RESOLUCIÓN N° 38 /2.023.-

POR LA CUAL SE APRUEBA EL MANUAL DE COPIAS DE SEGURIDAD Y RECUPERACION DE DATOS, DEL INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA – IPTA.

Asunción, 31 de Enero de 2.023.-

VISTO: El Memorando DTIC N° 02/2.023, de fecha 13 de enero de 2.023, presentada por la Dirección de Tecnología de la Información y Comunicación – TIC's, y dirigida a la Dirección General de Asesoría Jurídica, a través del cual solicita el parecer jurídico para la posterior aprobación del **Manual de copias de seguridad y recuperación de datos**, elaborado por ésta dirección, que tiene como objetivo "***Contar con un esquema de copias de Seguridad de los Activos, Servicios, Aplicaciones, Bases de Datos y Códigos Fuentes del IPTA, con el fin de contar con estos archivos en caso de existir algún evento o daño"*** y salvaguardarlo teniendo en cuenta el volumen de datos con que cuenta la institución, y;

CONSIDERANDO: ***Que***, la Dirección de Asesoría Jurídica, por Dictamen D.A.J. N° 03/23, de fecha 18/01/2.023, expresa que la implementación del mismo no contraviene disposición alguna y en consecuencia sugiere proseguir con los trámites administrativos de rigor, salvo mejor parecer de la presidencia.
Que: la Dirección de Tecnología de la Información y Comunicación TIC`s, a través de su Providencia Nº 01/2023, de fecha 19/01/2023, remite a la Dirección de Gabinete - IPTA, para consideración de la máxima autoridad institucional.
Que: la Dirección de Gabinete a través de su Providencia, remite el expediente aprobado, a la Dirección de Secretaría General, para la emisión de la Resolución correspondiente.

POR TANTO: *En uso de las atribuciones y facultades, que le confiere la Ley N° 3.788/10;*

EL PRESIDENTE
DEL INSTITUTO PARAGUAYO DE TECNOLOGÍA AGRARIA (IPTA)
R E S U E L V E:

Artículo 1°.- ***APROBAR***, el "**Manual de Copias de Seguridad y Recuperación de Datos**", del Instituto Paraguayo de Tecnología Agraria, conforme al Anexo de quince (15) páginas, que forma parte integrante de la presente Resolución.

Artículo 2°.- ***COMUNICAR***, a quienes corresponda y cumplido archivar.

Ing. Agr. César Espínola
Director de Secretaría General

Ing. Agr. ***EDGAR A. ESTECHE A.***
Presidente

Instituto Paraguayo de Tecnología Agraria
Dirección de Tecnología de la Información y Comunicación

MANUAL DE

COPIAS DE SEGURIDAD Y RECUPERACIÓN

Ing. Agr. César Espinol
Director Secretaria Gener

AÑO 2023

Versión 1.0

ING. AGR. EDGAR A. ESTIGARRIBIA
Presidente

Ing. Hugo A. Carrillo G.
Director
Dirección de TIC's

1. INTRODUCCIÓN

Este documento hace referencia a las copias de respaldo y de restauración de la información que posee la Dirección de Tecnología de la Información y Comunicación - DTIC del Instituto Paraguayo de Tecnología Agraria - IPTA en sus servidores y servicios instalados y corriendo sobre ellos.

La DTIC a través de sus Dpto. de Desarrollo de Software y Dpto. de Redes y Comunicaciones se encargará de implementar medidas de seguridad para proteger y garantizar que los recursos de los sistemas de información (Activos, Aplicaciones, Bases de Datos, Servicios) de la institución, se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.

2. OBJETIVOS

2.1. Objetivo General

Contar con un esquema de copias de seguridad de los Activos, Servicios, Aplicaciones, Bases de Datos y Códigos Fuentes del IPTA, con el fin de contar con estos archivos en caso de existir algún evento o daño.

2.2. Objetivos Específicos

- Diseñar el esquema de backups que debe poseer el IPTA.
- Designar los responsables de la realización de los backups.
- Contar con un registro de los backups realizados.

3. PLANIFICACIÓN Y ORGANIZACIÓN

3.1. La DTIC como parte de los Planes de la Entidad

La DTIC realizará coordinadamente la elaboración del Plan de Contingencia de la Institución, presidiendo un Comité que se reunirá anualmente y estará integrado además de la DTIC, el Dptos. de Redes y Comunicaciones.

A partir del Plan de Contingencia del IPTA se fijan los objetivos por área con las inversiones precisas para cumplir la misión asignada, el área de informática es una de las áreas contempladas. La Institución al evaluar los objetivos contempla las oportunidades de optimización de recursos que brinda el área de la DTIC colaborando en el logro de los propósitos de la institución y fija las necesidades de inversión tecnológica y del personal requerido para el logro de las metas, asentando los requerimientos financieros en el POA del año.

3.2. Modelo de la Arquitectura de Información

La información a resguardar deber ser consistente con las necesidades de la institución. La información se debe identificar, capturar y comunicar en forma apropiada, en el momento justo, de tal manera que las personas puedan ejecutar sus responsabilidades efectivas y oportunamente. En consecuencia, se debe crear y mantener un modelo de datos de arquitectura de información que comprenda el Modelo de Datos de la Institución y la información relacionada a los sistemas de información que acceden a los mismos.

3.3 Planes de Contingencia e Infraestructura Tecnológica

El Plan de Contingencia es primordial dentro de la estructura de la Institución, siempre se tiene especial cuidado en su actualización, en el manejo de los backups y la disponibilidad de equipos tecnológicos y humanos que garanticen su efectividad.

3.4. El Plan de Contingencia de la Plataforma considera:

Los Servidores y algunos dispositivos considerados por su importancia están instalados sobre un sistema protegido por UPS y Generadores para evitar la pérdida y/o alteración de datos permitiendo un apagado normal del sistema si la situación lo requiriese. Al evaluar una contingencia si el daño se considera irrecuperable y el equipo por lo tanto ha quedado fuera de servicio se procederá a activar el servidor de emergencia, utilizando y actualizando los datos contenidos en los backups diarios.

4. DEFINICIONES

Atributo

Propiedad característica de un objeto que puede distinguirse cuantitativa o cualitativamente por medios humanos o automatizados.

Auditoría

Proceso sistemático, independiente y documentado para la obtención de evidencias de auditoría y evaluarlas objetivamente para determinar el grado en que se cumplen los criterios de auditoría

Alcance de auditoría

Extensión y límites de una auditoría

Ing. Agr. César Espínola
Director Secretaría General

Ing. Hugo D. Carrillo G.
Director
Dirección de TIC's

Autenticación

Provisión de una garantía de que una característica afirmada por una entidad es correcta

Autenticidad

Propiedad de que una entidad es lo que expresa ser

Disponibilidad

Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.

Competencia

Capacidad de aplicar los conocimientos y habilidades para alcanzar resultados previstos

Confidencialidad

Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados

Conformidad

Cumplimiento de un requisito

Control

Medida que está modificando el riesgo

Datos

Colección de los valores asignados a la medida base, medidas derivadas y/o indicadores

Instalaciones de procesamiento de información

Cualquier sistema de procesamiento de la información, servicio o infraestructura o la ubicación física de la locación que lo aloja

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información

NOTA 1 a la entrada: Adicionalmente, otras propiedades, tales como autenticidad, responsabilidad, no repudio, y confiabilidad pueden también estar involucradas.

Sistema de información

Aplicaciones, servicios, bienes de tecnología de información u otros componentes de manejo de información

Ing. Hugo M. Carrillo G.
Director
Dirección de TIC's

Integridad

Propiedad de exactitud e integridad

No repudio

Capacidad para demostrar la ocurrencia de un evento o acción afirmados y sus entidades de origen

Amenaza

Causa potencial de un incidente no deseado, el cual puede resultar en daños al sistema o a la organización

Backup (Copia de Respaldo o Seguridad)

Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte de Unidad de Disco (disco duro, disco extraíble, Unidad de DVD, pendrive, etc) y/o en la nube, 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 (diario o semanal, por ejemplo), en función del trabajo y de la importancia de los datos manejados.

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 enforma de texto, números, gráficos, sonido o vídeo.

Contingencia

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

Ing. Agr. César Espinol
Director Secretaría Gener

Hosting

Alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet unsistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web.

Log ("registro", en español)

Es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

ING. AGR. EDGAR A. ESTECHE
Presidente

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Plan de Contingencia

Procedimientos alternativos de una entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando algunas 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.

Respaldo

Es la copia de información a un medio del cual se pueda recuperar y restaurar la informaciónoriginal.

Restauración (Restore)

Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otrodispositivo después de un desastre.

Servidor

Se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyopropósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Sistemas de Información

Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Snapshot (foto instantánea)

Es una instantánea del estado de un sistema en un momento determinado. El término fue acuñado como una analogía a la de la fotografía

Ing. Agr. César Espinola
Director Secretaría General

5. COPIAS DE SEGURIDAD Y RECUPERACIÓN EN DESASTRES

Una de sus funciones más esenciales es asegurar que nunca se pierda la información de la entidad y que las aplicaciones estén disponibles, a pesar de caídas del servidor, apagones o desastres naturales.

No sólo se debe hacer copia de seguridad de la información, también se debe verificar que dichas copias sean "recuperables" y, además, que se pueda hacer en un intervalo concreto de tiempo.

ING. AGR. EDGAR A. ESTECHE A.
Presidente

Ing. Hugo R. Carrillo
Director
Dirección de TIC's

Los Dptos. de Desarrollo de Software y de Redes y Comunicaciones trabajarán en forma coordinada a fin de realizar las copias de seguridad de las aplicaciones, sistemas, códigos fuente y sus versiones y programas en general que tengan a su cargo para el correcto desarrollo de las actividades de sus dependencias, la omisión de esta tarea es pasible de sanciones, deberán contar con una planilla de registros de realización de copias de seguridad, que deberá ser informada a la Dirección de TIC de manera periódica.

- Tipo de Backup completo (Full): Es cuando todos los archivos seleccionados son copiados. En respaldos subsecuentes, la totalidad de los archivos es respaldada de nuevo. La ventaja es que al restaurarlo se tiene la totalidad de los archivos cada vez. Las desventajas son dos: El tiempo consumido para este respaldo es muy largo, y ocupa mucho más espacio cuando se compara con los respaldos incrementales o diferenciales.

- Tipo de Backup Diferencial: Es el respaldo de todos los archivos que han sido modificados desde el último respaldo COMPLETO. Con el respaldo diferencial, se hace un primer respaldo completo y en los siguientes solo se guardan los cambios hechos desde el ultimo backup completo.El resultado es que se obtiene el respaldo más rápido de los 3 y el espacio utilizado es el menor posible. Con esta modalidad solo tendríamos la última versión de los archivos respaldados.

- Tipo de Backup FTP: Este es un tipo de respaldo en el que la transferencia de los datos se hace utilizando el protocolo FTP sobre Internet. Tipicamente la información se encuentra en un centro de datos conectado y es otra modalidad del respaldo offsite.

5.1. Pruebas de Restauración de Backup.

Como medida de protección, durante el año se harán pruebas de los backup que se resguardan en la DTIC del IPTA en los lugares donde cada Dpto. lo defina, según el plan a presentar a la DTIC.

Las pruebas de restore se realizarán de manera mensual y estarán bajo exclusiva responsabilidad de los Dptos. de Desarrollo de Software y de Redes y Comunicaciones, se deberá completar una planilla de registros, que se comunicará a la Dirección periódicamente, para cada caso se han definido los siguientes periodos:

- Se realizarán pruebas de restore cada mes para las bases de datos en un servidor de pruebas.

- Cuando sea necesario restaurar información para la implementación de ambiente de pruebas.

Ing. Hugo R. Carrillo G.
Director
Dirección de TIC's

Se deberá verificar posteriormente que el respaldo se esté ejecutando de forma correcta y/o que la restauración de la información se haya ejecutado, revisando el log que genera la restauración de información en bases de datos, para verificar que se haya ejecutado satisfactoriamente, en caso de no restaurar correctamente, se deberá tomar el backup anterior a la fecha del restaurado.

Con el fin de verificar las copias de respaldo cada mes, se realizarán pruebas de restauración de la información almacenada en dispositivos físicos determinados y/o en la nube. Se escogerá de forma aleatoria un dispositivo de almacenamiento de backup de bases dedatos y se restaurará para validar que la información almacenada se registre de forma correcta en un servidor de pruebas para tal fin, posteriormente será validada por el responsable funcional.

En caso de presentarse inconvenientes se debe revisar directamente el servidor desde el que se realizóel backup.

6. ESTRATEGIAS

6.1. Estrategias de Backup

Cada Dpto. deberá contar con un plan de copias y restauración, según Anexo con las estrategias de copias de seguridad bien definidas (tipo de copia de seguridad y frecuencia), de cada uno de los servidores miembros del dominio del IPTA.

Esta estrategia permitirá realizar una recuperación de inmediato cuando se presente un daño, por motivos muy diversos, desde infecciones del sistema por virus, malware, fallos de hardware (cortes de corriente y picos de tensión, excesos de temperatura y daños en los dispositivos), apagados incorrectos del equipo, problemas motivados por algún programa, daños del usuario al borrar archivos por error, robo de equipo, etc.

Puntos a tener en cuenta para la realización del plan de cada departamento:

a) Frecuencia de las Copias de Respaldo.
b) Configuración de la Copia de Respaldo.

Instituto Paraguayo de Tecnología Agraria
Dirección de Tecnologías de la Información y Comunicación
IPTA

Ing. Hugo R. Carrillo G.
Director
Dirección de TIC's

c) Lugar asignado para alojar la Copia de Respaldo. (equipo diferente al que están los datos originales)
d) Responsabilidad.
e) Validar la integridad del Backup.

7. CONSIDERACIONES AL PLAN DE BACKUP

Cuando se desarrolla un plan de backups se debe tener en cuenta lo siguiente:

- Determinar el tipo de información a ser resguardada, lo que indica que cada copia debe estar debidamente identificada respecto a la información que debe contener.

- Prever los aspectos relacionados con la fiabilidad de la copia, ya que se debe garantizar la integridad de los archivos a ser copiados y de los soportes a utilizar.

- Incluir una prueba de tensión del hardware de backup (unidades de almacenamiento, unidades ópticas y controles) y del software (programas de backup y unidades de dispositivo).

- Establecer las políticas de seguridad con los responsables para el acceso a las copias, así como la protección física del lugar donde están almacenados.

8. INFORMACIÓN QUE SE DEBE RESPALDAR

- Los servidores que manejan aplicaciones web, incluyendo su código fuente y sus distintas versiones.

- Las bases de datos que soporten aplicaciones del IPTA.

- Los Controladores de Dominio.

- Equipos de red (router de borde, switch, Access point, entre otros).

- Repositorio de información asignado a las áreas para el almacenamiento de información.

- Portal Web y cuentas de correo.

- Programas y ejecutables utilizados en la institución, incluyendo su código fuente y sus

Ing. Agr. César Espínola
Director Ejecutivo

Ing. Agr. EDGAR A. ESTRACHE A.
Presidente

Lic. Hugo A. Carrillo G.
Director
Dirección de TIC's

versiones.

Nota:

En los casos que el IPTA contrate la provisión o infraestructura que soporte alguna de las informaciones mencionadas anteriormente, se deberá asegurar que el TERCERO cumpla con la política descrita en el presente manual.

8.1. Controladores de dominio

Las copias de seguridad en el servidor donde se encuentra el Controlador de Dominio se deberá realizar de acuerdo a la siguiente plantilla como mínimo cada 15 días.

8.2. Bases de Datos

El Plan de Backups diarios se efectuarán de forma automática, agendándolos por horas de acuerdo a los criterios definidos por el Dpto. de Desarrollo de Software:

Base de Datos	Tipo de backup	Días	Horario
BD 1	Diferencial	Todos los días	12:20 a.m. 7:20 p.m.
	Full	Viernes	1:21 a.m.
BD 2	Diferencial	Todos los días	9:45 a.m. 18:45 p.m.
	Full	Sábados	10:32 a.m.

8.3. Aplicativos Web y Aplicaciones de escritorio

La institución posee aplicativos web, los cuales son programas diseñados para o por los usuarios, para facilitar la realización de tareas específicas en la computadora, sistemas de gestión de base de datos, que deberá contar con un plan de backup diario que se genere automáticamente, y se deberá consignar el lugar donde guardarlos.

8.4. Servidor de archivos de las áreas de la Institución

Se deberá presentar la estrategia a fin de proteger estos archivos que representan la memoria institucional.

Ing. Agr. César Espinola
Director Secretaría General

ING. AGR. EDGAR A. ESTECHE A.
Presidente

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

8.5. Portal Web e Intranet

Generar respaldos semanales mínimamente (backup) del Portal Institucional e Intranet del IPTA.

8.6. Backup de la configuración de los Servidores

Para proteger los controladores de dominio y el directorio activo se debe realizar la copia de seguridad del "System State" en el servidor (máquinas virtuales), con el fin de proteger la información de las cuentas de los usuarios vinculados al IPTA, se procederá a efectuar una copia completa de dicho repositorio (Directorio Activo) y, dada la baja actualización de información, se procederá a efectuar los respaldos con una periodicidad quincenal.

8.7. Backup de Buzones

Se deberá respaldar la información del correo institucional.

8.8. Código fuente y control de versiones

Se deberá contar con un repositorio web de acceso restringido, o en su defecto guardarlos en un servidor el cual cuente con su respectiva política de respaldo, el Dpto. de Desarrollo de Software será el encargado de disponibilizar todos estos archivos, y de tener un respaldo offline de todos ellos, como así también llevar el control en una planilla con la firma del responsable.

8.9. Equipos de red

Se deberá mantener una copia de manera quincenal mínimamente de los archivos de configuración de los equipos de red.

8.10. Para archivos y programas

La distribución de estas carpetas o subdirectorios se encuentran en el principal o sea en "sistema". Por ejemplo para el modulo general se creo una subcarpeta o subdirectorio "general" visto de la sgte. forma /sistema/general y asi sucesivamente /sistema/ahorros, /sistema/prestamos, /sistema/caja, etc.

Dentro de cada carpeta encontramos las sgtes. Subcarpetas o Subdirectorios:

inp: Donde almacenamos los programas fuentes de los forms.
rex: Donde almacenamos los programas fuentes de los reportes.
pck: Donde almacenamos las rutinas (package) del sistema.
sql: Donde almacenamos las estructuras de tablas a creadas en el sistema.
view: Donde almacenamos las vistas del sistema.
ctl: Donde almacenamos los archivos de control del sqlloader (Importador ascii).

Ing. Agr. César Espínola
Director Ejecutivo General

Instituto Paraguayo de Tecnología Agraria

Instituto Paraguayo de Tecnología Agraria

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

ANEXOS

Planillas

Deben mantener la misma estructura, serán de uso interno de la Dirección, se podrán realizar cambios, agregar más información si fuera necesario.

Instituto PARAGUAYO DE TECNOLOGÍA AGRARIA | GOBIERNO NACIONAL | Paraguay de la gente

INSTITUTO PARAGUAYO DE TECNOLOGÍA AGRARIA
DIRECCIÓN DE TICs

PLANILLA DE BACKUP DE CORREO

AÑO 2023

NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			
NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			
NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			
NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			
NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			
NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			
NRO	Fecha:	Modelo				Observación	Firma
	Zimbra	dir		xva			
	Storage	SI		NO			
	FTP	dir		xva			
	Snapshot	dir		DB			

Ing. Agr. Cesar Espinola
Director Secretaría General

ING. AGR. EDGAR A. ESTECHE
Presidente

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

INSTITUTO PARAGUAYO DE TECNOLOGÍA AGRARIA
DIRECCIÓN DE TICs

PLANILLA DE BACKUP DE SERVIDOR DE SISTEMAS

AÑO 2023

NRO	FECHA	INGRESOS	AGRONEGOCIOS	PATRIMONIO	SEMOVIENTES	METEOROLOGIA	KRONOS	RESPONSABLE	OBSERVACION

Ing. Agr. César Espinol
Director Secretaría Gener

Ing. Agr. EDGAR A. ESTECHE
Presidente

Ing. Hugo H. Carrillo C
Director
Dirección de TIC's

Instituto PARAGUAYO DE TECNOLOGÍA AGRARIA

GOBIERNO NACIONAL

Paraguay de la gente

INSTITUTO PARAGUAYO DE TECNOLOGÍA AGRARIA
DIRECCIÓN DE TICs

PLANILLA DE CÓDIGO FUENTE Y CONTROL DE VERSIONES
AÑO 2023

NRO	FECHA	SISTEMA	VERSION	RESPONSABLE	FIRMA	OBSERVACION
		IPTANET				
		AGRONET				
		PATRIMONIO				
		SEMOVIENTES				
		METEOROLOGIA				
		RRHH				
		MESA DE ENTRADA				
		KRONOS				
		IPTANET				
		AGRONET				
		PATRIMONIO				
		SEMOVIENTES				
		METEOROLOGIA				
		RRHH				
		MESA DE ENTRADA				
		KRONOS				

Ing. Agr. César Espínola
Director Secretaría General

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's