MANUAL DE SEGURIDAD INFORMATICA

INSTITUTO TÉCNICO NACIONAL DE COMERCIO

“SIMÓN RODRIGUEZ”

Santiago de Cali, Valle

2015

TABLA DE CONTENIDO

0. INTRODUCCIÓN

La Oficina de Tecnología Informática (TI), de Intenalco, realiza el manual de seguridad y políticas de informática para que sea el instrumento para concientizar a sus funcionarios acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la entidad cumplir con su misión.

De esta manera la seguridad informática en la institución pretende cumplir con los estándares de seguridad de los sistemas de información, garantizando la confidencialidad de datos (información y de hardware) en los servicios ofrecidos como en los servicios internos a la comunidad educativa.

Actualmente vivimos en una sociedad que depende de los Sistemas de Información (Tic's), que se encuentran tanto en la parte interna como externa de toda organización, sin embargo para poder acceder a esta información es necesario que estos sistemas se encuentren interconectados por medio de un recurso llamado Red, recurso constituido por equipos (router, bridges, switch, etc.), de medios de comunicación (Fast Ethernet, Gigabyte Ethernet, E1, T1, E3, STM-1, etc.), adicionalmente, las redes internas se conectan a otras redes (corporativas, Internet), lo que hace que se vuelvan más complejas y robustas. Es por ello, que se hace necesario el uso de herramientas para dar el soporte adecuado y óptimo. La ISO "International Standards Organization", creó un modelo de administración, donde se definen claramente las funciones de los administradores de redes, en 5 áreas:

1. Administración del Desempeño (Performance Management): Encargada de monitorear y medir varios aspectos de rendimiento, funcionamiento y utilización de la red, con el fin de mantener en niveles aceptables los servicios que se encuentran disponibles, así como rastrear todos los efectos en su operación.

2. Administración de la configuración (Configuration Management): Encargada de los aspectos de configuración de los dispositivos de la red, archivos de configuración de dichos dispositivos, y administración del software; almacenamiento en un lugar que sea accesible por el personal autorizado.

3. Administración de la Contabilidad (Accounting Management): Encargada de generar la información que permita describir el uso de los recursos que conforman la red. El primer paso es medir la utilización de todos los recursos para luego realizar un análisis de que proporcione el patrón de comportamiento actual de uso de la red, de aquí también se puede obtener información que ayude a planear un crecimiento o actualización de cada elemento que forma parte de la red, así como determinar si dicho uso es justo y adecuado.

4. Administración de Fallas (Fault Management): Encargada de detectar, registrar, aislar, notificar y corregir fallas en aquellos equipos que son parte de la red que presenten algún problema que afecte el buen funcionamiento de la red. Es importante aclarar que cualquier problema que se presente se verá reflejado como una degradación en los servicios que ofrece la red. El proceso inicia desde la detección y determinación de síntomas hasta el registro del problema y su solución.

5. Administración de la Seguridad (Security Management): Controlar el acceso a los recursos de la red, de acuerdo a las políticas establecidas con el fin de evitar algún abuso y la perdida de la confidencialidad; entre las funciones está identificar los recursos sensibles y críticos de la red, monitorear los accesos.

GLOSARIO

ANTIVIRUS: Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

DOMINIO: Sistema de denominación de hosts (estaciones de trabajo) en red, está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

ENCRIPTAR: Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

GATEWAY: Es un punto de red que actúa como entrada a otra red.

HARDWARE: Maquinaria. Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

MALWARE: Cualquier programa cuyo objetivo sea causar daños a computadoras, sistemas o redes y, por extensión, a sus usuarios.

ROUTERS: Es un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino.

SERVIDOR: Computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

SOFTWARE: Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

SWITCHES: Equipo que por medio de la dirección física del equipo (Mac address) en los paquetes de data determina a que puerto reenviar la data. Usualmente se asocia con el Gateway.

TI: Tecnologías de la información

UPS: Siglas en ingles de Uninterruptible Power Suply, es un aparato que incluye una batería que en caso que se vaya la electricidad, puede, por ejemplo, mantener una computadora funcionando lo suficiente para que el usuario pueda apagarla y guardar data importante.

VIRUS: Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

1. DESARROLLO GENERAL

1.1. Aplicación

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información (TI) de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el Área de TI en cuanto a la mejora y al cumplimiento de los objetivos institucionales.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de Intenalco Educación Superior. Facilitando una mayor integridad confidencialidad y confiabilidad de la información generada por el Área de TI al personal, al manejo de los datos, al uso de los bienes informáticos disponibles, minimizando los riesgos en el uso de las tecnologías de información.

2. SEGURIDAD INSTITUCIONAL

Política: Toda persona que ingresa como usuario nuevo a Intenalco Educación Superior para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente manual.

2.1. Usuarios Nuevos

Todo el personal nuevo de la Institución, deberá ser notificado ante el proceso de TI (Tecnologías de la información); para asignarle los derechos correspondientes (Equipo de cómputo, Creación de Usuario en el Servidor (Perfil en el servidor) o en caso de retiro anular y cancelar los derechos otorgados como usuario informático.

2.2. Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir con las Políticas y Estándares de Seguridad Informática para Usuarios en el presente manual.

2.3. Capacitación en seguridad informática

Todo servidor o funcionario nuevo en Intenalco Educación Superior deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, según sea el área operativa y en función de las actividades que se desarrollan; de la misma forma las sanciones en que pueden incurrir en caso de incumplimiento.

2.4. Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial, o ser encontrado culpable de delito informático.

3. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Política: Para el acceso a los sitios y áreas restringidas se debe notificar a la oficina de TI para la autorización correspondiente, así proteger la información y los bienes informáticos.

3.1. Protección de la información y de los bienes informáticos

El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

Los servidores, sin importar al dominio o grupo de trabajo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el administrador y las personas responsables de TI.

El usuario o funcionario deberán reportar de forma inmediata al proceso de TI (tecnologías de la información) cuando se detecte riesgo alguno real o potencial equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

3.2. Controles generales

En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.

Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la institución que se encuentre almacenada en los equipos de cómputo que tengan en su estación de trabajo.

3.3. Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones de Intenalco educación Superior, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y/o herramientas que no sean propiedad de Intenalco educación superior; en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

La oficina de tecnologías de la información deberá llevar el registro del mantenimiento que se realizan a los equipos de cómputo. Se debe establecer los periodos de mantenimiento preventivo.

Dentro de las instalaciones, habrá un espacio dedicado única y exclusivamente al área de servidores, la cual se mantiene separado mediante una división de pared y protegido su acceso bajo llave. Cualquier actividad anómala, efectuada dentro de las instalaciones físicas de procesamiento de información será cancelada en el momento en que se constatase la actividad.

3.4. Protección y ubicación de los equipos

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del proceso de TI, en caso de requerir este servicio deberá solicitarlo mediante el debido formato y con mínimo un día de anterioridad.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas dentro de Intenalco Educación Superior.

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente aquella que contiene el sistema operativo, generalmente; la D.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos ni ingerir líquidos.

Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

Se debe mantener el equipo informático en un lugar limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar la reubicación de cables con el personal de TI.

Cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al proceso de TI.

Queda terminantemente prohibido que el usuario o funcionario distinto al personal de TI abra o destape los equipos de cómputo.

3.5. Mantenimiento de equipos

Únicamente el personal autorizado por el Área de TI podrá llevar a cabo el mantenimiento preventivo y correctivo de los equipos informáticos.

Los usuarios deberán asegurarse de respaldar en copias o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en él equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

Cualquier falla efectuada en las aplicaciones o sistema, por la manipulación errónea de archivos, posterior mantenimiento deberá ser notificada y reparada por el personal técnico encargado en dicha función.

3.6. Pérdida de Equipo

El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El servidor o funcionario deberá de informar de inmediato al proceso de TI y almacén la Desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

3.7. Uso de dispositivos extraíbles

El uso de los quemadores externos o grabadores de disco compacto es exclusivo para backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

El servidor o funcionario que tengan asignados estos tipos de dispositivos serán responsables del buen uso de ellos.

Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por TI con el respectivo visto bueno de vicerrectoría Administrativa y financiera.

Todo funcionario o servidor de Intenalco Educación Superior deberá reportar al proceso de TI el uso de memorias, USB asignadas para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

3.8. Daño del equipo

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

4. ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO

Política: Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de Intenalco Educación Superior. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna de la institución, a otras dependencias de sedes alternas o redes externas como Internet.

Los usuarios y funcionarios de Intenalco Educación Superior que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso (malware) y/o virus.

TI establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.

Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar al sitio donde se encuentren los servidores, debe solicitar mediante comunicado interno debidamente firmado y autorizado por el Jefe inmediato de su sección o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de la Rectoría, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del proceso de TI.

El proceso de Tecnologías de la Información deberá llevar un registro escrito de todas las visitas autorizadas a los Centros de Cómputo restringidos.

Todo equipo informático ingresado a los Centros de Cómputo restringidos deberá ser registrado en el libro de visitas en portería.

Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

El proceso de Tecnologías de la Información deberá solicitar a la Alta Dirección, los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

4.1. Uso de medios de almacenamiento

Los usuarios y servidores de Intenalco Educación Superior deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información (TI) de Intenalco Educación Superior serán registradas y podrán ser objeto de auditoría.

4.2. Adquisición de software.

Los usuarios y funcionarios que requieran la instalación de software que sea propiedad de Intenalco Educación Superior, deberán justificar su uso y solicitar su autorización al proceso TI con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

Se considera una falta grave que los usuarios o funcionarios Instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o

cualquier equipo conectado a la red de Intenalco Educación Superior, que no esté autorizado por TI.

El Instituto Técnico Nacional de Comercio “Simón Rodríguez”, posee un contrato de Alquiler de uso de Software con la Compañía Microsoft, esto nos garantiza en gran medida la legalidad del software adquirido. Cualquier otro software requerido, y que no pueda ser provisto por la compañía Microsoft, será adquirido a otro Proveedor debidamente certificado, el cual deberá entregar al momento de la compra, el programa y la licencia del software con toda la documentación pertinente y necesaria que certifique la originalidad y validez del mismo.

El Grupo de Apoyo de TI tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Institución.

En el proceso de reinstalar un programa el personal de TI debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

4.3. Licenciamiento de Software

Para el Control de Licenciamiento de Software: INTENALCO EDUCACIÓN SUPERIOR cuenta con un contrato con vigencia anual, con la Compañía MICROSOFT S.A., además como política de seguridad se tiene establecido mediante la red académica restringido la instalación de software en las salas de informática. El Grupo de TI realiza periódicamente un inventario físico de los programas y software instalados en cada uno de los computadores de la Institución.

4.4. Identificación del incidente

El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al proceso de TI lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar a TI.

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de Intenalco Educación Superior debe ser reportado al proceso de TI.

4.5. Administración y seguridad de la Red

Los usuarios de las áreas de Intenalco Educación Superior no deben tener acceso físico y/o manipulación de los servidores, switches, routers, puntos y elementos activos de red y las bases de datos que almacenan información privilegiada y transacciones propias de la institución. Estas acciones serán realizadas única y exclusivamente por el personal de la Oficina de TI autorizados para realizar estas labores.

Se prohíbe a los usuarios de Intenalco redactar, transmitir, acceder o recibir vía Internet, haciendo uso de las redes o equipos de cómputo de Intenalco información con contenido que pudiera ser discriminatorio, ofensivo, obsceno,

amenazante, intimidante o destructivo para cualquier individuo u organización. Ejemplos de contenido inaceptable incluyen, entre otros, comentarios en general o imágenes con contenido sexual, discriminación racial, otro tipo de comentarios o imágenes que pudieran ofender a algún individuo con base en su raza, edad, orientación sexual, creencias religiosas, orientación política, nacionalidad, limitaciones físicas o cualquier otra característica especial protegida por la ley.

4.6. Uso del Correo electrónico

Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re-direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a Intenalco Educación Superior, a menos que cuente con la autorización del proceso de TI.

Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de Intenalco Educación Superior. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.

Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

4.7. Controles contra virus o software malicioso

Para revisar si el antivirus se actualiza correctamente, seleccione el icono de su programa antivirus Kaspersky que se encuentra en la barra de herramientas, este debe estar siempre de color rojo, se actualiza automáticamente siempre y cuando haya conexión a internet.

En el caso de un equipo de cómputo que presente el ícono en color gris (es decir desactualizado), se debe tener conexión a internet, con clic derecho sobre el ícono del antivirus (kasperky), dar clic en actualizar.

Los usuarios de Intenalco Educación Superior deben verificar que la Información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software de antivirus autorizado por el proceso de TI.

Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario

debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Ningún funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del proceso de TI.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificara al proceso de TI para la revisión y erradicación del virus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sea implantadas por TI en: Antivirus, Outlook, office, Navegadores u otros programas.

Debido a que algunos virus son extremadamente complejos, ninguno usuario o funcionario de Intenalco Educación Superior, distinto al personal del proceso TI deberá intentar erradicarlos de las computadoras.

4.8. Controles para la Generación y Restauración de Copias de Seguridad (Backups).

Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente de los equipos de cómputo administrativos y servidores.

Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.

Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.

Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.

Se utilizará el programa Nero Express en caso que el usuario no tenga USB o Disco Duro Externo para la realización de su backups.

- Aplicación PC, Copiar Disco
- Opción Datos: se escoge CD o DVD
- Se añaden los archivos o carpetas
- Clic en cerrar
- Clic en siguiente
- Se introduce un CD o DVD en blanco en la unidad quemador de CD o DVD
- Colocar nombre al disco (16 caracteres)
- Si la información no abarca 700 megas en CD o 4.3 gigas en DVD se habilita la pestaña: Permitir añadir archivos posteriormente.
- Clic en grabar
- Marcar el CD o DVD colocándole la fecha de la copia y entregar a su Jefe inmediato para su almacenamiento y custodia.

  Las copias de seguridad o Backups, se deben realizar al menos una vez a la semana, periódicamente el proceso de TI realizará un seguimiento del

cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

4.9. Planes de Contingencia ante Desastre

Definición: Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos, **ver procedimiento de contingencia**.

4.9.1. Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total.

4.9.2. Disponibilidad de plataformas computacionales, comunicaciones e información necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados.

4.9.3. Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.

4.9.4. Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware, software y

comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la compañía.

4.9.5. Disponibilidad de copias de respaldo (externas) para restablecer las operaciones en las áreas de misión crítica definidas.

4.10. Internet

4.10.1. El acceso a Internet provisto a los usuarios y funcionarios de Intenalco Educación Superior es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

4.10.2. Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por Intenalco Educación Superior, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por la por la oficina de TI.

4.10.3. Los usuarios del servicio de navegación en Internet, al utilizar el servicio están aceptando que:

• Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

•Saben que existe la prohibición de descarga de software sin la autorización de la Oficina de TI.

5. ACCESO LÓGICO

Política: Cada usuario y funcionario es responsable de los mecanismos de control de acceso que les sean proporcionado; esto es, de su "ID" login de usuario y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de Intenalco Educación Superior, por lo que se deberá mantener de forma confidencial. El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de Intenalco Educación Superior, debe ser proporcionado por el dueño de la información, con base en el principio de "Derechos de Autor" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

5.1. Controles de acceso lógico

5.1.1 Todos los usuarios de servicios de información son responsables por el usuario y contraseña que recibe para el uso y acceso de los recursos.

5.1.2 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Oficina de TI, antes de poder usar la infraestructura tecnológica de Intenalco Educación Superior.

5.1.3 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de Intenalco Educación Superior, a menos que se tenga el visto bueno del dueño de la información y de la Oficina de TI y la autorización de vicerrectoría administrativa y financiera o de su Jefe inmediato.

5.1.4 Cada usuario que acceda a la infraestructura tecnológica de Intenalco Educación Superior debe contar con un identificador de usuario (ID) único y

personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

5.1.5 Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

Todo cambio en roles, funciones o cargo que requiera asignar al usuario atributos para acceso a diferentes prestaciones de la infraestructura tecnológica en INTENALCO Educación Superior debe ser notificado a la Oficina de TI por el Jefe inmediato Correspondiente a la dependencia o por el Vicerrector Administrativo y financiero o en su defecto por la Rectoría.

5.2. Administración de privilegios

5.2.1 Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a la Oficina de TI para el cambio de privilegios.

5.3. Equipos desatendidos

5.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas previamente instalados autorizados por la Oficina de TI.

5.4. Administración y uso de contraseñas

5.4.1 La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

5.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir a la Oficina de TI para que se le proporcione una nueva.

5.4.3 Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso o dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.

5.4.4 Sin importar las circunstancias, las contraseñas nunca se deben Compartir o ser reveladas.

5.5. Controles para Otorgar, Modificar y Retirar Accesos a Usuarios

5.5.1 Todo usuario debe quedar registrado, en Usuarios y Roles del directorio activo de Intenalco Educación Superior. La creación de un nuevo usuario y/o solicitud para la asignación de otros roles, deberá de venir acompañado del reporte debidamente firmado por el Jefe de Área y con el visto bueno de la Alta Dirección.

5.5.2 La Oficina de TI será la responsable de ejecutar los movimientos de, bajas o cambios de perfil de los usuarios.

5.6 Control de accesos remotos

5.5.1 La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y de la Oficina de TI.

6. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política: La Oficina de TI. Tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas.

Dentro del sistema integral de gestión de calidad se cuenta con los formatos para realizar seguimiento a las políticas de seguridad informática y copias de seguridad de la información.

7. DERECHOS DE PROPIEDAD INTELECTUAL

7.1 Los Software utilizados dentro de Intenalco Educación superior serán de propiedad de la Institución.

8. CLÁUSULAS DE CUMPLIMIENTO

8.1 La Oficina de TI realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

8.2 La Oficina de TI podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos.

8.3 Los jefes y responsables de los procesos establecidos en Intenalco Educación Superior deben apoyar las revisiones y el cumplimiento de las políticas y estándares de seguridad informática.

9. VIOLACIONES DE SEGURIDAD INFORMÁTICA

9.1 Está prohibido el uso de herramientas como hardware o software por parte de los usuarios de Intenalco Educación Superior para violar los controles de seguridad informática a menos que sea autorizado por la Oficina de TI.

9.2 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de Intenalco Educación Superior.

10. EQUIPOS EN EL ÁREA ADMINISTRATIVA

10.1 La Alta Dirección del Instituto Técnico Nacional de Comercio Simón Rodríguez deberá poner a disposición de la Oficina de TI. la información contractual de los equipos informáticos de Cómputo, así como de los servicios de soporte y mantenimiento.

10.2 La Oficina de TI, será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos.

10.3 La Oficina de TI, tendrá bajo su resguardo las licencias de software, para su debida instalación en los equipos de cómputo de la institución.

10.4 Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el Jefe del Área solicitante, lo cuales serán evaluados por la Oficina de TI para su autorización.

10.5 La Oficina de T.I, es el área encargada de tramitar las asignaciones, reasignaciones, bajas, etc. de equipos informáticos de cómputo escritorio, portátiles y periféricos ante la vicerrectoría administrativa y financiera, proceso encargado del Inventario de activos para su ejecución, con base a las solicitudes realizadas al respecto y las revisiones de aprovechamiento de los mismos.

10.6 Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar a la Oficina de TI el movimiento así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.

10.7 La Oficina de TI deberá elaborar el pase de salida cuando algún bien informático de cómputo Escritorio, Portátiles y periférico requiera ser trasladado fuera de las instalaciones de Intenalco Educación Superior por motivo de garantía, reparación o evento.

10.8 Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o

foráneas para realizar sus labores, dicho bien estará bajo resguardo de responsable que retira el equipo.

10.9 Queda prohibida la baja de equipo de cómputo que no cuente con evaluación técnica por parte de la Oficina de TI.

10.10 La Oficina de TI no es responsable de proporcionar asesoría técnica, mantenimiento preventivo o correctivo a equipo de cómputo propiedad del usuario.

10.11 El usuario que ingrese equipos de su propiedad a las instalaciones de Intenalco Educación Superior es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad de la Oficina de TI.

10.12 Queda prohibido instalar software no autorizado o que no cuente con licencia, la Oficina de TI deberá realizar las instalaciones de acuerdo con los estándares de Intenalco Educación Superior.

10.13 En el caso de reinstalaciones de equipo, el usuario será el responsable de verificar que toda la información y archivos de trabajo estén contenidos en el equipo asignado, el usuario deberá firmar la solicitud o asignación del servicio proporcionado por el técnico o ingeniero.

10.14 La Oficina de TI no es responsable de la configuración de dispositivos personales tales como tabletas, iPod y teléfonos celulares propiedad del usuario.

10.15 El Software autorizado para todos los equipos de cómputo del cual Intenalco Educación Superior cuenta con Licencia de uso son los siguientes:

- Windows, en todas sus versiones
- Windows Server. En todas sus versiones

- Suite de Microsoft Office todas sus versiones
- Kaspersky (Programa antivirus).
- Visual Studio y Visual Studio .NET

11. FUNCIONES DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN.

- Administrar y evaluar los requerimientos de información de las distintas áreas de INTENALCO EDUCACION SUPERIOR.
- Coordinar con el Equipo de Apoyo de la Oficina de TI en la definición, factibilidad, especificación y validación de requerimientos.
- Vigilar la correcta aplicación de los estándares y metodologías de desarrollo de sistemas de Información, así como sugerir las mejoras que sean necesarias.
- Las distintas dependencias para la definición de requerimientos funcionales y no funcionales de los sistemas de información.
- Revisar, aprobar y mantener actualizados los manuales, concerniente a los sistemas de información y tecnologías (TI).
- Elaborar reportes de avance y estrategias de ejecución de los proyectos de desarrollo de sistemas de información.

- Desarrollar e implementar los sistemas de información que requieran las dependencias.

- Efectuar el mantenimiento y actualización de los sistemas de información, analizando los problemas o planteamientos de modificación, garantizando su correcta sincronización.

- Participar en los procesos de adquisición y pruebas de las soluciones informáticas de terceros. Asimismo, supervisar las actividades realizadas por terceros en el desarrollo e implementación de soluciones informáticas.

- Apoyar en la capacitación al usuario final y al personal designado de la Sección Soporte a usuarios, en el adecuado uso de los sistemas de información, proporcionando material de soporte y los medios necesarios para tales fines.

- Administrar en forma eficiente los recursos asignados a la Oficina, así como el centro de cómputo, velando por la seguridad de accesos y operatividad, protegiendo la información de ingreso, salida y almacenamiento.

- Participar en la elaboración de la propuesta del plan de actividades de la oficina, en los planes de contingencia y en la implementación de acciones que minimicen el riesgo de Tecnologías de Información.

- Verificar que el personal de la oficina de TI atienda oportuna y eficientemente los requerimientos de las dependencias, supervisando el

cumplimiento de las metodologías, estándares y/o técnicas implementadas en la sección.

- Cumplir y hacer cumplir las medidas correctivas recomendadas por los entes de vigilancia y control tanto externo como interno.

- Ejecutar los planes de respaldo y las recuperaciones de información que se requieran para garantizar la continuidad operativa de las actividades.

- Atender asuntos relativos al servicio de soporte técnico de primer nivel para la solución de problemas referidos a hardware, Software, comunicaciones y servicios de computación personal, efectuados por el personal de la Oficina y por todas las dependencias institucionales.

- Participar en los Procesos de Atención de Problemas y Reclamos.

- Atender consultas técnicas, operativas y funcionales a los usuarios, incentivándolos en el mejor uso y operación de las tecnologías de información.

- Ejecutar, instalar, configurar, y puesta en línea de los equipos de cómputo y periféricos en las oficinas Administrativas; cumpliendo con los procedimientos y estándares aprobados.

- Instalar y diagnosticar los daños del cableado estructurado de la red de las oficinas Administrativas.

- Coordinar y analizar las incidencias y magnitudes de un desastre, determinando prioridades de atención, disminuyendo el nivel de riesgos y traumatismos en la operación.

- Determinar y gestionar de inmediato las actividades a realizar para generar una solución y puesta en marcha en el menor tiempo posible de todos los sistemas de información colapsados en el desastre.

12. PROCEDIMIENTO DE CONTINGENCIAS

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un procedimiento de contingencia adecuado de forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la institución

12.1 Análisis de evaluación de riesgos y estrategias

Metodología aplicada:

Para la clasificación de los activos de las Tecnologías de Información de Intenalco Educación superior se han considerado tres criterios:

Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).

Frecuencia del Evento: Puede ser (Nunca, aleatoria, Periódico y continuo)

Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Procedimientos de Contingencia: Son pasos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

Leves (Caídas de energía de corta duración, fallas en disco duro, etc.)

Severas (Destrucción de equipos, incendios, etc.)

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

Riesgos Naturales: tales como mal tiempo, terremotos, etc.

Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.

Riesgos Sociales: como actos terroristas y desordenes.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la entidad se describirá los activos que se pueden encontrar dentro de las tecnologías de información de la institución:

Activos susceptibles de daño

- Personal
- Hardware
- Software y utilitarios

- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

Posibles Daños

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.
    - Acceso no autorizado
    - Ruptura de las claves de acceso a los sistema computacionales
    - Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario.
    - Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).

- Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red Switches, cableado de la Red, Router, FireWall).

Clases de Riesgos

- Incendio o Fuego
- Robo común de equipos y archivos
- Falla en los equipos
- Equivocaciones
- Acción virus informático
- Accesos no autorizados

Incendio o Fuego

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Aleatorio

Grado de Impacto: Alto

Plan de Recuperación

Situación Actual	**Acción Correctiva**
La oficina donde están ubicados los servidores cuenta con un extintor cargado. De igual forma cada sala de informática y cada pasillo de oficinas	Se cumple

cuenta con extintores debidamente cargados.	
Se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios de la institución.	Se cumple

Robo Común de Equipos y Archivos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Moderado

Situación Actual	**Acción Correctiva**
Llenar libro en portería con descripción y fecha	Se cumple
Por la ubicación de la institución existe riesgo de hurto a mano armada.	Solicitar la colaboración de la Policía Nacional para que realice rondas periódicas por el sector donde se encuentra ubicadas las instalaciones de la institución

Falla en los Equipos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Situación Actual	**Acción Correctiva**
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Se realiza mantenimiento preventivo anualmente.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de equipos que están para dar de baja.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple en los procesos donde no puede interrumpirse el funcionamiento, se cuenta con UPS.

Equivocaciones manejo del sistema

Grado de Negatividad: Moderado

Frecuencia de Evento: Periódico

Grado de Impacto: Moderado

Situación Actual	**Acción Correctiva**
Equivocaciones que se producen de forma involuntaria, con respecto al manejo de información, software y equipos.	Realizar reinducción en el manual de políticas informáticas.
Algunas veces el usuario que tiene conocimiento en informática intenta navegar por sistemas que no están dentro de su función diaria.	Mediante el directorio activo se asignaran permisos y privilegios a cada usuario de acuerdo a sus funciones

Acción de Virus Informático

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Continuo

Grado de Impacto: Grave

Situación Actual	**Acción Correctiva**
Se cuenta con un software antivirus para la entidad, pero su actualización no se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad	Aún existen usuarios que lo incumplen.

Accesos No Autorizados

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Situación Actual	**Acción Correctiva**
Se controla el acceso al sistema de red mediante la definición de un administrador con su respectiva clave.	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.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica, sobre todo para el manejo de software.

12.2 Eventos considerados para los procedimientos de contingencia

Cuando se efectúa un riesgo, este puede producir un Evento, por tanto a continuación se describen los eventos a considerar dentro de los procedimientos de Contingencia.

RIESGO	EVENTO
Fallas Corte de Cable UTP. Fallas Tarjeta de Red. Fallas IP asignado. Fallas Punto de Swicht. Fallas Punto Pacht Panel. Fallas Punto de Red	NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR.
Fallas de Componentes de Hardware del Servidor. Falla del UPS (Falta de Suministro eléctrico). Virus. Sobrepasar el límite de almacenamiento del disco. Computador de Escritorio funciona como servidor	FALLAS EN EL EQUIPO SERVIDOR.
Falla de equipos de comunicación: SWITCH, Antenas. Fibra Óptica. Fallas en el software de Acceso a Internet. Perdida de comunicación con proveedores de Internet	PERDIDA DE SERVICIO DE INTERNET.
Incendio Sabotaje Corto Circuito Terremoto	INDISPONIBILIDAD DEL CENTRO DE COMPUTO (DESTRUCCIÓN DE LA SALA DE SERVIDORES)

No hay comunicación entre cliente – servidor

1. Requerimiento del usuario, que no cuenta con acceso a la red.

2. El técnico de sistemas procederá a identificar el problema.

3. Si se constata problema con el Pacht Panel, realizar cambio del mismo.

4. Si no se resuelve el problema proceder a constatar si existe problema en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma.

5. Si persiste el problema revisar los puntos de red, utilizando el diagrama lógico.

6. Testear el cable UTP. Si existe daño, realizar el cambio del cable.

7. Realizar mantenimiento del punto de red del usuario y del gabinete de comunicaciones.

8. Recuperación del sistema de red para el usuario.

Falla del Servidor

Puede producir Pérdida de Hardware y Software, Perdida del proceso automático de Backup y restore e Interrupción de las operaciones. A continuación se describen algunas causas del fallo en un Servidor:

Error Físico de Disco de un Servidor

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 en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.

8. Habilitar las entradas al sistema para los usuarios.

Error de Memoria RAM

1. En este caso se dan los siguientes síntomas:
2. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
3. Ante procesos mayores se congela el proceso.
4. Arroja errores con mapas de direcciones hexadecimales.

Error de Tarjeta(s) Controladora(s) de Disco

Para los errores de cambio de Memoria RAM o Tarjeta Controladora de disco se deben tomar las siguientes acciones:

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 la posición de la pieza a cambiar.

4. Retirar la pieza con sospecha de deterioro y tener a la mano otra igual o similar.

5. Retirar la conexión de red del servidor, 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. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

1. Caída del servidor de archivos por falla de software de red.
2. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
3. Bajar incorrectamente el servidor de archivos.
4. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

Recursos de Contingencia

- Componente de Remplazo (Memoria, Disco Duro, etc.).

- Backup diario de información del servidor

Interrupción del fluido eléctrico durante la ejecución de los procesos.

1. Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.

2. Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones, para que no corten bruscamente el proceso que tienen en el momento del apagón.

3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de UPS a corriente normal (Corriente brindad por la empresa eléctrica).

Recursos de contingencia

Asegurar que el estado de las baterías del UPS, se encuentren siempre cargadas.

Perdida de servicio internet

1. Realizar pruebas para identificar posible problema dentro de la institución

2. Si se evidencia problema en el hardware, se procederá a cambiar el componente.

3. Si se evidencia problema con el software, se debe reinstalar el sistema operativo del servidor.

4. Si no se evidencia falla en los equipos de la institución, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.

5. Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.

6. Realizar pruebas de operatividad del servicio.

7. Servicio de internet activo

Recursos de Contingencia

Hardware

- Router

- Software

- Herramientas de Internet.

Destrucción del Centro de Cómputo

1. Contar con el inventario total de sistemas actualizado.

2. Identificar recursos de hardware y software que se puedan rescatar.

3. Salvaguardar los Backups de información realizados.

4. Identificar un nuevo espacio para restaurar el Centro de Cómputo.

5. Presupuestar la adquisición de software, hardware, materiales, personal y transporte.

6. Adquisición de recursos de software, hardware, materiales y contratación de personal.

7. Iniciar con la instalación y configuración del nuevo centro de cómputo.

8. Reestablecer los Backups realizados a los sistemas.

Es de vital importancia definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre que afecten la infraestructura tecnológica tanto académica como administrativa.

Las actividades a realizar en un plan de recuperación se pueden clasificar en tres etapas:

12.3 Actividades previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de los activos de la infraestructura tecnológica de la Institución, que nos aseguren un proceso de Recuperación con el menor costo posible.

12.4 Establecimiento del Plan de Acción

Equipos de Cómputo: Es necesario realizar un inventario actualizado de los equipos, especificando su contenido (software y licencias).

Respaldos de Información o 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 del Software y/o Sistemas operativos. Copias del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos), Software de uso diario, herramientas de trabajo, Bases de Datos, Aplicativos.

- Uso obligatorio de un registro detallado y control de los Backups.

- 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.

- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad.

12.5 Actividades durante el Desastre

Una vez presentada la contingencia, Falla o Siniestro, se deberá ejecutar el siguiente procedimiento:

12.6 Procedimiento de Emergencias

Se establecen las acciones a realizar cuando se presente una falla o desastre, así como la coordinación y comunicación de las mismas.

Es muy conveniente prever los posibles escenarios de ocurrencia del Siniestro, el cual se puede dar en horario diurno, como nocturno.

Los procedimientos deben contemplar la participación y actividades a realizar por todas las personas que se pueden encontrar presentes en el área de ocurrencia, detallando, salidas de emergencia, vías de evacuación, señalización y demarcación de las señales de auxilio (extintores, caja de breakers, linternas y lámparas de mano, números telefónicos de emergencia y nombres de funcionarios a contactar).

12.6.1 Actividades después del Desastre

Después de ocurrido el Desastre es necesario realizar:

- Evaluación de Daños: Inmediatamente después de concluido el desastre, de deberá evaluar la magnitud del daño producido, equipos estimación del tiempo.
- Ejecución de Actividades: La recuperación y puesta en marcha del servicio afectado, se realizara en dos fases, la primera restablecer el servicio usando los recursos propios (Equipos de respaldo) y la segunda con el apoyo de proveedores y entes tanto gubernamentales como no gubernamentales.
- Evaluación de Resultados: Finalizada las fases de recuperación, se debe evaluar objetivamente.
- Las actividades realizadas, porcentaje de eficiencia y efectividad, tiempo, inconvenientes, colaboración y apoyo.
- Retroalimentación del Plan de Acción: Con la evaluación de resultados, se debe actualizar el plan de acción original, mejorando las actividades más complejas y reforzando las que respondieron adecuadamente.

12.7 Amenazas

- Incendio: el fuego es una de las principales amenazas y causas de desastre, contra todo tipo de infraestructuras físicas. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los humanos.
- Inundaciones: Daños por agua pueden ocurrir como resultado de goteras y filtraciones del techo, goteras de tuberías o del aire acondicionado cerca a equipos electrónicos.

- Terremotos: Catástrofe natural se pueden presentar en cualquier momento y sin previo aviso, por tanto es de suma importancia incluir en el plan de acción, recomendaciones a seguir, dando prioridad a salvaguardar la vida de los funcionarios del instituto.
- Instalaciones eléctricas: Para que funcionen adecuadamente, los computadores de escritorio necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible. Por lo general los computadores personales toman la electricidad de los circuitos eléctricos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una corriente alterna (AC), ya que alterna el positivo con el negativo. La mayor parte de los computadores incluyen un elemento denominado fuente de alimentación, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes del equipo informático. Se recomienda tener redes eléctricas reguladas y contar con dispositivos reguladores, estabilizadores de potencia y ups.
- Bases de Datos y aplicativos: La Red de datos es la que permite transmitir información de un computador a otro. La estructura de Red que posee INTENALCO EDUCACION SUPERIOR es cliente/servidor, por lo que el servidor es uno de los componentes importantes de la Red. El cableado es estructurado y topología es estrella extendida, se cuenta con tecnología

inalámbrica. El elemento activo de comunicaciones es el switch de datos, conectado a un router, el cual permite trasladar a cada nodo (host) los paquetes de datos para que se intercambie información en toda la Red. Es una Red de Área Local (LAN), lo que limita su cobertura de servicios estrictamente, sin embargo, a través de un proveedor de servicios, se puede tener acceso a la Red Internacional (Internet) para utilizar este recurso como herramienta pedagógica en el proceso enseñanza – aprendizaje y complementar labores diarias en la parte administrativa. Es por ello, que debe ser de suma importancia el poder detectar las fallas en la red de datos, ya que de esa forma se permitirá prestar en un cien por ciento (100%) de sus recursos disponibles a la comunidad educativa.

- Cableado estructurado: El cableado estructurado es la plataforma de comunicaciones en la red que posee INTENALCO EDUCACION SUPERIOR, este cableado usualmente es UTP cable de par trenzado no apantallado) y su importancia radica que es el medio de transmisión por el cual se transmite la información de un nodo a otro. Es posible que por problemas de cableado, se tengan problemas de conectividad, sin embargo, en la mayoría de casos, el cableado entregado debe estar debidamente certificado por el proveedor y supervisada por la Oficina de TI.
- Equipos de comunicación: El elemento activo de comunicación que se utiliza en el Instituto es el swicth de datos, el cual es un elemento que permite la transmisión de tramas (paquetes de datos) desde la tarjeta de Red del Transmisor a la tarjeta de Red del Receptor. Este elemento activo de comunicaciones es de suma importancia, y no debe estar apagado, ya que en ese momento se tendría una caída en la Red de datos. Usualmente estos elementos activos de comunicación son de 24 puertos, los cuales poseen unos led (indicadores visuales) que señalan el estado de

funcionamiento de cada puerto, en el momento en que está activo el puerto, el led del mismo debe estar encendido. Cada puerto conecta a un nodo o computador por lo que una de las formas de detectar que hay falla de comunicación es observar el puerto, obviamente, cada puerto debe estar relacionado con el punto de red respectivo.

- Problemas en el switch de datos: Si el elemento activo tiene una falla de tipo eléctrico este no encenderá y se tendrá un problema similar al caso anterior.
- Problemas de puerto: es posible que por alguna variación de voltaje, se queme una cantidad limitada de puertos, se recomienda verificar los led que indican conectividad.

- Problemas en la tarjeta de Red: puede existir la posibilidad de que la tarjeta de red este fallando, una forma rápida de verificar su funcionamiento es identificar si el led de la tarjeta de red está funcionando, en caso contrario es posible que la tarjeta no esté operando adecuadamente. Otro caso probable es que este desactivado desde el sistema operativo.

- En el caso de falla en el suministro de energía eléctrica, se recomienda colocar un UPS dedicado para el elemento activo.es recomendable que la UPS tenga un regulador de voltaje integrado para evitar picos de voltaje.

- Por problemas de puerto: una forma sencilla de verificar que el puerto está fallando, es verificar que el led de la tarjeta con que está conectado el puerto esta encendido, si al realizar un ping al server, este no contesta, entonces, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, si al realizar un ping al server y este contesta, entonces, se puede concluir que el puerto es el que

está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.

- Por problemas en la tarjeta de red: La tarjeta puede estar deshabilitada desde el sistema operativo, será necesario revisar si este está habilitado o no, en el caso que este deshabilitado, habilitarlo inmediatamente desde el sistema operativo. Si está habilitada la tarjeta de red y no hay comunicación, será necesario reinstalar el "driver" de la tarjeta de Red, o revisar si posee dirección Ip.

13. POLITICA Y REGLAMENTO PARA LA OPERACIÓN DEL SITIO WEB DE LA INSTITUCIÓN

Intenalco entiende el sitio web como un medio de comunicación en todo lo relativo a contenidos e imagen gráfica, entendidos estos como: el carácter institucional de la institución y la comunicación externa e interna, reconoce y asume el valor de este espacio virtual como herramienta de promoción, comunicación y apoyo permanente a los procesos de enseñanza, aprendizaje.

a) La Oficina de TI como proceso de Gestión tecnológica tiene la responsabilidad de garantizar la integridad de la información.

b) Está prohibido la publicación de información privada o sensible sin la respectiva autorización del personal involucrado.

c) Todos los contenidos que aparecen en la página Web, son responsabilidad del área que los emite.

Antes de publicar la información en la página web se debe verificar la redacción y ortografía.

d) El nombre de dominio "www.intenalco.edu.co" y todos aquellos que sirvan para acceder de forma directa al sitio oficial de la institución son de titularidad exclusiva de Intenalco. La indebida utilización de los mismos supondría una infracción de los derechos conferidos por su registro y será perseguido por los medios previstos en la Ley.

e) Quedan exceptuados de esta protección aquellos archivos o programas de computador que no sean de titularidad de la institución y de acceso gratuito o aplicaciones que tienen el carácter de dominio público por voluntad de sus autores.

f) Cualquier link o vínculo a páginas externas a Intenalco, deberá ser autorizado por la Oficina de Informática y la vicerrectoría administrativa.

g) Toda solicitud para realizar cambios o publicaciones en la página web debe estar sustentada por un comunicado escrito o correo electrónico.

14. SEGURIDAD DE LA INFORMACIÓN DE LOS PROCESOS MISIONALES

En los procesos misionales se busca la protección y tratamiento de la información de acuerdo a la ley 1581 de 2012, la cual debe ser integra, estar disponible y ser confidencial, con el fin de garantizar la no expedición de la información sensible sin previa autorización del personal involucrado.

Para INTENALCO, es crucial proteger la información sensitiva, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indiscriminada.

Intenalco establece actividades para evitar el fraude, espionaje, sabotaje o vandalismo que puedan alterar la seguridad de la información, se cuenta con software de información en los procesos críticos, los cuales permiten una mejor administración y protección de la información.

Que información debe ser protegida:

- Información con datos de los estudiantes y comunidad educativa.
- Información en los Sistemas (SIGA, SEVENET, software contables, entre otros que contengan información confidencial y datos sensibles).
- Oficios enviados por fax.
- Oficios físicos.
- Archivo digital en disco duro o USB.
- Datos en las Bases de datos.

AMENAZAS ASOCIADAS AL USO DE LA INFORMACIÓN

- Uso de las Contraseñas.
- Correo Electrónico y Mensajería Instantánea.
- Virus Informáticos y SPAM.

- INTERNET.
- Conexiones Publicas (cafes internet) y Spyware (SW espía).
- Phishing (suplantación identidad)
- Hackers (Acceso no Autorizado)
- Dispositivos Móviles.

14.1 Actividades de seguridad

- Bloquear y proteger las unidades cuando no estén siendo utilizadas (guardar bajo llave).
- No colocar medios removibles cerca de fuentes electromagnéticas (Imanes).
- Marcar los medios indicando su contenido.
- Destruir siempre los medios de almacenamiento removibles antes de der desechados.
- Realizar inventario de los contenidos de los medios extraíbles con frecuencia, eliminando datos que no sean necesarios almacenar en estos.

14.2 Logs de aplicaciones sensibles

Todas las aplicaciones de producción que manejen información sensible de la Institución, deben generar logs que muestren cada modificación, incorporación y borrado de la información. Esto incluye modificaciones a los sistemas de producción y modificaciones a los sistemas fuente.

Los sistemas que manejen información valiosa, sensible o crítica deben además contener y activar forzosamente el log sobre todos los eventos o procesos

relacionados con la seguridad de acceso a los mismos. Ejemplo: Varios intentos de contraseña, intentos de uso de privilegios no autorizados, entre otros.

Los logs de procesos relevantes deben de proveer información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad.

Todos los comandos emitidos por los operadores de sistemas deben ser rastreables o identificables para especificar su uso individual.

El período que debe activarse y depurarse un log es por lo menos cada mes. Durante este período, el administrador del sistema y/o dueño de la información, se debe asegurar que éste no sea modificado, y cerciorarse de que no sea leído por personal no autorizado. Estos aspectos son importantes para la corrección de errores, auditorías o brechas de seguridad.

Para evitar conductas inapropiadas, crear un sentido de responsabilidad del usuario, y permitir una administración adecuada de los sistemas, todas las actividades de los usuarios que afecten producción deben ser trazables desde el log. Las aplicaciones y otros manejadores de Bases de Datos, deben tener logs para las actividades de los usuarios y estadísticas relacionadas a estas actividades que les permitan identificar y detectar alarmas de posibles problemas o mal uso, y que reflejen eventos misionales de la institución sospechosos. El objetivo es que todos los movimientos que se realizan dentro de las operaciones críticas o sensibles de la institución, sean registrados, para detectar y reducir el riesgo de violación o fraudes. Estas herramientas sirven como evidencia y apoyo para la detección de la fuente del problema ocasionado, identificando sus posibles causas y posibles soluciones.