera sido necesario contratar.

Grupo de Trabajo y definir roles Se propuso la integración del Grupo de Trabajo involucrando a las siguientes personas:

ROLES	PUESTO	OCUPANTE ACTUAL

Determinar los eventos que pueden afectar adversamente a la Administración y su infraestructura, con interrupciones ó desastres en materia informática

Los desastres y crisis son eventos que pueden inhabilitar a la Administración de proveer normalmente sus servicios a los usuarios internos y la atención al público

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

en General, por lo que deben identificarse, analizar su nivel de riesgo y tomarse las medidas necesarias de prevención. Identificación de Amenazas:

- Terremoto
- Incendio
- Inundación y humedad
- Corte de Energía
- Falla de la red de voz y datos
- Fallas en Hardware o Software
- Sabotaje o daño accidental
- Vandalismo y manifestaciones

Tomando en cuenta los resultados del Análisis de Riesgos realizado para el Sistema de Administración, se definieron los siguientes eventos para ser considerados dentro de este Plan de Contingencia Informático:

TERREMOTO SIN PÉRDIDA O DAÑOS MENORES DEL EDIFICIO: El siniestro puede afectar únicamente parte de la estructura del edificio, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera del edificio; el impacto que provocaría en la Administración sería menor, puesto que las actividades se interrumpirían por unas horas o a hasta por un día completo.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

CON PÉRDIDA DEL EDIFICIO: La pérdida de las instalaciones afectaría gravemente a las operaciones de la Administración y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

INCENDIO ÁREA DE SISTEMAS: Se tiene gran impacto en la información ya que los sistemas utilizados residen en los Servidores y dispositivos de comunicación localizados en el área de sistemas y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de instalar nuevamente el sistema, configurar el Servidor y restaurar los respaldos para continuar trabajando.

ÁREAS DISTINTAS A LA OFICINA DE SISTEMAS: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación localizados en el Centro de Cómputo. En el caso de las primeras el impacto que tendría en la Administración es menor, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto. Ejemplos de riesgos asociados con el evento de un incendio:

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto
5	Incendio / negación de servicio (3)	Oficina de sistemas	No hay extintores dentro del centro de cómputo. (5)	Media (2)	Alto (3)

CORTE DE ENERGÍA Las operaciones informáticas de la Administración se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las

Gerencia@esehospitalsanjose.com
Kilometro 1, Vía Lorica, San Bernardo del Viento, Cordoba, Colombia.

operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos. Actualmente la Administración cuenta con una planta de energía con capacidad para restablecer la energía inmediatamente después de la perdida de luz. No todos los equipos cuentan con NO BREAK, por lo tanto, una pérdida de datos en algunos equipos sería inminente. Ejemplos de riesgos asociados con el evento de corte de energía:

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto
16	Falla eléctrica / negación de servicio (3)	Servidores	Funcionan con energía eléctrica. (4)	Media (2)	Alto (3)
20	Personal técnico de mantenimiento / descarga electroestática (2)	PC	Funcionan con energía eléctrica. (4)	Media (2)	Bajo (1)
55	Falla eléctrica / Negación de servicio (3)	Ruteadores, switches y firewalls	Funcionan con energía eléctrica. (4)	Media (2)	Alto (3)

FALLAS DE LA RED DE VOZ Y DATOS RED: Representa la columna vertebral de las operaciones de la Administración, si la red falla en su totalidad, las operaciones se detienen con la consecuente falta del servicio informático.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

APLICACIONES: La falla en los sistemas utilizados, representa un impacto medio en las operaciones totales de la Administración, ya que pueden ser reinstalados casi de inmediato.

FALLAS EN HARDWARE O SOFTWARE Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo, si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

VANDALISMO Y MANIFESTACIONES Un intento de vandalismo ya sea menor o mayor, podría afectar a las PC's, periféricos y servidores, así como las comunicaciones. Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado a la ciudadanía.

A continuación, se menciona en forma enunciativa una serie de medidas preventivas:

- Establecer vigilancia mediante cámaras de seguridad en el cual registre todos los movimientos de entrada del personal.
- Instalar identificadores mediante tarjetas de acceso.
- Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiarán los datos e información crítica).

- Contar, ya sea bajo contrato o mediante convenio, con un centro de cómputo alterno de características físicas y equipo de cómputo adecuado para darle continuidad a las operaciones críticas de la Administración, aún en forma limitada de cobertura y de comunicaciones. El paro total de las operaciones dentro de la Administración afectaría principalmente a los servicios que son proporcionados a la ciudadanía, no se podría llevar a cabo el mantenimiento y monitoreo del equipo informático, ya que los manifestantes bloquearían las entradas e impediría el acceso para realizar cualquier operación. Los principales conflictos que pudieran presentarse son: En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas. Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la Administración, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc; en un sitio alterno, ya que no contarían con copia de la información. En caso de presentarse un paro total de las operaciones.

- Determinar lugares especiales, fuera del centro de datos, para almacenar los respaldos y copia de la documentación de referencia.

- El personal clave del Plan de Contingencia Informático, debe de dar la alerta del paro total y sacar los respaldos de información fuera del edificio dentro de un tiempo límite antes de ser declarada la huelga.

Gerencia@esehospitalsanjose.com
Kilometro 1, Vía Lorica, San Bernardo del Viento, Cordoba, Colombia.

- Personal de la Dirección de debe prever un sitio alterno para continuar con las operaciones críticas. Asimismo, se tendrá que establecer un tiempo límite de espera de solución de la huelga como por ejemplo 24 horas con el fin de que no afecte el servicio proporcionado al público en general, si después de este intervalo la huelga continuara, se determinará el lugar o lugares de reubicación alternos.

2. Evaluar la efectividad de los controles y dispositivos de seguridad

Se debe contar con un sistema de seguridad en materia informática, conformado por la Administración, considerando los medios a su alcance que permitan el normal desarrollo de las diversas actividades laborales, previniendo las posibles causas, condiciones de accidentes y siniestros, mediante normas, disposiciones y controles de seguridad. Así como también, es necesario determinar las medidas más convenientes y llevarlas a cabo realizando inspecciones periódicamente.

Una vez que se tiene el inventario de los dispositivos de seguridad implantados, se debe evaluar su efectividad; lo anterior va muy relacionado al grado de actualización y modernidad de los elementos de seguridad identificados, por ejemplo, si se cuenta con extinguidores y éstos son demasiado antiguos, deben probarse y certificarse, con el objeto de que llegado el momento sean realmente utilizables y efectivos, de lo contrario, deberán ser sustituidos por equipos modernos.

Actualmente la Administración cuenta con algunos extinguidores de fuego instalados en las instalaciones de la Administración, dichos extinguidores no se les da el mantenimiento adecuado y se encuentran al alcance del personal en caso de suceder un conato de incendio. La oficina de sistemas carece de detectores de

Gerencia@esehospitalsanjose.com
Kilometro 1, Vía Lorica, San Bernardo del Viento, Cordoba, Colombia.

humo y alarma contra incendio, por lo que se pretende el análisis y estudio con diversos proveedores para la adquisición de los dispositivos necesarios para la detección y extinción de Incendio, Instalación, montaje, canalización del cableado, configuración y programación de dichos dispositivos.

Nota: Una vez que se haya realizado la adquisición del Sistema de detección y extinción de Incendio, se recomienda actualizar este punto, especificando las características del equipo adquirido.

3. Procedimientos de Respaldo y Recuperación.

Establecer normas de seguridad como son:

1. Definir los procedimientos que indiquen los datos, programas, etc., que es importante respaldar; por servidor, sistema y ubicación.
2. Identificar cada uno de los métodos que se utilizan, para llevar a cabo los respaldos de información, así como los procedimientos para su ejecución y restauración.
3. Especificar el lugar donde se encuentran custodiados los respaldos de información o copia de los respaldos, ya sea en un lugar fuera de las instalaciones o en una Institución Bancaria.
4. En esta parte, debe incluirse los procedimientos de respaldo y recuperación de la información de los sistemas, así como de los programas o aplicaciones y de los sistemas operativos. Es importante contar con algunos ejemplares del software de los programas comerciales que se utilicen normalmente, como es el MS Office, Windows 98, 2000, XP, etc.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Establecer los procesos informáticos criticos y las prioridades de recuperación de los sistemas, de forma tal que el tiempo de recuperación sea alcanzado La importancia para el Plan de Contingencia es el conocer los procesos informáticos críticos de la Dirección y su inter-relación, con el objeto de fijar o establecer las prioridades de recuperación al activarse dicho plan.

LISTA DE SERVICIOS CRITICOS

Determinar los tiempos de recuperación y los requerimientos mínimos de recursos Para cada una de las fases críticas que se cubrirán con el Plan de Contingencia Informático, se deben determinar los tiempos mínimos requeridos para el establecimiento del plan, esto es, cuánto tiempo debe transcurrir desde el momento en que se inicia o activa el plan, hasta que las actividades, funciones o sistemas se encuentren en operación total o parcialmente.

Es conveniente definir un tiempo aceptable y viable para que la red y la aplicación principal estén nuevamente activas.

Para situaciones críticas:

- Incluir el traslado de los medios de almacenamiento magnético que se encuentren fuera de las instalaciones.
- La copia de los datos a los nuevos medios de almacenamiento magnético y la habilitación de las comunicaciones, servicios de Internet y correo electrónico.
- El personal mínimo requerido para continuar operando.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

- Tiempo de restauración de cada uno de los servicios de Red, Comunicaciones, Internet y Correo Electrónico.
- El tiempo determinado debe ser conocido y aceptado por todos los usuarios principales que operan los sistemas o cuentan con un equipo crítico. Para situaciones de bajo riesgo:
- Tiempo de reparación o reposición de una estación de trabajo (PC)
- Tiempo de configuración de las PC
- Tiempo de respuesta del proveedor para la reparación de los servidores (verificar contratos y garantías).
- Tiempos de reparación de fallas eléctricas.
- Tiempo de restauración de cada uno de los servidores y sus aplicaciones.
- Desarrollar los procedimientos detallados de respuesta de emergencia
- Desarrollar e implantar los procedimientos de respuesta de emergencia de la situación que sigue a un incidente o evento, incluyendo establecer y gestionar un Centro de Operaciones de Emergencia.

TERREMOTO Análisis de daños:

En caso de daño mayor e imposibilidad de acceder al edificio: Este tipo de procedimiento se tomará únicamente cuando el daño en el edificio haga imposible la continuación de las actividades, por lo que es preciso el traslado de las mismas a las oficinas consideradas como alternas (Instalaciones Centro de Convivencia Ciudadana). Mientras las operaciones continúan en las instalaciones alternas, se evaluará la posibilidad de regresar a las instalaciones de la Administración, ó

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

establecer operaciones en un nuevo sitio. Los respaldos de información, serán custodiados fuera de las Instalaciones de la Administración, para lo cual se trasladó y resguardo en las oficinas de la institución.

Procedimientos y Responsables Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones. Responsable: Coordinador de Redes y Comunicaciones. Restaurar la información de las bases de datos y programas. Responsable: Coordinador de Sistemas. Revisar y probar la integridad de los datos. Responsable: Coordinador de Sistemas. Iniciar las operaciones.

En caso de daño menor Procedimientos y Responsables Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.

Responsable: Coordinador de Soporte y Mantenimiento.
Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.
Responsable: Coordinador de Redes y Comunicaciones.
Instalar el sistema operativo.
Responsable: Coordinador de Redes y Comunicaciones.
Restaurar la información de las bases de datos, y programas.
Responsable: Coordinador de Sistemas.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

INCENDIO Análisis de daños

- **En caso de daño mayor e imposibilidad de acceder al edificio**

Este tipo de procedimientos se tomará únicamente cuando la reparación del edificio llegase a tardar mucho tiempo, durante este periodo de restauración se debe dar continuidad a las operaciones por lo que es preciso el traslado de las operaciones a otras oficinas, como el centro de convivencia ciudadana.

Mientras las operaciones continúan en otras oficinas, se evaluará la posibilidad de regresar a las instalaciones de la Administración ó establecer operaciones en un nuevo sitio.

Asimismo, los responsables del grupo de Trabajo del PCI, deberán reunirse a la brevedad con Director, con el objeto de hacer un recuento rápido de los daños, determinar si es posible o no continuar utilizando las instalaciones y/o por cuanto tiempo aproximadamente se deberá operar fuera de las instalaciones o si la emergencia afectará solo a una parte del edificio. En esa reunión se determinará la ubicación o ubicaciones alternas que ocupará cada una de las áreas y la manera como se llevará a cabo la coordinación y control de las operaciones de la Administración. Los respaldos de información, serán custodiados fuera de las Instalaciones de la Delegación, para lo cual se trasladó y resguardo en las oficinas Alternas.

Procedimientos y Responsables Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Responsable: Coordinador de Redes y Comunicaciones.
Restaurar la información de las bases de datos y programas.
Responsable: Coordinador de Sistemas.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.

En caso de que durante el evento hubiera ocurrido algún accidente y se contara con personal afectado físicamente y que por tal motivo no pudiera continuar prestando sus servicios por algún tiempo, o en forma permanente, deberán tomarse las decisiones correspondientes y comunicarlas al personal involucrado.

Por lo que respecta a las operaciones de la oficina de sistemas, se continuará con la activación del Plan de Contingencia Informático, conforme al tipo de gravedad que se hubiere presentado, pudiendo inclusive, verse en la necesidad de iniciar los preparativos y ocupar las instalaciones alternas con el Proveedor correspondiente.

El responsable de la Dirección, deberá definir al personal que apoyará en la recuperación y retiro de los documentos, equipos y demás materiales importantes (cada área debe contar con una lista describiendo cada uno de ellos y la ubicación física en donde se encuentran), así como también deberá definir en conjunto con el Director, si se contratará el servicio de mudanza o será con el personal y recursos de transporte propios quienes efectuarán la movilización, dependiendo de la cantidad de materiales a retirar. Durante el retiro de los documentos, equipos, materiales, mobiliario, etc. importantes y necesarios para la continuidad de las operaciones de la Administración, se deberá ir señalando en las listas aquellos documentos que se retiran (en cajas de preferencia), la persona que quedará como responsable de su transporte y el lugar de destino. Lo anterior es importante para

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

posteriormente estar en mejores condiciones de determinar el inventario final de pérdidas y daños de documentación importante, equipos, mobiliario, etc.

- En caso de daño menor

Procedimientos y Responsables Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
Responsable: Coordinador de Soporte y Mantenimiento.
Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.
Responsable: Coordinador de Redes y Comunicaciones.
Instalar el sistema operativo.
Responsable: Coordinador de Redes y Comunicaciones.
Restaurar la información de las bases de datos, y programas.
Responsable: Coordinador de Sistemas.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.

Es indispensable señalar que el daño en los distintos equipos puede variar desde el simple daño superficial hasta el daño permanente por lo que será necesario realizar la prueba de los equipos para poder determinar el grado de daño. Se considera daño mayor a toda aquella afección que imposibilite la utilización de los equipos y que esta afección no tenga reparación ó bien por su naturaleza dicha reparación tardaría un periodo prolongado de una ó más semanas.

Gerencia@esehospitalsanjose.com
Kilometro 1, Vía Lorica, San Bernardo del Viento, Cordoba, Colombia.

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES

1. Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
2. No debes concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
3. Verificar las condiciones de extintores e hidrantes y capacítate para su manejo.
4. Si fumas, procura no arrojar las colillas a los cestos de basura, verifica que se hayan apagado bien los cigarrillos y no los dejes en cualquier sitio, utiliza ceniceros.
5. No almacenes sustancias y productos inflamables
6. No hagas demasiadas conexiones en contactos múltiples, evita la sobrecarga de circuitos eléctricos.
7. Por ningún motivo mojes las instalaciones eléctricas, recuerda que el agua es un buen conductor de la electricidad.
8. Si detectas cualquier anomalía en los equipos de seguridad (Extintores, hidrantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, repórtala de inmediato a la Coordinación de Protección Civil.
9. Mantén siempre tu área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
10. Ten a la mano los números telefónicos de emergencia.
11. Porta siempre carnet de identificación

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Antes de un Incendio debemos estar siempre alertas, recuerda que la mejor manera de combatirlo es la prevención.

DURANTE

1. Si descubres un conato de incendio, actúa tranquilamente.
2. Si conoces sobre el manejo de extintores, intenta sofocar el fuego; si éste es considerable no trates de extinguirlo con tus propios medios, solicita ayuda.
3. Si hay humo donde te encuentras y no puedes salir, mantente al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de él, intenta el traslado a pisos superiores.
4. Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que le humo tenga una vía de salida y se descongestionen las escaleras.
5. Si es posible moja tu ropa.
6. Verifica si las puertas están calientas antes de abrirlas, si lo están, busca otra salida.
7. Ten presente que, DURANTE un incendio, el pánico es tu peor enemigo.

DESPUES

1. Retirate inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.
2. No obstruyas las labores del personal especializado, deja que los profesionales se encarguen de sofocar el incendio.
3. Personal calificado realizará una verificación física del inmueble y definirá si está en condiciones de ser utilizado normalmente.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

4. Colabora con las autoridades.

La colaboración con las autoridades DESPUES de un incendio puede salvar vidas.

INUNDACIÓN Análisis de daños

En caso de daño mayor

Este tipo de procedimientos se tomará únicamente cuando el acceso a las instalaciones de la Administración esté restringido y se tenga la certeza de que el daño en los equipos es irreversible.

Mientras las operaciones continúan en las instalaciones u oficinas alternas, se evaluará la posibilidad de regresar a la Administración, ó establecer operaciones en nuevo sitio. Asimismo, el Coordinador General, deberá reunirse a la brevedad con el Presidente del Grupo de Trabajo del PCI, con el objeto de hacer un recuento rápido de los daños, determinar si es posible o no continuar utilizando las instalaciones y/o por cuanto tiempo aproximadamente se deberá operar fuera de las mismas o si la emergencia afectará solo a una parte del edificio. En esa reunión se determinará la ubicación(es) alternas que ocupará cada una de las áreas y la manera como se llevará a cabo la coordinación y control de las operaciones. Los respaldos de información, serán custodiados fuera de las Instalaciones de la Administración.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Procedimientos y Responsables

Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones.
Responsable: Coordinador de Redes y Comunicaciones.
Restaurar la información de las bases de datos y programas.
Responsable: Coordinador de Sistemas.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.

En caso de que durante el evento hubiera ocurrido algún accidente y se contara con personal afectado físicamente y que por tal motivo no pudiera continuar prestando sus servicios por algún tiempo, o en forma permanente, deberán tomarse las decisiones correspondientes y comunicarlas al personal involucrado.

Por lo que respecta a las operaciones del centro de cómputo, se continuará con la activación del Plan de Contingencia Informático, conforme al tipo de gravedad que se presente, pudiendo inclusive, verse en la necesidad de iniciar los preparativos y ocupar las instalaciones alternas.

En caso de daño menor

Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
Responsable: Coordinador de Soporte y Mantenimiento.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.
Responsable: Coordinador de Redes y Comunicaciones.
Proceder (si lo amerita) al traslado de dichos datos al centro de respaldo u oficinas alternas con el propósito de reiniciar las operaciones.
Responsable: Coordinador de Redes y Comunicaciones.
Instalar (si lo amerita) el sistema operativo.
Responsable: Coordinador de Redes y Comunicaciones.
Restaurar (si lo amerita) la información de las bases de datos, y programas.
Responsable: Coordinador de Sistemas. Revisar y probar de la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar de las operaciones.

En caso de inundación las pérdidas son nulas, ya que el Site de cómputo se encuentra en una zona alta y no está expuesto a sufrir este tipo de daño.

CORTE DE ENÉRGIA

Revisar que la planta de energía cuente con combustible, y se active en su momento.
Responsable: Coordinador de Redes y Comunicaciones.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.
En el caso de cortes de energía, la Administración cuenta con una planta de energía la cual entra en funcionamiento inmediatamente, en el caso de que no entre automáticamente la planta, siempre se cuenta con la opción de encenderla manualmente.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Si por alguna razón la planta no funcionara se evaluaría el tiempo de reparación de la misma, si el tiempo de reparación excede de 72 hrs. o el corte de Luz dura más 8 hrs., se trasladarán las operaciones a las oficinas alternas.

FALLA DE LA RED DE VOZ Y DATOS

Evaluación de las fallas.
Responsable: Coordinador de Redes y Comunicaciones.
Si las fallas se derivan del mal funcionamiento de un equipo se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
Responsable: Coordinador de Redes y Comunicaciones.
Si resulta ser un problema de configuración, se procede a su reconfiguración inmediata.
Responsable: Coordinador de Redes y Comunicaciones. Revisar y probar la integridad de las comunicaciones.
Responsable: Coordinador de Redes y Comunicaciones. Iniciar de las operaciones.

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

FALLAS EN HARDWARE O SOFTWARE

Análisis y Evaluación del daño causado por la alteración En el caso de que la alteración haga imposible el inicio inmediato de las operaciones se procede como sigue:

Recoger los respaldos de datos, programas, manuales y claves del lugar en el que se encuentren resguardados.
Responsable: Coordinador de Redes y Comunicaciones.
Si las fallas se derivan del mal funcionamiento de un equipo (Hardware) se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento. Responsable: Coordinador de Redes y Comunicaciones.
Instalar (si lo amerita) el sistema operativo.
Responsable: Coordinador de Redes y Comunicaciones.
Restaurar la información de las bases de datos y programas.
Responsable: Coordinador de Sistemas.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.

En los casos en que la alteración puede ser corregida sin problemas graves, se procede conforme a lo siguiente:

Corrección de las alteraciones que se localicen en los servidores Hardware.
Responsable: Coordinador de Redes y Comunicaciones.
Corrección de las alteraciones que se localicen en los servidores Software.
Responsable: Coordinador de Sistemas.
Revisión y prueba de la integridad de los datos.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Responsable: Coordinador de Sistemas. Iniciar las operaciones.

Las alteraciones que sufran los servidores tanto en Software y Hardware pueden ser corregidas en la mayoría de los casos, sin embargo en algunas ocasiones, las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días sin tener la absoluta certeza de que las correcciones que se hicieron fueron las necesarias, por tal motivo es mejor acudir a los respaldos de información y restaurar los datos, de esta forma las operaciones del día no se verán afectadas y al mismo tiempo se ponen al día los datos faltantes de la operación del día anterior.

SABOTAJE Ó DAÑO ACCIDENTAL

Análisis y Evaluación de los daños ó pérdidas:

En el caso de que la eliminación haga imposible el inicio inmediato de las operaciones se procede con lo siguiente:

Recoger los respaldos de datos, programas, manuales y claves del lugar en el que encuentren resguardados.
Responsable: Coordinador de Redes y Comunicaciones.
Restaurar la información de las Base de datos y programas.
Responsable: Coordinador de Sistemas.
Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

En los casos en que la información eliminada se pueda volver a capturar sin mayor problema se procede conforme a lo siguiente:

Capturar los datos faltantes en las bases de datos de los sistemas.
Responsable: Áreas afectadas Revisar y probar la integridad de los datos.
Responsable: Coordinador de Sistemas. Iniciar las operaciones.
La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse demasiado hasta por días, sin tener la absoluta certeza de que las capturas que se hicieron fueron las correctas, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectadas.

VANDALISMO Y MANIFESTACIONES

Análisis y Evaluación del daño causado por la alteración

En el caso de que la alteración ocasione un daño mayor y haga imposible el inicio inmediato de las operaciones se procede como sigue:

Este tipo de procedimientos se tomará únicamente cuando el acceso a las instalaciones de la Administración esté restringido y se tenga la certeza de que el daño en los equipos es irreversible. Mientras las operaciones continúan en las instalaciones u oficinas alternas, se evaluará la posibilidad de regresar a la Administración, ó establecer operaciones en nuevo sitio. Asimismo, se hará una reunión, con el objeto de hacer un recuento rápido de los daños, determinar si es

Gerencia@esehospitalsanjose.com
Kilometro 1, Via Lorica, San Bernardo del Viento, Cordoba, Colombia.

Responsable: Coordinador de Soporte y Mantenimiento.

Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.

Responsable: Coordinador de Redes y Comunicaciones.

Proceder (si lo amerita) al traslado de dichos datos al centro de respaldo u oficinas alternas con el propósito de reiniciar las operaciones.

Responsable: Coordinador de Redes y Comunicaciones.

Instalar (si lo amerita) el sistema operativo.

Responsable: Coordinador de Redes y Comunicaciones.

Restaurar (si lo amerita) la información de las bases de datos, y programas. Responsable: Coordinador de Sistemas. Revisar y probar de la integridad de los datos. Responsable: Coordinador de Sistemas. Iniciar de las operaciones.