OBJETIVO

Proteger la información, bases de datos y documentación crítica para la Universidad Pedagógica Nacional, con el fin de que se conserven así como la restauración de la misma en el momento que se necesite, prevaleciendo la confidencialidad, integridad y disponibilidad de la información.

ALCANCE

Las directrices de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control, estas deben ser cumplidas por todos los servidores públicos de la Universidad Pedagógica Nacional, dando cumplimiento de las respectivas funciones y el adecuado nivel de protección de la información sensible que administre, aportando con su participación en la toma de medidas preventivas y/o correctivas aplicándola inicialmente a salvaguardar la información y termina con la verificación del Backup y custodia segura de la información.

NORMATIVIDAD

Ley 679 de 2000; por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

Resolución 0696 del 16 de junio de 2005; Por la cual se adopta el manual de Políticas, Normas y Procedimientos para la administración de los recursos computacionales, informáticos, multimediales y de comunicaciones de propiedad de la Universidad Pedagógica Nacional.

ISO/IEC 27000; Conjunto de estándares desarrollados o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

RESPONSABLE

Subdirección Sistemas de Información

APLICACIONES:

BACULA: Software especializado en realizar Backup a los datos, bases de datos.

DEFINICIONES

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la universidad y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en los que los servidores públicos de la Universidad o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de carácter confidencial de la universidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la institución.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Archivos log: Es un registro oficial de eventos durante un rango de tiempo en particular, es usado para registrar datos o información sobre quién, qué, cuándo y por qué un evento ocurre para un dispositivo en particular o aplicación.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Backups : Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un medio magnético que sean confiables, con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto. Es conveniente realizar copias de seguridad y verificación de las mismas a intervalos temporales fijos (por ejemplo diario, semanal, quincenal, mensual, etc.) en función del trabajo y de la importancia de los datos manejados.

Backup completo: Es una copia de seguridad de los archivos que incluye a toda la información que está alojada en un sitio local o en un servidor que pueden ser bases de datos, archivos de forma completa, se realiza el Backup en un medio magnético que sea confiable.

Backup incremental: Es una copia de seguridad de los archivos que incluye solo la información que se haya modificado desde la última copia de seguridad, en el determinado tiempo establecido del Backup incremental, por ejemplo se inicia con un Backup completo y luego se realizan son Backup s incrementales de bases de datos completas y archivos.

Base de Datos: Conjunto de datos que pertenecen al mismo contexto almacenados Sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o Vídeo.

Copia de Respaldo o Seguridad: Acción de copiar archivos o datos de forma que estén

disponibles en caso de que un fallo produzca la pérdida de información almacenada en los servidores.

Copias de Seguridad: Copias de la información en un medio magnético que se almacena en un lugar seguro y con la respectiva custodia de seguridad.

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder dicha información. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27001, con el fin de garantizar que la información sea accesible sólo para aquellos autorizados a tener acceso".

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Contingencia: Conjunto de procedimientos de recuperación. Las acciones a contemplar aplican para Antes- Durante- Después con el fin de reducir las pérdidas de información.

Centros de cableado: Son sitios o espacios físicos donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que el centro de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de protección eléctrica y condiciones de temperatura y humedad relativa adecuados.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores -servidores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares mínimos con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Disponibilidad: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran y/o necesiten.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información: Directrices para catalogar la información de la institución y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Integridad: Propiedad que busca mantener los datos libres de modificaciones no autorizadas; es decir mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, con la exactitud y estado completo de los todos los activos de información.

ISO: Sigla (International Organization for Standardization)

IEC: Sigla (International Electrotechnical Commission).

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes al instituto.

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propietario de la información: Es el área, la unidad organizacional o proceso donde se crean los activos de información.

Plan de Contingencia: Procedimientos alternativos de una institución, cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando alguna de sus funciones se vean afectadas por un accidente interno o externo.

Recuperación: Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Restauración: Volver a poner algo en el estado inicial. Una base de datos se restaura en otro dispositivo después de un desastre.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la universidad.

Registro: Documento donde son registrados los resultados de eventos que se ha identificado en los sistemas de información, recursos tecnológicos y redes de datos de la institución (UPN, IPN). Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas, conformado por todo componente de software ya sea de origen interno, es decir desarrollado por la universidad o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Sistemas de Misión Crítica: Aquellos servidores que ejecutan aplicaciones esenciales que, si fallan, tienen un impacto significativo en el funcionamiento de cualquier empresa, organización o institución que dependa de su información.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

Condiciones Generales de la Política de Backup y Restructuración de la Información

1. Las cintas de Backup o medios magnéticos, deben ser retirados del Centro de cómputo donde se realizan y estas deben ser custodiadas en un sitio externo a la UPN, por una empresa especializada en el almacenamiento y custodia que garantice la seguridad, ambiente seguro y disponibilidad de las mismas.

2. Las cinta de Backup debe quedar registrada por la máquina o aplicación de Backup , donde son realizados (logs de aplicación) y en un archivo externo (texto, planilla, etc.) que permita dejarlo disponible para controles o auditorías y en los cuales se puedan confirmar que el respaldo de la información efectivamente fue realizado.

3. El encargado de las copias de seguridad (operador o administrador del servidor) es el encargado de registrar todas las actividades relacionadas con los Backups, restauraciones de la información. Estos registros deberán quedar disponibles en dos copias impresas, una copia para el área de infraestructura y la otra copia para la subdirección de Sistemas Informáticos.

4. La recuperación de información debe ser solicitada por el usuario final y debe venir con la autorización del Jefe de Área, de acuerdo al formato unificado FOR005GSI - “Control Copia de seguridad y restauración de Backups ” previamente establecido por el Sistema

de Gestión Integral de la Universidad y enviándolo al correo electrónico a mesa de ayuda

5. La plataforma de Backup son medios de respaldo (cintas, librería, etc.) deben ser monitoreados mensualmente usando la misma plataforma de Backup con el que se realiza el respaldo de la información que permita revisar el estado de la plataforma de Backup .

6. Mensualmente debe ser enviado por correo electrónico al responsable de Infraestructura con copia al Subdirector de Sistemas de Información, un informe detallado con los resultados de los Backups y restauraciones del mes e indicando la información que fue respaldada y en caso que por algún motivo el proceso de Backup falle, informar el plan de contingencia usado como copia local o copia a un servidor externo con su respectiva fecha.

7. Debe quedar disponible en El Data Center un Directorio de teléfonos de contacto, en caso de ser necesario solicitar soporte de la plataforma de respaldo de la SSI (proveedor, nombres, correos y teléfonos de contacto, modelos y números de serie de los medios que conforman la plataforma de respaldo).

8. Las claves de usuario no serán respaldadas, es responsabilidad de los usuarios el buen manejo de las contraseñas.

9. Todo Servidor Público de la universidad y que por motivos de culminación de contrato, retiro o una licencia, la Subdirección de Personal y/o grupo de contratación debe informar al Área de SSI para que efectué el Backup y deje registro del resultado, realizado mediante el formato establecido y esto será parte integral del Paz y Salvo para la gestión del retiro de los servidores públicos.

10. Información que no se considere relevante para el trabajo diario de la UPN y que resida en los servidores de la UPN, esta información no será respaldada. La utilidad de la información será determinada por el área o dependencia competente.

11. La frecuencia de los Backups de las bases de datos y aplicaciones serán diarios, semanales y/o mensuales, según la importancia de la información almacenada en los servidores, así mismo estos se almacenarán los Backups anuales de acuerdo a la tabla de retención de la información por al menos cinco (5) años en cinta, a partir de la fecha de la publicación de este instructivo, después de este periodo de tiempo se procederá a la eliminación de esta información.

12. Los medios magnéticos en donde se realizan los Backups de información deben ser llevados a un sitio externo donde se garantice la custodia, seguridad y disponibilidad con un tercero en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica.

13. Deben realizarse Backups a todas las aplicaciones misionales y funcionales que existen en la actualidad y a las aplicaciones nuevas, desarrolladas, implementadas a la posterior

publicación de este documento; se les realizara “Backup completo” el primer día y el tercer domingo de cada mes a las 23:00 horas. El “Backup incremental” se realizara de lunes a domingo a las 23:00 horas.

14. La Subdirección de Gestión de Sistemas de Información debe diligenciar el formato ***“FOR005GSI Control copia de seguridad y restauración de Backup”,*** es responsabilidad de los administradores de infraestructura de las aplicaciones o bases de datos según sea el caso) y en donde se indique la fecha, hora, estado, e información a la que se realiza el “Backup ” y de igual manera la información de las cintas utilizadas en el proceso, estas debe etiquetarse con el estándar que previamente haya sido definido en la SSI.

15. Los medios magnéticos pueden ser utilizados, sin embargo deben cumplir con el estándar en su etiquetado que debe contener los siguientes datos: Diario, semanal, mensual y con el formato de (dd/mes/año) incremental o completo.

16. En caso de que algún medio magnético presente un deterioro o falla debe ser reemplazado por uno nuevo que garantice el respaldo de la información de manera correcta.

17. Los administradores de servidores o de bases de datos encargados de los Backups dentro de la Subdirección Sistemas de Información, debe documentar en el formato *“FOR005GSI* Control Copia de seguridad y restauración de Backups”, todas las acciones realizadas en lo que se refiere al Backup de información, estos formatos se entregaran mensualmente al grupo de infraestructura con copia a la jefatura de la SSI y deben ser archivadas de acuerdo a la tabla de retención de la subdirección, para que sean para que sean el soporte ante cualquier solicitud de auditoria del proceso, ya sea a nivel interno o externo.

18. La Subdirección de Gestión de Sistemas de Información SSI – recibe el formato *FOR005GSI,* evalúa la solicitud y da una respuesta de aprobación o negación, según la solicitud de restauración del Backup de información de la universidad con el debido proceso de autorización por parte del área de SSI o un ente externo que sea una autoridad competente como fiscalía, etc.

19. El resguardo y almacenamiento de las copias de seguridad es responsabilidad de la Subdirección de Sistemas de Información

20. Es responsabilidad de la Subdirección de Gestión de Sistemas de Información realizar Backup de la información de Sistemas de Misión Crítica procesada y contenida en los servidores Institucionales. Deberá responder también por la custodia de medios que contienen dicha información y garantizar su recuperación en caso de desastre.

21. Es responsabilidad de los usuarios realizar Backup , custodia de la información y del correo institucional, localizado en su computador que le sea asignado como herramienta de trabajo , según lo enunciado en la Resolución 0696 del 16 de junio de 2005 en el capítulo IV artículo 11 ,así:

"1.- Cada usuario se responsabiliza de conservar y salvaguardar la integridad de la información y del bien informático a su cargo.

2.- "Deberá mantener el respaldo de la información requerida para su trabajo, incluyendo en ello, el respaldo de los mensajes de correo electrónico que requiera conservar".

Así mismo, en el capítulo VI artículo 15 :

1- "Por efecto de privacidad y confidencialidad, todo usuario de correo electrónico, deberá mantener copias de seguridad de los mensajes de correo electrónico que requiera conservar".

Los usuarios solicitarán a la Mesa de Ayuda de la Subdirección de Gestión de Información el apoyo e instrucciones técnicas y capacitación especial, en caso de ser necesario, para realizar esta labor.

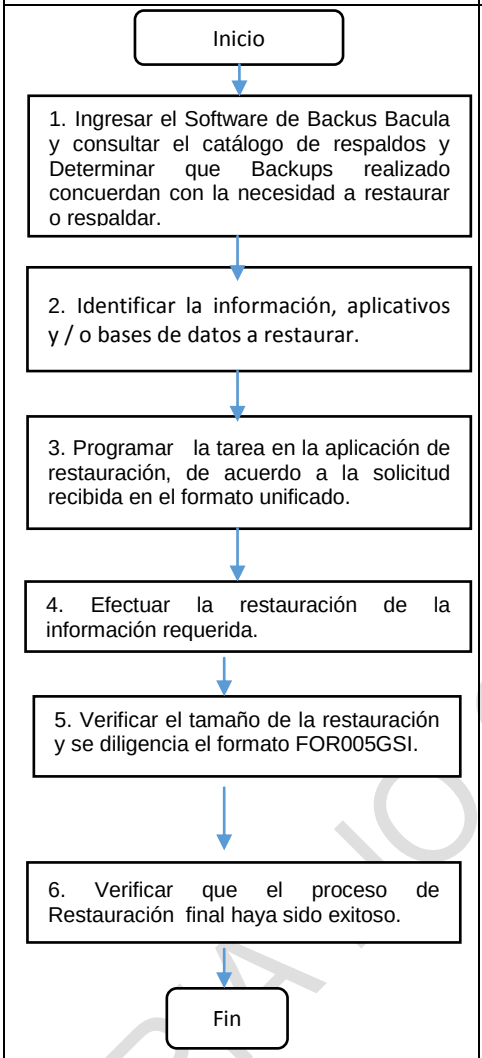
Descripción pasos a seguir para la realización de Copias de Seguridad a manera de Backup de la información contenida en los servidores institucionales:

Pasos para realizar las Copias de Seguridad a manera de Backup de la información

SUBDIRECCIÓN DE GESTION DE SISTEMAS DE INFORMACION (SSI)

TAREA	REGISTRO	TIEMPO ESTANDAR	OBSERVACIONES
Inicio			
1. Ingresar al Software Bacula, que gestiona y realiza las copias de seguridad a manera de Backups a Cinta.			Diligenciar FOR005GSI "Copias de Seguridad a manera de Backup ".
2. Identificar la información, aplicativos y/o bases de datos a respaldar.			Se identifica el número de aplicativos y/o bases de datos para el respaldo. Inventario aplicativos
3. Programar la tarea en la aplicación de backup, da cuerdo a la rotación de backup.			
4. Realizar el respaldo de forma local en servidor.			Se realiza copia de manera diaria, semanal, mensual y anual de acuerdo a la política de Backup en un dispositivo de almacenamiento (servidor o SAN), todas las copias y enviar a custodia externa.
5. Ordenar el respaldo o copia de seguridad en Cinta	FOR005GSI	1 Semana	
6. Verificar el log del Backup, para validar el resultado del respaldo			Se verifican los archivos log del aplicativo utilizados para la copia de seguridad. Ingeniero administrador del servidor o de base de datos
7. Verificar el tamaño del backup realizado según los resultados de la realización del Backup y se diligencia el formato FOR005GSI			Almacenar la copia y para el caso de ser un medio magnético (cinta de Backup) se marca con la respectiva fecha y aplicaciones
8. Almacenar y enviar a custodia externa de medios de las cintas de backups.	Registro Proveedor del Servicio y Copia para Data Center		Se envían las cintas de Backups a Custodia, almacenamiento y conservación externa de medios.
Fin			Fin del procedimiento

Pasos para la restauración de las Copias de Seguridad a manera de Backup de la información

	TAREA	REGISTRO	TIEMPO ESTANDAR	OBSERVACIONES
SUBDIRECIÓN DE GESTION DE SISTEMAS DE INFORMACION (SSI)		FOR005GSI	15 días	Diligenciar FOR005GSI “Copias de Seguridad a manera de Backup”. Se identifica el número de aplicativos y/o bases de datos para el respaldo. Inventario aplicativos Se realiza la restauración del aplicativo. Si es una base de datos, se determina la hora para la respectiva restauración y se informa a los usuarios para suspender el aplicativo mientras se realiza la restauración Se registra la restauración realizada, si es una base de datos se guarda el registro o bitácora del mismo

Control de Cambios

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
07-07-2016	1	Creación del documento

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Equipo de Trabajo-Gestión de Sistemas Informáticos	César Mauricio Beltrán López **Subdirector Sistemas de Información**	Adolfo León Atehortúa Cruz **Rector**