Protocolo de Entrega de Equipos de Cómputo, Usuarios y Políticas de Seguridad de la Información

1. Objetivo

Establecer un procedimiento seguro, trazable y estandarizado para la recepción, uso y devolución de los equipos de cómputo entregados por el cliente, garantizando el cumplimiento de las políticas de seguridad de la información establecidas por KAP y por los Clientes cuando estos tengan algún requerimiento específico.

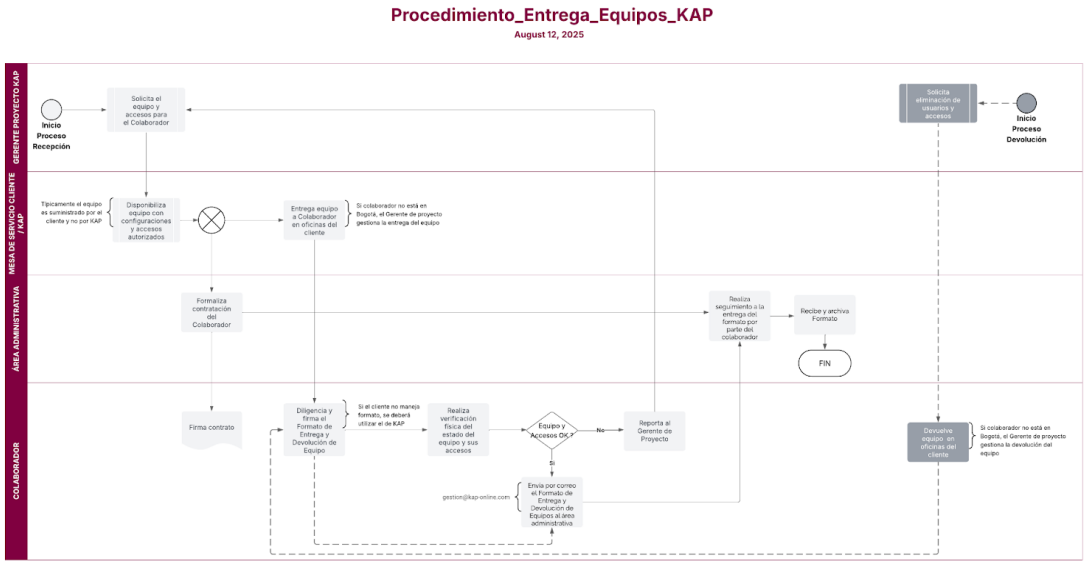
2. Alcance

Aplica a todo el personal de KAP que reciba, custodie o utilice equipos de cómputo proporcionados por un cliente, durante la ejecución de cualquier proyecto.

3. Responsables

- Gerente del Proyecto
- Colaborador (receptor del equipo y usuarios)
- Mesa de Servicio Cliente/KAP
- Área Administrativa

4. Proceso de Entrega de Equipo y Accesos



Paso	Descripción	Responsable
1	Solicitud equipo y accesos al cliente	Gerente Proyecto KAP
2	Disponibilización de equipo con herramientas de monitoreo de seguridad y accesos	Mesa de Servicio Cliente o KAP (si aplica)
3	Formalización Contratación	Área Administrativa y Colaborador
4	Recepción del equipo en Oficinas del Cliente	Colaborador
5	Diligenciamiento y firma del Formato de Entrega y Devolución de Equipo. (Si el cliente no maneja formato, se deberá utilizar el de KAP Formato KAP Entrega y Devolución de Equipos)	Colaborador
6	Verificación física del estado del equipo y sus accesos. (Si existe anomalía alguna se debe reportar al Gerente de Proyecto)	Colaborador
7	Gestión con el cliente de cualquier especificación errada en el equipo o sus accesos	Gerente Proyecto KAP
8	Seguimiento a la entrega del formato por parte del colaborador	Area Administrativa
9	Envío digital del Formato de Entrega y Devolución de Equipos al área administrativa (gestion@kap-online.com)	Colaborador
10	Recepción y archivo del Formato	Área Administrativa

5. Proceso de Devolución del Equipo

Paso	Descripción	Responsable
1	Solicitud de eliminación de usuarios y accesos bajo el protocolo definido por el cliente.	Gerente Proyecto KAP
2	Devolución del equipo en oficinas del cliente. Si el colaborador reside en Bogotá, deberá realizar la entrega directamente en las oficinas del cliente, si no reside en Bogotá, la devolución deberá ser coordinada por el Colaborador con el Gerente de Proyecto.	Colaborador o Gerente de Proyecto KAP
3	Diligenciamiento y firma del Formato de Entrega y Devolución de Equipo. (Si el cliente no maneja formato, se deberá utilizar el de KAP Formato KAP Entrega y Devolución de Equipos)	Colaborador
4	Seguimiento a la entrega del formato por parte del	Área

	colaborador	Administrativa
5	Envío digital del Formato de Entrega y Devolución de Equipos al área administrativa (gestion@kap-online.com)	Colaborador
6	Recepción, archivo del Formato y notificación interna para autorización de pago	Área Administrativa

6. Políticas de Seguridad de la Información

Acceso Seguro

1. El equipo deberá utilizar contraseñas robustas y únicas, con renovación obligatoria cada 90 días, o según especificaciones del cliente.
2. Según definiciones del cliente, se podrá habilitar doble autenticación (2FA) para acceso a sistemas críticos.
3. Los usuarios, claves y equipos son de uso personal e intransferible, bajo ninguna circunstancia se podrán ceder o prestar.

Uso Aprobado

4. El equipo y usuario deberán contar únicamente con los accesos requeridos para el desarrollo de sus funciones

5. El equipo se usará exclusivamente para tareas relacionadas con el proyecto del cliente.

6. Si el equipo usado para el desarrollo de las funciones contratadas es entregado directamente por un cliente, no es permitida la instalación directa de software o aplicaciones adicionales. Cualquier instalación adicional debe ser gestionada con el cliente.

Gestión de Información

7. Toda información del cliente deberá almacenarse únicamente en el repositorio definido por el cliente.

8. Se deben evitar respaldos locales; usar las plataformas de almacenamiento oficial del cliente o KAP.

9. La transferencia de información confidencial debe realizarse bajo los mecanismos definidos por el cliente en internet (Sharepoint, Onedrive, Dropbox, Google Drive, etc.)

10. No utilizar información de la Compañía para fines personales o diferentes a los requeridos para el cumplimiento de funciones.

Protección Antimalware

11. El equipo deberá contar con antivirus actualizado y sistema de detección de intrusos habilitado.

12. No se podrán desactivar manualmente las protecciones instaladas.

Protección Física

13. Evite colocar el equipo en lugares con polvo, humedad, calor excesivo o exposición directa al sol.

14. Evite golpes o movimientos bruscos al manipular el equipo. Si es una laptop, procure guardarla en un estuche acolchado cuando la transportes.

15. Limpie el exterior del equipo con un paño suave y seco para eliminar el polvo y la suciedad.

16. Evite derramar líquidos sobre el equipo. Si esto ocurre, desconecte inmediatamente el equipo de la corriente y seque con un paño suave y seco.

17. Asegúrese de que las ranuras de ventilación del equipo no estén obstruidas para evitar el sobrecalentamiento.

18. Utilice un regulador de voltaje o un SAI (Sistema de Alimentación Ininterrumpida) para proteger el equipo de variaciones de voltaje.

19. Desconecte el equipo de la corriente y de la línea telefónica o red durante tormentas eléctricas para evitar daños por rayos.

20. Si utiliza una laptop, no deje la batería conectada a la corriente constantemente. Carguela cuando sea necesario y desconecte cuando alcance un nivel adecuado.

21. Evite forzar las teclas, el mouse o la pantalla. Si es necesario limpiarlos, utiliza productos adecuados y evite los limpiadores abrasivos.

Red y Conectividad

22. Se debe evitar el uso de redes Wi-Fi públicas o no seguras.

23. Cuando el proyecto lo exija, se conectará mediante VPN del cliente o de KAP.

Bloqueo y Custodia Física

24. El equipo debe bloquearse automáticamente tras 5 minutos de inactividad o según políticas configuradas por el cliente en el equipo.

25. En caso de viaje o trabajo remoto, el equipo debe permanecer bajo custodia directa del usuario.

Pérdida o Robo

26. Toda pérdida o robo deberá reportarse inmediatamente al Gerente de Proyecto y éste a su vez al cliente.

27. Se activará el protocolo de contención y bloqueo remoto de datos si el equipo lo permite.

Devolución del Equipo

28. Se hará una revisión del estado del equipo.

29. El equipo será formateado y/o restaurado a estado original si así lo exige el cliente.

30. Se firmará un Acta de Devolución.

Certificación Políticas de Seguridad de la Información

31. Todo usuario que inicie labores en nombre de KAP, a través de contrato directo o a través de una alianza, deberá llevar a cabo la capacitación de ingreso y la certificación anual de Políticas de Seguridad

Nota: El incumplimiento de cualquiera de las Políticas de Seguridad establecidas por KAP o por el cliente, así como cualquier otra no conformidad del servicio contratado, puede conllevar a un llamado de atención con copia a la hoja de vida.

Así mismo, la omisión del reporte de un incidente de seguridad por parte de personal de KAP es causal de llamado de atención con copia a hoja de vida.

7. Anexos sugeridos

1. Formato KAP Entrega de Equipos
2. Políticas de Seguridad de la Información