Política de **protección y seguridad de la información**

AGQ Colombia SAS tiene como política el garantizar y cumplir con las leyes y regulaciones para la protección de la información proporcionada por sus clientes y sus derechos de propiedad (Datos personales, patentes, derechos de autor, procesos, programas, etc.), así mismo ha establecido los correspondientes procedimientos para proteger la transmisión electrónica y almacenamiento de los resultados emitidos.

Respecto a la información propia del cliente así como la generada a partir de los servicios prestados, AGQ Colombia S.A.S., se compromete con sus clientes a que todas las labores desarrolladas por sus empleados mantengan la confidencialidad de la información aportada por el cliente y por el laboratorio y que solo serán entregados y divulgados al cliente quien solicito el servicio según lo descrito los procedimientos internos; firmar y cumplir con la cláusula de confidencialidad en sus contratos y custodiar sus claves de acceso a la información electrónica. Cualquier incumplimiento de lo anterior será causal de terminación del contrato y disposiciones legales que apliquen.

Los subcontratistas que presten servicios de consultorías, auditorias, análisis de muestras, personal de apoyo para monitoreos, asesorías y demás que pueda requerir AGQ Colombia SAS deberán de firmar el acuerdo de confidencialidad, integridad y juicio, además de custodiar la información de la empresa para evitar manipulación, pérdida o alteración de esta. La información recopilada y almacenada por los subcontratistas u organismos externos dentro de la ejecución de las actividades propias de AGQ Colombia es confidencial y no puede ser compartida, divulgada, transmitida sin previa autorización.

Es obligación por parte de los empleados directos o indirectos reportar al área de sistemas local o corporativo cualquier novedad asociada a la seguridad o vulnerabilidad de la información a través del siguiente correo: cybersecurity@agqlabs.com o mediante comunicación directa con el responsable encargado del área de sistemas. En estos casos, es importante no tomar ninguna decisión por parte del colaborador hasta no tener el aval por parte del área de sistemas de AGQ Colombia SAS y/o corporativo, ya que esto puede poner en riesgo la información.

Es considerado una falta grave compartir usuarios y contraseñas de las cuentas corporativas nominales tipo nombre.apellido@agqlabs.com que, de acuerdo con cada permiso, puede llegar a dar acceso a correo, teams, VPN, Terminal Server, SIL, X3, Cotizador y GLPI tickets de IT Corporativo. **Para el trabajador que cede su usuario y contraseña es un problema doblemente grave**, ya que pone en riesgo la continuidad de la compañía donde trabaja y se pone en riesgo personalmente, ya que ante cualquier acción malévola que se realice con su usuario corporativo nominal contra los sistemas de AGQ (sea él mismo o alguien a quién le cedió su contraseña) será el propietario de la cuenta el responsable legal y AGQ, si fuera necesario, tomará contra él las medidas legales que se consideren oportunas. Es necesario si se identifica que su usuario y contraseña pueden estar comprometidos por almacenamiento en los equipos de cómputo, debe inmediatamente realizar el cambio a través de la plataforma Teams2Go y loguearse a través del siguiente enlace https://agq.myteam2go.com/ para iniciar con el cambio.