VISTO, el proyecto denominado "Políticas de Backup de la Facultad de Ciencias Humanas", presentado por el Área de Tecnologías de la Información y de las Comunicaciones –TICs.hum- de esta Unidad Académica, y

CONSIDERANDO:

Que dicho Proyecto fue presentado oportunamente por el Responsable del Área mencionada, Sr. Gustavo Gaumet (DNI Nº 25490736), a solicitud del agente Tec. Erié Eduardo Maseda (DNI Nº 21407331), él cual es el autor del mismo, y avalado por la Directora General de esta Facultad de Ciencias Humanas, Srta. Claudia Vescovi (DNI Nº 23226108).

Que el mencionado Proyecto, guarda coherencia con la norma similar aprobada oportunamente por el Consejo Superior.

Que se cuenta con el Dictamen Nº 7913 de la Dirección de Asuntos Jurídicos de esta UNRC, de fecha 02 de agosto/2016, según el cual nada tiene que observarse desde lo legal, al tiempo que se trata de una real necesidad institucional.

Que la Comisión de interpretación y Reglamento del Consejo Directivo, no tiene nada que observar al Proyecto presentado, sugiriendo en consecuencia: aprobar el Proyecto denominado "Políticas de Backup de la Facultad de Ciencias Humanas", presentado por el Área de Tecnologías de la Información y de las Comunicaciones -–TICs.hum-.

Que fue aprobado en Sesión Ordinaria de este Consejo Directivo de fecha 06 de septiembre de 2016.

Por ello y en uso de las atribuciones que le confiere el Artículo 32 del Estatuto de la Universidad Nacional de Río Cuarto.

EL CONSEJO DIRECTIVO
DE LA FACULTAD DE CIENCIAS HUMANAS
RESUELVE:

ARTICULO 1º: Aprobar el proyecto denominado "Políticas de Backup de la Facultad de Ciencias Humanas", elaborado por el agente Tec. Erié Eduardo Maseda (DNI Nº 21.407.331), del Área de Tecnologías de la Información y de las Comunicaciones –TICs.hum- de esta Unidad Académica, el que se consigna en el único Anexo de la presente.-

ARTICULO 2º: Regístrese, comuníquese, publíquese. Tomen conocimiento las áreas de competencia, cumplido, archívese.

DADA EN LA SALA DE SESIONES DEL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS HUMANAS A LOS SEIS DIAS DEL MES DE SEPTIEMBRE DEL AÑO DOS MIL DIECISEIS.

RESOLUCIÓN C.D. Nº 349/2016.

ANEXO
Resol. C.D. Nº 349/2016

Políticas de Backup

de la Facultad de Ciencias Humanas

ESTADO FORMAL:

Elaboró:	**Revisó:**	**Aprobó:**
Erié Eduardo Maseda TP 7 – Técnico ATIC 13/06/2015	Gustavo David Gaumet TP 4 - Responsable ATIC	Claudia Noemí Vescovi A1 - Coordinadora General

OBJETIVO

Asegurar que la información generada por las diferentes unidades administrativas, no se pierda y esté disponible en caso de desastre, o cualquier contingencia, como daño en los discos duros, o eliminación accidental de la Información o bien un caso de desastre físico.

ALCANCE

Las Políticas de Backup deben ser conocidas y cumplidas por toda la comunidad universitaria de la facultad, tanto se trate de funcionarios políticos, docentes, no docentes, estudiantes, contratados, y toda persona que de alguna manera esté relacionada con la facultad, sea cual fuere su nivel jerárquico y su situación de revista.

MARCO LEGAL

Decisión Administrativa N° 669/2004 de la Jefatura de Gabinete de Ministros.
http://www.infoleg.gov.ar/infolegInternet/anexos/100000-104999/102188/norma.htm
Norma Internacional ISO/IEC 27001.

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103
Norma Internacional ISO/IEC 27002.

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50297
Ley 11.723 - Régimen legal de la Propiedad Intelectual
http://www.infoleg.gov.ar/infolegInternet/anexos/40000-44999/42755/texact.htm
Ley 24.286 - Modificas las penas de multa del Código Penal y de otras leyes.
http://infoleg.mecon.gov.ar/infolegInternet/anexos/0-4999/684/norma.htm
Ley 25.036 - Propiedad Intelectual - Modificación Ley 11.723
http://infoleg.mecon.gov.ar/infolegInternet/anexos/50000-54999/54178/norma.htm
Ley 25.326 - Protección de los Datos Personales
http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
Ley 26.388 - Código Penal
http://www.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

RESPONSABILIDADES

- De los Sistemas Centrales: El administrador de Sistemas de la Facultad de Ciencias Humanas es responsable de conocer, adoptar e implementar la presente política de backup.
- De las Estaciones de Trabajo o PC de Escritorio: El usuario es responsable de los respaldos de los equipos personales. Los usuarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo.

APLICACIÓN

- El administrador de los servidores deberá plasmar los procedimientos para el respaldo y recuperación, antes de entrar en producción el servidor. Los mismos serán controlados por el administrador de la aplicación, para verificar que es clara y completa, los procedimientos deberán contemplar como mínimo los siguientes elementos:
    1. El sistema operativo de los servidores y su configuración.
    2. Los parches y paquetes de software de base necesarios para que la aplicación se ejecute.
    3. Los programas que componen la aplicación.
    4. Los archivos y/o bases de datos del sistema.
    5. Horario de ejecución de la copia de respaldo.

NOTA: No se pondrá en ejecución ningún servidor que no cumpla este requerimiento.

- Todas las copias de respaldo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo
    1. Número de secuencia.
    2. Tipo de backup.
    3. Nombre del sistema o aplicativo.
    4. Datos necesarios para su reconocimiento.
    5. Equipo al que pertenece.
    6. Fecha y hora de ejecución.
    7. Frecuencia.

- Todos los procedimientos de respaldo deberán generar un registro en el sistema de backup que permita la revisión del resultado de la ejecución.
- Queda estrictamente prohibido almacenar, en las carpetas a las cuales se les va a realizar el respaldo, archivos de juegos, música, reproductores de música y/o video, programas de cómputo sin licencia y cualquier otra información ajena a la Institución.
- Se efectuarán pruebas de recuperación de las copias de respaldo por parte del administrador del sistema de backup cada semestre y serán supervisadas por el administrador del servidor. Con esto se podrá evidenciar que los datos grabados en la cinta se pueden obtener correctamente al momento de ser necesarios. Las pruebas se deberán formalizar en un acta escrita y firmada por los responsables.
- Los procedimientos de generación y grabación de estos archivos serán automáticos, con el fin de evitar su modificación.
- Todos los respaldos deberán conservarse conformé lo acordado con las áreas usuarias correspondientes.
- Se realizará un backup diario de los datos contenidos en los servidores. En caso de utilizar backups incrementales se realizará un backup del sistema completo cada 15 días.
- Todos los equipos de Sistemas Centrales deberán contar con Planes de Contingencia.

- Tanto para las Estaciones de Trabajo como para los Sistemas Centrales no se harán backup de los ficheros con extensiones: avi, mp3, mp4, divx, mpg, wvm, mkv o extensiones de características similares. Si por motivos de trabajo se crean este tipo de archivos se debe notificar al ATICs.hum vía email, junto con una descripción del motivo. El ATICs.hum junto con las autoridades de la facultad estudiará el caso y tomará una decisión que será notificada.
- No se realizaran backups de máquinas personales.

PLAN DE RECUPERACION

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, o desastre en el área de Informática

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

Las actividades a realizar en un Plan de Recuperación se pueden clasificar en tres etapas:

1. Actividades Previas a la falla o desastre.
2. Actividades Durante la falla o Desastre.
3. Actividades Después de la falla o Desastre.

DESTRUCCIÓN DEL BACKUP

La información en un medio de respaldo será destruida de dos formas:

1. Reutilización del medio para otro uso: El encargado de la administración y manejo de los backups deberá tener definido un rol para la reutilización de los medios, para esto debe llevar el control del contenido actual de cada respaldo. Cuando se reutilice algún medio se debe actualizar la información del mismo.
2. Daño físico del medio de respaldo: Deberán hacerse en forma periódica pruebas de restauraciones de información en un área temporal con el fin de probar el buen estado del medio de respaldo. Si se comprueba que el medio tiene un daño y no puede leerse su contenido, se debe destruir físicamente y documentar el número de medio y su último contenido. Se debe tratar que rescatar la información contenida y guardarla en otro medio.

BACKUPS DE COMPUTADORAS EN SERVICIO TECNICO

Todo equipo, léase Computadora, Notebook, Netbook o Tablet, que ingrese al área para un servicio técnico y cuando las tareas a ejecutar sobre los equipos pongan en riesgo la información que contienen, se le hará automáticamente un backup, aunque el usuario no lo solicite, y se guardará por el término de un mes. Pasado el mes de retirado el equipo, del área de servicio técnico, se enviará un mail al responsable del mismo avisándole que se borrará la información que se guardó, si durante la semana siguiente no se recibe una respuesta, se procederá al borrado seguro y definitivo de los datos.

Para realizar cualquier backup se necesitara contar con el consentimiento escrito, libre y expreso del usuario, conforme lo dicta el artículo 5 de la ley 25.326 de protección de los datos personales.

PLAN DE MEJORA CONTINUA

Cada seis meses se revisarán los procedimientos para copia y restauración de los equipos (tanto servidores como estaciones de trabajo) para efectuar mejoras, acciones correctivas y/o comprobar la eficacia de todos los procedimientos implementados.

GLOSARIO DE TERMINOS

Con el fin de comprender algunos de los términos utilizados, se definen los siguientes conceptos:

Amenaza Cibernética: Se trata de cualquier acción que pueda resultar de un acceso no autorizado, exfiltración, manipulación o menoscabo de la integridad, confidencialidad o disponibilidad de un sistema de información o de la información almacenada, procesada o en tránsito en un sistema de información electrónico, sea cual fuera la finalidad de dicha acción.

Backup: Es la copia total o parcial de información importante del Disco Rígido, CDs, DVDs, Bases de Datos u otro medio de almacenamiento. Los backups se utilizan para tener una o más copias de información considerada importante y así poder recuperarla en el caso de pérdida de la copia original.

Ciberseguridad: Comprende normas, procesos y acciones que permiten a las organizaciones practicar técnicas para detectar ataques y reducir al mínimo el número de incidentes en infraestructuras informáticas.

Consentimiento del interesado: Toda manifestación de voluntad, libre, expresa e informada, mediante la cual el titular autorice el tratamiento de sus datos personales.

Copia de Respaldo: en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Copia de Seguridad: (ver Copia de Respaldo).

Contingencia: Posibilidad de que una cosa suceda o no suceda.

Datos Informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

Datos Personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos Sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Infraestructuras Críticas: Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información situados en el Sector Público Nacional, en organismos provinciales, municipales o privados cuya interrupción o destrucción genere una repercusión importante en la salud, la seguridad, la información, la integridad física o el bienestar económico y social de los ciudadanos o en el eficaz funcionamiento de las instituciones estatales y las administraciones públicas.

Infraestructuras de Información: Involucra al marco básico de los sistemas de información cuyos activos se basan en procesar, transmitir, recibir y/o

almacenar información por vía digital, incluyendo dispositivos electrónicos, de comunicación y todo otro hardware, software o dato a ellos asociado.

Medios: son los soportes para realizar los Backup, podrán ser cintas, discos, CD, DVD y demás soportes lógicos con probada perdurabilidad temporal al deterioro.

Plan de Contingencia: es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

Protección: Son las acciones llevadas a cabo para garantizar, defender y/o reducir las vulnerabilidades de un sistema de información, así como para mitigar las amenazas cibernéticas, mejorando la seguridad y la capacidad de recuperación de los sistemas y activos asociados.

Recuperación: Adquisición de lo que antes se poseía.

Restauración: Reparación o arreglo de los desperfectos de un equipo, PC, servidor u otra cosa.

Sistemas Centrales: Definimos Sistemas Centrales a aquellas máquinas que dan servicio común a la Facultad: Servidor de correo, Web, archivos, discos, etc.

Titular de los Datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la ley.

Tratamiento de Datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general, el procesamiento de datos personales así como también, su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Usuario de Datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

ANEXOS

Anexo I - Formulario Autorización para el tratamiento de datos personales.

Anexo II - Software recomendado para backup de los servidores.

Anexo III - Software recomendado para el backup de las Estaciones de Trabajo o PCs.

Anexo IV - Software recomendado para el borrado seguro de información y/o Backups.

Elaboró

Revisó

_____

_____

Tec. Erié Eduardo Maseda
ATICs.hum
Responsable ATICs.hum

Sr. Gustavo David Gaumet

Aprobó

_____

Srta. Claudia Noemí Vescovi
Coordinadora Administrativa

Anexo I - Formulario Autorización para el tratamiento de datos personales

AUTORIZACION PARA EL TRATAMIENTO DE DATOS PERSONALES

DATOS DEL SOLICITANTE
Nombre y Apellido:
…….. DNI N°……
Ubicación del Equipo que alberga los datos
……..……
…….
Número de Patrimonio del equipo que alberga los datos
…….

Por medio del presente escrito manifiesto libre y expresamente mi autorización al personal de área de las Tecnologías de la Información y las Comunicaciones, (ATICs.hum), a realizar un backup de mis datos personales presentes en el equipo, léase computadoras/Notebook/Netbook/Tablet asignado para mi uso, en la facultad de Ciencias Humanas de la Universidad Nacional de Río Cuarto, de conformidad con el artículo 5 de la Ley Nº 25.326, y el artículo 5 de la Reglamentación de la Ley Nº 25.326 aprobada por Decreto Nº 1558/01.
Pasado un mes de retirado el equipo, del área de servicio técnico, y de no mediar solicitud contraria por escrito ante ATICs.hum, autorizó a realizar un borrado seguro y definitivo de los datos almacenados en cualquier dispositivo que se hubiese utilizado para realizar el backup antes mencionado.
En la ciudad de Río Cuarto, a los ..... días del mes de
..... de 201.....

Firma
Aclaración
Documento de Identidad

Anexo II - Software recomendado para Backup de los Servidores.

- ARCserve Unified Data Protection.
- Norton System Recovery Server.
- NovaBackup Business Essentials 17.
- Bacula Backup System.
- Amanda Network Backup.
- Rsync.

Anexo III - Software recomendado para el Backup de las Estaciones de Trabajo o PCs.

- Acronis True Image 2015.
- Genie Backup Manager Pro 9.0.
- Norton Backup Exec 15.
- Norton System Recovery Desktop Edition.
- NovaBackup 17 Professional.
- Paragon Backup & Recovery 15.
- Bacula Backup System.
- Amanda Network Backup.

Anexo IV - Software recomendado para el borrado seguro de información y/o Backups.

- **Eraser**: Empezamos con este programa con un nombre muy sencillo y directo, Eraser, borrador en inglés. Desde su ventana principal o desde el menú contextual te permitirá eliminar de forma segura tus archivos usando uno de los muchos sistemas de borrado disponibles que van de una pasada a siete, usando distintos algoritmos de borrado, algunos de ellos usados por las fuerzas armadas estadounidenses.
- **DeleteOnClick**: En este caso, este programa para el borrado seguro de archivos funciona desde el menú contextual de Windows, por lo que para usar DeleteOnClick tendrás que hacer clic derecho con el ratón directamente encima del archivo.
- **WipeFile**: En este programa de borrado seguro de archivos te las verás con hasta 14 métodos distintos con los que eliminar el documento más rebelde. Entre sus ventajas de WipeFile: no necesita instalación, es gratuito, está disponible en varios idiomas, y sus algoritmos de borrados son usados por la OTAN y el Departamento de Defensa de Estados Unidos.
- **Active@ KillDisk**: El caso de KillDisk es distinto a los anteriores, ya que no se trata de borrar archivos concretos, sino de eliminar particiones y discos enteros. Para ello, cuenta con los mejores algoritmos de borrado seguro de archivos, de 2 a 35 pasos.
- **File Shredder**: Terminamos con uno de las simples, pero efectivos. File Shredder ofrece cinco algoritmos de borrado seguro. Además, no sólo permite borrar archivos y carpetas concretas, también puede limpiar el espacio libre para evitar la posible recuperación de ficheros en ese espacio.

La calidad de la mayoría de estos programas de borrado seguro de archivos es muy alta. Escoger entre uno u otro dependerá del nivel de seguridad que necesitemos, teniendo en cuenta que cuantos más pasos realice un algoritmo de borrado, más tiempo tardará en estar completada la eliminación. Cabe recordar que tras aplicar estos programas, no se podrá recuperar los archivos eliminados.