UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

DIRECCION GENERAL DE ADMINISTRACION

Centro de Cómputo

PLAN DE CONTINGENCIAS INFORMÁTICO:

Versión 1.1
Setiembre 2008

Ingº Manuel Peñaloza Figueroa
Centro de Cómputo de la Dirección General de Administración

PLAN DE CONTINGENCIAS

El Plan de Contingencias es un documento que contiene los procedimientos y/o actividades para la toma de decisiones en caso que ocurra una emergencia que interrumpa la operatividad de los sistemas. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para proteger y salvaguardar la integridad y seguridad de la información que maneja la Dirección General de Administración (DIGA) en relación con contingencias producidas en los Servidores de Base de Datos, los Equipos de Comunicación de Datos y Enlaces de Comunicación, el Software de Aplicaciones y los datos, y garantizar su continuidad en las operaciones.
Como instrumento de gestión apoya en el buen manejo de las Tecnologías de la Información y de las Comunicaciones (TICs).

El plan de contingencias deberá ser actualizado anualmente. Así mismo, es revisado/evaluado cuando se materializa u ocurre una amenaza.

I. OBJETIVO

Restablecer y/o recobrar el servicio informático en caso de presentarse contingencias graves en la DIGA, ocasionadas por fallas de la plataforma informática (infraestructura de red, servidores, PCs, dispositivos de comunicación, y software de aplicaciones).

II. ALCANCE

El presente documento es de aplicación y cumplimiento obligatorio del personal que labora en la Dirección General de Administración (DIGA), y otras dependencias administrativas que están en relación directa con la gestión financiera, contable y presupuestal de la Institución.

III. RESPONSABILIDAD

El Director de la Dirección General de Administración es el responsable de la implementación de este dispositivo.

El Personal encargado del Centro de Cómputo – DIGA es el responsable de supervisar y coordinar las acciones para que se procesen y remitan los respaldos, y que llegan a los sitios externos de respaldo, y de tomar las medidas y acciones de recuperación de restauración del servicio.

Los usuarios y operadores de las dependencias de la DIGA son los responsables de ejecutar los procedimientos en los cuales estén involucrados para superar las contingencias detalladas en el presente procedimiento.

IV. VIGENCIA

Versión 1.1: a partir del 01/09/2008
Aprobado con Resolución: Nº R-2237-2237-UNSAAC del 22 de Octubre del 2008

Versión 1.0: a partir del 01/08/2007

V. BASE LEGAL

- Constitución Política del Perú:
  1993
- Directiva Nº 008-95-INEI/SJI
  "RECOMENDACIONES TECNICAS PARA LA PROTECCION FISICA DE LOS EQUIPOS Y MEDIOS DE PROCESAMIENTO DE LA INFORMACION EN LA ADMINISTRACION PUBLICA".
- DIRECTIVA Nº 010-95-INEI/SJI
  "RECOMENDACIONES TECNICAS PARA LA ORGANIZACION Y GESTION DE LOS SERVICIOS INFORMATICOS PARA LA ADMINISTRACION PUBLICA".
- DIRECTIVA Nº 016-2002-INEI/DTNP
  "NORMAS TÉCNICAS PARA EL ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN PROCESADA POR LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA".
- R.D. Nº 320-2006-CG
  Aprueban las "Normas de Control Interno".

VI. REFERENCIAS

- Guía para la elaboración de un Plan de Contingencias Informático INEI – Diciembre 2002.

VII. MEDIDAS

El plan de contingencias contempla la aplicación de 3 tipos de medidas:

- Medidas preventivas: cuyo objeto es disminuir la probabilidad de que el fallo llegue a producirse (pruebas y revisiones constantes).
- Medidas alternativas o de respaldo: orientadas al mantenimiento de la actividad una vez sucedido el fallo, bien sustituyendo el componente que falla ó prescindiendo del mismo.
- Medidas correctivas: orientadas a la corrección del fallo y recuperación de la operatividad del componente fallido.

VIII. POLÍTICAS DE GOBIERNO

Respecto a las políticas y actividades iniciales, en el Plan de Contingencias se deben considerar los siguientes aspectos:

Apoyo de la Alta Dirección
No se podrá conseguir el éxito del Plan de Contingencias, si la Alta Dirección no conoce la necesidad de estos en la Institución, ni apoyan su desarrollo y su ejecución.

Apoyo de los Usuarios
No se podrá conseguir el éxito total del Plan de Contingencias, si los usuarios no colaboran en el desarrollo y aplicación del mismo.

IX. ANÁLISIS DE RIESGO

Identificar aquellos elementos de la Institución ó funciones que puedan ser críticos ante cualquier eventualidad ó desastre y jerarquizarlos por orden de importancia dentro de la Institución.

Clasificación de los recursos informáticos en orden crítico:

Definir un sistema de clasificación de los recursos informáticos para determinar la criticidad de los recursos.

En lo fundamental el análisis de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Cuánto puede operar un área sin los sistemas?
- ¿Cuál es el riesgo y/o pérdida económica?
- ¿Existe impacto en la imagen de la Institución?
- ¿Se puede perder registros y/o datos vitales como resultado de la discontinuidad de los recursos?
- ¿Existen alternativas de procesamiento ante una falla?

Los recursos informáticos pueden ser clasificados de la siguiente forma:

1. **Hardware**
   - Computadoras de escritorio
   - Portátiles
   - Servidores
   - Impresoras de escritorio
   - Impresoras de red

2. **Software**
   - Base de datos
   - Aplicaciones locales
   - Aplicaciones integradas
   - Aplicaciones Web

3. **Comunicaciones**
   - Dispositivos para la comunicación local
     - Hubs
     - Switches
   - Dispositivos para la comunicación remota
     - Modems
     - Routers

4. **Infraestructura de red**
   - Cableado
   - Pozos de tierra

5. **Servicios**
   - Central telefónica
   - Telefonía fija
   - Conexión de Internet

Niveles de Severidad:
Se definen los siguientes niveles de severidad:

1. **Nivel 4: Crítica**
   Aplicaciones ó actividades extremadamente críticas o vitales para la continuidad de la Institución. Estos son recursos informáticos que deben estar disponibles para que la organización sea viable.

2. **Nivel 3: Moderada**
   Actividades o aplicaciones importantes que deben ser recuperadas dentro un periodo razonable de tiempo para mejorar el nivel de las operaciones.

3. **Nivel 2: Baja**
   Funciones que pueden ser excluidas de la lista de criticidad, que podrían ser convenientes para la eficiencia en las operaciones.

4. **Nivel 1: No importante ó trivial**
   Recursos que pueden ser excluidos del plan, pues no afectan a las operaciones de la Institución

Tipos de Riesgos:

Riesgo	Probabilidad del Factor de Riesgo				
	Muy bajo	Bajo	Medio	Alto	Muy Alto
Fallas en los equipos			X		
Fallas en las aplicaciones		X			
Alteración de información	X				
Accesos no autorizados	X				
Virus			X		
Robo (común y de datos)	X				
Incendio		X			
Fallas en la red eléctrica			X		
Fallas en la red LAN (/ WAN)		X			

X. GESTIÓN DEL RIESGO

Realizar un plan de continuidad compuesto a su vez de un conjunto de planes para cada una de las áreas críticas. Cada plan describirá los recursos, papeles de personal, procedimientos y tiempo ó fechas para la implantación.

Se podrán llevar a cabo las siguientes acciones con el objeto de minimizar los riesgos:

Minimización del Riesgo:

1. Realizar copias de respaldo ó backups de la información
2. Fortalecer la seguridad física de las instalaciones
3. Fortalecer el control de acceso
4. Identificar documentos de seguros y contratos
5. Revisar procedimientos de personal y de control
6. Seguridad de la infraestructura informática.
7. Definir acuerdos de continuidad con clientes y proveedores.
8. Utilizar servicios de outsourcing.
9. Desarrollo de opciones preventivas y de planeación
10. Capacitación.
11. Servicios generales
12. Renta de equipos de respaldo.

Procedimientos de backups:

En relación a los procedimientos para la realización de las copias de respaldo ó backups se tomará en cuenta lo siguiente:

- Periodicidad de cada tipo de backup:
    a. Sistemas más importantes (SIAF, Logística): diario
    b. Planilla Electrónica: mensual
    c. Otros sistemas: semanal, mensual, anual, a demanda
- Almacenamiento de los backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad.
- Una copia de los backups del SIAF y Logística deben de ser guardados en un medio de almacenamiento digital que se encuentre fuera de las instalaciones del CC-DIGA.

Directivas generales para el adecuado uso de los sistemas y equipos:

1. Salir de las aplicaciones en casos de ausentarse por periodos largos.
2. Apagar los equipos al final de la jornada de trabajo.
3. No crear recursos compartidos en las PCs, salvo que fuera estrictamente necesario por cuestiones de una mejor gestión de la oficina, en cuyo caso, los recursos compartidos deberán ser accesibles sólo a usuarios autorizados.
4. Uso de contraseñas "fuertes" (8 caracteres como mínimo, con al menos 1 dígito y 1 signo de puntuación y no tener los nombres, ni apellidos, ni la fecha de nacimiento del usuario).
5. Si necesario, empleo de bloqueos de pantalla para el caso de inactividad de la PC por un periodo nnn de tiempo.
6. No abrir mensajes de correo cuya procedencia sea dudosa, no conocida y/o no solicitada.

Directivas generales para el cuidado de los equipos:

1. En las oficinas no deben existir materiales que sean altamente inflamables y que despidan humos sumamente tóxicos.
2. Promover paredes que queden perfectamente selladas y no despidan polvo.
3. Mantener los partes externas de los equipos libres de polvo.
4. Evitar la luz solar directa sobre los equipos.
5. Planificar mantenimientos preventivos programados.

Directivas generales para la prevención del robo:

1. Mantener los servidores, los switches, los UPS y los equipos adicionales tras elementos que limiten el acceso a los mismos y brinden seguridad física del caso.
2. Mantener las PC clientes dentro de ambientes que tengan elementos de seguridad física como puertas, chapas, rejas.
3. A nivel del personal de seguridad de la Institución, promover personal de competente, de calidad profesional y que conozca de procedimientos de seguridad.
4. Promover equipos de personas que establezcan y comprueben las técnicas y procedimientos de seguridad.
5. Ejecutar un análisis de riesgo por pérdidas potenciales por delitos intencionados como el robo.

6. Si necesario, elaborar una lista de datos y/o aplicaciones susceptibles de robo por su valor en el mercado ó por su demanda en el mismo; asimismo, establecer los mecanismos de protección correspondientes.

Directivas generales para el adecuado uso del software antivirus:

1. Instalar solo software antivirus con licencia cuya tiempo de vigencia sea de 1 año ó mas.
2. Llevar registro de la fecha de instalación ó de caducidad del software antivirus.
3. Permitir que el software del antivirus realice la actualización de su registro de virus, lo cual sucede normalmente al momento de prender el equipo al inicio de la jornada de trabajo.
4. Reportar al responsable del CC-DIGA mensajes de “Antivirus desactivado”, "El servicio de antivirus se encuentra desactivado", “Licencia de antivirus vencida”, “Periodo de validez de la licencia expirado”, "Usuario ó contraseña inválidos", "User and password invalid", etc. para que se tomen las acciones del caso.

XI. PROBLEMAS Y TIPO DE SOLUCIÓN

1. **Inoperatividad irrecuperable del Servidor de Archivos:**
   - **Reconocimiento:**
     - No se puede interactuar con las aplicaciones del servidor.
     - No se puede acceder a la consola del servidor.
     - Posibles mensajes de "crash" en la consola del servidor.
     - El servidor se reinicia en forma aleatoria.
     - Mensajes de error de E/S en la consola del servidor.
     - Mensajes de error en el disco en la consola del servidor.
     - Mal funcionamiento del S.O. de red.
   - **Severidad:** Crítica
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
   - **Recursos:**
     - Instalador del SO de la red.
     - Instalador de las aplicaciones o sistemas de software.
     - Última copia de seguridad de los datos.
     - Servidor de contingencias (una PC alternativa para la función de servidor), con el SO de red pre-instalado.
   - **Acciones:**
     - Instalación del SO de la red en la PC alternativa (si necesario).
     - Configuración de opciones de red y direcciones IP.
     - Configuración de recursos compartidos.
     - Configuración de grupos de usuarios y usuarios.
     - Instalación de las aplicaciones.
     - Restauración de los datos.
     - Pruebas
     - Luz verde.
     - El Responsable del CC-DIGA, solicita al proveedor ó CAS del fabricante, ó a la UMSA la reparación del servidor dañado, dependiendo de si el equipo servidor está dentro de los límites ó no de la garantía respectiva.

2. **Inoperatividad del Servidor causada por daño en la tarjeta de red:**
   - **Reconocimiento:**
     - No se puede interactuar con las aplicaciones del servidor.
     - Mensaje de pérdida de conexión con el servidor.
     - Mensaje de que los recursos compartidos en el servidor no están disponibles.
     - Ping desde el servidor a cualquier otra PC no responde,
     - Diagnósticos de operatividad de la tarjeta de red negativos.
   - **Severidad:** Crítica
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
   - **Recursos:**
     - Tarjeta de red (redundante ya instalada).
     - Tarjeta de red.
     - Instalador (driver) de la tarjeta de red.
   - **Acciones:**
     - Re configuración de la tarjeta de red redundante.
     - Pruebas.
     - Posteriormente:
       - Instalación de la tarjeta de red.
       - Configuración de la tarjeta de red.
       - Pruebas.
       - Re configuración de la tarjeta de red redundante (estado de stand by).
     - Luz verde.

3. **Inoperatividad del Servidor causada por daño severo en el disco duro**
   - **Reconocimiento:**
     - Mensajes de error de volumen en la consola del servidor.
     - Mensajes de error de E/S en la consola del servidor.
     - Mensajes de error en el disco en la consola del servidor.
   - **Severidad:** Crítica
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
   - **Recursos:**
     - Instalador del SO de la red.
     - Instalador de las aplicaciones o sistemas de software.
     - Última copia de seguridad de los datos.
     - Disco duro alternativo de la misma tecnología que el disco duro dañado de repuesto, el mismo que está en estado de stand-by.
   - **Acciones:**
     - Retiro del disco duro dañado e instalación del disco duro de repuesto.
     - Instalación del SO de la red.
     - Configuración de opciones de red y direcciones IP.
     - Configuración de recursos compartidos.
     - Configuración de grupos de usuarios y usuarios.
     - Instalación de las aplicaciones.
     - Restauración de los datos.
     - Pruebas.
     - Luz verde
     - Pruebas.

4. **Corrupción de índices en las tablas de la BD de una aplicación**
   - **Reconocimiento:**
     - Mensajes de error de índice dada por la aplicación:
       - La tabla no está ordenada
       - Índices duplicados
       - Parte de los registros inaccesibles a pesar que tiene la certeza que existen
   - **Severidad:** Crítica
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
     - Personal autorizado
       - Girador(a) de O/C – UC
       - Girador(a) de comprobantes de pago – UT
   - **Recursos:**
     - Utilitarios de la propia aplicación.
     - Software utilitario ya instalado para ese propósito.
   - **Acciones:**
     - Cerrar todas las tablas de la BD que pudieran haber quedado abiertas, haciendo uso por ejemplo de la consola del servidor.
     - Si requerido, cerrar todas las sesiones que estén conectadas con la BD.
     - Realizar copia de seguridad de los datos.
     - Ejecutar los utilitarios de la aplicación ó el utilitario previamente instalado en las opciones correspondientes a generación de índices, recreación de índices, reindexamiento, ó mantenimiento de archivos.
     - Pruebas.
     - Luz verde

5. **Inconsistencias en los datos de una aplicación**
   - **Reconocimiento:**
     - Valores de consolidados desfasados.
     - Saldos desfasados.
   - **Severidad:** Crítica
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
     - Personal autorizado de apoyo:
       - Girador(a) de O/C – UC
       - Girador(a) de Comprobantes de Pago – UT
   - **Recursos:**
     - Utilitarios de la misma aplicación.
   - **Acciones:**
     - Cerrar todas las tablas de la BD que pudieran haber quedado abiertas.
     - Si requerido, cerrar todas las sesiones que estén conectadas con la BD.
     - Realizar copia de seguridad de los datos.
     - Ejecutar los utilitarios de la misma aplicación, referentes a mantenimiento de archivos y de "refrescar".
     - Pruebas.
     - Luz verde

6. **Corrupción de tablas en el SIAF**
   - **Reconocimiento:**
     - Mensajes de tabla "xxx" dañada al estar realizando alguna de la siguientes tareas en el SIAF:
       - transmisión de información entre SIAF-DIGA (Cusco) y MEF (Lima)
   - **Severidad:** Moderada
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
     - Residente del SIAF
   - **Recursos:**
     - Utilitarios de la propia aplicación:
       Corrige_la_tabla_esta_dañadas_y_debe_repararse.exe
   - **Acciones:**
     - Cerrar todas las tablas de la BD que pudieran haber quedado abiertas, a través de la consola del servidor.
     - Si requerido, cerrar todas las sesiones que estén conectadas con la BD, a través de la consola del servidor.
     - Realizar copia de seguridad de los datos.
     - Ejecutar el utilitario de la aplicación.
     - Pruebas.
     - Luz verde

7. **Duplicidad de índices en las tablas del SIAF**
   - **Reconocimiento:**
     - Mensajes de "violación de unicidad de clave" en la tabla "xxx" al estar realizando alguna de la siguientes tareas en el SIAF:
       - transmisión de información entre SIAF-DIGA (Cusco) y MEF (Lima)
       - contabilizaciones
   - **Severidad:** Moderada
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
     - Residente del SIAF
   - **Recursos:**
     - Utilitarios de la propia aplicación:
       Repara_Duplicidad_de_Indices.exe
     - Archivo de texto:
       Tabla_Reparar.txt
   - **Acciones:**
     - Cerrar todas las tablas de la BD que pudieran haber quedado abiertas, a través de la consola del servidor.
     - Si requerido, cerrar todas las sesiones que estén conectadas con la BD, a través de la consola del servidor.
     - Realizar copia de seguridad de los datos.
     - Editar el archivo de texto y solamente tipear lo siguiente:
       nombre_de_la_tabla.DBF
     - Ejecutar el utilitario de la aplicación.
     - Pruebas.
     - Luz verde

8. **Inoperatividad de una PC o Estación cliente**
   - **Reconocimiento:**
     - Diferentes mensajes ó señales del mal funcionamiento de la PC ó estación cliente.
   - **Severidad:** Moderada
   - **Posibilidad de ocurrencia:** Baja a mediana
   - **Rol(es):**
     - Responsable del CC-DIGA
     - Personal autorizado de apoyo:
       - Girador(a) de Comprobantes de Pago – UT
   - **Recursos:**
     - Experiencia
     - Software utilitario de diagnóstico.
   - **Acciones:**
     - Diagnóstico.
     - Curso a seguir (existen varias posibilidades de acuerdo al diagnóstico).
     - Se puede ejecutar acciones tales como:
       1. Recuperar la información propia del usuario si posible y si necesaria.
       2. Re-instalar o instalar el software dañado.
       3. etc.
     - Otras acciones a ejecutar podrían ser:
       1. Reparar, cambiar la(s) parte(s) dañada(s) si posible ó solicitar la reparación y/o mantenimiento a través de terceros llevando a cabo la solicitud correspondiente a la UMSA (Unidad de Mantenimiento y Servicios Auxiliares).
       2. etc.
     - Hacer recomendaciones del caso si fuera necesario.

9. **Interrupción general repentina del suministro de energía eléctrica que afecte directamente al servidor y eventualmente a los switches de borde**
   - **Reconocimiento:**
     - Sonido de alerta emitido por los UPS que protegen a los servidores.
   - **Severidad:** Moderada a crítica
   - **Posibilidad de ocurrencia:** Baja
   - **Rol(es):**
     - Responsable del CC-DIGA
     - Oficina de Ingeniería de Obras
     - Personal autorizado
     - Usuarios
   - **Recursos:**
     - UPS on-line.
   - **Acciones:**
     - En el servidor cerrar todas las tablas de las BDs que pudieran haber quedado abiertas.
     - En el servidor cerrar todas las conexiones.
     - Proceder al apagado normal de los servidores.
     - Proceder al apagado de los switches de red.
     - Proceder al apagado del UPS.
     - Coordinar con la Oficina de Ingeniería de Obras sobre la solución de la falta de energía eléctrica y si necesario lleve a cabo las gestiones correspondientes con el proveedor local de la energía eléctrica.
     - Esperar al retorno de la energía eléctrica.
     - Encender primero el UPS.
     - Encender los switches de red.
     - Encender los servidores.

- Pruebas.
- Luz verde

10. **Interrupción de la transmisión de la información entre el SIAF-DIGA y el MEF**
    - **Reconocimiento:**
        - Mensajes de error de transmisión de datos entre el SIAF-DIGA (Cusco) y el MEF (Lima).
        - Mensajes de que no se encontró el servidor del MEF ó no se pudo validar el usuario.
    - **Severidad:** Moderado a Crítico
    - **Posibilidad de ocurrencia:** Baja
    - **Rol(es):**
        - Responsable del CC-DIGA
        - Residente del SIAF
    - **Recursos:**
        - Canal de comunicación a través de Internet (el mismo que ya previamente configurado y coordinado con la RCU-UNSAAC).
        - Línea telefónica directa en la oficina del SIAF-UNSAAC no compartida.
        - Canal de comunicación a través de módem (acceso telefónico a redes) (el mismo que ya fue configurado con las conexiones de acceso telefónico TCI – infovia y TCI - router).
    - **Acciones:**
        - Acceder a la configuración de la transmisión de datos del SIAF.
        - Cambiar el orden de uso del canal de comunicación de modo tal que quede como primera opción el canal que no se estaba usando por defecto y del cual se presume que está full operativo, y que quede como segunda opción el canal actual que en ese momento estaba interrumpido o con problemas.
        - Pruebas.
        - Si a pesar de estas acciones la comunicación no se restableciera, llevar a cabo las coordinaciones del caso con la Residente del SIAF en el Cusco y/o con el soporte del SIAF en Lima. También se deberá evaluar la posibilidad de que los canales de comunicación del proveedor de servicio de telefonía y de Internet local se hubiera "caído"; en este caso si posible se realizarán las coordinaciones con este proveedor y se deberá esperar hasta que el servicio del proveedor de telefonía e Internet se restablezca.
        - Pruebas.
        - Luz verde

11. **Ralentización de la transmisión de la información entre el SIAF-DIGA y el MEF**
    - **Reconocimiento:**
        - Tiempos de transmisión de datos excesivamente largos entre el SIAF-DIGA (Cusco) y el MEF (Lima).
    - **Severidad:** Moderado a Crítico
    - **Posibilidad de ocurrencia:** Baja
    - **Rol(es):**
        - Responsable del CC-DIGA
        - Residente del SIAF
    - **Recursos:**
        - Canal de comunicación a través de Internet (el mismo que ya previamente configurado y coordinado con la RCU-UNSAAC).
        - Línea telefónica directa en la oficina del SIAF-UNSAAC no compartida.

- Canal de comunicación a través de módem (acceso telefónico a redes) (el mismo que ya fue configurado con las conexiones de acceso telefónico TCI - infovia y TCI - router).

- **Acciones:**
  - Acceder a la configuración de la transmisión de datos del SIAF.
  - Cambiar el orden de uso del canal de comunicación de modo tal que quede como primera opción el canal que no se estaba usando por defecto y del cual se presume que está full operativo, y que quede como segunda opción el canal actual que en ese momento estaba lento.
  - Pruebas.
  - Luz verde

12. **Inoperatividad del módem que transmite la información al MEF**
    - **Reconocimiento:**
      - Mensajes de error de Módem.
      - Mensaje de ausencia de tono de discar.
    - **Severidad:** Moderado a Crítica
    - **Posibilidad de ocurrencia:** Baja
    - **Rol(es):**
      - Responsable del CC-DIGA
      - Personal autorizado de apoyo:
        - Girador(a) de Comprobantes de Pago – UT
    - **Recursos:**
      - Módem USB alternativo de respaldo.
      - Configuración del módem en la PC que realiza las transmisiones de datos del SIAF (configuración ya llevada a cabo con anterioridad).
    - **Acciones:**
      - Conectar el módem a un puerto USB.
      - Si fuera necesario ajustar la configuración del módem al puerto USB utilizado.
      - Cambiar las configuraciones del acceso telefónico a redes para que utilice este módem alternativo.
      - Pruebas.
      - Luz verde

13. **Ralentización ó intermitencia de la interacción entre los usuarios y las aplicaciones**
    - **Reconocimiento:**
      - Interacción con las aplicaciones demasiado pesada.
    - **Severidad:** Moderada
    - **Posibilidad de ocurrencia:** Baja
    - **Rol(es):**
      - Responsable del CC-DIGA
      - Personal autorizado de apoyo:
        - Girador(a) de O/C – UC
        - Girador(a) de Comprobantes de Pago – UT
    - **Recursos:**
      - Utilitarios de la misma aplicación para mantenimiento y/o depuración de la BD y recreación de índices.
      - Otros utilitarios para el mantenimiento de las BDs.
      - Experiencia.
    - **Acciones:**
      - Llevar a cabo el fin de sesión de los usuarios de la aplicación.
      - Si necesario, en el servidor cerrar todas las conexiones.
      - Si necesario, realizar una copia de respaldo de la BD.

- Si necesario y dable, revisar el directorio de la aplicación y borrar los todos los archivos temporales.
- Si necesario, ejecutar los utilitarios.
- Pruebas.
- Luz verde

14. **Incendio en las instalaciones de la DIGA**
    - **Reconocimiento:**
        - Fuego, humo y/o emanación de gases tóxicos.
    - **Severidad**: Crítica
    - **Posibilidad de ocurrencia:** Baja
    - **Rol(es):**
        - Todo el personal de la DIGA
    - **Recursos:**
        - Extintores.
        - Capacitación en el uso de extintores a todo el personal de la DIGA.
    - **Acciones:**
        - Tomar el extintor y usarlo en la zona del incendio.
        - Desconectar y retirar los equipos críticos de la zona del incendio (si posible).
        - Si necesario, llamar a los bomberos.
        - Una vez controlado el incendio, llevar a cabo una evaluación de daños.
        - Estimar el tiempo de recuperación de la operatividad de la zona siniestrada.
        - Llevar a cabo las acciones del caso, para restaurar la operatividad de la zona siniestrada.
        - Luz verde.

15. **Incendio en las instalaciones del CC-DIGA**
    - **Reconocimiento:**
        - Fuego, humo y/o emanación de gases tóxicos.
    - **Severidad**: Crítica
    - **Posibilidad de ocurrencia:** Baja
    - **Rol(es):**
        - Responsable del CC-DIGA
        - Persona del Trámite Documentario de la DIGA
        - Todo el personal de la DIGA
    - **Recursos:**
        - Extintores.
        - Capacitación en el uso de extintores a todo el personal de la DIGA.
    - **Acciones:**
        - Tomar el extintor y usarlo en la zona del incendio.
        - Enviar el mensaje de "Salir de la red y apagar las computadoras" (si el tiempo lo permite).
        - Cerrar las conexiones y apagar el servidor (si el tiempo lo permite).
        - Desconectar y retirar el servidor y otros equipos críticos de la zona del incendio (si posible y si el tiempo lo permite), tomando en cuenta la magnitud del incendio.
        - Si necesario, llamar a los bomberos.
        - Una vez controlado el incendio, llevar a cabo una evaluación de daños.
        - Estimar el tiempo de recuperación de la operatividad de la zona siniestrada.
        - Llevar a cabo las acciones del caso para restaura la operatividad de la zona siniestrada.

16. **Caso de Virus en la PC ó Estación Cliente**
    - **Reconocimiento:**
        - Mensajes de virus detectado y no eliminado emitido por el software antivirus instalado.
        - Ralentización de la interacción del usuario con el equipo.
        - Cambios inesperados en los directorios de archivos.
        - Grupos de archivos de documentos que muestran el mismo tipo de corrupción.
        - Cambio del año del sistema, mientras la fecha aparentemente permanece correcta.
        - Al intentar ejecutar la aplicación del antivirus mensaje que "*otro programa está siendo utilizando este archivo*".
        - Al intentar ejecutar alguna utilidades del sistema que "*otro programa está siendo utilizando este archivo*".
        - Cambio inesperado en la página Web por defecto al iniciar un navegador, comúnmente página en idioma "chino".
        - Opcionalmente mensajes de ataques de virus en la PC de monitoreo del Responsable del CC-DIGA.
    - **Severidad**: Moderada
    - **Posibilidad de ocurrencia:** Medio
    - **Rol(es):**
        - Responsable del CC-DIGA
        - Personal autorizado de apoyo:
            - Girador(a) de Comprobantes de Pago – UT
    - **Recursos:**
        - Software antivirus diferente al instalado y en el cual se tenga confianza.
        - Experiencia.
    - **Acciones:**
        - Verificar si la PC cliente tiene actualizado su registro de virus a la fecha del día.
        - Verificar si el antivirus ya no actualiza el registro de virus:
            - Por caducidad de la licencia
            - Por Usuario y contraseña inválidos
            - Clave ó llave en la "lista negra".
        - Si necesario, desconectar físicamente la PC cliente de la red.
        - Instalar el software antivirus alternativo.
        - Actualizar el registro de virus vía Internet (si posible) ó a través de la copia de sus files de actualización en la PC cliente.
        - Ejecutar el software antivirus.
        - Evaluar los resultados de desinfección mostrados por el software antivirus.
        - Llevar a cabo las siguientes evaluaciones:
            - Evaluar el QUIEN y el COMO de estos eventos.
            - Evaluar el porque el software antivirus originalmente instalado no cumplió a cabalidad su trabajo.
            - Evaluar la posibilidad de que la fuente de la infección esté fuera del control de la red administrativa.
        - Hacer seguimiento a la capacidad de desinfección del antivirus originalmente instalado.
        - Tomar las decisiones el caso en base a los resultados de las diferentes evaluaciones llevadas a cabo.

17. **Caso de Robo común**
    - **Reconocimiento:**
        - Falta comprobada del dispositivo ó accesorio informático, ó útil de oficina.
    - **Severidad**: Moderada
    - **Posibilidad de ocurrencia:** Muy Bajo
    - **Rol(es):**
        - Usuario afectado
        - Responsable del CC-DIGA
    - **Recursos:**
        - Ninguno.
    - **Acciones:**
        - Reportar el robo al Jefe inmediato superior y a la Dirección General de Administración.
        - De acuerdo a la magnitud del robo, solicitar la investigación correspondiente.
        - En caso que se trate de elementos informáticos, evaluar las medidas de seguridad física y de control del acceso físico a las oficinas. Tomar las decisiones el caso en base a los resultados de las evaluaciones llevadas a cabo.

Anexos

Glosario de términos:

Análisis de riesgo:
Estudio sistemático para analizar cuales son los riesgos relativos a la calidad y a la seguridad a los que se encuentra sometido un proceso en una organización, sus costes asociados y las contramedidas más eficientes para reducir o eliminar los riesgos identificados.

Backup:
ver Copia de seguridad.

Confidencialidad:
Condición que asegura que la información no pueda estar disponible o ser descubierta por las personas, las entidades o los procesos no autorizados.

Contraseña:
Palabra clave que identifica al usuario para proteger el acceso a un equipo, a una aplicación ó a un módulo de una aplicación.

Copia de seguridad:
Replicación periódica y almacenamiento externo (usualmente en discos, CDs, memorias USB, etc.) de datos y programas en previsión de posibles contingencias. Reproducción de los datos actuales guardados en un soporte informático, para tenerlos disponibles en caso de que un desastre del sistema impida recuperar los datos con los que se está trabajando.

Dispositivo de almacenamiento:
Elemento físico que almacena información de forma permanente.

Experiencia:
La capacidad, conocimiento y "know how" que poseen los expertos en un determinado dominio que les permite llevar a cabo eficientemente una tarea.

Medio de almacenamiento:
ver Dispositivo de almacenamiento.

Parche:
Código que aplicado a un programa, modifica el funcionamiento de este, bien para solucionar un problema, o bien para dotarlo de funcionalidad adicional.

Password:
ver Contraseña.

Plan de contingencias:
Es un documento que establece una estrategia de respuesta para atender en forma oportuna, eficiente y eficaz, un desastre, evento natural u otros, por culpa de algún incidente tanto interno como externo a la Institución. En el se definen las responsabilidades de la entidades y persona que intervienen en la operación, se provee información básica sobre posibles áreas afectadas y recursos susceptibles de sufrir interrupción en el funcionamiento. También sugiere cursos de acción para hacer frente al evento presentado, de manera que se permita racionalizar el empleo de personal, equipos e insumos disponibles, para proteger en su orden: la vida humana (empleados), la infraestructura, bienes (de la Institución y de terceros) y el ambiente (recursos: agua, aire, suelo, flora y fauna).

Política de seguridad:
Conjunto de principios y reglas, propias de la organización, que declaran como se especificará y gestionará la protección de los activos de información de una manera consistente y segura.

----- 0 -----