POLÍTICA DE RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN

Versión 1.0

Versión	Fecha	Modificaciones
1.0	14/08/2025	Primera versión del documento

	Nombre	Puesto	Firma	Fecha
Elaborado	Ysrael Salazar	TI		14/08/2025
Revisado	Raúl Véliz	Gerente General		
Aprobado	Rául Véliz	Gerente General		

POLÍTICA DE RESGUARDO Y RECUPERACIÓN DE INFORMACIÓN

1. OBJETIVO

La presente política tiene como objetivo principal establecer las directrices y responsabilidades para el resguardo sistemático y la recuperación efectiva de la información digital almacenada en los equipos de cómputo y teléfonos móviles corporativos de Water Partners.

Los objetivos específicos de esta política son:

1.1 Asegurar la Continuidad del Negocio

Garantizar que las operaciones críticas puedan reanudarse con mínima interrupción después de un incidente adverso, como ciberataques, fallos de hardware, robo o desastres naturales.

1.2 Proteger la Propiedad Intelectual

Salvaguardar los activos de información vitales de la empresa, incluyendo, pero no limitándose a, datos de clientes, diseños, contratos y otros datos confidenciales.

1.3 Mitigar la Pérdida de Datos

Proveer un mecanismo confiable para recuperar información que haya sido eliminada o corrompida accidentalmente por los usuarios.

2. ALCANCE

Esta política es de cumplimiento obligatorio para todos los empleados de WaterPartners que utilicen un equipo de cómputo (laptop o escritorio) proporcionado por la empresa. Los activos cubiertos son todos los datos almacenados localmente en las laptops y computadoras de escritorio. Quedan excluidos los servidores y la información en plataformas de terceros no gestionadas directamente bajo esta iniciativa, salvo que se especifique lo contrario.

2.1 Inclusión de Dispositivos Móviles Corporativos

Esta política también se extiende a teléfonos móviles corporativos entregados al personal, siempre que estos contengan información relevante del negocio, acceso a plataformas corporativas (ej: correo Gmail, CRM Escala, Drive), o herramientas de comunicación interna. El Departamento de TI será responsable de garantizar mecanismos de backup o exportación de dicha información en caso de desvinculación del colaborador.

2.2 Uso de Equipos Móviles Corporativos y Respaldo

Todos los dispositivos móviles entregados por la empresa y configurados con líneas corporativas son propiedad de Water Partners, incluyendo la línea, el equipo y la información almacenada en él durante la relación laboral. Como parte de la política de resguardo de información, los teléfonos móviles corporativos deberán ser configurados por el Departamento de TI para realizar respaldos automáticos mediante la herramienta autorizada (iDrive Mobile Backup).

3. VIGENCIA

La presente política entra en vigor a partir de la fecha de su aprobación. Será revisada anualmente o cuando ocurran cambios significativos en la estructura o tecnología de la empresa, para asegurar su continua relevancia y efectividad.

4. DEFINICIONES

- **Respaldo (Backup)**
  Proceso de copiar y archivar datos de la empresa para que puedan ser recuperados en caso de una pérdida de información.

- **iDrive Backup**
  Herramienta de software autorizada por la empresa para la ejecución de respaldos en dispositivos.

- **WhatsApp Business**
  Aplicación de mensajería diseñada para empresas, de uso obligatorio en

dispositivos corporativos para separar la comunicación laboral de la personal.

- **SaaS (Software as a Service)**
  Modelo de distribución de software donde las aplicaciones están alojadas en la nube y son accesibles a través de internet (ej. Gmail, CRM Escala, iDrive).

5. LINEAMIENTOS ESPECIFICOS

5.1. Gobernanza de la Información del Backup (Equipos de Cómputo)

5.1.1. Información Sujeta a Respaldo

Se respaldará el perfil de usuario completo de cada equipo, lo cual incluye: Escritorio, Documentos, Imágenes, Carpetas de sistema instalados (Ejm; ContaNet, etc.) u Autorizados por gerencia. Audio (solo si contiene archivos relacionados con el trabajo), Videos (solo si contiene archivos relacionados con el trabajo)

5.1.2. Información Explícitamente Excluida del Respaldo

- Archivos de sistema operativo (Ej: Carpeta C:\Windows).
- Archivos de programas instalados (Ej: Carpetas C:\Archivos de Programa y C:\Archivos de Programa (x86)).
- Archivos temporales del sistema o de aplicaciones.
- Archivos históricos y credenciales de los navegadores (Ejm: Chrome, Edge, FireFox, etc.).
- Contenido multimedia de carácter personal (música, videos, fotografías no relacionadas con la actividad laboral).

5.2. Gobernanza de la Información del Backup (Dispositivos Móviles)

5.2.1. Información Sujeta a Respaldo

El respaldo incluye, pero no se limita a:

- Contactos sincronizados.
- Archivos descargados y generados en apps laborales.
- Archivos multimedia relacionados al trabajo.
- Configuración básica del dispositivo.

5.2.2. Información Explícitamente Excluida del Respaldo

Se excluyen expresamente archivos personales, fotografías, mensajes o aplicaciones de uso estrictamente privado, salvo que estos afecten la seguridad o integridad de la información corporativa.

5.2.3. Uso de WhatsApp Business

Todos los dispositivos móviles corporativos deberán utilizar la aplicación WhatsApp Business en lugar de WhatsApp estándar, con el fin de separar la comunicación personal de la empresarial, facilitar la continuidad operativa, y estandarizar la recuperación y control de información laboral.

5.3. Ciclo de Vida y Retención de Datos

5.3.1. Frecuencia de Respaldo

Los respaldos se ejecutarán de manera diaria. El objetivo es no perder más de veinticuatro (24) horas de trabajo.

5.3.2. Período de Retención

Las copias de seguridad se conservarán en el sistema activo por un período de treinta (30) días calendarios.

5.3.3. Política de Retención para Ex-Empleados

Se realizará un backup final y completo de la información del equipo del usuario.

Este backup final será exportado y almacenado en un repositorio de archivo permanente y seguro.

Pasados tres (3) meses desde la fecha de desvinculación, los backups asociados serán eliminados de la consola activa de iDrive, manteniendo el último backup bajo la denominación:

NOMBRE EQUIPO + NOMBRE USUARIO + FECHA

(Ejm: LPVENTAS01_JPEREZ_20250630).

5.4. Seguridad, Almacenamiento y Sistemas Externos

5.4.1. Almacenamiento

Toda la información respaldada será almacenada en la nube mediante el servicio SaaS provisto por iDrive.

5.4.2. Cifrado

Todos los datos serán cifrados tanto en tránsito como en reposo.

5.4.3. Control de Acceso

El acceso a la consola de administración y la autorización para realizar restauraciones estará restringido al Departamento de TI y/o la Gerencia General.

5.4.4. Respaldos de Sistemas Externos y en la Nube

El Departamento de TI coordinará estrategias de respaldo para:

- ContaNet: exportación semanal de base de datos o archivos contables.
- CRM Escala: coordinación con proveedor sobre periodicidad de backup.
- Gmail y Drive: respaldo mediante Google Vault o exportaciones manuales según criterios definidos.

6. CONSIDERACIONES

Esta política se basa en y se alinea con los siguientes lineamientos externos y normativas:

- Reglamento Interno de Trabajo de Water Partners.
- Contrato de Trabajo individual de cada colaborador.
- Ley de Protección de Datos Personales vigente.
- Código Penal en lo referente a delitos informáticos y violación de la confidencialidad.

7. ROLES Y RESPONSABILIDADES

- **Dueño de la Política (Gerente General)**

  Es responsable de aprobar, revisar y garantizar el cumplimiento de esta política a

nivel organizacional.

- **Departamento de TI (Administrador del Sistema)**
  Es responsable de la implementación técnica, gestión periódica, monitoreo, mantenimiento del sistema de backups y ejecución de los procesos de restauración.

- **Usuario Final (Empleado)**
  Es responsable de cumplir con todas las reglas establecidas, guardar la información de trabajo en las ubicaciones designadas, no almacenar información crítica en lugares excluidos y reportar proactivamente cualquier fallo.

8. INCUMPLIMIENTO DE LA POLÍTICA

El incumplimiento de las directrices establecidas podrá dar lugar a medidas disciplinarias, de acuerdo con el reglamento interno. La eliminación deliberada de información clave sin autorización será considerada falta grave y podrá dar lugar a la máxima sanción disciplinaria, incluyendo la terminación del contrato y las acciones legales que correspondan.

9. REVISIÓN DE LA POLÍTICA

Esta política será revisada anualmente o cuando ocurran cambios significativos en la estructura o tecnología de la empresa, para asegurar su continua relevancia y efectividad.

10. AVISO LEGAL

Esta política es de cumplimiento obligatorio. La empresa podrá modificar su contenido en cualquier momento, comunicando los cambios a los colaboradores. A partir de la comunicación de la presente Política, surte efectos para todos los trabajadores.