UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

LA FACULTAD DE ECONOMÍA.
"Vasco de Quiroga"

"Green Data Center"

Presenta

PLAN DE CONTINGENCIA DE SEGURIDAD INFORMÁTICA

RESPALDOS DE INFORMACIÓN Y RECUPERACIÓN DEL DESASTRE

2018 – 2019

Facultad de Economía
"Vasco de Quiroga"

Elaborado por: Prof. Carlos Urquiza Villegas (MCSE)
Servicio Social: C.L.E. Benito Tapia Gálvez
Morelia, Mich., a 16 de mayo de 2018

ÍNDICE

==========

PRESENTACIÓN

Este propuesta de trabajo, trata sobre implantar un “Plan de Contingencia de Seguridad Informática”, Respaldos de Información y Recuperación del Desastre dentro de la Facultad de Economía “Vasco de Quiroga”.

Se hace esta propuesta, después de haber hecho un análisis minucioso de los posibles riesgos a los cuales pueden estar expuestos los controles de Dominios computacionales, los equipos de cómputo y los sistemas de información que abastecen los centros de cómputo y de comunicaciones de redes - “Intranet y extranet” de la Facultad de Economía “, y en consecuencia dentro y fuera del Campus de la Universidad Michoacana de San Nicolás de Hidalgo.

Corresponde al Departamento de Sistemas de Información (DSI) de la FEVaQ, implantar e instrumentar estos planes como medidas de seguridad para proteger datos e información relevantes al quehacer académico y administrativo de la facultad y estar preparados para afrontar desde un siniestro hasta una contingencia informática en general.

El alcance de estos planes guardan relación con la infraestructura informática actual, así como los procedimientos relevantes asociados con la plataforma tecnológica. La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Facultad de Economía. Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal del DST realiza frecuentemente al interactuar con sus propios Controles de Dominio siendo estos: www.economia.umich.mx, www.economia.umich.mx/cursos, http://www.posgradofevaq.mx/joomla15/ y www.greendatacenter.umich.mx, estos con sus respectivos directorios activos y cuentas de acceso a áreas de datos públicos y privados como la generación de reportes y listados y consultas virtuales a la biblioteca universitaria por parte de toda una comunidad de usuarios autentificados.

Este Plan de Contingencia y Seguridad Informática está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de pérdida de datos, estableciendo medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por errores humanos.

La información como uno de los activos más importantes de la Facultad de Economía, es el fundamento más importante de estos dos palanes: el de contingencia de seguridad informática y, el de recuperación del desastre y restauración del sistema de resguardos.

Al existir estas posibilidades de desastres y pese a todas nuestras medidas de seguridad, es necesario que estos dos planes de contingencia de seguridad se definan como un objetivo importante para poder así restaurar las bases de información como corregir y mejorar también los servicios de soporte técnico y de comunicación dentro y fuera de la facultad de forma más rápida, eficiente y con el menor costo de pérdidas de datos posibles a profesores, estudiantes y administrativos.

RESUMEN

La protección de la información es vital ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de planes completos de contingencia de seguridad informática como también un sistema de recuperación de operaciones computacionales.

Los planes nos indican las acciones que deben tomarse inmediatamente tras un desastre. Un primer aspecto importante de estos dos planes, es la organización de la contingencia en el que se detallan los nombres de los responsables y las responsabilidades del equipo de trabajo. El segundo aspecto crítico de estos planes, son las acciones y la preparación del plan de recuperación y restauración del sistema de respaldos ya cronometrados" o (Backups), como el sistema de comunicación web y en el línea, elementos primordiales y necesarios para la recuperación total de los Dominios. El tercer aspecto, es la preparación de un plan de recuperación temporal, otro parcial y un total, donde se establecen las prioridades reales de tiempo y forma, afectando así las posibilidades más críticas dentro de un periodo de tiempo aceptable. Otro aspecto importante de los planes de contingencia y de recuperación, es identificar el equipo de soporte técnico, los nombres, números de teléfono, asignaciones específicas, necesidades de formación y otros datos esenciales, para cada miembro de este equipo que participa, sepa de forma explícita los pasos a seguir .

La base del plan de contingencia de seguridad informática y su posterior recuperación, es establecer prioridades claras sobre qué tipo de procesos son los más esenciales. Es necesario por tanto la identificación previa de cuáles de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

El Plan de Recuperación del Desastre (PRD), provee mecanismos de recuperación para los registros vitales, sistemas alternativos de operación y comunicaciones, evacuación de personal, fuente alternativa de provisión de servicios, debe ser comprobado de forma periódica para detectar y eliminar

problemas posteriores. La manera más efectiva de comprobar si un PRD funciona correctamente, es programar simulaciones de desastres. Los resultados obtenidos deben ser cuidadosamente revisados y son la clave para identificar posibles defectos en el plan de contingencia de seguridad y manejo de la Información dentro de la FEVaQ.

Este plan de contingencia debe contemplar los planes de emergencia, respaldos, recuperación y comprobación, mediante un simulador de mantenimiento predictivo, preventivo y correctivo. Dos planes de contingencia adecuados, deben ayudar a la facultad a recobrar rápidamente el control y capacidades para procesar información y restablecer la marcha normal de todos los sistemas operativos con dominios y las unidades organizacionales que componen.

¿Cuál es el grado de preparación de la “FEVaQ”; Para estos desastres, las contingencias han demostrado que la capacidad de recuperarse ante ellos es crucial para la supervivencia física, mental y emocional de sus usuarios finales.

La dirección de la FEVaQ, deberá comprender los principales riesgos y las posibles consecuencias de un desastre de pérdida de información. Un plan de contingencias adecuado, identifica las necesidades de todas las áreas y departamentos involucrando a “**TODO”** el personal de la FEVaQ.

CAPITULO I. ANÁLISIS DE LA SITUACIÓN INFORMÁTICA ACTUAL EN LA FACULTAD DE ECONOMÍA.

1.1. Introducción

Los planes de contingencia de seguridad y de recuperación de la Información, serán para la Facultad de Economía, un instrumento de gestión para el buen funcionamiento y administración de las TIC´s en los Dominios: www.economia.umich.mx/respaldos y el Centro de Datos Verde de la FEVaQ bajo el nombre: www.greendatacenter.umich.mx junto con el soporte técnico interno.

Estos planes contienen las medidas técnicas y organizativas necesarias para garantizar la recuperación de datos y el levantamiento del sistema en operación, como también la continuidad y el acceso a la información generada y respaldada dentro de la facultad; Propuesta hecha por el Departamento de Sistemas y Tecnologías (DST).

Otras escuelas y facultades como la propia Universidad Michoacana de San Nicolás de Hidalgo, pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías dentro de las instituciones académicas como en las organizaciones modernas, los planes de contingencia de Seguridad Informática y de recuperación del desastre serán los más relevantes a considerar e implementar.

Los planes de contingencia de seguridad informática y recuperación, seguirán el ciclo de vida iterativo PDCA (plan-do-check-act, es decir planificar-hacer-checar y actuar), nacerá de un análisis de contingencias, donde, entre otras amenazas se identificarán los riesgos que afecten a toda la comunidad de la FEVaQ.

Estos planes deberán ser revisados periódicamente, generalmente la revisión será consecuencia de un nuevo análisis de riesgos. En cualquier caso, estos planes de de seguridad y de recuperación, siempre son cuestionados cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces.
- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces.

El plan de contingencia, comprenderá tres sub-planes. Cada uno determinará las contramedidas necesarias en cada momento de las amenazas:

- **El plan de respaldos.** Contempla las medidas preventivas **antes** de que suceda una amenaza, su finalidad es evitar dicho suceso.
- **El plan de emergencia.** Contempla las contramedidas necesarias durante la amenaza, su finalidad es paliar los efectos adversos de la amenaza.

- **El plan de recuperación.** Contempla las medidas necesarias **después** de la materializada y controlada la amenaza, su finalidad es restaurar el estado de los datos tal y como se encontraban antes del siniestro.

Estos planes de contingencia de seguridad, también contemplan someramente las siguientes contramedidas:

Medidas técnicas:

- Extintores contra incendios
- Detectores de humo
- Salidas de emergencia
- Dispositivos informáticos de respaldo

Medidas organizativas:

- Seguro de incendios
- Equipo informático de soporte técnico y ubicación alternativa
- Procedimiento de copias de respaldo
- Procedimiento de actuación en caso de incendio o explosión

Medidas humanas:

- Formación para actuar en caso de siniestros
- Designación de un coordinador del departamento
- Asignación de roles y responsabilidades para las copias de respaldo

Los sub-planes contendrán las siguientes previsiones:

- Plan de respaldo
- Revisión de extintores
- Simulacro de incendio y escape
- Realización de copias de respaldo

Nuestro sistema de red de computadoras (ordenadores, periféricos y dispositivos móviles), están expuestos a riesgos de afectación y contaminación convirtiéndose así en fuente de problemas. El Hardware y 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 que se ha perdido, en que día y hora se ha producido y que tan 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 (discos duros, memorias USB etc.), 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 es una fuerte inversión en recursos humanos y técnicos para recuperar la Intranet o sistema de red e información de bases de datos.

1.2. Importancia del Plan de Contingencia de Seguridad Informática

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y el Control de Dominios locales que son: http://www.economia.umich.mx, www.economia.umich.mx/cursos, www.posgradofevaq.mx/joomla15 y www.greendatacenter.umich.mx, Garantizar la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de cuentas de usuarios autentificados e información de las bases de datos.
- Permite realizar un conjunto de acciones con el fin de evitar fallos, o en su caso, disminuir las consecuencias que de él se puedan derivar.
- Permite realizar un análisis de riesgos, respaldo de datos y su posterior recuperación de los mismos.

En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso dentro de la FEVaQ. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría un daño importante para la facultad.

1.3. Sistema de Red Intranet / Extranet de Comunicaciones en la FEVaQ.

La red de la FEVaQ, cuenta con tecnologías de la información y de comunicaciones en lo referente a sistemas de cómputo, sistemas de información, conectividad y servicios de soporte técnico que se brindan de forma permanente a toda la comunidad.

Se resume que la administración de la red Intranet se divide en dos rubros: 1).- La conectividad: Que se encarga de la conexión local e inalámbrica de los dispositivos periféricos, y 2).- El manejo de servidores: Que se encarga de hospedar todos los servicios y sistemas de comunicación interna y externa.

Los servicios de red de comunicaciones y soporte técnico implementados dentro de la Facultad de Economía son implementados en sus servidores, y son los siguientes:

- Servidor de Correo Electrónico – Google App @.net (?)
- Servidor de Seguridad Respaldos Cronometrados - (Pendientes)
- Servidor de Seguridad a Base de Datos (Cuentas de usuarios)
- Servidor de Telefonía IP. (Conmutador de llamadas)
- Servidor de Políticas de Grupo – Controlador de Dominios
- Directorio Activo de usuarios y cuentas autentificadas
- Soporte técnico general - Predictivo, Preventivo y Correctivo

CAPITULO II. PLAN DE REDUCCIÓN DE RIESGOS

El presente análisis, implica la realización de un estudio de todas las posibles causas a las cuales puede estar expuesto nuestro equipo conectado a la red universitaria, así como la información contenida en cada medio de

almacenamiento. Se realizará un análisis de riesgo y el plan de operaciones tanto para reducir la posibilidad de ocurrencia como para reconstruir el sistema integral de Información y/o el sistema de red de computadoras en caso de un siniestro.

Los presentes “Planes de Contingencia y Seguridad Informática y Recuperación”, incluyen la formación de equipos de trabajo durante las actividades de implementación de los planes de acción, tanto para las etapas predictivas, preventivas y correctivas 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 detallado.

2.1. 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 en general

b) Hardware y periféricos

c) Software y utilerías

d) Datos e información relevante

e) Documentación administrativa

f) Suministro de energía eléctrica (Apagones)

g) Suministro de telecomunicaciones (Conmutador)

Daños:

Los posibles daños pueden referirse a:

Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, causas naturales o errores humanos.

- 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 o lógico de información clave, procesos de información no deseado.
- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante robo, intrusión o invasión.

Fuentes de daño

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

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistema computacionales
- Desastres naturales como movimientos telúricos, inundaciones, fallas en el suministro eléctrico causadas por el medio ambiente
- Fallas de personal clave por los siguientes inconvenientes: Enfermedad, accidentes, renuncias, abandono de sus puestos de trabajo
- Fallas de Hardware, software y servidores
- Falla en los switches, cableado de la red, ruteadores o contrafuegos

Incendios

2.1.1. Características

El análisis de riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el costo de protección del área informática y medios versus el costo de volverla a reactivar.

Durante el estudio análisis de riesgo, se define claramente:

- Lo que intentamos proteger
- El valor relativo para la UMSNH/FEVaQ
- Los posibles eventos negativos que atentarían con lo que intentamos proteger.
- La probabilidad de ataques cibernéticos y la contaminación de la Intranet.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un plan adecuado.

Los criterios que usaremos para tipificar los posibles problemas son:

2.1.2. Clases de Riesgo

El factor de probabilidad por clase de riesgo en función a la ubicación geográfica de la institución y a su entorno institucional; por ejemplo, si la FEVaQ:

- Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.
- Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.
- Se ubica en zona industrial las probabilidades de “Fallas en los equipos” será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.

- Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.

Identificación de Amenazas:

Estos valores son estimados y corresponden a la apreciación de antecedentes históricos registrados en la UMSNH durante los últimos años.

Correspondería al plan de contingencia de seguridad y anti-siniestros minimizar estos índices con medidas predictivas, preventivas y correctivas sobre cada caso de riesgo, (Ver propuesta de Plan de Contingencia Anti-siniestros)…

En lo que respecta a fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios de techos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar cortos circuitos e inundaciones).

2.1.2.1. Clase de riesgo: Incendio o fuego

- Grado de Negatividad: Muy severo
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable

Situación actual y acciones predictivas, preventivas y correctivas…

El área de Servidores del DTS-FEVaQ cuenta con un extintor cargado, ubicado dentro del área de Servidores. Se cumple!

El centro y aula de cómputo de la FEVaQ ya cuentan con extintores. Verificar fechas de expiración del centro de cómputo y el aula de cómputo de la FEVaQ.

No se ejecuta un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios - lo que no es eficaz para enfrentar un incendio y sus efectos. Implantar un programa de capacitación para el manejo de extintores.

Debido al incremento del número de computadoras por departamento se hace necesario contar con extintores en los corredores de oficinas e incrementar el número de extintores por cada área.

Una probabilidad máxima de contingencia de este tipo en la FEVaQ puede alcanzar a destruir hasta un 50% de las computadoras antes de lograr controlarlo, también podemos suponer que en el área de **Servidores** tendría un impacto mínimo por las medidas de seguridad y ambiente que lo protege. Esta información permite resaltar el tema sobre el lugar donde almacenar los respaldos, (outside-backup-storage), o sea almacenamiento de respaldos externo.

El incendio a través de su acción calorífica, es más que suficiente para destruir los dispositivos de almacenamiento, tal como CD's, DV's, cartuchos, discos duros etc., las mismas que residen en una caja fuerte (medio de seguridad que nos protege frente a robo o terremoto, pero no del calor).

Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se colocaran estratégicamente en lugares distantes, con una segunda copia de seguridad custodiada en un lugar externo de la UMSNH.

Las áreas funcionales distribuidas en el campus de la UMSNH, existe al menos una computadora, por lo que se debe incrementar los elementos y medidas de seguridad contra incendios **"over all", "en todo"**.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extintores. Su uso conlleva a colocarlos cerca del las posibles áreas de riesgo que se debe proteger.

A continuación se describe el procedimiento para el uso de extinguidores en caso de incendio:

2.1.2.2. Clase de Riesgo: Robo común de equipos y archivos

- Grado de Negatividad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Moderado

Grado de Certidumbre: Aleatorio

Situación actual: Acción Predictiva

Vigilancia permanente. No existe vigilancia! La salida de un equipo informático no es registrada por el personal de la FEVaQ ni por el personal de seguridad en turno dentro de la UMSNH.

No se verifica si el **"Personal de Seguridad"** cumple con la inspección de los usuarios sobre su obligación de cerrar puertas y ventanas al finalizar su jornada. Al respecto, el **"Personal de Seguridad"** tampoco emite recomendaciones sobre medidas de alerta y seguridad.

Remitir aviso a **"Patrimonio Universitario"**, para retirar equipo informático. No se cumple!

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre el coordinador del área funcional. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

Según antecedentes de otras facultades e institutos, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la FEVaQ. Es relativamente fácil remover un disco duro del CPU, una disquetera, o tarjeta de dispositivo etc. y no darse cuenta del faltante hasta días después. Estas

situaciones se han presentado en la FEVaQ. Se recomienda siempre estar alerta. (Instalar cámaras de video).

2.1.2.3. Clase de Riesgo: Vandalismo

- Grado de Negatividad: Moderado
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable

Situación actual: Acción Preventiva

La FEVaQ se encuentra en una zona donde el índice de vandalismo es ALTO, no existe vigilancia permanente.

Se presentan casos muy aislados durante el proceso de inscripción de cursos; que no están conformes con algunas normativas académico-administrativas tal que al efectuar sus reclamos personalmente asumen actitudes retroactivas que muchas veces ofenden al trabajador y sin medir las consecuencias pueden llegar a dañar alguna instalación de la FEVaQ.

Continuar con la política de gestión de mejorar la atención de los usuarios, brindando la información previa a procesos académicos.

Alguna probabilidad de turbas producto de manipulaciones políticas. Mantener buenos vínculos y coordinaciones permanentes con la Seguridad Local.

La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.

2.1.2.4. Clase de Riesgo: Falla en los equipos

- Grado de Negatividad: Grave
- Frecuencia de Evento: Aleatorio

- Grado de Impacto: Grave
- Grado de Certidumbre: Probable

Situación actual Acción Correctiva

La red de servidores en la FEVaQ cuenta con una red eléctrica estabilizada y polarizada. Proponer un estudio para actualizar sus datos.

No existe un adecuado tendido eléctrico en algunas oficinas de la FEVaQ. Tomar previsiones económicas para implementar un adecuado tendido eléctrico.

Cada área funcional se une a la red a través gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red: los Sistemas Informáticos, teléfonos IP y mantenimiento remoto. Proteger los gabinetes y su adecuado apagado y encendido, dependen los servicios de red en el área. La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo. Ya existe mantenimiento de los equipos de cómputo.

Contar con proveedores, en caso de requerir reemplazo de piezas y de ser posible contar con repuestos.

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño.

Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos.

El equipo de aire acondicionado y ambiente adecuado en el área de servidores favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía más frecuentes:

- Fallas de energía
- Transistores y pulsos
- Bajo voltaje
- Ruido electromagnético
- Distorsión
- Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de picos
- Estabilizadores
- Sistemas de alimentación ininterrumpida (UPS)

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a tierra o puestas a tierra

Se denomina así a la comunicación entre el circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados

profundamente en tierra húmeda, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial.

La toma a tierra tiene las siguientes funciones principales: a) protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas, b) protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales., c) facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Las inspecciones deben realizarse trimestralmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los meses de verano o en tiempo de sequía. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

- Extensiones del Sistema de Distribución Eléctrica, Líneas de Transmisión y Capacidad de la Subestación.

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño

físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.
- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar; Se debe utilizar los enchufes de pared siempre que sea posible.
- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.
- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.
- Adquirir toma de corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.

Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

2.1.2.5. Clase de Riesgo: Equivocaciones

- Grado de Negatividad: Moderado
- Frecuencia de Evento: Periódico

- Grado de Impacto: Moderado
- Grado de Certidumbre: Probable
- Situación Actual: Continua la Correctiva

Las equivocaciones que se producen en forma rutinaria son de carácter involuntario. Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con el Manual de Procedimientos

Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas. En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina.

La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información. Reuniones y Actas de Trabajo para fortalecer los procedimientos.

La FEVaQ no recibe comunicación del personal de reemplazo por vacaciones por lo tanto supone que es la oficina usuaria la que tiene la capacidad reemplazante. Se debe informar al DSI del reemplazo para su registro y accesos a la red y a los sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituyen los valores originales a ambos usuarios.

Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas.

Convocar reuniones de capacitación antes nuevas opciones en los sistemas.

2.1.2.6. Clase de Riesgo: Virus informático

- Grado de Negatividad: Muy Severo
- Frecuencia de Evento: Continuo
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable

- Situación actual Acción correctiva

Se cuenta con un Software Antivirus corporativo. Pero no hay un contrato anual para su actualización. Se cumple. Se debe evitar que las licencias no expiren, se requiere la renovación de contrato anualmente.

Todo Software (oficina, desarrollo, mantenimiento, drivers, controladores etc.) es manejado por personal de DST, quienes son los encargados de su instalación en las PC's con su respectiva configuración. Se cumple.

Se tiene un programa permanente de bloqueo y acciones, como cambiar configuraciones de red, acceso a los servidores, etc. Se cumple a través de políticas de grupos.

Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de entrar a una maquina vía (dominio), se comprueba la existencia de virus en la PC. Se cumple!

En los últimos 20 años, las acciones de los virus informáticos ha sido contrarrestada con una diversidad de productos que ofrece el mercado de software. Las firmas y/o corporaciones que proporcionan software antivirus, invierten mucho tiempo en recopilar y registrar virus, indicando en la mayoría de los casos sus características y el tipo de daño que puede provocar, por este motivo se requiere de una actualización periódica del software antivirus.

2.1.2.7. Clase de Riesgo: Fenómenos naturales

- Grado de Negatividad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable
- Situación actual Acción correctiva

La última década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, aluviones, etc. Medidas de prevención.

Potencialmente existe la probabilidad de sufrir inundaciones debido a lluvias que ocurren en épocas de verano. Medidas de prevención.

Tenemos épocas fuertes lluvias (Fenómeno del Niño) que causas estragos en viviendas de material rustico. Las instalaciones de la UNP están adecuadamente protegidas, sin embargo se debe verificar el tema del suministro eléctrico. Al ocurrir un corte de energía el personal de vigilancia deberá comunicar al personal del CIT, para desconectar el sistema de red de manera preventiva.

El ambiente donde se encuentra los Servidores principales, es apropiado ante las filtraciones. Ubicación apropiada. Pero ante resultado de posibles filtraciones realizar trabajos de mantenimiento preventivo.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Computación Central, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

2.1.2.8. Clase de Riesgo: Accesos no autorizados

- Grado de Negatividad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable
- Situación actual Acción correctiva

Se controla el acceso al Sistema de Red mediante la definición de “Cuenta” o “Login” con su respectiva clave Se cumple

A cada usuario de Red se le asigna los “Atributos de confianza” para el manejo de archivos y acceso a los sistemas. Se cumple

Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera. Se cumple de modo extemporáneo, siendo lo indicado actualizar los accesos al momento de producirse el cese o cambio.

Se forman Grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos Se cumple

Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado. En algunos casos los usuarios escriben su contraseña (Red o de Sistemas) en sitios visibles. Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica.

No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves Se debe implementar

Todos los usuarios sin excepción tienen un “login” o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de cinco (5) dígitos. No se permiten claves en blanco. Además están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas en la UNP, si lo tuviere.

2.1.2.9. Clase de Riesgo: Robo de Datos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual Acción correctiva

Las Oficinas tienen disponible disqueteras, quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador. Personal de Planta debe manejar información delicada de la Oficina.

El servicio de Internet es potencialmente una ventaja abierta para el robo de información electrónica Existen políticas que regulan el uso y acceso del Servicio de Internet.

Los documentos impresos (informes, reportes, contratos, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser. Si no se toma conciencia que esta es una manera de atentar contra el Sistema Informático del UNP el problema persistirá. Resguardar la información en archivos. Destruir los reportes malogrados, sobre todo de contenido relevante. (Existen papeleros que convierten el papel en picadillo).

El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas se seguridad se impide el ingreso a los Servidores. Se cumple parcialmente

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

♣ La primera modalidad consiste en sacar “copia no autorizada” a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.

♣ La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.

♣ La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Empresarial.

2.1.2.10. Clase de Riesgo: Manipulación y Sabotaje

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual Acción correctiva

Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje La protección contra el sabotaje requiere:

- Una selección rigurosa del personal.
- 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 persona la responsabilidad de la protección de los equipos en cada área.

Existe el antecedente de origen sabotaje interno. Como es el caso de trabajadores que han sido despedidos y/o están enterados que van a ser rescindidos su contrato, han destruidos o modificado archivos para su beneficio inmediato o

futuro. Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado.

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Instituciones que han intentado implementar Programas de Seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes.

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.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática u un problema “puntual”, sino que requiere un constante y continuo esfuerzo y dedicación.

Resumen de la Clase de Riesgos

2.2. 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.

Por ejemplo, en el uso del Servicio Virtual Público de Red (VPN), implica una vía de acceso a la Red Central de UNP, la seguridad en este servicio es la validación de la clave de acceso.

2.3. 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 llave de bloqueo del teclado.

Al robo de datos, se cierra la puerta principal y gavetas de escritorios. Varias computadoras disponen de llave de bloqueo del teclado.

Al fuego, en la actualidad se encuentran instalados extintores, en sitios estratégicos y se brindara entrenamiento en el manejo de los extintores al personal, en forma periódica.

2.3.1. Seguridad de información

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 se 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.

2.3.1.1. Acceso no autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados:

Control de acceso a los Centro de Cómputo

La libertad de acceso puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que trabaja en esta oficina. Cualquier otra persona puede tener acceso únicamente bajo control.

Debemos mantener la seguridad física de la Oficina como primera línea de defensa. Para ello se toma en consideración el valor de los datos, el costo de protección, el impacto institucional por la pérdida o daño de la información. La forma propuesta de implantar el Control de Acceso al CIT, sería la siguiente:

Para personas visitantes, vigilancia otorgara el Credencial de Visitante.

Para personal de la FEVaQ, con autorización del encargado de la Oficina

Acceso limitado a computadoras personales y/o terminales de la red.

Los terminales que son dejados sin protección pueden ser mal usados. Cualquier Terminal puede ser utilizado para tener acceso a los datos de un sistema controlado.

Control de acceso a la información confidencial.

Sin el debido control, cualquier usuario encontrara la forma de lograr acceso al Sistema de Red, a una base de datos o descubrir información clasificada. Para revertir la posibilidad de ataque se debe considerar:

Programas de control a los usuarios de red

El sistema Operativo residente en los servidores de la FEVaQ es Windows 2008 y Linux Ubuntu Server 12.4 LTS. A través del Servicio de “Active Directory” permite administrar a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

Palabra de acceso (password)

Es una palabra o código que se ingresa por teclado antes que se realice un proceso.

Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. La identificación del usuario debe ser muy difícil de imitar y copiar.

El Sistema de Información debe cerrarse después que el usuario no autorizado falle tres veces de intentar ingresar una clave de acceso. Las claves de acceso no deben ser largas puesto que son más difíciles de recordar. Una vez que se obtiene la clave de acceso al sistema, esta se utiliza para entrar al sistema de Red de Información vía Sistema Operativo.

La forma común de intentar descubrir una clave es de dos maneras:

Observando el ingreso de la clave

Utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar.

En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice de forma periódica el “password” a los usuarios.

No se puede depender de un operador o responsable de terminal, que trabe la operatividad normal de la FEVaQ, por lo que será necesario establecer el procedimiento para tener un duplicado de Claves de Acceso, bajo el esquema de niveles jerárquicos en sobre lacrado.

El administrador de Redes deberá entregar al Jefe del Centro de Cómputo las claves de acceso de su personal en un sobre lacrado, debiendo registrar en un Cuaderno de Control, la fecha y motivo de algún cambio.

Niveles de Acceso

Las políticas de acceso aplicadas, deberá identificar los usuarios autorizados a emplear determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas. Cada palabra clave deberá tener asignado uno de los niveles de acceso a la información o recursos de red disponibles en la FEVaQ.

La forma fundamental de autoridad la tiene el Administrador de Redes con derechos totales. Entre otras funciones puede autorizar nuevos usuarios, otorgar derechos para modificar estructuras de las Bases de Datos, etc.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

Nivel Concepto

Consulta de la información El privilegio de lectura está disponible para cualquier usuario y solo se requiere presentaciones visuales o reportes. La autorización de lectura permite leer pero no modificar la Base de Datos.

Mantenimiento de información Permite el acceso para agregar nuevos datos, pero no modifica los ya existentes, permite modificar pero no eliminar los datos.

Para el borrado de datos, es preferible que sea responsabilidad de la DST.

2.3.1.2. Destrucción

Sin adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas o sabotaje, etc.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos, bases de datos, documentos o trabajar sin ellos.

Esta comprobado que una gran parte del espacio en disco esta ocupado por archivos de naturaleza histórica, que es útil tener a mano pero no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia conservados como documentos de referencia o plantilla. Si se guarda una copia de seguridad de estos archivos las consecuencias de organización pueden ser mínimas.

Los archivos Electrónicos Contable son de disposición diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo. Generalmente la institución recurre a esta información para la toma de decisiones.

Sin los datos al día, si el objetivo se vería seriamente afectado. Para evitar daños mayores se hacen copias de seguridad de la información vital para la institución y

se almacenan en lugares apropiados (de preferencia en lugar externo a las instalaciones).

Hay que protegerse también ante una posible destrucción del hardware o software por parte del personal no honrado. Por ejemplo, hay casos en la que, trabajadores que han sido recientemente despedidos o están enterados que ellos van a ser cesados, han destruido o modificado archivos para su beneficio inmediato o futuro. Depende de los Jefes inmediatos de las áreas funcionales dar importancia a estos eventos, debiendo informar al Jefe del CIT para el control respectivo.

2.3.1.3. Revelación o Deslealtad

La revelación o deslealtad es otra forma que utilizan los malos trabajadores para su propio beneficio. La información de carácter confidencial es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

Control de uso de información en paquetes/ expedientes abiertos, cintas/disquetes y otros datos residuales. La información puede ser conocida por personal no autorizadas.

Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de esa a aquellas personas que pueden usar mal los datos residuales de estas.

Mantener información impresa o magnética fuera del trayecto de la basura. El material de papel en la plataforma de descarga de la basura puede ser la fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Para tener una mayor seguridad de protección de la información residual y segregada, esta deberá ser destruida, eliminada físicamente, manualmente o mecánicamente (picadoras de papel).

Preparar procedimientos de control para la distribución de información. Una manera de controlar la distribución y posible derivación de información, es

mantener un rastro de copias múltiples indicando la confidencialidad o usando numeración como “página 1 de 9”

Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de la Oficinas y relativamente disponible a gran número de personas.

2.3.1.4. Modificaciones

Hay que estar prevenido frente a la tendencia a asumir que “si viene de la computadora, debe ser correcto”.

La importancia de los datos modificados de forma ilícita, esta condicionada al grado en que la institución, depende de los datos para su funcionamiento y toma de dediciones. Esto podría disminuir su efecto su los datos procedente de las computadoras se verificaran antes de constituir fuente de información para la toma de decisiones.

Los elementos en la cual se han establecido procedimientos para controlar modificaciones ilícitas son:

Los programas de aplicación: adicionalmente a proteger sus programas de aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionales a los datos o a su uso no autorizado.

La información en Bases de Datos: como medidas de Seguridad, para proteger los datos en el sistema, efectuar auditorias y pruebas de consistencia de datos en nuestros históricos. Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

Nuestra mejor protección contra la perdida/modificación de datos consiste en hacer copias de seguridad, almacenando en copias no autorizadas de todos los archivos valiosos en un lugar seguro.

Los usuarios: los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados, profundizarse con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema.

Para la realización de las Copias de Seguridad se tiene que tomar algunas decisiones previas como:

¿Qué soporte de copias de seguridad se va utilizar?

¿Se van a usar dispositivos especializados para copia de seguridad?

¿Con que frecuencia se deben realizar las copias de seguridad?

¿Cuáles son los archivos a los que se le sacara copia de seguridad y donde se almacenara?

El DST establecerá Directivas y/o Reglamentos en estas materias, para que los usuarios tomen conocimiento de sus responsabilidades. Tales reglas y normativas deben incorporarse en una campaña de capacitación educativa.

La institución debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

Hacer de la copia de seguridad una política, no una opción.

Hacer de la copia de seguridad resulte deseable.

Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).

Hacer de la copia de seguridad una función obligatoria.

CAPITULO III: PLAN DE RECUPERACIÓN DEL DESASTRE Y RESPALDO DE LA INFORMACIÓN

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El costo de recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 7.0, o un incendio no controlable, estará dado por el valor no asegurado de equipos informáticos e información más el costo de oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de actividades posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Típicamente las personas pueden ser: personal del DST, o personal de seguridad.

Las actividades a realizar en un plan de recuperación de desastres, se clasifican en tres etapas:

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

3.1. Actividades previas al desastre.

Se considera 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 la institución.

3.1.1. Establecimientos del Plan de Acción

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

- a. Sistemas e Información.
- b. Equipos de Cómputo.
- c. Obtención y almacenamiento de los respaldos de Información (BACKUPS).
- d. Políticas (Normas y procedimientos de respaldos).

La FEVaQ, deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por profesores y alumnos. Los Sistemas y Servicios críticos para la FEVaQ, son los siguientes:

Lista de Sistemas

- Sistema Integral de Información Académica (SIIA): Sistema de información asociado a la ejecución y manejo de calificaciones de registro único. Lo opera la oficina central de cómputo de la UMSNH - “Edificio “N”.
- Sistema Integrado de Gestión Académica: Sistema de información que permite el registro y control de los Procesos académicos, permite al

alumno realizar consultas académicas consulta vía WEB. Lo operan las Oficinas Académicas, y los órganos académicos de control.

- Sistema de Tramite Documentario: Sistema de información que permite el registro y seguimiento de los documentos. Lo operan todas las áreas funcionales de la UMSNH.
- Sistema de Gestión Administrativa – Ingresos: Sistema de información que permite el registro y control de los ingresos. Lo operan todas las áreas funcionales Administrativas de la UMSNH.
- Sistema de Abastecimientos: Sistema de información que permite el registro y control de las Órdenes de Trabajo, almacén. Lo opera la Secretaría Administrativa de la FEVaQ.
- Sistema de Control de Asistencia del personal: Lo opera la Oficina Central de Recursos Humanos de la UMSNH.
- Sistema de Banco de Preguntas para la elaboración de Exámenes de admisión vía SIIA/UMSNH.

Lista de Servicios

- Sistema de comunicaciones
- Servicio de correo académico
- Servicios Web: Publicación de páginas Web, noticias de la FEVaQ, Inscripción comedor universitario, Inscripción de cursos.
- Internet, Intranet.
- Servicios Proxy
- VPN: servicios de acceso privado a la red de la Institución desde cualquier lugar.
- Servicio de Monitoreo de la red: monitorea los equipos de comunicación distribuidos en la red de la FEVaQ.
- Servicios de telefonía Principal: teléfonos IP
- Servicios de enseñanza de manera virtual.
- Servicio de Antivirus

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

Se debe emplear 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. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.
- Obtención y almacenamiento de Copias de Seguridad (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 de los sistemas en la institución. Las copias de seguridad son las siguientes:
- Respaldo del Sistema Operativo: o de todas las versiones de sistema operativo instalados en la red.
- Respaldo de Software Base: (Lenguajes de Programación utilizados en el desarrollo de los aplicativos institucionales).
- Respaldo del software aplicativo: backups de los programas fuente y los programas ejecutables.
- Respaldo de base de datos, contraseñas y todo archivo necesario para la correcta ejecución del software aplicativo en la facultad).

- Respaldo del Hardware, se puede implementar bajo dos modalidades:

Modalidad Externa: mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puestos a nuestra disposición al ocurrir una continencia mientras se busca una solución definitiva al siniestro producido.

En este caso se debe definir claramente las condiciones del convenio a efectos de determinar la cantidad de equipos, periodos de tiempo, ambientes, etc., que se puede realizar con la entidad que cuente con equipo u mantenga un Plan de Seguridad de Hardware.

Modalidad Interna: si se dispone de mas de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas son susceptibles de ser usados como equipos de emergencia.

Es importante mencionar que en ambos casos se debe probar y asegurar que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas.

Políticas (Normas y Procedimientos)

Se debe establecer procedimientos, normas y determinación de responsabilidades en la obtención de los “Backups” o Copias de Seguridad. Se debe considerar:

Periodicidad de cada tipo de respaldo: los Backups de los sistemas informáticos se realizan de manera diferente:

Sistema Integrado de Gestión Académico: en los procesos académicos de Inscripción de curso y registro de Actas se realiza respaldo diario, para los demás periodos se realiza el respaldo semanal.

- Sistema de Ingresos: Respaldo diario Apoyos académicos
- Sistema Integral de administración (SIIA): Respaldo semanal

- Sistema de trámite documentario: Respaldo diario
- Sistema de abastecimientos: Respaldo semanal
- Control de asistencias del personal: Respaldo semanal
- Sistema de banco de preguntas: Respaldo periodo exámenes

El respaldo de información de movimientos entre los periodos que no se sacan respaldos, días no laborales, feriados, etc. en estos días, es posible programar un respaldo automático.

Uso obligatorio de un formulario de control de ejecución del programa de respaldos diarios, semanales y mensuales: es un control a implementar, de tal manera de llevar un registro diario de resultados de las operaciones realizadas y su respectivo reporte de almacenamiento.

El almacenamiento de respaldos, deberá estar en condiciones ambientales optimas, dependiendo del medio magnético empleando.

Reemplazo de respaldos en forma periódica, antes que el medio magnético de soporte se pueda deteriorar. No se realiza reemplazos pero se realiza copias de las mismas, considerando que no se puede determinar exactamente el periodo de vida útil del dispositivo donde se ha realizado el respaldo.

Almacenamiento de los respaldo en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local). Esta norma se cumple con la información histórica, es decir se tiene distribuidos los backups de la siguiente manera: una copia reside en las instalaciones del DST, y una segunda copia reside en la Oficina que genera la información..

Pruebas periódicas de los respaldo (Restore), verificando su funcionalidad, a través de los sistemas comparando contra resultados anteriormente confiables. Esta actividad se realizara haciendo una comparación entre el contenido de la primera y segunda copia realizada o con el contenido de la información que se encuentra el Servidor de información histórica.

3.1.1.1 Sistemas de Información

La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

- La relación de Sistemas de Información deberá detallar los siguientes datos :
- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Dirección (Gerencia, Departamento, etc) que genera la información base (el «dueño» del Sistema).
- Las unidades o departamentos (internos/externos) que usan la información del Sistema.
- El volumen de los archivos que trabaja el Sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del Sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el Sistema de Información (Actividades de recuperación).

Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la FEVaQ pueda recuperar su operatividad perdida durante el desastre (contingencia).

3.1.1.2 Equipos de Cómputo

Aparte de las normas de seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:

El inventario actualizado de los equipos de manejo de información (computadoras, impresoras y otros periféricos), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso académico.

- Pólizas de Seguros. Como parte de la protección de los activos institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del equipo de cómputo siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
- Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con Información importante o estratégica y color verde a las PC's de contenidos normales.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

3.1.1.3. Creación y almacenamiento de información y respaldos (BACKUPS).

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la

correcta ejecución de los Sistemas o aplicativos de la FEVaQ. Para lo cual se debe contar con:

1) Respaldos (backups) del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

2) Respaldos del Software Base (Paquetes y/o aplicaciones con los cuales han sido desarrollados o interactúan nuestros aplicativos institucionales).

3) Respaldos del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes y cualquier otro software o procedimiento que también trabaje con datos internos produciendo resultados positivos que permita al usuario final continuar con su trabajo). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

4) Respaldos de los Datos (Bases de Datos, índices, tablas de validación, contraseñas, y todo archivo necesario para la correcta ejecución del Software Aplicativo a la Facultad de Economía).

5) Respaldos del Hardware. Se puede implementar bajo dos modalidades:

Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

- Modalidad Interna. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son

susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

- En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

3.1.1.4. Políticas (Normas y procedimientos de respaldos)…

- Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto «c», debiéndose incluir:
- Periodicidad de cada Tipo de Backup.
- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (Backups incrementales).
- Uso obligatorio de un formulario estándar para el registro y control de los Backups (se incluye un formato tipo en el anexo «IV».)
- Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa (mencionado en el punto «a»), y los Backups efectuados.
- 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).
- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local estudiado).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

3.1.2. Formación de equipos operativos

En cada unidad operativa, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de su unidad. Pudiendo ser el Jefe Administrativo de dicha Área, sus funciones serán las siguientes:

- Contactarse con los autores de las aplicaciones y personal de mantenimiento respectivo.

El equipo del encargado en el DST - FEVaQ, está formado por las siguientes unidades:

  - Unidad de Telecomunicaciones
  - Unidad de Soporte Tecnológico.
  - Unidad de Administración de Servidores.
  - Unidad de Desarrollo Tecnológico.
  - Unidad Académica.

Proporcionar las facilidades (procedimientos, técnicas) para realizar copias de respaldo.

Esta actividad está dirigida por el Equipo de Soporte y Mantenimiento.

Supervisar el procedimiento de respaldo y restauración

Establecer procedimientos de seguridad en los sitios de recuperación

Organizar la prueba de hardware y software: el encargado y el usuario final dan su conformidad.

Ejecutar trabajos de recuperación y comprobación de datos.

Participar en las pruebas y simulacros de desastres: en esta actividad deben participar el encargado de la ejecución de actividades operativas, y los servidores

administrativos del área, en el cumplimiento de actividades preventivas al desastre del Plan de Contingencias.

3.1.3. Formación de Equipos de Evaluación (Auditoria de cumplimiento de los procesos de seguridad)

Esta función debe ser realizada preferentemente por el personal de Departamento DST de la FEVaQ, de no se posible, lo realizaría el personal del área de informática de la UMSNH y Autoridades Locales de la FEVaQ, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

Revisar que las normas y procedimientos con respecto a los respaldos, seguridad de equipos y data se cumpla.

Supervisar la realización periódica de los respaldos, por parte de los equipos operativos, es decir, información generada en el DST/FEVaQ, software general y hardware.

Revisar la correlación entre la relación de los Sistemas de información necesarios para la buena marcha de la Facultad de Economía y los respaldos realizados.

Informar de los cumplimientos e incumplimientos de las normas para las acciones de corrección necesarias.

3.2. Actividades durante el Desastre

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

a. Plan de Emergencias

b. Formación de Equipos

c. Entrenamiento

3.2.1 Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, 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 siniestro. 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 siniestro 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 siniestro causen mas daños o destrucciones. Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda. Todo el personal debe conocer lo siguiente:

Localización de vías de Escape o Salida: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape

Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por la autoridad local. Esa actividad se realizará utilizando las vías de escape mencionadas en el punto anterior.

Las ubicaciones y señalización de los elementos contra el siniestro: tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales.

La Secuencia de llamadas en caso de alguna contingencia o siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad etc.

3.2.2 Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de una contingencia informática o de otra naturaleza. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos de cómputo y periféricos, de acuerdo a los lineamientos o clasificación de prioridades.

3.2.3. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc.

Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los alumnos, autoridades y administrativos de la FEVaQ, dando el ejemplo de la importancia que la Dirección otorga a la Seguridad de la Facultad de Economía “Vasco de Quiroga”.

3.3. Actividades después del desastre

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

a. Evaluación de Daños.

b. Priorización de Actividades del Plan de Acción.

c. Ejecución de Actividades.

d. Evaluación de Resultados.

e. Retroalimentación del Plan de Acción.

f. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo.

En el caso de la Facultad de Economía, se debe atender los procesos académicos y administrativos como documentarios; que son las actividades que no podrían dejar de funcionar, por la importancia estratégica de orden. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, será prioritario.

b. Priorizar 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 ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

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.

Los trabajos de recuperación tendrán dos etapas:

La primera la restauración del servicio usando los recursos de la institución o local de respaldo.

La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta ultima etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectado por el siniestro, debemos de 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.

De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos 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 cual hubiera sido el costo de no contar con el Plan de Contingencias en la institución.

3.3.1. Acciones frente a los tipos de riesgo.

Cuando el daño a las instalaciones ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. El procedimiento de respuesta a esta emergencia se ve en la figura A1.

Cuando el daño ha sido menor:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

b) Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

♣ Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.

♣ No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.

♣ Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.

♣ Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.

♣ No almacenar sustancias y productos inflamables.

♣ No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.

♣ Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.

♣ Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Seguridad.

♣ Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.

♣ Tener a la mano los números telefónicos de emergencia.

♣ Portar siempre el fotocheck de identificación.

DURANTE

♣ Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

♣ En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente del CIT.

♣ Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios, solicitar ayuda.

♣ Si el fuego está fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.

♣ No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.

♣ Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de el, intenta el traslado a pisos superiores.

♣ Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.

♣ Si es posible mojar la ropa.

♣ Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUES

♣ Retirarse inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.

♣ No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.

♣ El personal calificado realizara una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.

♣ Colaborar con las autoridades.

3.3.1.2. Clase de Riesgo: Robo común de equipos y archivos

Analizar las siguientes situaciones:

♣ En qué tipo de vecindario se encuentra la Institución

♣ Las computadoras se ven desde la calle

♣ Hay personal de seguridad en la Institución y están ubicados en zonas estratégicas

♣ Cuánto valor tienen actualmente las Bases de Datos

♣ Cuánta pérdida podría causar en caso de que se hicieran públicas

♣ Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.

♣ Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

3.3.1.3. Clase de Riesgo: Vandalismo

♣ Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

♣ A continuación se menciona una serie de medidas preventivas:

o Establecer vigilancia mediante cámaras de seguridad en el Site, el cual registre todos los movimientos de entrada del personal.

o Instalar identificadores mediante tarjetas de acceso.

o Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).

♣ Los principales conflictos que pudieran presentarse son:

o En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.

o Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la Delegación Miguel Hidalgo, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc; en un sitio alterno, ya que no contarían con copia de la información.

3.3.1.4. Clase de Riesgo: Equivocaciones

♣ Cuánto saben los empleados de computadoras o redes.

♣ Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

♣ Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

3.3.1.5. Clase de Riesgo: Fallas en los equipos

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración. El procedimiento de respuesta a esta emergencia se ve en la figura A2.

Casos

♣ Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.

2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.

4. Bajar el sistema y apagar el equipo.

5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.

6. Restaurar el último backup, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

7. Verificación el buen estado de los sistemas.

8. Habilitar las entradas al sistema para los usuarios.

♣ Error de Memoria RAM y Tarjeta(s) Controladora(s) de Disco

En el caso de las memorias RAM, se dan los siguientes síntomas:

• El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios.

• Ante procesos mayores se congela el proceso.

• Arroja errores con mapas de direcciones hexadecimales.

• Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

2. El servidor debe estar apagado, dando un correcto apagado del sistema.

3. Ubicar las memorias malogradas.

4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.

5. Retirar la conexión del servidor con el concentrador, ello evitará que al encender el sistema, los usuarios ingresen

6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

7. Probar los sistemas que están en red en diferentes estaciones.

8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

3.3.1.6. Clase de Riesgo: Acción de Virus Informático

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

• Se contará con antivirus para el sistema; aislar el virus para su futura investigación.

• El antivirus muestra el nombre del archivo infectado y quién lo usó.

• Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

• Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.

• Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el escaneado, reconstruir el “Boot Sector” del disco duro.

3.3.1.7. Clase de Riesgo: Accesos No Autorizados

Enfatiza los temas de:

♣ Contraseñas. Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos infructuosos. El CIT implementa la complejidad en sus contraseñas de tal forma que sean mas de siete caracteres y consistentes en números y letras.

♣ Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

♣ Privilegio. En los sistemas informáticos de la UNP, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en “Grupos” con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

3.3.1.8. Clase de Riesgo: Fenómenos naturales

a) Terremoto e Inundación

♣ Para evitar problemas con inundaciones ubicar los servidores a un promedio de 50 cm de altura.

♣ En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

♣ Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.

♣ Cuando el daño ha sido menor se procede:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

b) Recoger los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

3.3.1.9. Clase de Riesgo: Robo de Datos

Se previene a través de las siguientes acciones:

♣ Acceso no Autorizado: Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

o Área de Sistemas.

o Computadoras personales y/o terminales de la red.

o Información confidencial.

♣ Control de acceso al Área de Sistemas: El acceso al área de Informática estará restringido:

o Sólo ingresan al área el personal que trabaja en el área.

o El ingreso de personas extrañas solo podrá ser bajo una autorización.

♣ Acceso Limitado a los Terminales: Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema, las siguientes restricciones pueden ser aplicadas:

o Determinación de los períodos de tiempo para los usuarios o las terminales.

o Designación del usuario por terminal.

o Limitación del uso de programas para usuario o terminales.

o Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).

♣ Niveles de Acceso: Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

o Nivel de consulta de la información.- privilegio de lectura.

o Nivel de mantenimiento de la información.- El concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.

3.3.1.10. Clase de Riesgo: Manipulación y Sabotaje

♣ La protección contra el sabotaje requiere:

1. Una selección rigurosa del personal.

2. Buena administración de los recursos humanos.

3. Buenos controles administrativos.

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

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

♣ A continuaciones algunas medidas que se deben tener en cuenta para evitar acciones hostiles:

1. Mantener una buena relación de trabajo con el departamento de policía local.

2. Mantener adecuados archivos de reserva (Backups).

3. Planear para probar los respaldos (Backups) de los servicios de procesamiento de datos.

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

5. Usar rastros de auditorías o registros cronológicos (logs) de transacción como medida de seguridad.

♣ Cuando la información eliminada se pueda volver a capturar, se procede con lo siguiente:

o Capturar los datos faltantes en las bases de datos de los sistemas. Responsable: Áreas afectadas

o Revisar y probar la integridad de los datos. Responsable: Desarrollo de Sistemas.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectados.

CONCLUSIONES

♣ El presente Plan de contingencias y Seguridad en Información de la UNP, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.

♣ Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Evaluación de riesgos, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.

♣ Un Plan de Contingencia es la herramienta que la institución debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

♣ No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos mas conocido como Centro de Cómputo.

♣ Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

RECOMENDACIONES

♣ Programar las actividades propuestas en el presente Plan de Contingencias y Seguridad de Información.

♣ Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de la UNP.

♣ Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

♣ Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa.

BIBLIOGRAFIA

https://revista.seguridad.unam.mx/numero-10/medidas-preventivas-para-resguardar-la-informacion. Universidad Nacional Autónoma de México.

ϖ R.J. N° 340-94-INEI , Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.

ϖ R.J. N° 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.

ϖ R.J. N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.

ϖ R.J. Nº 070-2007-J-CONIDA, Comisión Nacional de Investigación y Desarrollo Aeroespacial – CONIDA.

ϖ Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información. INEI.

ϖ Manual de Operación y Funciones del Centro de Informática y Telecomunicaciones.

ϖ Manual de Reglamento Interno del Centro de Informática y Telecomunicaciones.

Elaborado por: Carlos Urquiza Villegas (MCSE)
Morelia, Mich., a 21 de mayo de 2018