MEDIDAS TÉCNICAS Y ORGANIZATIVAS

(PARA CLIENTES)

Las presentes Medidas técnicas y organizativas (las "**MTO**") constituyen una parte integral del Contrato/Anexo/Adjunto/de la Adenda/Cláusula sobre Tratamiento de Datos personales (o cualquier otro documento equivalente, según proceda) suscrito entre Avaya (incluidas sus Filiales mundiales) y el Cliente (incluidas sus Filiales mundiales, si las hubiera), y se incorporan al referido documento mediante la presente Adenda.

1. Control de acceso a las instalaciones

Avaya impedirá a las personas no autorizadas el acceso físico al equipo de tratamiento de Datos personales, de la siguiente manera:

1.1. Avaya pondrá en práctica y mantendrá medidas de seguridad físicas con el fin de impedir un acceso no autorizado. Ello se verá acompañado de las siguientes medidas:

1.1.1. un sistema electrónico de control de acceso con conservación de registros durante 90 días;

1.1.2. una grabación en vídeo las 24 horas y los 7 días de la semana de las instalaciones físicas, con conservación de registros durante 30 días; y

1.1.3. detección de intrusión/alarma antirrobo o contratación de agentes de seguridad en las instalaciones.

1.2. Avaya restringirá el acceso a varias zonas en sus instalaciones en función de los puestos y revalidará periódicamente el acceso a los titulares de la autorización.

1.3. Avaya implantará medidas de seguridad para el personal y para visitantes a fin de impedir el acceso no autorizado, que se materializarán a través de las siguientes medidas:

1.3.1. El personal debe exhibir identificadores;

1.3.2. Los visitantes deben registrarse;

1.3.3. Los visitantes serán acompañados por el personal, dentro de lo razonable; y

1.3.4. Los visitantes deben llevar una insignia que los identifique fácilmente como tales.

2. Control de acceso a uso del sistema

A fin de impedir a personas no autorizadas el acceso lógico a su equipo de tratamiento de Datos personales, Avaya pondrá en práctica y mantendrá las siguientes medidas:

2.1. Avaya solo concederá acceso al equipo de tratamiento de Datos personales a personas físicas con

2.1.1. un identificador único de usuario para su acceso mediante un proceso de autorización formal, y

2.1.2. una contraseña única con las características siguientes:

2.1.2.1. contraseña compleja, compuesta de ocho caracteres y tres de los cuatro grupos de caracteres;

2.1.2.2. una validez máxima de la contraseña de noventa días; y

2.1.2.3. un bloqueo de cuenta ante inicios de sesión fallidos.

2.2. Avaya concederá acceso a cada persona en función de su puesto de trabajo y de los siguientes criterios:

2.2.1. acceso en función del puesto;

2.2.2. acceso menos privilegiado; y

2.2.3. acceso únicamente cuando se necesite conocer la información.

2.3. La pantalla de los terminales se bloqueará automáticamente al cabo de 20 minutos de inactividad.

2.4. Avaya registrará los accesos al equipo de tratamiento de datos.

2.5. Avaya hará uso de una autenticación basada en múltiples factores de la red privada virtual (VPN) de Avaya para accesos a distancia.

2.6. Avaya pondrá en práctica y mantendrá una administración central de usuarios.

2.7. Avaya encriptará los terminales que suministre.

3. Control de acceso a Datos personales

Avaya impedirá a personas no autorizadas el acceso lógico a Datos personales mediante la implantación y mantenimiento de las medidas adecuadas que impidan la lectura, copia, alteración o retirada no autorizadas de soportes que contengan Datos personales, así como la introducción no autorizada en memorias, la lectura, la alteración o la eliminación de los Datos personales almacenados. Ello se verá acompañado de las siguientes medidas:

3.1. Avaya solo concederá acceso a los Datos personales a personas físicas con:

3.1.1. un identificador único de usuario para su acceso mediante un proceso de autorización formal, y

3.1.2. una contraseña única con las características siguientes:

3.1.2.1. contraseña compleja, compuesta de ocho caracteres y tres de los cuatro grupos de caracteres;

3.1.2.2. una validez máxima de la contraseña de noventa días; y

3.1.2.3. un bloqueo de cuenta ante inicios de sesión fallidos.

3.2. Avaya concederá acceso a los Datos personales a cada persona en función de su puesto de trabajo y de los siguientes criterios:

3.2.1. acceso en función del puesto;

3.2.2. acceso menos privilegiado; y

3.2.3. acceso únicamente cuando se necesite conocer la información.

3.3. La pantalla de los terminales se bloqueará automáticamente al cabo de 20 minutos de inactividad.

3.4. Avaya registrará los accesos al equipo de tratamiento de datos.

3.5. Avaya mantendrá unas listas de control de acceso (LCA).

3.6. Avaya realizará copias de seguridad de datos y recuperaciones, a través de un soporte de copia de seguridad para almacenamiento seguro y copias de seguridad de prueba.

3.7. Avaya pondrá en práctica y mantendrá un programa de gestión de cambios en el control de acceso formal.

3.8. Avaya pondrá en práctica y mantendrá políticas internas y normas que incluyan políticas y normas de seguridad, tanto a nivel corporativo como en cada unidad de negocio.

3.9. Avaya realizará formaciones periódicas obligatorias respecto a la protección de datos personales y supervisará y exigirá la participación en la formación.

3.10. Avaya pondrá en práctica y mantendrá programas antivirus, que serán actualizados y monitorizados de forma centralizada, y realizará con regularidad análisis antivirus.

3.11. Avaya realizará un borrado y/o una supresión de datos de forma segura.

4. Control de transmisión

Avaya impedirá cualquier acceso no autorizado a Datos personales a través de la implantación de canales de comunicación y registros seguros, de la siguiente manera:

4.1. Avaya utilizará una VPN con autenticación basada en múltiples factores para los accesos a distancia.

4.2. Avaya utilizará cortafuegos con los siguientes procesos y características:

4.2.1. con inspección de estado;

4.2.2. se ponen en práctica reglas de denegación de acceso por defecto, a menos que se aprueben explícitamente las reglas de acceso;

4.2.3. acceso en función del puesto de trabajo y del rango de privilegios, cuando resulte necesario “conocer” determinada información;

4.2.4. registro y alerta de accesos; y

4.2.5. revisión anual de las reglas de cortafuegos.

4.3. Avaya utilizará un correo electrónico cifrado si el Cliente así lo habilita, utilizando como metodología la seguridad de la capa de transporte (TLS).

4.4. Avaya pondrá en práctica y mantendrá políticas y normas de seguridad, tanto a nivel corporativo como en cada unidad de negocio.

5. Control de aportaciones

Avaya garantizará la posibilidad de comprobar y establecer si se han introducido, modificado o eliminado Datos personales en el equipo de tratamiento de Datos personales, así como quién es el responsable de ello, de la siguiente manera:

5.1. Las personas que accedan a datos personales necesitarán un identificador de usuario único y autorización para su acceso.

5.2. Avaya pondrá en práctica y mantendrá políticas y normas de seguridad, tanto a nivel corporativo como en cada unidad de negocio.

5.3. El equipo de tratamiento de Datos personales tendrá funcionalidades que le permitan mantener un registro.

5.4. Avaya concederá solamente acceso a los Datos personales a cada persona en función de su puesto de trabajo y de las siguientes categorías:

5.4.1. acceso en función del puesto;

5.4.2. acceso menos privilegiado; y

5.4.3. acceso únicamente cuando se necesite conocer la información.

6. Control de organización

6.1. Avaya se asegurará de que en caso de tratamiento de datos encargado a un tercero, los Datos personales sean tratados en estricta conformidad con las instrucciones del Cliente.

6.2. El Cliente facilitará instrucciones claras a Avaya respecto al alcance del tratamiento de datos personales, y Avaya respetará dichas instrucciones.

7. Control de disponibilidad

Avaya impedirá cualquier destrucción o pérdida accidental de Datos personales mediante las siguientes medidas apropiadas:

7.1. Avaya pondrá en práctica y mantendrá una alimentación eléctrica ininterrumpida, alarmas antiincendios y de humo, sistemas de extinción de incendios, generadores, sistemas de refrigeración y entarimado de suelos.

7.2. Avaya pondrá en práctica y mantendrá un plan de recuperación ante desastres, y lo revisará y probará con carácter anual.

7.3. Avaya pondrá en práctica y mantendrá una estrategia de copia de seguridad y procedimientos de copia de seguridad.

7.4. Avaya pondrá en práctica y mantendrá programas antivirus y sistemas cortafuegos.

8. Control de separación de datos

Avaya pondrá en práctica y mantendrá las medidas apropiadas que permitan el tratamiento separado de datos que hayan sido recogidos con distintos fines, de la siguiente manera:

8.1. Avaya separará los Datos personales de distintos clientes, almacenando dichos Datos personales en bases de datos separadas de forma lógica.

8.2. Avaya distinguirá entre datos productivos y de prueba.

- FIN DE LAS MTO -