****

**UNIVERSIDAD PEDAGOGICA NACIONAL**

**SUBDIRECCION DE GESTION DE SISTEMAS DE INFORMACION**

**Plan de Continuidad y de Recuperación de Desastres.**

***CONTENIDO***

INTRODUCCIÓN..........................................................................................

GENERALIDADES ........................................................................................

Objetivos ...................................................................................................

Objetivo General.......................................................................................

Objetivos Específicos.................................................................................

Alcance ......................................................................................................

MARCO CONCEPTUAL .................................................................................

Definiciones: ...............................................................................................

ANALISIS DE LA EVALUACIÓN DE RIESGOS …………………… ........................

Factores de afectan la seguridad física y la infraestructura.......................

Posibles daños: ...........................................................................................

Fuentes de daño: ........................................................................................

Clases de riesgo..........................................................................................

Factores asociados con la seguridad lógica .............................................

Factores asociados con la seguridad técnica integral ...............................

Minimizar el Riesgo ...............................................................................

Incendio o fuego.............................................................................

Robo común de equipos y archivos ..................................................

Falla en los equipos.......................................................................

Acción de virus informático............................................................

Terremoto ....................................................................................

Sabotaje.......................................................................................

PLAN DE RECUPERACION DE DESASTRES.....................

Actividades ............................................................

***INTRODUCCIÓN***:

Este plan de contingencia de la información vital de la UPN ante la posible pérdida, destrucción, robo y otras amenazas, contempla la infraestructura que se encuentra en el Centro de Computo de la sede Principal de la Universidad en la Calle 72.

Cualquier Sistema ya sea (Almacenamiento, Librerías, Servidores, Switches, Router) 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. La Subdirección de Sistemas tiene el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a eso es importante contar con un Plan de contingencia adecuado de forma que ayude a la Universidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la Universidad.

***GENERALIDADES***

***Objetivos***

***Objetivo General***

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la Universidad, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la UPN.

***Objetivos Específicos***

Evaluar, analizar y prevenir los riesgos informáticos en la UPN que pueda ser suspendida completa o parcialmente la prestación del servicio.

***Alcance***

El Plan de Contingencias Informático está basado en la realidad que manifiesta la Universidad, y puede servir como punto de partida hacia la adecuación y establecimiento de políticas en los diferentes procesos.

***MARCO CONCEPTUAL***

***Definiciones:***

***AMENAZA:*** probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

***CONTIGENCIA***: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de esta Universidad.

***ELEMENTOS EN RIESGO:*** Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

***VULNERABILIDAD:*** La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de “0” (no hay daños) a “1” (daño total).

***RIESGO:*** Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

***GRAVEDAD:*** Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

***SEGURIDAD:*** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

***DATOS:*** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

***INCIDENTE:*** Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

***ACTIVO:*** Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

***ANALISIS DE LA EVALUACIÓN DE RIESGOS***

**Factores que afectan la seguridad física y la infraestructura.**

|  |  |
| --- | --- |
| **Situación de Riesgo** | **Plan de Contingencia** |
| Desastre Natural | Backup en cinta de la Información y se guarda la cinta de backup en custodia al proveedor de custodia de medios semanalmente. |
| Ataque terrorista y/o Pedrea al Interior de la Sede Principal de la Universidad en la calle 72 | Backup en cinta de la Información y se guarda la cinta de backup en custodia al proveedor de custodia de medios semanalmente. |

|  |  |
| --- | --- |
| Caídas de energía de corta duración. | Se cuenta con respaldo de UPS y Planta Eléctrica |
| Fallas en disco duro | Se cuenta con Garantía Extendida para la Infraestructura de servidores |
| Daño de archivos | Se cuenta con Backup de archivos de Servidores de aplicaciones y Servidores de Bases de Datos, se cuenta con contratos de Soporte correctivo para la Infraestructura de servidores y el Firewall (seguridad perimetral), también cuenta con contrato de soporte correctivo. |
| Daño de equipo | Se cuenta con Backup de archivos de Servidores de aplicaciones y Servidores de Bases de Datos, se cuenta con contrato de Soporte correctivo para los servidores y el Firewall (seguridad perimetral), también cuenta con contrato de soporte correctivo. |
| Falla en los Canales de comunicación Internet | Se cuenta con un contrato vigente para el servicio de conectividad, que contempla soporte correctivo a todos los canales de Internet que tiene la UPN, en la instalación principal de la Universidad en la Calle 72, se tiene alta disponibilidad en los equipos de comunicación. |
| Fallas de hardware (fallas en los servidores o falla en el cableado de red, Switches, Router) | Se tienen switches de backup e ingenieros con conocimiento en los equipos con que cuenta la UPN para este fin.. |
| Factores asociados con la seguridad técnica integral Fallas, daños y/o deterioros por mal uso, fallas de mantenimiento y/u obsolescencia para, Servidores. | La Universidad cuenta con un grupo de Ingenieros en el Área de Infraestructura que dan soporte correctivo y preventivo a los Servidores de Aplicaciones, Bases de Datos, Almacenamiento, Infraestructura Virtual. |

**Incendio o fuego**

**Grado de negatividad: Muy Severo**

**Frecuencia de evento: Aleatorio Grado de impacto: Alto**

|  |  |
| --- | --- |
| **Situación de Riesgo** | **Plan de Contingencia** |
| La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma todos los pisos de la institución cuenta con un extintor debidamente cargados. | Se cumple |

|  |  |
| --- | --- |
| Se ejecuta un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a todo el personal perteneciente a la brigada de emergencia. Lo que es eficaz para enfrentar un incendio y sus efectos. | Se cumple |
| Se realiza copia de seguridad diariamente. | Se hace Backup en cinta de toda la Información de la Universidad, Diario, Semanal y Mensual y se guarda la cinta de backup en custodia al proveedor de custodia de medios semanalmente. |

**Robo común de equipos y archivos Grado de negatividad:**

**Grave Frecuencia de evento: Aleatorio**

**Grado de impacto: Moderado**

|  |  |
| --- | --- |
| **Situación de Riesgo** | **Plan de Contingencia** |
| Se toma registro de la hora de entrada y salida de las personas particulares que ingresan a la Universidad. En caso de que se presente un incidente, se pasará a mirar las cámaras de seguridad. | Se cumple el control de acceso con el diligenciamiento de una bitácora, adicionalmente se cuenta con cámaras de seguridad para el centro de cómputo y el acceso al centro de cómputo principal se lleva a cabo por medio de huella y tarjeta de proximidad. |
| Autorización escrita firmada por coordinador del área o el responsable para salidas de equipos. | Se cumple. |
| 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 |

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del Jefe de Cada Área y el subdirector de Sistemas, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado. Tampoco se han reportado casos donde haya habido hurtos de nuestro sistema computo en la Universidad sin embargo se recomienda siempre estar alerta.

**Falla en los equipos**

|  |  |
| --- | --- |
| **Situación de Riesgo** | **Plan de Contingencia** |
| La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza. | Se realiza mantenimiento preventivo de los equipos una vez al año, Se genera diagnóstico de la Infraestructura, se actualizan los Backups de configuración. |
| La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata. | Se cuenta con contratos de Garantías extendida con los fabricantes de los equipos, en caso de requerir remplazo de piezas, la garantía extendida es para toda la Infraestructura. |
| El daño de equipos por fallas en la energía eléctrica requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo. | Se tiene UPS y Planta Eléctrica para el Centro de Computo |

Analizando el riesgo de falla de los equipos, es recomendable estar realizando mantenimiento preventivo a los equipos computo que no tienen garantía extendida.

**Acción contra virus informático**

|  |  |
| --- | --- |
| **Situación de Riesgo** | **Plan de Contingencia** |
| Se cuenta con un software antivirus para la entidad. | La Universidad cuenta con un contrato de soporte preventivo y correctivo para el Software Antivirus institucional y cuenta con las licencias de antivirus para Servidores y para estaciones de trabajo. |
| Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo con su necesidad. | Se cumple para todos los Equipos que se administran en el Centro de Computo. |
| Los antivirus se actualizan periódicamente en cada equipo. | Se cumple. |

**En caso de Terremoto**

• Sin Pérdida O Daños Menores De Las Instalaciones: El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo.

• Con Pérdida De Las Instalaciones: La pérdida de las instalaciones afectaría gravemente a las operaciones de la Universidad y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

**En caso de Sabotaje**

La protección contra el sabotaje requiere:

• Una selección rigurosa de los colaboradores.

• 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 sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. 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.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

• Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.

• Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.

• Siempre habrá que tomarse en cuenta las Políticas de Seguridad en casos como terrorismo y sabotaje. Es importante la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.

• Mantener adecuados archivos de reserva (backup)

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

• Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.

• Usar rastros de auditoría o registro cronológico (Logs) de transacción como medida de seguridad.

**PLAN DE RECUPERACION DE DESASTRE**

**Actividades básicas:**

* Resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. La Universidad cuenta con el servicio de custodia de Medios, permitiéndonos tener los Backup en cinta, fuera de las instalaciones de la Universidad.
* Para los Sistemas de Información: La Universidad cuenta con una relación de los Sistemas de Información de software, para respaldarla con backup.
* Para los Equipos de Cómputo: Se cuenta con Garantías Extendidas para la Infraestructura de servidores y equipos de comunicaciones (datos y voz), también se tienen los respectivos Backup de configuración.

**La Universidad también ha contemplado los siguientes criterios sobre identificación y protección de equipos:**

* Pólizas de seguros, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
* Marcación o etiquetamiento de las computadoras de acuerdo con la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante.
* Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la entidad.

**Falla en las comunicaciones (Teléfono, internet)**

* Ante una falla en las comunicaciones (telefonía fija e internet), se opta por la telefonía móvil, para lo cual se han adquirido celulares corporativos asegurado la comunicación de los directivos de la Universidad responsables de las áreas críticas de la UPN.
* También se cuenta con redundancia en el Servicio de Internet, es decir se cuenta con un canal principal y otro de respaldo que entraría en funcionamiento en caso de algún incidente con el canal principal.
* La central telefónica para telefonía fija y celufijos, tiene su contrato preventivo y correctivo, asegurando la atención al incidente de manera inmediata y con el proveedor especialista de la solución telefónica que tiene la Universidad.