MEDIDAS TÉCNICAS Y ORGANIZATIVAS

(PARA PROVEEDORES)

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

Respecto a estos TOMS, el término "**Datos**" se refiere a ambos "**Datos Personales**" y "**Datos No Personales**", siempre que en el último caso esté sujeto a obligaciones de confidencialidad según el Contrato.

1. Control de acceso a las instalaciones

El Proveedor tomará medidas razonables para impedir a las personas no autorizadas el acceso físico al equipo de tratamiento de Datos, de la manera siguiente:

1.1. Implantación de un control de acceso electrónico para entrar en instalaciones que alojen Datos.

1.2. Implantación de un control de acceso electrónico para zonas sensibles dentro de las instalaciones como centros de datos, salas telefónicas, armarios para red LAN y laboratorios donde el tratamiento de los datos tenga lugar.

1.3. Confirmación de que se instauran políticas que garanticen que únicamente las personas autorizadas obtienen acceso a zonas sensibles como centros de datos, salas LAN, armarios de cableado telefónico y cualquier otra ubicación en que se traten o almacenen Datos. Comprobación de que todos los derechos de acceso a dichas zonas se revalidan dos veces al año.

1.4. Creación y conservación de registros de acceso a áreas sensibles como centros de datos, armarios LAN, salas de teléfonos, y cualquier otra localización física donde los datos estén almacenados, durante un mínimo de 90 días.

1.5. Comprobación de que las puertas del recinto y las zonas sensibles están vigiladas y se graban en circuito cerrado de TV las 24 horas y los 7 días de la semana. Comprobación de que todas las grabaciones de CCTV se conservan durante al menos 30 días.

1.6. Mantenimiento de un sistema de alarma supervisado activamente que proteja físicamente las zonas sensibles (como las salas de red LAN y cualquier otra zona donde tenga lugar el tratamiento de Datos).

1.7. Comprobación de la presencia de guardas de seguridad en toda instalación en la que se traten Datos.

1.8. Comprobación de la instauración de procesos que validen la identidad de una persona antes de asignarle una insignia de identificación.

1.9. Los visitantes deben registrarse y llevar una insignia que los identifique fácilmente como tales. Los visitantes serán acompañados por el personal durante su presencia en el centro donde el tratamiento de los datos tenga lugar. Todos los registros de visitantes deben conservarse durante un año como mínimo.

1.10. Limitación y control de acceso a instalaciones de centros de datos y almacenamiento de soportes que contengan Datos para contratistas externos como guardas de seguridad o servicios de intendencia.

1.11. Mantenimiento de un programa de control de llaves documentado para las instalaciones en las que se traten Datos, con un registro de llaves maestras. Las llaves de armarios, cuartos de equipamiento y cajas de cableado deben mantenerse bajo la correcta custodia, facilitarse únicamente a personas autorizadas y ser objeto de seguimiento hasta su devolución.

1.12. Comprobación de que el administrador revisa los registros de control de acceso y examina la actividad de alarmas, incluidas alarmas de puerta retenida o puerta forzada.

2. Control de acceso a uso del sistema

A fin de impedir a personas no autorizadas el acceso lógico a su equipo o aplicaciones de tratamiento de Datos, el Proveedor tomará medidas razonables para poner en práctica y mantener las medidas siguientes:

2.1. Asegurarse de que se asocia un identificador único a cada usuario de un sistema (red, servidor, base de datos, aplicación) que esté tratando Datos.

2.2. Asegurarse de que se emiten cuentas de acceso y privilegios bajo la aprobación de la dirección y que se revisan cada 6 meses.

2.3. Mantener una lista de control de acceso (LCA) para todos los sistemas que contengan Datos y revisarla con regularidad.

2.4. Aplicar la regla de mínimo privilegio y el principio del derecho a conocer la información a la hora de conceder acceso al usuario.

2.5. Aplicar la separación de obligaciones.

2.6. Asegurarse de que existen procesos en marcha para poder suspender las autorizaciones de acceso en 24 horas relativas a los usuarios que finalicen su empleo con el Proveedor (cese, traslado, etc.).

2.7. Desactivar las cuentas de usuarios al cabo de 90 días de inactividad y borrarlas una vez transcurridos 120 días de inactividad.

2.8. Asegurarse de que se comprueba la identidad de cada usuario cuando este intenta iniciar sesión a través del uso de contraseñas, de la autenticación basada en múltiples factores o de datos biométricos. Los intentos de inicio de sesión, tanto correctos como incorrectos, habrán de registrarse y conservarse durante 1 año.

2.9. Configurar el bloqueo de pantalla automático de protección de contraseña al cabo de 20 minutos de inactividad.

2.10. Las contraseñas del usuario deben contar con una longitud mínima de 8 caracteres y contener al menos un carácter de 3 de las 4 categorías (mayúscula, minúscula, número y carácter especial).

2.11. Las contraseñas de cuentas privilegiadas deben contar con una longitud mínima de 15 caracteres y contener al menos un carácter de 4 de las 4 categorías (mayúscula, minúscula, número y carácter especial).

2.12. Las contraseñas de nivel del sistema deben tener una longitud mínima de 15 caracteres, que contengan al menos un carácter de 4 de las 4 categorías (mayúscula, minúscula, número y carácter especial). Debe configurarse para que caduque después de 60 días de inactividad. Debe cambiarse cada 30 días. Debe utilizar autenticaciones de dos factores cuando sea posible.

2.13. Las contraseñas de las cuentas de servicio no deben ser utilizadas por usuarios humanos. Debe cambiarse inmediatamente cuando la contraseña esté expuesta a una persona no autorizada. Debe tener 32 caracteres generados al azar o un máximo permitido por la arquitectura, pero no menos de 26 caracteres, que contengan al menos un carácter de 4 de las 4 categorías (mayúscula, minúscula, número y carácter especial). No deben ser cuentas privilegiadas. Deben configurarse de modo que no puedan utilizarse para iniciar sesión o interactuar. Deben ser exclusivos del servicio que están destinados a soportar. No se requiere que caduquen periódicamente o por inactividad.

2.14. Las contraseñas deben caducar por lo menos al cabo de 90 días.

2.15. Las nuevas contraseñas deben ser distintas de las últimas 10 contraseñas por lo menos.

2.16. Una cuenta se bloqueará después de no más de 5 intentos infructuosos de inicio de sesión.

2.17. Todas las contraseñas de instalación y del proveedor que se faciliten por defecto con un nuevo hardware, sistema de software o nuevas aplicaciones deben volver a configurarse tras la instalación.

2.18. Las contraseñas deben almacenarse y transmitirse en formato cifrado.

2.19. La contraseña y el identificador temporales de inicio deben ser comunicados de forma segura. Las contraseñas e identificadores con texto claramente explicitado no deben nunca enviarse en un mismo correo electrónico.

2.20. Asegurarse de que la identidad del usuario se ha validado antes de permitir el reajuste de la contraseña o de facilitar una contraseña al usuario.

2.21. Normalizar los servidores, las compilaciones de sistema operativo y la configuración de conformidad con las normas de la industria de modo que resistan a eventuales ataques.

2.22. Asegurarse de que los sistemas que almacenan o tratan Datos están en segmentos de red separados en función de la etiqueta o nivel de clasificación de la información almacenada en los servidores, para garantizar que tan solo las personas autorizadas pueden comunicar con sistemas que sean necesarios a fin de cumplir sus responsabilidades específicas.

2.23. Mantener un proceso de gestión de parches documentado y realizar actualizaciones sobre los sistemas con vulnerabilidades Críticas y de Alto riesgo en un plazo de 2 semanas desde la publicación del parche, y todas las demás en un plazo de un mes. Además, se deberá corregir de inmediato cualquier parche cuando así lo solicite Avaya.

2.24. El software antivirus debe cargarse y estar operativo en todos los servidores y PCs que procesen Datos. Los proveedores harán uso de técnicas de detección de software malicioso cuando resulte posible (p. ej.: análisis de correo electrónico, análisis de sistema de archivos, análisis de tráfico de Internet, etc.).

2.25. El software de análisis de antivirus debe actualizarse diariamente como mínimo y deberá ser compatible con actualizaciones de firma urgentes y extemporáneas.

2.26. El software antivirus debe configurarse de modo que los usuarios no privilegiados no puedan desactivarlo. Sujeto al correspondiente control de cambios, sujetos privilegiados podrán desactivar el software cuando sea apropiado.

3. Control de acceso a Datos.

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

3.1. Mantener una política por escrito sobre clasificación y manejo de datos, así como un inventario de registros con la clasificación y con la ubicación física y electrónica facilitada.

3.2. El Proveedor se asegurará de que los Datos están cifrados en tránsito a través de protocolos estándar de la industria que no estén proscritos (p. ej., SSH/SCP/SFTPV2, TLSv1.2 o superiores).

3.3. El Proveedor garantizará un nivel de cifrado de Datos acorde a la norma de la industria y apropiado para los riesgos que presente el tratamiento de Datos en reposo. No obstante, todas las copias de seguridad de Datos serán cifradas en soportes de copia de seguridad.

3.4. Los Datos solo deben descargarse en un PC, ordenador portátil, dispositivo móvil o soporte de almacenamiento extraíble del Proveedor, en caso de que se habilite el cifrado del disco duro en dicho dispositivo.

3.5. Asegurarse de la rotación y gestión periódica de claves de cifrado.

3.6. Los Datos no podrán usarse nunca en entornos de desarrollo, de prueba y/o de preproducción, a menos que se encuentren pseudo-anonimizados y tal uso esté autorizado por Avaya por escrito.

3.7. Si se manipula, se almacena o se trata de algún modo la información de titulares de la tarjeta de crédito, los sistemas del Proveedor deben tener la certificación PCI DSS.

4. Control de transmisión

El Proveedor tomará medidas razonables para impedir cualquier acceso o modificación no autorizadas a los Datos durante la transmisión, a través de la implementación de canales de comunicación seguros, y habrá de poner en práctica un registro de transmisiones de la manera siguiente:

4.1. Asegurarse de que las redes del perímetro están física y lógicamente separadas de las redes internas que contengan Datos.

4.2. Instalar cortafuegos entre: Internet y sistemas web; sistemas web y sistemas de aplicación; sistemas de aplicación y redes internas que traten Datos. Estos cortafuegos serán dispositivos físicamente únicos.

4.3. Utilizar Sistemas de detección de intrusión en la red (NIDS) como parte de la estrategia de seguridad de red además de los cortafuegos en rede que traten Datos. Todos los registros NIDS serán supervisados con regularidad para detectar intentos probables de acceso no autorizado a Datos.

4.4. Los cortafuegos se utilizarán con inspección de estado y las reglas de cortafuegos se revisarán por lo menos anualmente.

4.5. Restringir y controlar el acceso inalámbrico a la red a través de protocolos estándar de seguridad inalámbrica en la industria, pero que sean de una seguridad menor a WPA2.

4.6. Restringir y controlar el acceso a la red a distancia y exigir el uso de VPN con autenticación de doble factor.

5. Control de aportaciones

El Proveedor tomará medidas razonables para garantizar la capacidad de comprobar y establecer si se han introducido, modificado o eliminado Datos en el equipo de tratamiento de datos, así como quién es el responsable de ello, de la siguiente manera:

5.1. Todo cambio en la configuración de servidores, redes, bases de datos o en aplicaciones de empresa, o cambios en los propios Datos deberá ser registrado mediante contraseña. Los registros de auditoría garantizarán que pueden rastrearse las acciones hasta una persona en particular, e incluirán como mínimo la hora, la fecha y el tipo de acción. Los registros de auditoría se conservarán durante 1 año.

5.2. Los registros de auditoría, de cambio, de evento y de control de acceso serán supervisados, revisados de forma activa y se agregarán de modo central a todos los sistemas que traten o controlen Datos personales en reposo y en tránsito a través de un mecanismo de recogida aprobado por la industria, como SIEM. Deberán crearse alertas por acceso no autorizado y anomalías. Deberán facilitarse informes de auditoría de registros y de anomalías previa petición.

5.3. Mantener la gestión de configuración, incluidas configuraciones seguras de base.

5.4. Supervisar para detectar y generar alertas por cambios no autorizados.

5.5. Asegurarse de que los cambios de emergencia implican la aprobación del correspondiente nivel de dirección antes de su puesta en práctica.

5.6. Estandarice los servidores y los sistemas operativos construidos y configurados de acuerdo con los estándares de la industria para resistir los ataques.

6. Control de organización

El Proveedor tomará medidas razonables para disponer la organización interna de tal modo que cumpla los requisitos concretos de protección de datos y ponga en práctica y mantenga las siguientes medidas:

6.1. Mantener una política por escrito en materia de seguridad de la información que sea aprobada anualmente por el equipo de dirección del Proveedor y se publique y comunique a todos los empleados del mismo, así como a los terceros correspondientes.

6.2. Mantener una función específica de cumplimiento y seguridad para diseñar, mantener y operar la seguridad en asistencia a su "plataforma de confianza" y de acorde con las normas de la industria. Esta función habrá de centrarse en la integridad del sistema, la aceptación de riesgo, el análisis y valoración de riesgo, la evaluación de riesgo, la gestión de riesgo y las declaraciones de tratamiento de aplicabilidad y gestión de proveedores.

6.3. Someterse con regularidad a revisiones de seguridad de terceros independientes y aportar informes de auditoría como el SSAE16 o ISAE3402.

6.4. Mantener un programa, procedimientos y herramientas de protección de datos, sensibilización de la seguridad y cumplimiento que aborden las amenazas y las mejores prácticas en seguridad de la información; así como políticas, procedimientos y controles de seguridad de la información que estén instaurados para proteger los Datos.

6.5. Mantener y proveer acceso a Avaya, previa petición, políticas, procedimientos y herramientas de notificación que faciliten acceso a la documentación relevante y notificaciones correspondientes sobre la implementación, efectividad y de ser necesario, corrección de las medidas convenientes relacionadas con el tratamiento de Datos.

6.6. Mantenga una política de clasificación y manejo de datos por escrito y un inventario de registros con clasificación con ubicación física y electrónica proporcionada.

6.7. Asegúrese de que las consecuencias de las infracciones de la política se establezcan, se comuniquen y se actúe en consecuencia.

7. Control de disponibilidad

El Proveedor tomará medidas razonables para impedir cualquier destrucción o pérdida accidental de Datos mediante las siguientes medidas apropiadas:

7.1. Supervisar incidencias de seguridad y configurar procesos de notificación y alerta en todos los servidores, redes y bases de datos que contengan Datos.

7.2. Gestionar un proceso de respuesta a incidentes de seguridad.

7.3. Mantener políticas, procedimientos y herramientas de planificación de contingencias que definan los roles y responsabilidades y ofrezcan una orientación y formación clara sobre el correcto tratamiento de contingencias como: incidencias de amenazas naturales como inundaciones, tornados, terremotos, huracanes y tormentas de hielo; sucesos de amenazas accidentales como vertidos químicos y fallos mecánicos o eléctricos; por último, actos intencionados como violaciones de la privacidad y de la seguridad, amenazas de bomba, asaltos y robos.

7.4. Tener instaurado un plan de continuidad de la actividad/recuperación ante desastres para el restablecimiento de los procesos y operaciones más importantes de los servicios del Proveedor en el lugar o lugares desde donde se suministren los servicios del mismo. El Proveedor tendrá igualmente instaurado un plan que asista en la respuesta a desastres de un modo planificado, y testeado por lo menos anualmente.

7.5. Poner en práctica y mantener, conforme a las normas de la industria, una alimentación eléctrica redundante, alarmas antiincendios y de humo, sistemas de extinción de incendios, generadores, sistemas de refrigeración y entarimado de suelos en los centros de datos que traten Datos.

7.6. Realizar copias de seguridad completas de las bases de datos que contengan Datos, de un modo seguro, para garantizar la disponibilidad de acuerdo con la importancia de los datos.

8. Control de activos

A fin de garantizar la protección del equipo o aplicaciones de tratamiento de Datos, el Proveedor tomará medidas razonables para poner en práctica y mantener las siguientes medidas:

8.1. Asegurarse de que se ponen en práctica procedimientos y herramientas para identificar y rastrear todo el equipo y soportes utilizados en el tratamiento de Datos.

8.2. Asignar la responsabilidad de todo el equipo y soportes a uno o más custodios.

8.3. Realizar una revisión y un visto bueno de la exactitud del inventario de activos e identificar el equipo y medios que falten de forma por lo menos anual.

9. Control de aplicaciones, redes, sistemas y bases de datos.

A fin de garantizar la protección de aplicaciones de tratamiento de Datos, el Proveedor tomará medidas razonables para poner en práctica y mantener las siguientes medidas:

9.1. Mantenga un proceso de proceso de administración de parches documentado y realice actualizaciones en sistemas con vulnerabilidades Críticas y de Alto Riesgo dentro de las 2 semanas posteriores a la publicación del parche y de todos los demás dentro de un mes. Además, deberá remediar cualquier parche inmediatamente según lo solicite Avaya.

9.2. Utilice servicios de terceros independientes reconocidos por la industria para realizar evaluaciones de vulnerabilidad y, si corresponde, pruebas de penetración de redes, sistemas, aplicaciones y bases de datos donde los datos se encuentran en reposo, en tránsito y en uso. El Proveedor deberá clasificar las vulnerabilidades identificadas y remediar las vulnerabilidades Críticas dentro de las 4 semanas posteriores a la publicación del parche y las vulnerabilidades Altas de acuerdo con los estándares de la industria generalmente aceptados.

9.3. Si fuera aplicable, antes de la publicación de la aplicación, realizar pruebas de penetración, pruebas de vulnerabilidad de la aplicación en la web y una atenuación de vulnerabilidades de alta gravedad.

9.4. Realizar pruebas de penetración al menos una vez al año en su entorno informático y facilitar a Avaya copias escritas de los resultados de dichas pruebas de penetración que haya realizado el Proveedor o sus subencargados de tratamiento, en un plazo no superior a 30 días desde que el Proveedor obtenga los resultados o informes.

9.5. En caso de que se desarrollen aplicaciones que traten Datos para el suministro de servicios por parte del Proveedor a Avaya, asegurarse de que los desarrolladores están formados en las mejores prácticas para un desarrollo seguro conforme a los estándares de la industria.

9.6. Asegurarse de que las aplicaciones que vayan a tratar Datos se desarrollan de modo seguro a través de un proceso del Proveedor formal y documentado que aporte la prueba de que no están presentes vulnerabilidades en la seguridad de la aplicación antes de pasar a la fase de producción. En lo sucesivo se realizarán nuevas pruebas al menos cada trimestre, así como después de cada cambio significativo. Las vulnerabilidades en la seguridad de la aplicación incluirían, como mínimo, las del SANS Top 20 y del OWASP Top 10.

9.7. Las vulnerabilidades en la seguridad de la aplicación que afecten a los Datos serán corregidas en un plazo razonable a contar desde su identificación.

9.8. Estos requisitos deberán ser validados por herramientas como el análisis dinámico de la aplicación y/o análisis de código estático.

10. Cambio y separación de control de datos

El Proveedor tomará medidas razonables para poner en práctica y mantener las siguientes medidas de control de cambios para el tratamiento de Datos:

10.1. Mantener procesos de gestión de cambios que incluyen la documentación de los fines, del análisis de impacto en la seguridad, del plan y resultados de pruebas y de la autorización para todos los cambios en sistemas que traten Datos.

10.2. La configuración de sistemas que traten Datos debe estar validada antes de su publicación en la red de producción.

10.3. Los cambios en entornos de producción que contengan Datos serán revisados y aprobados por la dirección del Proveedor con documentación de la disponibilidad de revisión/aprobación en el supuesto de una auditoría.

10.4. Mantener física y/o lógicamente separados los entornos de desarrollo, de prueba, de preproducción, respecto a los entornos de producción donde se traten Datos.

10.5. El Proveedor conservará física o lógicamente separadas las bases de datos para el tratamiento de Datos en beneficio de Avaya.

- FIN DE LAS MTOs -