PLAN DE CONTINGENCIA

SISTEMA AUTOMATIZADO PARA EL CONTROL DE CITAS, NÓMINA E INVENTARIO EN EL CONSULTORIO ODONTOLÓGICO “SONRISA FELIZ”

(V. 01)

Maracaibo – Estado Zulia

Elaborado por:	Aprobado por:	Revisado por:	Fecha:
González, Eduardo Martínez M., María E. Morales, Valentina Valdez, Gressia	Acosta, Genyelbert	Martínez M., María E	Julio 2018

ÍNDICE GENERAL

1. Introducción

El plan de contingencia es importante para cualquier entidad, ya que ante la posible pérdida, destrucción, robo u otras amenazas, se debe abarcar la preparación e implementación de un completo plan de contingencia Informático para solucionar los desastres que se presenten.

Cualquier Sistema de redes de computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgos que puede ser fuente de problemas, asi como también, el hardware y el software están expuestos a diversos factores de riesgo tanto humano como físicos. Estos problemas sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (disco duro), grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable.

El objetivo de la realización de este plan de contingencia es el de proteger la información y así asegurar su procesamiento y desarrollo. En base a eso es importante contar con un plan de contingencia adecuado de forma que ayude al Centro Odontológico Sonrisa Feliz a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del centro odontológico.

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

2. Objetivos del Plan de Contingencia

2.1. Objetivo General

Formular un adecuado plan de contingencias, que permita la continuidad de los procedimientos informáticos del Centro Odontológico Sonrisa Feliz, así como enfrentar las posibles fallas y eventos inesperados, con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna, buscando asi la mejora de la calidad en los servicios que brinda el centro odontológico.

2.2. Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos en el Centro Odontológico Sonrisa Feliz que puedan suspender completa o parcialmente la prestación del servicio.
- Establecer los niveles de complejidad de las fallas del sistema.
- Minimizar la posible pérdida financiera y operativa que se genere por la presencia de una falla técnica o humana en la plataforma tecnológica.

- Restablecer el funcionamiento de los sistemas de información en el menor tiempo posible dependiendo de la anomalía que se presente.

3. Alcance y Responsabilidades

El Plan de Contingencias Informático está basado en la realidad que manifiesta el Centro Odontológico Sonrisa Feliz, y puede servir como punto de partida hacia la adecuación y establecimiento de políticas en los diferentes procesos.

Roles y responsabilidades

- Coordinador del plan de contingencias de TI

El Coordinador del Plan es el canal de comunicación entre el Grupo de Desarrollo del Plan y Grupo encargado del Proyecto a través del cual se transmitirán las decisiones tomadas en torno a las acciones del Plan de Contingencias TI, los niveles de ejecución del Plan y el estado de los recursos informáticos que cubre el Plan. Es el que autoriza la puesta en marcha del Plan de Contingencias TI cuando lo considere necesario de acuerdo con el reporte dado por el grupo de desarrollo del Plan.

<u>Responsabilidades</u>

- Proponer políticas y acciones al Plan de Contingencias TI

- Mantener actualizado el Plan de Contingencias de TI.

- Autorizar la ejecución del Plan de Contingencias de TI.

- Elaborar los informes referidos al Plan.

- Proponer reuniones para revisión del Plan de Contingencias de TI.

- Encargado de monitorear y asegurar el estricto cumplimiento del Plan y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo.

- Grupo de desarrollo del Plan

Está conformado por funcionarios responsables de la ejecución de las tareas definidas dentro del plan. El grupo estará conformado por:

- Funcionarios administradores de los sistemas de información críticos.

- El grupo de centro de cómputo.

- Grupo de soporte técnico.

Funciones

- Ejecutar en tiempo y forma, cada una de las actividades planeadas.
- Documentar y formalizar el Plan de contingencias de TI.
- Ordenar la documentación inherente y los papeles de trabajo de la contingencia.
- Realizar las pruebas necesarias al Plan de Contingencias de TI, antes y después de una contingencia.

- Grupo de seguimiento y control

Quienes se encargarán de hacer seguimiento y control a las labores que se ejecuten, velando por el respeto del plan y la seguridad en su efectiva aplicación,

así como la coherencia y consistencia en la aplicación de los procedimientos establecidos, la de verificar que el plan se encuentre dentro del alcance y presentar los informes del plan a el Consultorio Odontológico Sonrisa Feliz.

4. Análisis de Evaluación y riesgo

4.1. Activos susceptibles a daños:

- El mobiliario
- El equipo computo en general (Procesadores, unidades de disco, impresoras)
- En las comunicaciones (líneas telefónicas, servidores, router, switches)

4.2. 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 voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución sea mediante robo o infidelidad del personal.

4.3. Fuentes de daños

- Acceso no autorizado.
- Ruptura de las claves de acceso a los sistemas computacionales.

- Desastres naturales (terremotos, inundaciones, falla en los equipos de soportes causados por el ambiente, la red de energía eléctrica o el mal acondicionamiento de los equipos.
- Fallas del personal clave (enfermedad, accidente, renuncias, abandono del puesto de trabajo.)
- Fallas de hardware (fallas en los servidores o falla en el cableado de red, Router, etc.)
- Factores ambientales, como inundaciones, terremotos, tormentas, etc.

4.4. Clases de Riesgos

4.4.1. Externos

- Caída o interrupción del sistema eléctrico

Riesgo externo. Corresponde al corte del servicio de energía eléctrica en el Consultorio Odontológico Sonrisa Feliz por parte de falla externa en el proveedor del servicio, corte eléctrico que genera interrupción del funcionamiento de los equipos donde se alojan los aplicativos críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

- Caída del canal de internet

Riesgo externo. Consiste en las fallas técnicas por parte del proveedor del servicio de internet en el Consultorio Odontológico Sonrisa Feliz, lo que ocasionaría suspensión de los servicios de correo y de los aplicativos críticos de la entidad. Tipo de riesgo: Tecnológico.

- Caída del Servicio Telefónico

Riesgo externo correspondiente a la suspensión del servicio por daños o fallas en el software o hardware de telefonía IP de telefonía en el Consultorio Odontológico Sonrisa Feliz, que de presentarse genera la ausencia de comunicación telefónica en la entidad. Tipo de riesgo: Tecnológico.

- Caída de servicios por virus informático

Riesgo externo. Es el riesgo de infección de los equipos servidores y de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia o inestabilidad de los sistemas. Tipo de riesgo: Tecnológico.

- Suspensión del servicio por sismo, inundación o incendio

Riesgo externo. Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo, inundación o incendio que afecte la infraestructura tecnológica de los sistemas de información críticos del Consultorio Odontológico Sonrisa Feliz generando suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia de los sistemas o inestabilidad de los mismos. Tipo de riesgo: Operativo.

- Otros:

Infiltración, sabotaje, ataque distribuido de denegación de servicio, robo de hardware, accidentes, atentado.

4.4.2. Internos

- Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles

Riesgo interno que se relaciona con deficientes procesos de análisis, evaluación, planeación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas y con el probable desconocimiento de las características y especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones elegidas. Al materializarse el riesgo la infraestructura tecnológica puede generar inoperancia de los sistemas de información. Tipo de riesgo: Operativo.

- Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción.

Riesgo interno que consiste en el robo, alteración o extracción de la información que es considerada confidencial o clasificada como reservada por deficiencia en las políticas de seguridad o Configuración ineficiente del cortafuegos de la entidad. Al materializarse, el impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional. Tipo de riesgo: Tecnología.

- Falla técnica en equipos servidores, de escritorio o de comunicaciones.

Riesgo interno que corresponde al daño físico o lógico de un equipo servidor, de escritorio o de comunicaciones que afecta el funcionamiento de un sistema de información crítico o de servicio por falta de mantenimiento

preventivo a los equipos o por mal uso de los equipos por parte de los usuarios que hace que el servicio quede inoperante o Inestable. Tipo de riesgo: Tecnológico.

- Falla técnica en sistemas de información.

Riesgo interno, corresponde al riesgo de presentarse errores de lógica en programación o incompatibilidad entre software que afectan a los sistemas de información que genera Inoperancia o inestabilidad de los sistemas de información. Tipo de riesgo: Tecnológico.

- Ausencia de personal de la Dirección de Tecnologías de la Información y las Comunicaciones que brindan soporte y mantenimiento a los a los sistemas de información.

Riesgo interno. Corresponde a la falta o inasistencia en un momento dado, de un ingeniero o técnico de la Dirección de TIC que realiza actividades de soporte a usuarios o de administración técnica sobre un sistema de información crítico del Consultorio Odontológico Sonrisa Feliz por enfermedad, muerte o incapacidad de los funcionarios responsable o demoras en la asignación de funcionarios a la Dirección de TIC, lo que genera inoperancia o inestabilidad de los sistemas de información. Tipo de Riesgo: Operativo.

- Mal uso de hardware y/o software por parte del personal

Riesgo interno. Consiste en el riesgo que corre el Consultorio Odontológico Sonrisa Feliz por un uso inadecuado de los equipos de cómputo, software y/o sistemas de información por parte de los funcionarios por

deficiencias en el conocimiento y uso de las herramientas tecnológicas o por uso mal intencionado de los mismos lo que puede dejar generar interrupción del funcionamiento de los equipos donde se alojan los sistemas de información críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

- Calentamiento del centro de cómputo

Riesgo interno que consiste en el aumento de temperatura dentro del centro de cómputo y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, de comunicaciones y telefónicos dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos. Tipo de riesgo: Tecnología

5. Minimización del riesgo

Corresponde al plan de contingencia informático minimizar esta clase de riesgos con medidas preventivas y correctivas sobre cada uno. Es de tener en cuenta que en lo que respeta a fenómenos naturales, se han presentado últimamente en nuestra región incendios y movimientos telúricos de poca intensidad.

5.1. Incendio o fuego

- Grado de negatividad: Muy Severo
- Frecuencia de evento: Aleatorio
- Grado de impacto: Alto

Acciones:

- Equipar con un extintor cargado, la oficina donde están ubicados los servidores, así como todos los pisos de la institución.
- Ejecutar un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a todo el personal perteneciente a la brigada de emergencia. Lo que es eficaz para enfrentar un incendio y sus efectos.
- Realizar copia de seguridad diariamente al servidor de Backup y además realizar Backup del servidor mensual, almacenándolo en donde lo dispongan (CD-ROM, disco duro, base de datos u otros medios de almacenamientos).

5.2. Robo común de equipos y archivos

- Grado de negatividad: Grave
- Frecuencia de evento: Aleatorio
- Grado de impacto: Moderado

Acciones:

- Tomar registro de la hora de entrada y salida de las personas particulares que ingresan a la fundación. En caso de que se presente un incidente, se pasará a mirar las cámaras de seguridad.
- Solicitar la colaboración de la Policía Nacional para que realice rondas periódicas por el sector donde se encuentra ubicadas las instalaciones, evitando así el hurto a mano armada.

5.3. Falla en los equipos Situación

- Grado de negatividad: Grave
- Frecuencia de evento: Aleatorio
- Grado de impacto: Alto

Acciones:

- Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
- Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
- Colocar estabilizadores a todos los equipos dlel Consultorio El daño de equipos por fallas en la energía eléctrica

5.4. Acción de virus informático

- Grado de negatividad: Grave
- Frecuencia de evento: Aleatorio
- Grado de impacto: Alto

Acciones:

- Instalar software antivirus para la entidad y evitar que sus licencias expiren, se requiere renovación con anterioridad del nuevo antivirus.
- Únicamente el área de sistemas debe ser la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.

5.5. Terremoto

- **Sin Pérdida O Daños Menores De Las Instalaciones:** El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto provocaría en el Consultorio Odontológico Sonrisa Feliz sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo.

- **Con Pérdida De Las Instalaciones:** La pérdida de las instalaciones afectaría gravemente a las operaciones del Consultorio Odontológico Sonrisa Feliz 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.

5.6. Sabotaje

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.

- Buena administración de los recursos humanos.

- Buenos controles administrativos.

- Buena seguridad física en los ambientes donde están los principales componentes del equipo.

- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.

- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.

- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso como terrorismo y sabotaje. Es importante la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.

- Mantener adecuados archivos de reserva (backup)

- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.

- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.

- Usar rastros de auditoría o registro cronológico (Logs) de transacción como medida de seguridad.

6. Plan de recuperación y respaldo de la información

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. El paso inicial en el desarrollo del plan recuperación y respaldo de la información, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Las actividades por realizarse en un plan de recuperación y respaldo de información se clasifican en tres etapas:

- Actividades previas al desastre
- Actividades durante el desastre
- Actividades después del desastre

6.1. Actividades Previas al Desastre

En las actividades previas al desastre se consideran las actividades de planteamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguraran un proceso de recuperación con el menor costo posible para el centro odontológico sonrisa feliz.

6.1.1. Establecimientos del Plan de acción

En esta fase de planeamiento se establece los procedimientos relativos a:

a. Sistemas e Información

El centro odontológico deberá contar con un backup y una relación del sistema de información, Base de Datos, etc, lo cual permitirá la rápida identificación de la información, la relación debe contener:

a. Nombre del Sistema
b. Lenguaje o paquete con el que fue creado el sistema (programas que lo conforman tanto fuentes como ejecutables)
c. Área que genera la información base.
d. Áreas que utilizan la información del sistema
e. Volumen de los archivos que trabaja el sistema
f. Volumen de transacciones que maneja el sistema, diarias, semanales, mensuales
g. Equipamiento necesario para el manejo optimo del sistema
h. Fecha en que la información fue ingresada
i. Fecha de creación de los Sistemas
j. Fechas de adquisición del Software
k. Nivel de importancia estratégica que tiene la información del sistema para el centro odontológico.
l. Actividades que realizar para restablecer el sistema de información

b. Equipos de Cómputo

Se debe tener en cuenta el catastro de Hardware, impresoras, scanner, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Igualmente, se debe emplear algunos criterios sobre la identificación y protección de equipos, tales como:

- El mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente del sistema del centro odontológico.
- Gestionar pólizas de seguro comerciales para los equipos de cómputo (Servidores) como parte de protección de los mismos, pero haciendo la salvedad en el contrato, que, en casos de desastres, la destrucción total del computador, el cual, debe ser repuesto por un equipo de las mismas características o mejor aún, según los nuevos avances de la tecnología siempre y cuando los valores estén considerados dentro los montos asegurados.

c. Obtención y almacenamiento de los Respaldos de Información (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución del sistema del centro odontológico. Las copias de seguridad son las siguientes:

- **Backup del Sistema Operativo** o de todas las versiones de sistema operativo instalados en la Red.

- **Backup de Software Base** (Gestión, lenguajes de programación, paquetes de Diseño, etc).

- **Backup del software aplicativo** backups de los programas fuente y los programas ejecutables.

- **Backups de los datos** (Base de datos, password y todo archivo necesario para la correcta ejecución del software aplicativos de la institución).

d. Políticas (normas y procedimientos de backups)

En el presente ítem se establece los procedimientos, normas y determinación de responsabilidades en la obtención de los backups:

- Periodicidad de cada tipo de backups
  - Información fuente del sistema, se debe salvar mensualmente, especialmente cuando hay modificaciones en los programas fuente.
  - Información ejecutable salvar mensualmente.
  - Información data (BD, archivos), salvar diariamente.
  - Información diversa, salvar diariamente.

- Respaldo de información de movimiento entre los periodos que no se sacan backups

- Como mínimo realizar los backups diarios en discos adicionales externos o virtuales así como en memorias USB.

- Almacenamiento de los backups en condiciones ambientales optimas recomendando que se utilice productos de calidad en relación a los medios magnético.

- Reemplazo de los backups en forma periódica cada vez que el caso lo requiera y considerando también que los medios magnéticos son susceptibles y se pueden deteriorar.

- Almacenamiento de los backups en locales diferentes donde reside la información primaria.

- Realizar pruebas periódicas de los backups, verificando su integridad.

6.2. Actividades Durante el Desastre

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

a. Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o

madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el desastre. Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas.

Normalmente durante la acción del desastre es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de
prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del desastre cause más daños o destrucciones. Se debe tener los números de teléfono y direcciones de organismos e instituciones de ayuda.

b. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que
deberán realizar en caso de desastre. En caso de que el desastre lo permita (al estar en un inicio o estar en un área cercana, etc.), en el momento se debe combatir el desastre, igualmente, se debe haber un salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo

el personal en la lucha contra los diferentes tipos de desastres, para minimizar costos se pueden realizar recarga de extintores, etc. Es importante lograr que el personal tome conciencia de que los desastres (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos.

6.3. Actividades Después del Desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el desastre, son las siguientes:

a. Evaluación de Daños.

El objetivo es evaluar la magnitud del daño producido, es decir, si el sistema tuvo algún daño, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso del centro odontológico se debe atender gran parte de los procesos, tales como, la nómina, documentación, citas programas, etc, ya que son actividades que no pueden dejar de funcionar. La recuperación y puesta en marcha del servidor del sistema, es prioritario.

b. Priorización de Actividades del Plan de Acción.

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo, el sistema de información, compra de equipos dañados, etc.

c. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar actividades previamente planificadas en el Plan de Acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación y, en caso de producirse un problema, reportarlo de inmediato a la Jefatura a cargo del Plan de Contingencias.

d. Evaluación de Resultados.

Una vez concluidas las labores de recuperación de los sistemas que fueron afectado por el desastre, se debe evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del Plan de Acción, como se comportaron los equipos de trabajo, etc.

e. Retroalimentación del Plan de Acción.

Con la evaluación de resultados, se debe de optimizar el Plan de Acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los

elementos que funcionan adecuadamente. El otro elemento es evaluar cuál hubiera sido el costo de no contar con el Plan de Contingencias en el centro odontológico.

6.4. Plan de respaldo y establecimiento de requerimientos de recuperación según el tipo de desastre

A continuación, se puede observar el Plan de contingencia a aplicar dependiendo del tipo del tipo de desastre que ocurra:

Tipo	**Consecuencias**	**Modo de Recuperación**
Incendio	Dependiendo de la magnitud la gravedad será, con pérdida total del inmueble y su contenido	Respaldar y guardar en un banco de información externo, con copias constante, o adquirir un sistema de respaldo CLOUD(en la nube)
Temblor	Dependerá de la Magnitud, pero en caso de que se despoblé existirán equipos que soportaran y la información no será perdida en su totalidad	Respaldar y guardar en un banco de información externo, con copias constante, o adquirir un sistema de respaldo CLOUD(en la nube)
Robo	TI, es el área que más fácilmente sufre atracos, por ser equipos que fácilmente se	Respaldar y guardar en un banco de información externo, con copias constante, o adquirir un sistema de

	pueden vender, principalmente equipos pequeños o portátiles.	respaldo CLOUD(en la nube)
Virus Cibernético	Dependiendo en donde caiga el virus se definirá lo daños que cause, actualmente existen SW de recuperación que rescatan en un 90% la información	En caso de pérdida. Aplicar SW correctivo que permita recuperar los archivo o cualquier documento importante que se desee recuperar