1.0 TITULO:

INSTRUCTIVO: PLAN DE CONTINGENCIAS DE LA GERENCIA DE INFORMÁTICA DEL INSTITUTO SALVADOREÑO DE TRANSFORMACIÓN AGRARIA-ISTA

2.0 CONTROL DE CAMBIOS:

Revisión:	1	2	3	4	5	6	7	8
Fecha:								

3.0 DISTRIBUCION:

DOCUMENTO:	FECHA	COPIA
ORIGINAL DIGITAL	27/07/2011	1
COPIA IMPRESA	27/07/2011	LD_FIPR03-IN-I03_R0

4.0 CONTROL DE DOCUMENTOS:

Instituto Salvadoreño de Transformación Agraria (ISTA)

GOBIERNO DE EL SALVADOR
UNIR, CRECER, INCLUIR

DOCUMENTO CONTROLADO

Elaboró:	Revisó:	Autorizó:
Gerd Saelzer 20/07/2011	Pedro Peñate Salvador Palma 22/07/2011	**PABLO OCHOA QUINTEROS** 27/07/2011
Gerente de Planificación	Equipo de Revisión	Presidente-ISTA-

5.0 OBJETIVO

Establecer las acciones a seguir que permitan reducir el riesgo de siniestro de cualquier índole en lo relativo a informática en el Instituto Salvadoreño de Transformación Agraria, para la eficiente y correcta gestión en caso de siniestros.

6.0 ALCANCE

Este es aplicable a todas las unidades del Instituto Salvadoreño de Transformación Agraria.

7.0 DEFINICIONES Y MARCO CONCEPTUAL

Monitoreo: Verificación vía telefónica realizada una vez un usuario reporta una falla con el fin de conocer el tipo de falla si es leve o grave que presenten los recursos informáticos.

Hardware: Dispositivos o equipos tangibles utilizados para el procesamiento electrónico de información, captura, modificación e incorporación de datos.

Terminal: Computadora con características adecuadas para el procesamiento y almacenamiento de la información.

Servidor: Computadora con características adecuadas para el procesamiento y almacenamiento de la información adquirida a través de las terminales.

Enlace: Medio físico que une dos lugares distantes en términos geográficos.

Impresor de gran volumen: Impresores utilizados para la personalización de reportes.

Impresor de viñetas: Impresores utilizados en la impresión de viñetas de los despachos.

Sucursal: Oficina descentralizada de la Dirección General de Correos en la cual se recibe y distribuye correspondencia.

BASE LEGAL

El presente documento tiene su base legal en:

- Reglamento de Normas Técnicas Específicas del Instituto Salvadoreño de Transformación Agraria-ISTA.

8.0 DESARROLLO:

PLAN DE CONTINGENCIA INFORMÁTICO

El Plan de Contingencia de equipos de cómputo considera dos aspectos importantes:

- Incluye las actividades que se deben realizar y los grupos de trabajo o responsables de operar.
- El control, referido a las pruebas y verificaciones periódicas sobre la operatividad y actualización del Plan de Contingencia.

I. ACTIVIDADES PREVIAS AL DESASTRE

a. Establecimiento del plan de acción, que comprende:

1. Sistema de información: son los sistemas producidos en la institución y fuera de esta que son vitales para el adecuado funcionamiento de la misma.
2. Equipos de cómputo: Se cuenta con el inventario actualizado de Hardware y Software, especificación técnica, ubicación física y el área a la que está asignada.
3. Se encuentran reconocidas las computadoras de acuerdo a la importancia de su contenido a fin de tener prioridad en caso de evacuación.
4. La Gerencia de Informática es la responsable de identificar las computadoras de acuerdo a su importancia, para lo cual debe hacer uso del inventario de equipos de informática, el mismo que les proporcionará la información para probables reemplazos de equipos.
5. Obtención y almacenamiento de los Respaldos de Información (BACKUPS), que incluye:
   - Backup del Sistema Operativo por cada versión.
   - Backup del Software Base (paquetes y/o lenguajes de programación con los cuales han sido desarrollados o interactúan los aplicativos institucionales).
   - Backup del Software Aplicativo.
   - Backup de los Datos.
   - Backup del Hardware.
   - Procedimiento para los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia.
6. Políticas (normas y procedimientos de Backup), que considera:
   - Determinación de responsabilidades en la obtención del Backup mencionado anteriormente; debiéndose incluir:
   - Almacenamiento del Backup en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
   - Reemplazo del Backup, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
   - Pruebas periódicas del Backup,

b. Formación de equipos operativos, mediante la designación del responsable de seguridad de la información en cada unidad. Las funciones de los responsables serán:
   - Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
   - Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
   - Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
   - Supervisar procedimientos de respaldo y restauración.

- Supervisar la carga de archivos de datos de las aplicaciones y la creación de respaldos incrementales.

c. Formación de equipos de evaluación para realizar la auditoría de los procedimientos de seguridad; cuyas funciones serán:
   - Revisar la aplicación y cumplimiento de las normas y procedimientos con respecto a Backups.

d. Entrenamiento: Establecer un programa de prácticas periódicas para el personal, en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le haya asignado en los planes de evacuación de personal o equipos. Para este caso, la Gerencia de Operaciones y Logística deberá aprovechar las fechas de recarga de los extintores y propiciar charlas con organismos vinculados a siniestros. El personal debe tomar conciencia que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y deben asumir con seriedad y responsabilidad los entrenamientos. Los Funcionarios también están en la obligación de participar en los entrenamientos.

II. ACTIVIDADES DURANTE EL DESASTRE

a. Uso de extintores recargados y en buenas condiciones.

b. Formación de equipos: El personal del ISTA es el responsable del salvamento de equipos informáticos, de acuerdo a la prioridad del equipo bajo el apoyo y supervisión de la Gerencia de Informática.

III. ACTIVIDADES DESPUÉS DEL DESASTRE

a. Evaluación de los daños: Inmediatamente después de concluido el siniestro, se deberá evaluar la magnitud del daño producido. Qué sistemas se afectaron; qué equipos están no operativos; cuáles se pueden recuperar y en cuánto tiempo, e informar al Presidente de la Institución para preparar la reposición de equipos.

b. Priorizar las actividades del Plan de Acción.: Si el Plan de Acción es general y contempla una pérdida total; la evaluación de daños reales y su comparación contra el Plan, proporcionará la lista de las actividades a realizar en función de la prioridad. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, a fin de asignarlos en forma temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

c. Ejecución de actividades: Conformación de equipos de trabajo para realizar las actividades previamente establecidas en el Plan de Acción. Cada uno de los equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.
   El trabajo de recuperación consta de dos etapas:
   - Restauración del servicio usando los recursos de la Institución o local de respaldo,
   - Volver a contar con los recursos en las cantidades y lugares apropiados, debiendo ser esta etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución o local de respaldo.

d. Evaluación de resultados: Concluida la labor de recuperación del sistema afectada por el siniestro, se debe evaluar objetivamente, todas y cada una de las actividades realizadas, considerándose entre otros aspectos:
   - ¿Qué tan bien se hicieron?;

- ¿qué tiempo demando?;
- ¿qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del Plan de acción?;
- ¿cómo se comportaron los equipos de trabajo?.

De la Evaluación de resultados y del siniestro en si, deben obtenerse dos tipos de recomendaciones:

- Retroalimentación del Plan de Contingencias
- Lista de recomendaciones para minimizar la pérdida que ocasionó el siniestro.

e. Retroalimentación del Plan de acción: Con la evaluación de resultados, debe optimizarse el Plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente. Además se debe evaluar cual hubiera sido el costo de no tener un Plan de contingencias.

IV. RIESGO

Probabilidad de ocurrencia de eventos negativos que perjudiquen los equipos informáticos y periféricos. El análisis supone obtener una evaluación económica del impacto de dichos sucesos negativos.

a. Se considerarán los siguientes factores de riesgo:

- Falla del sistema eléctrico,
- Falla física y lógica de un servidor,
- Desastre Natural,
- Falla de un equipo informático cualquiera y
- Otros.

b. Se efectuará un resumen de los riesgos contemplados a continuación en el presente documento.

1. El análisis de riesgos supone responder a preguntas y determinar su grado de confiabilidad:

   a. ¿Qué puede ir mal?
   b. ¿Con qué frecuencia puede ocurrir?
   c. ¿Cuáles serían las consecuencias?

2. La evaluación de riesgos supone responder a preguntas con la mayor confiabilidad:

   a. ¿Qué se intenta proteger?
   b. ¿Cuál es el valor para la institución DGC o para la persona, frente a qué se intenta proteger?
   c. ¿Cuál es la probabilidad de un ataque?

c. Las Gerencias y Jefaturas del ISTA, sin excepción, están obligadas a brindar todo el apoyo necesario a la Gerencia de Informática, con el fin de una prevención de desastre.

V. FALLA O ACTIVIDADES DE EMERGENCIA

Los Gerentes y Jefes, designarán a los responsables de cada área usuaria para que brinden apoyo al personal de la Gerencia de Informática en los siguientes aspectos:

a. Falla / Actividad de Emergencia: **Computadora de una Oficina Regional**

- Actividades a Realizar:

  - ✓ Consultar y solucionar (si es posible) vía telefónica, si no realizar reparación (si es posible) a través de soporte control remoto, de lo contrario solicitar se envié a la central equipo.
  - ✓ Programar y realizar visita a la brevedad si es necesario,
  - ✓ En el caso que todas las terminales se dañen simultáneamente se realizará visita inmediatamente, llevando por lo menos una terminal lista para instalar.

- Recursos a Utilizar:

  - ✓ Técnico,
  - ✓ Teléfono,
  - ✓ Herramientas de trabajo,
  - ✓ Software de administración remota,
  - ✓ Vehículo,
  - ✓ Computadora(as) deberá(n) estar disponible.

b. Falla / Actividad de Emergencia**: Computadora Local**

- Actividades a Realizar:

  - ✓ Consultar y solución (si es posible) vía telefónica, si no realizar reparación (si es posible) a través de soporte electrónico remoto,
  - ✓ Programar y realizar visita a la brevedad si es necesario,

c. Falla / Actividad de Emergencia**: Sistema eléctrico**

- Actividades a Realizar:

  - ✓ Determinar el origen de la falla eléctrica.
  - ✓ Se cuentan con UPS con estabilizadores de voltaje, los cuales aseguran la continuidad de la operación de los equipos computacionales por un lapso de 5 minutos.
  - ✓ Esperar un lapso de tiempo adecuado para que la energía eléctrica se estabilice.
  - ✓ En caso que no se estabilice el servicio de energía eléctrica, apagar y desconectar los servidores, previa autorización de la Gerencia de Informática.
  - ✓ Notificar a los usuarios que los servicios prestados por la Gerencia de Informática serán suspendidos temporalmente.
  - ✓ Al restablecerse el sistema eléctrico, conectar y encender el equipo informático.
  - ✓ Reiniciar los servicios prestados por la Gerencia de Informática.
  - ✓ Informar a los usuarios que los servicios han sido restaurados.

d. Falla / Actividad de Emergencia: **falla física y lógica de un servidor**

- **Actividades a Realizar:**

  - ✓ Utilizar equipo redundante.
  - ✓ Apagar y desconectar el servidor para su revisión.
  - ✓ Determinar la causa de la falla física/lógica del servidor.
  - ✓ Corregir la falla física/lógica detectada en el servidor.
  - ✓ Restaurar la última copia de respaldo de información del servidor.
  - ✓ Informar a los usuarios que los servicios han sido reanudados.
  - ✓ Puesta en marcha del servidor.

e. Falla / Actividad de Emergencia: **Desastre natural**

- **Actividades a Realizar:**

  - ✓ Desalojar al personal de la Gerencia de Informática.
  - ✓ Revisar los daños ocasionados en el equipo informático.
  - ✓ Apagar y desconectar el equipo informático afectado y no afectado.
  - ✓ Aislar el equipo informático afectado o en amenaza.
  - ✓ Sacar el equipo informático no afectado.
  - ✓ Trasladar el equipo informático no afectado a un lugar más seguro.
  - ✓ Conectar y encender el equipo informático no afectado en la ubicación predeterminada.
  - ✓ Verificar que el equipo informático no afectado, se encuentre en buen estado y en buen funcionamiento.
  - ✓ Sacar los respectivos respaldos de información del equipo informático no afectado.
  - ✓ Verificar que las condiciones sean óptimas para la puesta en marcha de los servicios.
  - ✓ Restablecer los servicios proporcionados por la Gerencia de Informática.

f. Falla / Actividad de Emergencia **Falla de un equipo informático cualquiera**

- **Actividades a Realizar:**

  - ✓ Llenar formulario para retirar el equipo informático con falla.
  - ✓ Retirar el equipo informático de su localidad, para su revisión.
  - ✓ Revisar el equipo informático para detectar la falla que ocasiona el mal funcionamiento de este.
  - ✓ Reparar el equipo informático, en caso de que este tenga arreglo.
  - ✓ Dejar funcionando el equipo informático nuevamente.
  - ✓ Reemplazar el equipo informático defectuoso por uno nuevo, en caso de que este no tenga arreglo.
  - ✓ Preparar el equipo informático adecuadamente para su posterior utilización por parte del usuario.
  - ✓ Trasladar el equipo informático a su destino.

VI. OTROS

Falla / Actividad de Emergencia:

a. <u>Al fuego, que puede destruir los equipos y archivos:</u>
- ✓ Mantener extintores en sitios estratégicos y revisar periódicamente sus niveles de carga,
- ✓ La Gerencia de Operaciones y Logística debe realizar un Plan de entrenamiento para el uso de los mismos.

b. <u>Al robo común, llevándose los equipos y archivos.</u>
- ✓ Cerrar las puertas de entrada y ventanas de cada Oficina.
- ✓ Contar con personal de seguridad en las instalaciones.
- ✓ Todas las Pc deben estar bloqueadas con claves de acceso.

c. <u>Al vandalismo, que dañen los equipos y archivos.</u>
- ✓ Cerrar la puerta de entrada,
- ✓ La vigilancia debe rondar por todo el perímetro de las Instalaciones de cada oficina.

d. <u>A fallas en los equipos, que dañen los archivos</u>
- ✓ Realizar mantenimiento continuo por parte de personal calificado
- ✓ Revisar periódicamente las condiciones actuales del hardware y sus exposiciones a situaciones de riesgo
- ✓ Reemplazar el hardware dañado

e. <u>A equivocaciones, que dañen los archivos.</u>
- ✓ Realizar copias de los archivos que son vitales para la Institución,

f. <u>A la acción de virus, que dañen los equipos y archivos.</u>
- ✓ Realizar examen antivirus a todo software y hardware que se utiliza
- ✓ Los programas de dominio público y de uso compartido, sólo se usan si proceden de una fuente fiable.

g. <u>A terremotos, que destruyen el equipo y los archivos.</u>
- ✓ Sólo es válido un seguro contra siniestros

VII. DISPOSICIONES ESPECÍFICAS

1. La Gerencia de Informática evaluará las probables fallas en el sistema de seguridad.
2. La Gerencia de Informática es la responsable de formular, programar, realizar, coordinar, ejecutar, evaluar y controlar el Plan de Contingencias de equipos informáticos y periféricos.
3. La Gerencia Operaciones y Logística es la responsable del entrenamiento en el uso de extintores, para lo cual deberá programar las fechas en que se realizará tal entrenamiento.
4. La Gerencia Operaciones y Logística a través del Departamento de Servicios Generales (sección de Activo Fijo) es la responsable de proporcionar a la Gerencia de Informática el inventario de equipos informáticos y periféricos debidamente actualizados.
5. El Plan de Contingencias de equipos informáticos y periféricos tiene la clasificación de prioridad muy alta.
6. El Gerente de Informática es el responsable de velar por el estricto cumplimiento de lo dispuesto en la presente Plan.

7. El personal del ISTA independientemente de su nivel y cargo forma parte como un todo del Plan de contingencias.

Se contará con un comité de contingencia conformado por personal designado por el Gerente de Informática y que lo hará del conocimiento del Gerente de Recursos Humanos

9.0 DOCUMENTOS DE REFERENCIA

No Aplica.

10.0 ANEXOS: