PLAN DE CONTINGENCIA PAR A PREVER Y PÉRDIDA DE LA INFORMACIÓN

FUNDACION MULTIACTIVA ROBINSON DE LA HOZ

El Plan de Contingencia Informático implica un análisis de los posibles riesgos a los que pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde al Centro de Informática y Telecomunicaciones, aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos. El alcance de este plan guarda relación con la infraestructura informática, así como los procedimientos relevantes asociados con las diversas aplicaciones tecnológicas. La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la entidad. Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con las diferentes maquinas o equipos computacionales (entrada de datos, generación de reportes, consultas, etc.).
El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica para prevenir posibles desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre, ya que esta es uno de los activos más importantes de en una empresa, entidades o personas naturales, razón por la que es de mucha importancia contar con un plan de contingencia ya que siempre va existir la posibilidad de desastre, pese a todas nuestras medidas de seguridad. Es necesario que El Plan de Contingencia Informático incluya medidas de recuperación de forma rápida y eficiente al menor costo y perdidas posibles.

El plan de Contingencia indica las acciones que deben tomarse inmediatamente tras la pérdida, un primer aspecto importante del plan es la organización de las medidas de seguridad, en el que estén detallados los nombres y la responsabilidad de cada uno de los usuarios en sus puestos de trabajos. El segundo aspecto es contar con las directrices de respaldo de información a través de copias de seguridad en medios externos (Backus en discos duros, en la web), siendo estos elementos primordial y necesario para la recuperación.
La base principal de este plan es prever la vulneración de la información, estableciendo prioridades claras sobre qué tipo de procesos son los más esenciales, y poder identificar los recursos necesarios para garantizar el funcionamiento óptimo de las aplicaciones.
Además debe ser comprobado de forma periódica para detectar y eliminar problemas. La manera más efectiva de comprobar si un plan de prevención funciona correctamente, es programar simulaciones de desastres. Los resultados obtenidos deben ser cuidadosamente revisados, y son la clave para identificar posibles defectos.

DESCRIPCIÓN
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. Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y la estrategia a seguir para señalar con precisión, por ejemplo: ¿Qué componente ha fallado?, ¿Cuál es el dato o archivo con información se ha perdido, en que día y hora se ha producido y cuan rápido se descubrió? 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), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable.

Frente al mayor de los desastres solo queda el tiempo de recuperación, lo que significa adicionalmente la fuerte inversión en recursos humanos y técnicos para reconstruir su Sistema de Red y su Sistema de Información.
Hoy en día la materia prima de toda organización es su información, básicamente su "data" y el gran problema de toda organización es su implementación de seguridad informática, ya sea a nivel de hardware o software, para que la información no sea robada ni manipulada con fines maliciosos.
La protección de la información vital ante la posible pérdida, destrucción, robo y otras amenazas de una empresa, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático, el cual indica las acciones que deben tomarse inmediatamente tras el siniestro que se presente.

SEGURIDAD DE LA INFORMACIÓN
Es importante considerar la seguridad informática tanto desde el punto de vista físico como desde el lógico. La seguridad física se refiere a la seguridad de los componentes mismo de un equipo informático (HARDWARE), a la seguridad lógica se refiere a la seguridad de la información y los programas de almacenamiento en un equipo o una red de datos.
La Seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen institucional de las empresas, incluso la vida privada de personas. Es obvio el interés creciente que día a días se evidencia sobre este aspecto de la nueva sociedad informática. Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.
La Seguridad de información tiene tres directivas básicas que actúan sobre la Protección de Datos, las cuales ejercen control de:
La lectura
Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales y mantenimiento de la seguridad en el caso de datos institucionales.
La escritura
Es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad que se les ha confiado.
El empleo de esa información
Es Secreto de logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos.
Por otro lado, es importante definir los dispositivos de seguridad durante el diseño del sistema y no después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

Sistema de Red de Computadoras en Funmurobin

La Red de la fundación cuenta con Tecnologías de la información referente a: sistemas de comunicación, sistemas de información, conectividad y servicios Informáticos que se brinda de forma interna y externa a las diferentes dependencias que guardan relación con el contenido contractual celebrado con el ICBF a través de correos electrónicos, bases de datos, información en medios físicos o dispositivos digitales, conexión remota entre otras.

PLAN DE REDUCCIÓN DE RIESGOS

El presente documento implica la realización de un análisis de todas las posibles causas a los cuales puede estar expuestos nuestros equipos, así como la información contenida en cada medio de almacenamiento, por lo que se busca evitar al máximo de ocurrencia de riesgos que puedan ocasionar pérdida o daños en la información, y en el peor de los escenarios, saber tomar las acciones adecuadas en la etapa preventiva, correctiva y de recuperación. El Plan de Reducción de Riesgos es equivalente a un Plan de Seguridad, en la que se considera todos los riesgos conocidos, para lo cual se hará un Análisis de riesgos.

Análisis de Riesgos

El presente realiza un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos.

Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal
b) Hardware
c) Software y utilitarios
d) Datos e información
e) Documentación
f) Suministro de energía eléctrica
g) Suministro de telecomunicaciones

Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la compañía son:

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistemas computacionales
- Desastres Naturales:
  a) Movimientos telúricos
  b) Inundaciones

c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario)

- Fallas de Personal Clave: por los siguientes inconvenientes:
  a) Enfermedad
  b) Accidentes
  c) Renuncias
  d) Abandono de sus puestos de trabajo
  e) Otros.

Fallas de Hardware: a) Falla en los Servidores (Hw) b) Falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall)

Análisis en las fallas en la Seguridad

En este se abarca el estudio del hardware, software, la ubicación física de la estación su utilización, con el objeto de identificar los posibles resquicios en la seguridad que pudieran suponer un peligro.

Las fallas en la seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona, de ahí que resulte obvio el interés creciente sobre este aspecto. La seguridad de la información tiene dos aspectos importantes como:

- Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.
- Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

Protecciones actuales

Se realizan las siguientes acciones:

- Se hace copias de los archivos que son vitales para la institución.
- Al robo común se cierran las puertas de entrada y ventanas
- Al vandalismo, se cierra la puerta de entrada.
- A la falla de los equipos, se realiza el mantenimiento de forma regular.
- Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus.
- A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados.
- A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente Plan de contingencias da pautas al respecto.
- Al acceso no autorizado, se cierra la puerta de entrada. Varias computadoras disponen de claves de bloqueo del usuario.
- Al robo de datos, se cierra la puerta principal y gavetas de escritorios o closet donde se guardan los dispositivos de respaldo de copias de seguridad.

BLANCA DE LA HOZ VALENCIA
Representante Legal

ALEXANDER ROJAS CHAVEZ
Dpto. de Sistemas y Recursos Informáticos