POLITICA DE TRABAJO EN CASA O REMOTO.

- **Requisitos de seguridad para usuarios internos:**
  - Para el trabajo remoto la conexión con la organización se realiza por VPN cifrada con usuario registrado en el Directorio activo, asegurando la confidencialidad de la información transmitida a través de ella, adoptando las políticas de navegación y controles de acceso con los que cuenta la organización y manteniendo el registro de logs de las actividades del empleado y/o contratista.
  - El empleado o contratista autorizado no debe utilizar los dispositivos de la organización, para fines diferentes a la realización de sus actividades laborales.
  - Se realizan restricciones de los accesos de Recursos compartidos en la red interna de la empresa aplicando la matriz de roles y privilegios definida para cada rol y/o cargo en la empresa, de tal manera estas políticas quedan aplicadas en la configuración del firewall, restringiendo el acceso de los usuarios a recursos en la red con información confidencial o sensible.
  - Se asigna los diferentes entornos de trabajo en casa como conexiones remotas seguras por VPN y ambientes WEB, para que los usuarios no tengan que realizar el procesamiento y almacenamiento de información en sus computadores privados de forma no autorizada. Así mismo se indica a los usuarios que esta acción no está permitida.
  - A los trabajadores y/o contratistas se les asigna un usuario y ellos deben crear un contraseña segura para realizar sus funciones o actividades contratadas por DATA QUALITY SOLUTIONS; así mismo se informa la política de usuario desatendido y las mejores prácticas de la gestión de autenticación secreta, es responsabilidad de los usuarios cumplir con todas las políticas dispuestas por la empresa; así mismo desde las políticas aplicadas al sistema se realiza la configuración de gestión de contraseñas con el fin de garantizar que otras personas que usan el mismo alojamiento no ingresen a los sistemas de DQS de forma no autorizada.
  - Cuando el trabajador y/o contratista autorizado utilice dispositivos propios, deberá tener un antivirus configurado y actualizado, así mismo no está permitido conectarse desde redes públicas o café internet.
- **Requisitos de seguridad para usuarios externos (clientes)**
  - El único acceso a los sistemas de información de DQS que tienen los clientes, es la plataforma tecnológica IMPERIUM, para lo cual se firman los respectivos acuerdos de licenciamiento de la plataforma y de confidencialidad de la información.
- **Requisitos generales de seguridad:**
  - DQS cuenta con un firewall Pfsense para garantizar la seguridad de todo el sistema de información, el cual cuenta con una configuración pertinente que garantiza la seguridad en las operaciones que se realizan en la RED local, así mismo se cuentan con protección

antivirus, para la seguridad de los equipos. Para los servidores en la nube se contrata un hosting independiente con parámetros de seguridad definidos y protección de firewall respectivamente.

- **Directrices para el teletrabajo:**
  - DQS no suministra adecuaciones físicas como de oficina en casa, por tanto se permite el trabajo en computadores personales únicamente por los diferentes entornos: Trabajo a distancia, trabajo remoto, trabajo virtual, siempre y cuando se cumplan con las condiciones y requisitos de seguridad para trabajar bajo estas modalidades.
  - Los funcionarios que se encuentran bajo esta modalidad de trabajo están en la responsabilidad de aplicar todas las políticas y directrices definidas en la empresa y como tal el reglamente de trabajo, es decir la intensidad horaria de trabajo es la misma y el acceso a la información se aplica de la misma manera que se mantiene en las instalaciones físicas de la empresa, es decir los equipos de computo para la conexión remota son los mismos equipos que DQS dispone en las instalaciones físicas.
  - Los contratistas que se encuentran realizando sus actividades contractuales en esta modalidad, están en la responsabilidad de aplicar todas las políticas y directrices definidas en el empresa y como tal el Contrato de prestación de servicios y acuerdo de confidencialidad, las actividades a desarrollar son las mismas y el acceso a la información se aplica de la misma manera que se mantiene en las instalaciones físicas de la empresa, es decir los equipos de cómputo para la conexión remota son los mismos equipos que DQS dispone en las instalaciones físicas.
  - El ing. de infraestructura es la única persona responsable de realizar la configuración del Open VPN en los computadores de los usuarios para la conexión remota, y este solo podrá ingresar a la IP asignada con su usuario y contraseña los cuales son personales e intransferibles, de tal manera el área de TI son los únicos encargados de suministrar el acceso a los recursos en la nube como SharePoint.
  - Las directrices y controles de: seguridad física, usuarios desatendidos, política de escritorio y pantalla limpia, Mantenimientos de equipos, backups, continuidad del negocio; y demás políticas de la seguridad de la información serán aplicadas a la RED LAN de la empresa ya que no se suministran equipos de cómputo para trabajar de manera local fuera de las instalaciones de DQS, por tanto, toda la información que se procesa y almacena se realiza de manera local en el servidor de la empresa y en sus ambientes WEB.
  - Todos los funcionarios y contratistas de DQS tienen la responsabilidad en su rol de usuario final, de responder a cualquier proceso de auditoría y a los seguimientos de cumplimiento de seguridad de la información que se realicen en la empresa.
  - La comunicación entre la organización y el funcionario o contratista en condición de trabajo en casa será por contacto telefónico, correo electrónico, reuniones virtuales,

mensajería instantánea, grupos de WhatsApp dispuestos en la empresa y modulo de reporte de eventos e incidentes de SI de la plataforma tecnológica IMPERIUM.

- Cada vez que se realiza un cambio de cargo o finaliza la relación civil contractual, o laboral el área de TI realiza la suspensión y revocación de todos los usuarios suministrados al funcionario o contratista, de tal manera restringir los derechos de acceso a los sistemas de DQS.

Versión 3, del 22 de enero de 2022