# POLITICA PARA LA PROTECCIÓN DE DATOS

Para **CORALPACK** es fundamental y prioritario adoptar medidas técnicas, jurídicas, humanas y administrativas que sean necesarias para procurar la seguridad de los datos de carácter personal protegiendo la confidencialidad, integridad, uso, acceso no autorizado y/o fraudulento. Así mismo, se permite informar que internamente la Empresa cuenta con protocolos de seguridad de obligatorio cumplimiento para todo el personal con acceso a datos de carácter público, privado, personal, sensibles y a los sistemas de información que se tienen. Nos comprometemos a establecer objetivos internos de seguridad bajo las cuales se conserva la información del titular para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, como:

1. Generar controles en la Infraestructura tecnológica perimetral en la red de datos que tiene la Empresa

2. Generar acciones de control para el acceso a la información, aplicaciones y bases de datos.

3. Implementación de controles tecnológicos que minimizan el riesgo de las plataformas críticas ante desastres.

4. Acciones de implementación tecnológica que protegen los computadores y servidores de la organización de malware.

5. Implementación tecnológica para impedir la utilización de dispositivos USB de almacenamientos no autorizados.

6. Implementación tecnológica que controle el envío y transmisión electrónica caracterizada como confidencial.

7. Uso adecuado de las plataformas, correos, sistemas y de ingreso de datos privados y sensibles.

8. Implementación tecnológica que respalde la información contenida en las distintas plataformas.

9. Documento escrito sobre seguridad de la información y uso de las herramientas de información al interior de la Institución.

10. Acuerdo de confidencialidad con clientes, usuarios, proveedores y terceros.

11. Inclusión de cláusula de confidencialidad en los contratos laborales de empleados.

12. Procedimientos de Autocontrol y respuesta a Auditoría interna y Externa.

13. Captura información del cliente con la inclusión de Habeas data, con sus respectivas implicaciones.

14. Prohibición al uso de USB externas o personales.

Dada el 01 de Junio de 2022.

## POLITICA PARA LA PROTECCIÓN DE DATOS

Para **CORALPACK** es fundamental y prioritario adoptar medidas técnicas, jurídicas, humanas y administrativas que sean necesarias para procurar la seguridad de los datos de carácter personal protegiendo la confidencialidad, integridad, uso, acceso no autorizado y/o fraudulento. Así mismo, se permite informar que internamente la Empresa cuenta con protocolos de seguridad de obligatorio cumplimiento para todo el personal con acceso a datos de carácter público, privado, personal, sensibles y a los sistemas de información que se tienen. Nos comprometemos a establecer objetivos internos de seguridad bajo las cuales se conserva la información del titular para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, como:

15. Generar controles en la Infraestructura tecnológica perimetral en la red de datos que tiene la Empresa

16. Generar acciones de control para el acceso a la información, aplicaciones y bases de datos.

17. Implementación de controles tecnológicos que minimizan el riesgo de las plataformas críticas ante desastres.

18. Acciones de implementación tecnológica que protegen los computadores y servidores de la organización de malware.

19. Implementación tecnológica para impedir la utilización de dispositivos USB de almacenamientos no autorizados.

20. Implementación tecnológica que controle el envío y transmisión electrónica caracterizada como confidencial.

21. Uso adecuado de las plataformas, correos, sistemas y de ingreso de datos privados y sensibles.

22. Implementación tecnológica que respalde la información contenida en las distintas plataformas.

23. Documento escrito sobre seguridad de la información y uso de las herramientas de información al interior de la Institución.

24. Acuerdo de confidencialidad con clientes, usuarios, proveedores y terceros.

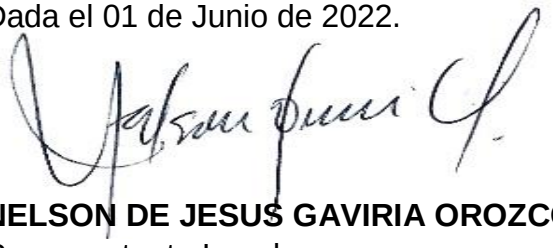
25. Inclusión de cláusula de confidencialidad en los contratos laborales de empleados.

26. Procedimientos de Autocontrol y respuesta a Auditoría interna y Externa.

27. Captura información del cliente con la inclusión de Habeas data, con sus respectivas implicaciones.

28. Prohibición al uso de USB externas o personales.

Dada el 01 de Junio de 2022.



**NELSON DE JESUS GAVIRIA OROZCO**
Representante Legal