1.0 Requirements Policy and Procedures

1.1.1 Acuerdos de confidencialidad con sus empleados.
1.1.2 Con respecto a las operaciones de procesamiento que se subcontrate, el subcontratado cumplirá con las obligaciones impuestas al importador de datos de este documento
1.1.3 Disponer de una Política de uso aceptable que describa el tipo de comportamiento esperado del personal al usar tecnología en el lugar de trabajo y las consecuencias por abusar de los privilegios tecnológicos.
1.1.4 Tener una política para informar, gestionar y recuperarse de los incidentes de riesgo de información, incluidas las pérdidas de datos personales y los incidentes de seguridad de las TIC, definir las responsabilidades y hacer que el personal conozca la política.

2.0 Network Security Management

2.1 Las listas de control de acceso (ACL) se deben mantener para los dispositivos de red.
2.2 Los administradores y usuarios del sistema del proveedor cambiarán sus contraseñas cada 90 días.
2.3 Todos los ordenadores/servidores, incluidos los portátiles, que almacenen información personal o confidencial deberán estar protegidas por un cifrado de disco duro como mínimo con acceso controlado por al menos nombre de usuario y contraseña como medio de autenticación.
2.4 Todos los ordenadores requieren bloqueo automático
2.5 El antivirus y el antispyware deben instalarse y mantenerse actualizados en todos los servidores, equipos de escritorio y computadoras portátiles que se usan para almacenar, procesar o transmitir información personal o confidencial.

3.0 Communications and Operations Management

3.1 El tráfico de red pasará a través de firewalls que son monitoreados y protegidos por sistemas de detección / prevención de intrusiones que permiten el registro del tráfico que fluye a través de los firewalls.
3.2 El acceso a los dispositivos de red para la administración requerirá un mínimo de cifrado de 256 bits
3.3. Los filtros anti-spoofing se habilitarán para el correo electrónico.

4.0 Data Storage and Handling of Client Personal Data

4.1 Medios móviles. Cuando se requiera el almacenamiento de datos personales en medios móviles digitales se requerirá que los datos almacenados en los medios móviles se

cifren utilizando una tecnología de encriptación estándar de la industria.

4.2 Se debe seudonimizar, enmascarar, desidentificar o anonimizar los datos personales.

4.3 Physical Transport of Data

4.3.1 El proveedor eliminará, destruirá y / o devolverá, de ser posible, cualquier Dato personal que ya no se requiera en relación con el proyecto.

5.0 Access Control

5.1 User Access Management

5.1.1 El Proveedor revisará los Registros de Control de Acceso por lo menos trimestralmente, o según lo acordado por las partes por escrito, para confirmar que los niveles de acceso siguen siendo apropiados para los roles individuales y para confirmar que las revocaciones de acceso para el Personal que se separó del proyecto se procesaron correctamente.

5.1.2 El proveedor debe otorgar acceso al sistema al personal del proyecto utilizando el concepto de Acceso menos privilegiado, lo que significa que a los individuos solo se les concede acceso a los recursos y sistemas necesarios para desempeñar su función.

5.2 Data Disposal

5.2.1 El proveedor eliminará, destruirá y / o devolverá, de ser posible, cualquier información personal que ya no se requiera en relación con el proyecto

Physical and Environmental Security

6.0 Physical Security

6.1 El proveedor implementará controles de seguridad físicos razonables en sus instalaciones por procedimientos de seguridad suficientes, donde se procesen los datos personales del cliente (por ejemplo, bloqueos de cable, bloqueos de pantalla, dispositivos portátiles seguros.

6.2 El proveedor implementará un proceso razonable para designar al personal que puede acceder a la instalación. Solo el personal del proveedor que tenga una necesidad razonable tendrá acceso a la instalación