CONTENIDO

INTRODUCCIÓN

El plan de contingencia de la información vital del Instituto 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), por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, fallos con el proveedor de servicios, etc.) que producen daño físico irreparable.

La coordinación de TIC tiene el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones. En base a eso es importante contar con un Plan de contingencia adecuado de forma que ayude al Instituto de Peluquería Canina a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del sitio web.

Los responsables del servicio informático están obligados a hacer de conocimiento y explicar con lenguaje entendible a los líderes de los procesos, las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso del sitio.

Para realizar el Plan de Contingencia Informático del Instituto de Peluquería Canina se tiene en cuenta la información como uno de los activos más importantes, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del Instituto. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos el servidor virtual, el de contingencia local y los 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 y los usuarios realizan frecuentemente al interactuar con la plataforma informática (acceso a las lecciones, entrada de datos, revisión de tareas y exámenes, consultas, etc.). El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad lógica y física 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 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 menor posible.

1. GENERALIDADES

1.1. Objetivos

1.1.1. Objetivo General

Formular un adecuado Plan de Contingencias, que permita la continuidad del sitio web del Instituto de Peluquería Canina, así como enfrentarnos a 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 la mejora de la calidad en los servicios que brinda la institución.

1.1.2. Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos en el Instituto de Peluquería Canina que pueda ser suspendida completa o parcialmente la prestación del servicio.
- Establecer los niveles de complejidad de las fallas del sistema y los posibles tiempos de no disponibilidad del sitio web.

1.2. Alcance

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

2. MARCO CONCEPTUAL

2.1. Definiciones:

AMENAZA: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

CONTIGENCIA: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

ELEMENTOS EN RIESGO: Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

VULNERABILIDAD: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de "0" (no hay daños) a "1" (daño total).

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

INCIDENTE: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

ACTIVO: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos del Instituto ante la eventualidad que lo afecte de forma parcial o total.

3. ANALISIS DE LA EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

3.1. Factores de afectan la seguridad física y la infraestructura

Dentro de estos factores se encuentran los riesgos de origen natural como los desastres y los riesgos artificiales como los ataques terroristas. Ambos riesgos tienen su origen de causas externas al Instituto de Peluquería Canina y su grado de previsión es muy mínimo. La probabilidad de origen natural es baja, mientras, que los riesgos artificiales son de probabilidad media.

De igual forma se encuentran los fallos con el proveedor del servidor virtual, las descargas o cortes eléctricos, los cuales pueden generar interrupción en el servicio que afectarían la atención a los usuarios.

Para la clasificación de los activos de la tecnología informática de la institución se han considerado tres criterios:

- Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderado, grave y muy severo).
- Frecuencia del evento: Puede ser (Nunca, aleatorio, periódico o continuo).
- Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de contingencia: Son procedimientos que definen como 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, equivocaciones, daño de archivos, acceso no autorizado, fallo con el servicio ofrecido por parte del proveedor del servidor etc.)
- Severas (Destrucción de equipos, incendios, inundaciones, daño de equipo, robos, etc.)

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

- Riesgos Naturales (Mal tiempo, terremoto, inundaciones, etc.)
- Riesgos tecnológicos (Problemas con el servicio del proveedor, incendios eléctricos, fallas de energía y accidentes de transmisión y transporte).
- Riesgos sociales (Actos terroristas, desordenes, entre otros).

Tipos de contingencias de acuerdo al grado de afectación:

- En el mobiliario
- En el equipo computo en general (Procesadores, unidades de disco)
- En comunicaciones (ruteadores, nodos, fibra óptica, cable)

3.1.1. Posibles daños:

- Imposibilidad de acceso a los recursos debido a problemas con el proveedor del servidor virtual, problemas físicos en las instalaciones con el servidor alternativo, problemas naturales o humanos.
- 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.

3.1.2. Fuentes de daño:

- 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.)

3.1.3. Clases de riesgo

- Incendio

- Robo común de equipos y archivos
- Falla en los equipos
- Acción de virus informático
- Fenómenos naturales
- Accesos no autorizados
- Ausencia del personal de sistemas.

3.2. Factores asociados con la seguridad lógica

Estos riesgos están asociados con fallas en el funcionamiento de los equipos o de los programas de protección, cuyo deterioro o mal uso pueden generar:

- Daños en Discos duros, controladores de red, etc.
- Fallas en equipos de comunicaciones (switches, Routers)
- Daños graves en los archivos del sistema, por error de Hardware o Software
- Ingreso de virus u otros programas malintencionados que puedan dañar los archivos y los equipos computo.

3.3. Factores asociados con la seguridad técnica integral

Fallas, daños y/o deterioros por mal uso, fallas de mantenimiento y/u obsolescencia para, switchs, dispositivos, backup.

3.4. Minimizar el 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.

3.4.1. 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 todos los pisos y zonas de la institución cuentan con un extintor debidamente cargados.	Se cumple

Situación Actual	Acción correctiva
Se ejecutó 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.	Se cumple
Se realiza una copia de seguridad diariamente a la base de datos del servidor de contingencias y además se realiza un backup semanal del sitio web, almacenándolo en un plan de Dropbox Empresarial, el cual es un servicio de un proveedor totalmente independiente de Godaddy (Proveedor del servidor virtual).	Se cumple

Analizando el riesgo de incendio y la forma como se almacenan los Backup en la nube, un incendio nunca afectará la seguridad de los respaldos.

3.4.2. Robo común de equipos y archivos

Grado de negatividad: Grave

Frecuencia de evento: Aleatorio

Grado de impacto: Moderado

Situación Actual	Acción correctiva
Se cuenta con cámaras de seguridad en todas las zonas de la institución, además de vigilancia presencial las 24 horas del día. A la salida del personal se realiza una revisión de las pertenencias, bultos y bolsos.	Se cumple
Autorización escrita firmada por coordinador del área para salidas de equipos de institución, además de anotación en la bitácora de los guardas de seguridad.	Se cumple
Hurto a mano armada.	Solicitar la colaboración de la Policía para que realice rondas

	periódicas por el sector donde se encuentra ubicadas las instalaciones

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del coordinador de Sistemas, esto demuestra que los equipos se encuentran protegidos. Tampoco se han reportado casos donde haya habido hurtos de nuestro sistema cómputo en la institución, sin embargo se recomienda siempre estar alerta.

3.4.3. Falla en los equipos

Situación Actual	Acción correctiva
Problemas presentados por parte del proveedor del servidor virtual, en el que se vea imposibilitado el acceso al sitio web del Instituto	Se cuenta con un servidor de respaldo en las instalaciones físicas del Instituto, con una réplica del sitio web y de la base de datos, con el fin de direccionar el tráfico de forma inmediata del servidor en producción en EEUU, al servidor de respaldo en Costa Rica. Con esto se garantiza la continuidad del servicio brindado
Problemas con el proveedor de internet en el enlace de fibra óptica de la empresa	Se cuenta con un enlace alternativo con Cable Tica, para garantizar la conexión del servidor de respaldo ante cualquier eventualidad.

Analizando el riesgo de falla de los equipos, es recomendable estar realizando mantenimiento preventivo a los equipos computo e implementar estabilizadores a los equipos para en caso de una falla de energía eléctrica los dispositivos se puedan apagar correctamente.

3.4.4. Acción de virus informático

Situación Actual	Acción correctiva
Se cuenta con un software antivirus para la entidad. Además se realizan actualizaciones periódicas ante nuevas amenazas.	Se cumple

Situación Actual	Acción correctiva
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple

Tener actualizado e instalado los antivirus para todos los equipos cómputo de la institución para prevenir daños por causa de un virus informático.

3.4.5. 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 la institución 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 de la institución En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente. Cabe destacar que el sitio web de la Institución no se vería afectado, al estar en un servidor en Estados Unidos.

3.4.6. 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 seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de los servicios de emergencia a mano y en lugares donde se pueda hacer un llamado.
- 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.

4. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

4.1. Actividades previas al desastre

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para el Instituto. Se establece los procedimientos relativos a: Sistemas e Información, Equipos de Cómputo, Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

- **Sistemas de Información:** El Instituto cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backup.
- **Equipos de Cómputo:** Se debe tener en cuenta el catastro de Hardware, equipo de red y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se emplean los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en el instituto.

4.2. Falla en las comunicaciones (Internet)

Ante una falla en las comunicaciones (TIGO) en fibra óptica, se optará por el enlace alternativo por cable coaxial (Cable Tica) para lo cual el encargado de sistemas realizará el redireccionamiento del tráfico al enlace correspondiente.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2022-FEB-23	01	Documento inicial.

ELABORÓ		REVISÓ		APROBÓ	
Nombre	Gabriel Contreras	**Nombre**	Leví Alvarado	**Nombre**	Aura Santacruz Bernal
Cargo	Auxiliar de TIC	**Cargo**	Encargado de TIC	**Cargo**	Representante por la Institución