Código de privacidad para los servicios de tratamiento de datos de Clientes de ADP

Introducción	2
Artículo 1: Alcance, aplicabilidad e implementación	2
Artículo 2: Acuerdo de servicios	4
Artículo 3: Obligaciones de cumplimiento	5
Artículo 4: Finalidades del Tratamiento de Datos	6
Artículo 5: Requisitos de seguridad	8
Artículo 6: Transparencia sobre los Empleados del Cliente	8
Artículo 7: Subencargados	9
Artículo 8: Supervisión y cumplimiento	10
Artículo 9: Políticas y procedimientos	14
Artículo 10: Formación	14
Artículo 11: Cumplimiento del control y la auditoría	15
Artículo 12: Cuestiones legales	17
Artículo 13: Sanciones por incumplimiento	21
Artículo 14: Conflictos entre este Código y la Legislación vigente con respecto al Encargado de los datos	21
Artículo 15: Cambios a este Código	22
Artículo 16: Implementación de periodos de transición	22
ANEXO 1: Definiciones de las NCV	25
ANEXO 2: Medidas de seguridad	35
ANEXO 3: Listado de las Empresas del Grupo sujetas al Código para Encargados de los datos	54

Código de privacidad para los servicios de tratamiento de datos de Clientes de ADP

Introducción

ADP ofrece a sus Clientes una amplia gama de servicios de gestión de capital humano. ADP se ha comprometido a la protección de los Datos personales en el **Código de conducta empresarial y ética de ADP.**

Este Código de privacidad para los servicios de tratamiento de datos de Clientes de ADP indica cómo se implementa dicho compromiso para el Tratamiento por parte de ADP de los Datos personales de los Empleados del Cliente en relación con el suministro de Servicios al Cliente y las Actividades de apoyo al Cliente. En este contexto, ADP trata Datos del Cliente en del Cliente en calidad de Encargado de los datos.

Para consultar las normas aplicables a los casos en los que ADP, en calidad de Responsable del tratamiento, trata Datos personales relativos a aquellas Personas con las que ADP tiene una relación comercial (por ej., Personas que representan a Clientes, Proveedores y Socios comerciales de ADP, otros Profesionales y Consumidores) y otras Personas cuyos Datos personales son tratados por ADP en el marco de sus actividades empresariales como Responsable del tratamiento, consulte el ***Código de privacidad de ADP para datos empresariales***.

Artículo 1: Alcance, aplicabilidad e implementación

Alcance: aplicabilidad a Datos en el EEE

1.1 Este Código aborda el Tratamiento de Datos personales de los Empleados de los Clientes por parte de ADP, en calidad de Encargado de los datos para los Clientes, en el proceso de suministrar Servicios al Cliente, en el caso en el que dichos Datos personales (a) estén sujetos a la Legislación vigente para el EEE (o se encontraran previamente sujetos a la Legislación vigente para el EEE antes de la transferencia de dichos Datos personales a una Empresa del Grupo situada fuera del EEE, en un país que no ha sido considerado apto, por las instituciones competentes del EEE, para proporcionar un nivel adecuado de protección de datos) y (b) sean tratados de conformidad con un Acuerdo de servicios en el que se especifica expresamente que este Código deberá aplicarse a dichos Datos personales.

Si se plantea la cuestión de la aplicabilidad de este Código, el Representante de privacidad pedirá asesoramiento al Equipo internacional de privacidad y gestión de datos antes de que tenga lugar el Tratamiento.

Tratamiento electrónico y en papel

1.2 Este Código se aplica al Tratamiento por parte de ADP de los Datos del Cliente por medios electrónicos y en sistemas de archivado en papel accesibles de manera reiterada.

Aplicabilidad de la legislación local **1.3** Nada de lo dispuesto en este Código podrá entenderse como una manera de retirar derechos o recursos legales que los Empleados del Cliente pudieran tener según la Legislación vigente. Siempre que la Legislación vigente proporcione más protección que este Código, deberán aplicarse las disposiciones pertinentes de la Legislación vigente. Siempre que este Código proporcione más protección que la Legislación vigente o proporcione garantías, derechos o recursos legales adicionales para Personas, deberá aplicarse este Código.

Políticas y directrices **1.4** ADP podrá complementar este Código mediante políticas, normas, directrices e instrucciones conformes a este Código.

Responsabilidad **1.5** Este Código es vinculante para ADP. Los Directores responsables darán cuenta del cumplimiento de este Código por parte de sus organizaciones empresariales. El Personal de ADP debe cumplir con este Código.

Fecha de entrada en vigor **1.6** Este Código ha sido aprobado por el Departamento jurídico, tras la presentación por parte del Director internacional de privacidad y ha sido adoptado por el Comité ejecutivo de ADP. Este Código entrará en vigor a fecha 11 de abril de 2018 **(Fecha de entrada en vigor)** Este Código (incluyendo una lista de las Empresas del Grupo implicadas en el Tratamiento de Datos del Cliente) se publicará en la página web www.adp.com. Asimismo, estará disponible para cualquiera que lo solicite.

Este Código será implementado por el Grupo ADP en base a los plazos estipulados en el Artículo 16.

Políticas anteriores **1.7** Este Código complementa las políticas de privacidad de ADP y sustituye afirmaciones previas hasta el punto en el cual sean contradictorias con este Código.

Función de la Entidad delegada de ADP **1.8** Automatic Data Processing, Inc. ha nombrado a ADP Nederland B.V., con su domicilio social en Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL (Países Bajos), como la Entidad delegada de ADP, a cargo de hacer cumplir con este Código dentro del Grupo ADP, y ADP Nederland, B.V. ha aceptado dicho nombramiento.

Artículo 2: Acuerdo de servicios

Acuerdo de servicios, Subencargados **2.1** ADP solo tratará Datos del Cliente en base a un Acuerdo de servicios que incorpore los requisitos obligatorios para contratar servicios de Tratamiento de datos, en virtud de la Legislación vigente con respecto al Encargado de los datos y para las Finalidades legítimas descritas en el artículo 4.

La Entidad contratante de ADP usa Subencargados, tanto Subencargados de ADP como Terceros Subencargados del Tratamiento, en el desarrollo habitual de los Servicios al Cliente. Los Acuerdos de servicios de ADP deberán autorizar el uso de dichos Subencargados, a condición de que la Entidad contratante de ADP sea responsable ante el Cliente del cumplimiento, por parte de los Subencargados, de los términos del Acuerdo de servicios. Las disposiciones del artículo 7 regularán de manera más detallada el uso de Subencargados.

Extinción del Acuerdo de servicios **2.2** Al término de los Servicios al Cliente, ADP deberá cumplir sus obligaciones con el Cliente estipuladas en el Acuerdo de servicios con relación a la devolución de Datos del Cliente, facilitándole los Datos del Cliente necesarios para la continuidad de las actividades empresariales del Cliente (si no se han suministrado los datos con anterioridad o no se ha dado al Cliente acceso a los mismos mediante la correspondiente funcionalidad del producto, tal como la posibilidad de descargar los Datos del Cliente).

Cuando ADP haya cumplido con sus obligaciones según el Acuerdo de servicios deberá destruir de manera segura todas las demás copias de los Datos del Cliente y, si el Cliente así lo solicita, entregarle la certificación de dicha destrucción. ADP podrá conservar una copia de los Datos del Cliente según lo exija la Legislación vigente, si el Cliente lo autoriza, o si fuera necesario para la resolución de conflictos. ADP dejará de tratar los Datos del Cliente, salvo en la medida necesaria para los fines mencionados anteriormente. ADP seguirá sujeto a las obligaciones de confidencialidad del Acuerdo de servicios asociado durante todo el tiempo en el que conserve una copia de dichos Datos del Cliente.

Auditoría de las medidas de extinción **2.3** En el plazo de 30 días tras la extinción del Acuerdo de servicios (salvo que la Autoridad competente de protección de Datos exija lo contrario), ADP deberá permitir, a petición del Cliente o de la Autoridad competente de protección de Datos, la auditoría de sus instalaciones de Tratamiento, según se especifica en los artículos 11.2 o 11.3 (según corresponda), a fin de comprobar el cumplimiento por parte de ADP de las obligaciones relacionadas con la extinción estipuladas en el artículo 2.2.

Artículo 3: Obligaciones de cumplimiento

Instrucciones del Cliente **3.1** ADP tratará Datos del Cliente en nombre del Cliente, solo de conformidad con lo establecido en el Acuerdo de servicios y en concordancia con las instrucciones recibidas por escrito por parte del Cliente o según sea necesario en cumplimiento con la Legislación vigente.

Cumplimiento de la Legislación vigente **3.2** ADP deberá tratar los Datos del Cliente de conformidad con la Legislación vigente con respecto al Encargado de los datos.

ADP deberá atender con prontitud y de manera adecuada las solicitudes de asistencia por parte del Cliente para ayudarle a cumplir con sus obligaciones, con arreglo a la Legislación vigente con respecto al Responsable del tratamiento y de acuerdo con lo establecido en el Acuerdo de servicios.

Incumplimiento, efecto adverso importante **3.3** Si una Empresa del Grupo toma conocimiento de que la Legislación vigente con respecto al Encargado de los datos de un país de fuera del EEE, o cualquier otro cambio en la Legislación vigente con respecto al Encargado de los datos de un país de fuera del EEE, o una instrucción del Cliente, podría tener un efecto perjudicial considerable para la capacidad de ADP de cumplir con las obligaciones descritas en los apartados 3.1, 3.2 o 11.3, dicha Empresa del Grupo deberá notificar a la Entidad delegada de ADP y al Cliente sin demora, en cuyo caso el Cliente tendrá el derecho de suspender temporalmente la transferencia de Datos del Cliente a ADP, hasta que se haya ajustado el Tratamiento para solventar el incumplimiento. En caso de que no se pueda realizar dicho ajuste, el Cliente tendrá derecho a cancelar la parte afectada del Tratamiento por ADP de conformidad con los términos establecidos en el Acuerdo de servicios. Estos derechos y obligaciones no serán aplicables cuando las circunstancias o cambios en la Legislación vigente con respecto al Encargado de los datos sean el resultado de Requisitos obligatorios.

Solicitud de comunicación de Datos del Cliente **3.4** Si ADP recibe una solicitud de comunicación de Datos del Cliente de un cuerpo de seguridad competente o un organismo de seguridad estatal que no sea de un país del EEE (Autoridad), primero evaluará caso por caso si dicha solicitud es legalmente válida y vinculante para ADP. Se evitará toda solicitud que no sea legalmente válida y vinculante con ADP de conformidad con la Legislación vigente.

Sin perjuicio de lo expuesto en el siguiente párrafo, ADP deberá informar sin dilación al Cliente, la DPA principal y la DPA correspondiente al Cliente, según el artículo 11.3, de cualquier solicitud de ese tipo por parte de una Autoridad que sea legalmente válida y vinculante con ADP y solicitará a dicha Autoridad un plazo razonable de espera a fin de que la DPA principal pueda emitir una opinión con respecto a la validez de dicha solicitud de comunicación.

Si se prohíbe la suspensión del cumplimiento o notificación a la DPA principal de una Solicitud de comunicación de datos personales legalmente válida y vinculante, como en el caso de una prohibición establecida por la legislación penal para preservar la confidencialidad de una investigación policial, ADP solicitará a la Autoridad que no aplique esta prohibición y documentará que ha realizado esta solicitud. ADP facilitará, cada año, información general a la DPA principal sobre el número y tipo de Solicitudes de comunicación de datos personales procedentes de las Autoridades recibidas durante los últimos 12 meses.

Este apartado no se aplica a las solicitudes que ADP reciba por parte de las autoridades en el desarrollo normal de sus actividades como proveedor de servicios de gestión de capital humano (tales como órdenes judiciales para embargo de sueldos), que ADP puede atender según la Legislación vigente, el Acuerdo de servicios y las instrucciones del Cliente.

Cliente Consultas **3.5** ADP deberá responder con prontitud y de manera adecuada a las consultas de los Clientes relacionadas con el Tratamiento de Datos del Cliente de acuerdo con los términos establecidos en el Acuerdo de servicios.

Artículo 4: Finalidades del Tratamiento de Datos

Finalidad legítima del negocio **4.1** ADP trata Datos personales (incluidas Categorías especiales de datos) que pertenecen a los Empleados del Cliente cuando es necesario para prestar Servicios al Cliente o Actividades de apoyo al Cliente, y para las finalidades adicionales descritas a continuación:

(a) Alojamiento, almacenamiento y otro Tratamiento necesario para la continuidad del negocio y la recuperación en caso de desastres, incluyendo la realización de copias de seguridad y copias de Archivo de Datos personales.

(b) Administración y seguridad de sistemas y redes, incluyendo la supervisión de infraestructuras, la gestión de identidades y credenciales, la verificación

y autenticación, y el control de acceso.

(c) Supervisión y otros controles necesarios para garantizar la integridad y la seguridad de las transacciones (por ej. transacciones financieras y actividades de circulación de capital) incluyendo las diligencias debidas (tales como verificar la identidad de la Persona o la aptitud de esta para recibir productos o servicios, tales como verificar la situación laboral o el estado de cuentas).

(d) Imponer el cumplimiento de contratos y proteger a ADP, sus Asociados, Clientes, los Empleados de los Clientes y el público frente a robos, responsabilidades legales, fraudes o abusos, incluyendo: (i) la supervisión, investigación, prevención y mitigación de los daños causados por fraudes, o intentos de fraudes, financieros o de identidad así como de otras amenazas a los bienes económicos y materiales, credenciales de acceso y sistemas de información; (ii) la participación en iniciativas externas de seguridad en el ciberespacio, contra el fraude y contra el blanqueo de dinero; y (iii) la protección de los intereses vitales de las Personas, por ejemplo mediante la notificación de cualquier peligro que se haya detectado.

(e) Ejecución y gestión de procesos empresariales internos de ADP que conllevan el Tratamiento incidental de Datos del Cliente para:

(1) auditorías internas y consolidación de informes,

(2) cumplimiento de normativas, incluidos los registros obligatorios, usos y divulgaciones de información exigidas por la Legislación vigente,

(3) disociación de Datos e inclusión de Datos disociados para minimización de datos y servicios de análisis,

(4) uso de Datos disociados y agregados, según lo permitan los Clientes, para proporcionar análisis, continuidad y mejora de los productos y servicios de ADP, y

(5) simplificación de la gestión corporativa, incluyendo fusiones, adquisiciones, enajenaciones y empresas conjuntas.

Artículo 5: Requisitos de seguridad

Seguridad de los datos **5.1** ADP utilizará medidas técnicas, físicas y de organización apropiadas y razonables desde el punto de vista comercial, a fin de proteger los Datos del Cliente de usos indebidos, así como de su destrucción, pérdida, alteración, divulgación, adquisición o acceso de manera accidental, ilegal o no autorizada durante su Tratamiento. Dichas medidas cumplen con los requisitos de la Legislación vigente para el EEE o aquellos requisitos más estrictos que se hayan impuesto en virtud del Acuerdo de servicios. ADP tomará, bajo todas las circunstancias, las medidas especificadas en el anexo 2 de este Código, pudiendo ser estas modificadas por ADP siempre y cuando esto no suponga una reducción significativa del nivel de seguridad establecido para los Datos del Cliente en el anexo 2.

Acceso a los Datos y confidencialidad **5.2** El Personal deberá estar autorizado a acceder a los Datos del Cliente únicamente en la medida necesaria para cumplir con las finalidades de Tratamiento correspondientes a los Datos en concordancia con el artículo 4. ADP impondrá obligaciones de confidencialidad a los miembros del Personal que tengan acceso a los Datos del Cliente.

Notificación de infracción de la seguridad de los datos **5.3** Tras enterarse de la existencia de una Infracción de seguridad de los datos, ADP notificará al Cliente dicha infracción sin retrasos indebidos, a menos que un agente de las fuerzas del orden o una autoridad supervisora determine que dicha notificación podría interferir en el curso de una investigación criminal, causar daños a la seguridad nacional o un abuso de confianza en ese sector industrial. En este caso, la notificación deberá retrasarse tal y como indique dicho agente de las fuerzas del orden o la autoridad supervisora. ADP responderá con prontitud a las preguntas del Cliente sobre dicha infracción de la seguridad de los datos.

Artículo 6: Transparencia sobre los Empleados del Cliente

Otras solicitudes de los Empleados del Cliente **6.1** ADP deberá informar al Cliente sin demora de las solicitudes o quejas relacionadas con el Tratamiento de Datos personales por parte de ADP que reciba directamente de los Empleados del Cliente sin responder a dichas solicitudes o quejas, a menos que así lo estipule el Acuerdo de servicios o por indicación del Cliente.

Si el Cliente solicita, en el Acuerdo de servicios, que se atiendan las solicitudes y denuncias de los Empleados del Cliente, ADP se asegurará de proporcionar a los Empleados del Cliente la información solicitada que sea razonable (como el

punto de contacto y el procedimiento) a fin de que los Empleados del Cliente puedan hacer la solicitud o presentar la queja de manera adecuada.

Las estipulaciones de este artículo 6.1 no serán aplicables a las solicitudes que ADP atiende normalmente en el proceso de la prestación de Servicios al Cliente y Actividades de apoyo al Cliente.

Artículo 7: Subencargados

Contratos de subencargo con terceros	**7.1**	Los Terceros Subencargados del Tratamiento solo podrán tratar los Datos del Cliente de acuerdo con un Contrato de subencargo. El Contrato de subencargo deberá imponer al Tercero Subencargado del Tratamiento términos parecidos en cuanto a protección de datos para el Tratamiento. Dichos términos no serán menos estrictos que los impuestos a la Entidad contratante de ADP por medio del Acuerdo de servicios y este Código.
Publicación del listado de Subencargados	**7.2**	ADP publicará un listado de las categorías de Subencargados involucrados en el desarrollo de los Servicios al Cliente correspondientes en la página web de ADP apropiada. Este listado se actualizará con rapidez en caso de cambios.
Notificación de nuevos Subencargados y derecho a oponerse	**7.3**	ADP deberá notificar al Cliente la contratación por parte de ADP de cualquier Subencargado nuevo que participe en la prestación de Servicios al Cliente. Durante los siguientes 30 días a la recepción de dicha notificación, el Cliente podrá oponerse al uso de dicho Subencargado mediante una notificación por escrito dirigida a ADP, alegando las razones, objetivas y justificables, por las que el Subencargado no tiene la capacidad para proteger los Datos del Cliente de acuerdo con las obligaciones del Contrato de subencargo, tal y como se especifican en el artículo 7.1. En caso de que las partes no puedan llegar a un acuerdo mutuamente aceptable, ADP podrá, a su elección, no conceder al Subencargado acceso a los Datos del Cliente, o permitir que el Cliente cancele los Servicios al Cliente correspondientes según lo dispuesto en los términos del Acuerdo de servicios.
Excepción	**7.4**	La estipulaciones de esta sección 7 no serán aplicables en la medida en la que el Cliente dé instrucciones a ADP de permitir el Tratamiento de Datos del Cliente por parte de un Tercero de conformidad con lo establecido en un contrato que el Cliente tiene directamente con dicho Tercero (por ej. un proveedor de prestaciones externo).

Artículo 8: Supervisión y cumplimiento

Director internacional de privacidad

8.1 El Grupo ADP deberá tener un Director internacional de privacidad que sea responsable de:

(a) presidir el Consejo directivo de privacidad,

(b) supervisar el cumplimiento de este Código,

(c) supervisar, coordinar, comunicar y asesorarse con los miembros relevantes de la Red de privacidad sobre cuestiones de privacidad y protección de los datos,

(d) ofrecer informes de privacidad anuales al Comité ejecutivo de ADP sobre riesgos en materia de protección de los datos y cuestiones relacionadas con el cumplimiento,

(e) coordinar investigaciones oficiales o consultas de organismos gubernamentales en torno al Tratamiento de los Datos del Cliente, junto con los miembros pertinentes de la Red de privacidad y el departamento jurídico de ADP,

(f) abordar conflictos entre este Código y la Legislación vigente,

(g) supervisar el proceso por el cual se llevan a cabo Evaluaciones del impacto de la privacidad (PIA, por sus siglas en inglés) y revisar las PIA como corresponda,

(h) supervisar la documentación, notificación y comunicación de las Infracciones de la seguridad de los datos,

(i) asesorar sobre procesos, sistemas y herramientas de gestión de los datos para implementar el marco de trabajo para la gestión de la privacidad y protección de los datos según lo establecido por el Consejo directivo de privacidad, incluyendo:

(1) mantener, actualizar y publicar este Código y las políticas y normas relacionadas,

(2) asesorar acerca de las herramientas para recopilar, mantener y actualizar inventarios que contengan información sobre la estructura y el funcionamiento de todos los sistemas para tratar Datos del Cliente,

(3) proporcionar, atender o asesorar al Equipo sobre formación en materia de seguridad, de manera que este comprenda y cumpla con sus responsabilidades en virtud de este Código,

(4) coordinarse con el departamento de Auditoría interna de ADP y otros para desarrollar y mantener un programa de aseguramiento apropiado para supervisar, auditar e informar sobre el cumplimento de este

Código, además de para permitirle a ADP que verifique y certifique dicho cumplimiento según sea necesario,

(5) implementar procedimientos según sea necesario para tratar las consultas, preocupaciones y reclamaciones sobre privacidad y protección de los datos, y

(6) asesorar acerca de las sanciones apropiadas por infracciones de este Código (por ej., normas disciplinarias).

Red de privacidad 8.2 ADP deberá establecer una Red de privacidad suficiente para controlar el cumplimiento de este Código dentro de la organización global de ADP.

La Red de privacidad deberá crear y mantener un marco de trabajo para apoyar al Director internacional de privacidad y realizar controles de aquellas tareas descritas en el artículo 8.1 y de otras tareas según convenga para mantener y actualizar este Código. Los miembros de la Red de privacidad deberán llevar a cabo, según corresponda a su cargo en la región o la organización, las siguientes tareas adicionales:

(a) supervisar la implementación de los procesos, los sistemas y las herramientas de gestión de los datos que permitan el cumplimiento del Código por parte de las Empresas del Grupo en sus regiones u organizaciones respectivas,

(b) apoyar y evaluar la gestión de la privacidad y la protección de los datos y el cumplimiento en general de las Empresas del Grupo dentro de sus regiones,

(c) asesorar periódicamente a sus Representantes de privacidad y al Director internacional de privacidad acerca de los riesgos regionales o locales en materia de privacidad y de cuestiones sobre cumplimiento,

(d) verificar que se hayan mantenido los inventarios apropiados de los sistemas para tratar Datos del Cliente,

(e) estar disponible para responder solicitudes relacionadas con aprobaciones o asesoramiento sobre privacidad,

(f) ofrecer la información necesaria para el Director internacional de privacidad a fin de completar el informe anual sobre privacidad,

(g) ayudar al Director internacional de privacidad en caso de que se realicen investigaciones oficiales o consultas por parte de organismos gubernamentales,

(h) elaborar y publicar políticas y normas sobre privacidad apropiada para sus regiones u organizaciones,

(i) asesorar a las Empresas del Grupo sobre la conservación y destrucción de los datos,

(j) informar al Director internacional de privacidad de reclamaciones y ayudar a atender dichas reclamaciones, y

(k) ayudar al Director internacional de privacidad, a otros miembros de la Red de privacidad, a Representantes de privacidad y a otros como sea necesario para:

(1) permitir que las Empresas del Grupo u organizaciones cumplan con el Código empleando las instrucciones, herramientas y formación que se ha elaborado,

(2) compartir las mejores prácticas para la gestión de la privacidad y la protección de los datos dentro de la región,

(3) confirmar que los requisitos sobre privacidad y protección de los datos se tienen en cuenta siempre que se implementen nuevos productos y servicios en las organizaciones o Empresas del Grupo, y

(4) ayudar a los Representantes de privacidad, Empresas del Grupo, unidades de negocio, áreas funcionales y personal de adquisiciones con el uso de Subencargados.

Representantes de privacidad

8.3 Los Representantes de privacidad son directivos de ADP que han sido nombrados por un Director responsable o la Dirección Ejecutiva de ADP para implementar y hacer cumplir el Código dentro de una unidad de negocio o ámbito funcional de ADP. Los Representantes de privacidad son responsables de la implementación efectiva del Código dentro de la unidad de negocio o área funcional pertinentes. En particular, los Representantes de privacidad deben verificar que los controles efectivos de gestión de la privacidad y de protección de los datos estén integrados en todas las prácticas comerciales que afectan a los Datos del Cliente, y que los recursos y el presupuesto adecuados estén disponibles para cumplir con las obligaciones de este Código. Los Representantes de privacidad podrían delegar tareas y deberán asignar recursos apropiados, cuando sea necesario, para cumplir con sus responsabilidades y alcanzar sus objetivos de cumplimiento.

Entre las responsabilidades de los Representantes de privacidad se incluyen:

(a) supervisar la gestión de la privacidad y de protección de los datos dentro de su Empresa del Grupo, unidad de negocio o área funcional, y verificar que todos los procesos, los sistemas y las herramientas elaborados por el Equipo internacional de privacidad y gestión de datos se hayan implementado con efectividad,

(b) confirmar que las tareas de gestión de la privacidad y de protección de los datos, así como las de cumplimiento, se hayan delegado adecuadamente en el desarrollo habitual del negocio, además de durante y tras restructuraciones de la organización, subcontrataciones, fusiones y adquisiciones, y desinversiones,

(c) colaborar con el Director internacional de privacidad y los miembros relevantes de la Red de privacidad para comprender y abordar cualquier requisito legal nuevo, y verificar que los procesos de gestión de la privacidad y de protección de los datos estén actualizados a fin de hacer frente a las circunstancias cambiantes y los requisitos legales y reguladores,

(d) consultar con el Director internacional de privacidad y los miembros relevantes de la Red de privacidad en todos los casos en los que exista un conflicto real o potencial entre la Legislación vigente y este Código,

(e) supervisar a los Subencargados usados por la Empresa del Grupo, unidad de negocio o área funcional para garantizar el cumplimiento continuado de este Código y de los Contratos de subencargo por parte de los Subencargados,

(f) confirmar que todo el Personal en la Empresa del Grupo, unidad de negocio o área funcional ha completado los cursos de formación en materia de privacidad requeridos, y

(g) ordenar que los Datos del Cliente almacenados sean borrados, destruidos, disociados o trasmitidos según lo requerido por el artículo 2.2.

Directores responsables **8.4** Los Directores responsables, como jefes de unidades de negocio o áreas funcionales, son responsables de garantizar la implementación de una gestión eficaz de la privacidad y de la protección de los datos en sus organizaciones. Cada Director responsable deberá (a) nombrar a un Representante de privacidad apropiado, (b) garantizar que los recursos y presupuestos adecuados estén disponibles para el cumplimiento, y (c) ofrecer apoyo al Representante de privacidad cuando sea necesario para abordar deficiencias en el cumplimiento y gestionar el riesgo.

Consejo directivo de privacidad **8.5** El Director internacional de privacidad deberá dirigir un Consejo directivo de privacidad compuesto por Representantes de privacidad, miembros de la Red de privacidad seleccionados por el Director internacional de privacidad y otros que pueden ser necesarios para ayudar a alcanzar el objetivo del Consejo. El Consejo directivo de privacidad deberá elaborar y mantener un marco de trabajo para apoyar las tareas según convenga para las Empresas del Grupo, unidades de negocio y las áreas funcionales a fin de cumplir con este Código, llevar a

cabo las tareas descritas en el mismo y apoyar al Director internacional de privacidad.

Miembros de la Red de privacidad predeterminada y Representantes de privacidad **8.6** Si en algún momento no existiera un Director internacional de privacidad asignado o con capacidad para ejercer las funciones asignadas al cargo, el Departamento jurídico deberá nombrar a una persona para que actúe como Director internacional de privacidad provisional. Si en algún momento no existiera un miembro de la Red de privacidad designado para una región u organización en particular, el Director internacional de privacidad deberá llevar a cabo las tareas de dicho miembro de la Red de privacidad descritas en el artículo 8.2.

Si en algún momento no existiera un Representante de privacidad designado para una Empresa del Grupo, unidad de negocio o área funcional, el Director responsable deberá asignar a una persona apropiada para llevar a cabo las tareas descritas en el artículo 8.3.

Cargos legales **8.7** Siempre que miembros de la Red de privacidad, por ej., los responsables de la protección de los datos en virtud de la Legislación vigente para el EEE, ostenten sus cargos conforme a la ley, estos deberán desempeñar las responsabilidades de su cargo en la medida en que no entren en conflicto con sus puestos legales.

Artículo 9: Políticas y procedimientos

Políticas y procedimientos **9.1** ADP deberá elaborar e implementar políticas, normas, directrices y procedimientos para cumplir con este Código.

Información sobre el sistema **9.2** ADP deberá mantener disponible con facilidad toda la información relacionada con la estructura y el funcionamiento de todos los sistemas y procesos para tratar Datos del Cliente, como los inventarios de sistemas y procesos que influyen en los Datos del Cliente, junto con la información generada en el curso de las Evaluaciones del impacto de la protección de datos. Se proporcionará bajo petición una copia de esta información a la DPA principal o a una DPA competente para el Cliente en virtud del artículo 11.3.

Artículo 10: Formación

Formación **10.1** ADP proporcionará formación a todos los miembros del personal con acceso a los Datos del Cliente, o con responsabilidades de Tratamiento de Datos del Cliente, según las obligaciones y principios descritos en este Código y otras obligaciones en materia de privacidad y seguridad de los datos.

Artículo 11: Cumplimiento del control y la auditoría

Auditorías internas

11.1 ADP deberá auditar procesos y procedimientos comerciales que conlleven el Tratamiento de Datos del Cliente para el cumplimiento con este Código. En particular:

(a) las auditorías podrían llevarse a cabo en el curso de las actividades habituales de la Auditoría interna de ADP (incluso mediante el uso de Terceros independientes) y otros equipos internos involucrados en funciones de garantía y según las necesidades bajo petición del Director internacional de privacidad,

(b) el Director internacional de privacidad también podría solicitar que un auditor externo dirija una auditoría e informará al Director responsable de la unidad de negocio pertinente o al Comité ejecutivo de ADP cuando proceda,

(c) se respetarán las normas profesionales aplicables sobre independencia, integridad y confidencialidad durante el proceso de auditoría,

(d) el Director internacional de privacidad y el miembro apropiado de la Red de privacidad deberán ser informados de los resultados de las auditorías,

(e) en la medida en que la auditoría revela un incumplimiento de este Código, se informará de estos resultados a los Representantes de privacidad y a los Directores responsables aplicables, el Representante de privacidad cooperará con el Equipo internacional de privacidad y gestión de datos para elaborar y ejecutar un plan de reparación apropiado,

(f) se proporcionará bajo petición una copia de los resultados de la auditoría relacionados con el cumplimiento de este Código a la DPA principal o a una DPA competente, según el artículo 11.3.

Auditoria del Cliente

11.2 ADP atenderá las solicitudes de auditoría del Cliente de acuerdo con lo dispuesto en este artículo 11.2. ADP responderá a las preguntas del Cliente en lo referente al Tratamiento de Datos del Cliente por parte de ADP. En el supuesto de que el Cliente considere razonablemente justificado, en base a las respuestas proporcionadas por ADP, un análisis más exhaustivo, ADP, en concordancia con el Cliente, deberá:

(a) proporcionar acceso a las instalaciones de Tratamiento de Datos del Cliente a un auditor externo cualificado, contratado por el Cliente, razonablemente adecuado para ADP y sujeto a obligaciones de confidencialidad satisfactorias para ADP. El Cliente entregará una copia del informe de auditoría al Director internacional de privacidad que será tratada como información confidencial. No se harán auditorías, en horas normales de trabajo, más de una vez al año, por cada Cliente, durante todo el Contrato de servicios, y dichas auditorías estarán sujetas a (i)

notificación por escrito, presentada a ADP, con 45 días de anterioridad a la fecha propuesta para la auditoría, (ii) un planteamiento escrito y detallado de la auditoría revisado y aprobado por la organización de seguridad de ADP y (iii) las políticas de seguridad locales de ADP. Dichas auditorías solo se realizarán en presencia de un representante de la Oficina internacional de seguridad de ADP y el Equipo internacional de privacidad y gestión de datos o ante una persona nombrada por el representante correspondiente. Las auditorías no deberán interferir en las actividades de Tratamiento de ADP ni poner en peligro la seguridad y confidencialidad de los Datos personales de otros Clientes de ADP.

(b) ADP deberá entregar al Cliente una declaración, expedida por un asesor externo independiente y cualificado, certificando el cumplimiento de este Código por parte de ADP en los procesos y procedimientos empresariales que impliquen Tratamiento de Datos del Cliente.

ADP podrá cobrar al Cliente unos honorarios razonables por dicha auditoría.

Este artículo 11.2 complementa o aclara los derechos a auditorías que los Clientes podrían tener en virtud de la Legislación vigente y los Acuerdos de servicios. En caso de contradicción, prevalecerán las disposiciones de la Legislación vigente y los Acuerdos de servicios.

Auditorias por parte de las DPA

11.3 Se autorizará la auditoria de la transferencia de datos correspondiente por parte de cualquier DPA de un país del EEE con competencia para auditar a un Cliente de ADP a fin de comprobar el cumplimiento de este Código, bajo las mismas condiciones que se aplicarían según la Legislación vigente con respecto al Responsable del tratamiento si esa DPA llevara a cabo una auditoría del Cliente directamente.

A fin de facilitar dicha auditoría:

ADP y el Cliente, a fin de intentar resolver la solicitud, colaborarán de buena gana presentando a la DPA información pertinente, tal como informes de auditorías de ADP, y facilitarán el diálogo entre la DPA y el Cliente y los expertos en la materia de ADP, quienes pueden comprobar el funcionamiento de los controles de seguridad, privacidad y operativos. El Cliente tendrá acceso a sus Datos del Cliente de acuerdo con lo establecido en el Acuerdo de servicios y puede delegar dicho acceso a representantes de la DPA.

Si la información disponible por dichos medios resultara insuficiente para satisfacer los objetivos indicados por la DPA, ADP brindará a la DPA la oportunidad de comunicarse con el auditor de ADP.

(a) Si esto también resulta insuficiente, ADP facilitará a la DPA el derecho de examinar directamente las instalaciones de ADP utilizadas para tratar los

Datos del Cliente, en base a una notificación previa con un plazo razonable, y durante horas laborables y con total respeto hacia la confidencialidad de la información obtenida y los secretos comerciales de ADP. La DPA solo podrá acceder a los Datos del Cliente que pertenezcan al Cliente.

Este artículo 11.3 complementa o aclara los derechos a auditorías que las DPA podrían tener en virtud de la Legislación vigente y los Acuerdos de servicios. En caso de contradicción, prevalecerán las disposiciones de la Legislación vigente.

Informe anual **11.4** El Director internacional de privacidad deberá producir un informe anual para el Comité ejecutivo de ADP a fin de cumplir con este Código, la privacidad, los riesgos de protección de los datos y otras cuestiones relevantes. Este informe reflejará la información proporcionada por la Red de privacidad y otra relacionada con desarrollos locales y cuestiones específicas dentro de las Empresas del Grupo.

Mitigación **11.5** ADP adoptará las medidas apropiadas para tratar cualquier caso de incumplimiento de este Código identificado durante las auditorías de cumplimiento.

Artículo 12: Cuestiones legales

Derechos de los Empleados del Cliente **12.1** Si ADP incumple el Código en lo referente a los Datos personales de un Empleado del Cliente amparado por este Código, dicho Empleado del Cliente, como tercera parte beneficiaria, podrá exigir el cumplimiento de los artículos 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8 y 14.3 de este Código para Encargados de los datos por parte de la Entidad contratante de ADP.

En la medida que el Empleado del Cliente imponga el cumplimiento de dichos derechos en contra de la Entidad contratante de ADP, la Entidad contratante de ADP podrá no depender del incumplimiento de sus obligaciones por parte de un Subencargado para evitar responsabilidades, salvo en la medida que la defensa del Subencargado también conlleve la defensa de ADP. Sin embargo, ADP podrá invocar la defensa o derechos que se hubiesen puesto a disposición del Cliente. Asimismo, para defenderse de la acusación de la Persona afectada, ADP también podrá sostener todas las alegaciones que ADP podría hacer valer contra el Cliente (tal como negligencia contributiva).

Procedimiento de reclamaciones **12.2** Los Empleados del Cliente pueden presentar una queja por escrito respecto a cualquier reclamación referente a lo descrito en el artículo 12.1 al Equipo

internacional de privacidad y gestión de datos mediante un mensaje de correo electrónico, o por correo postal, en la dirección indicada al final de este Código. Los Empleados del Cliente también podrán presentar una reclamación o demanda ante las autoridades o los tribunales de acuerdo con lo establecido en el artículo 12.3 de este Código.

El Equipo internacional de privacidad y gestión de datos será responsable de la tramitación de las reclamaciones. Cada reclamación será asignada a un miembro del Equipo apropiado (tanto de dentro del Equipo internacional de privacidad y gestión de datos como de dentro de la unidad de negocio o área funcional aplicable). Este Equipo:

(a) acusará recibo de la reclamación con prontitud,

(b) analizará la reclamación y, si fuera necesario, iniciará una investigación,

(c) si la reclamación está fundada, aconsejará al Representante de privacidad y al miembro pertinente la Red de privacidad, de manera que el plan de reparación pueda elaborarse y ejecutarse, y

(d) mantendrá registros de todas las reclamaciones recibidas, las respuestas proporcionadas y las medidas correctivas adoptadas por ADP.

ADP se esforzará dentro de límites razonables por resolver reclamaciones sin dilaciones indebidas, de manera que se dé una respuesta al Empleado del Cliente en un plazo de cuatro semanas a partir de la fecha en la que se presentó la reclamación. La respuesta se proporcionará por escrito y se enviará al Empleado del Cliente a través de los medios que el Empleado del Cliente utilizó originalmente para ponerse en contacto con ADP (por ej., por correo postal o electrónico). La respuesta destacará las medidas que ADP ha adoptado para investigar la reclamación e indicará la decisión de ADP con relación a qué medidas (si fuera el caso) adoptará como resultado de la reclamación.

En caso de que ADP no pueda completar razonablemente su investigación y responder en el plazo de cuatro semanas, deberá informar al Empleado del Cliente en un plazo de cuatro semanas de que la investigación continúa y de que se proporcionará una respuesta en las siguientes ocho semanas.

Si la respuesta de ADP no resulta satisfactoria para el Empleado del Cliente (por ej. si se deniega la petición) o ADP no respeta las condiciones del procedimiento de reclamaciones establecido en este artículo 12.2, el Empleado del Cliente puede presentar una reclamación o demanda ante las autoridades o los tribunales de acuerdo con el artículo 12.3.

Jurisdicción para las demandas de los Empleados del Cliente

12.3 Se anima a los Empleados del Cliente a seguir desde un principio el procedimiento de reclamaciones establecido en el artículo 12.2 de este Código antes de presentar cualquier reclamación o demanda ante las autoridades o los tribunales.

Los Empleados del Cliente podrán, según lo consideren oportuno, presentar las reclamaciones indicadas en el artículo 12.1 mediante la presentación de una demanda ante:
(i) la DPA del país en el que reside habitualmente, del lugar de trabajo o del lugar donde tuvo lugar el incumplimiento, contra la Entidad contratante de ADP o la Entidad delegada de ADP, o
(ii) la DPA principal o los tribunales de los Países Bajos, en cuyo caso la demanda será solo contra la Entidad delegada de ADP.

Los Empleados del Cliente podrán, según lo consideren oportuno, presentar las reclamaciones indicadas en el artículo 12.1 mediante la presentación de una demanda ante:
(i) los tribunales del país en el que reside habitualmente, o del lugar donde se originó la transferencia de datos amparados bajo este Código, contra la Entidad contratante de ADP o la Entidad delegada de ADP, o
(ii) la DPA principal o los tribunales de los Países Bajos, en cuyo caso la demanda será solo contra la Entidad delegada de ADP.

Las DPA y los tribunales deberán aplicar sus propias disposiciones procesales y de derecho sustantivo a las disputas. La elección que realice el Empleado del Cliente no perjudicará los derechos procesales y de derecho sustantivo que las partes pudieran tener en virtud de la Legislación vigente.

Derechos de los Clientes

12.4 El Cliente podrá hacer valer este Código frente a (i) la Entidad contratante de ADP o (ii) la Entidad delegada de ADP ante la DPA principal o los tribunales de los Países Bajos, pero solo en el caso de que la Entidad contratante de ADP no se encuentre en un país del EEE. La Entidad delegada de ADP deberá asegurarse de que se adopten las medidas adecuadas para abordar las infracciones de este Código por la Entidad contratante de ADP o cualquiera de las Empresas del Grupo involucradas.

La Entidad contratante de ADP y la Entidad delegada de ADP podrán no depender del incumplimiento de sus obligaciones por parte de otra de las Empresas del Grupo, o un Subencargado, para evitar responsabilidades, salvo en el caso de que la defensa de dicha Empresa del Grupo o Subencargado también conlleve la defensa de ADP.

Recursos legales disponibles, carga de la prueba para los Empleados del Cliente

12.5 En el supuesto de que un Empleado del Cliente tenga una reclamación amparada en el artículo 12.1, el Empleado del Cliente tendrá derecho a una indemnización por daños según lo establecido por la Legislación vigente para el EEE.

En caso de que los Empleados del Cliente presenten quejas por daños en virtud del artículo 12.1, corresponderá a los Empleados del Cliente demostrar que han sufrido daños y establecer hechos que muestren que parece plausible que los daños hayan ocurrido a consecuencia de una infracción de este Código. Posteriormente, la Entidad contratante de ADP (o la Entidad delegada de ADP, según corresponda) tendrá la carga de probar que dichos daños sufridos por el Empleado del Cliente, a causa del incumplimiento de este Código, no son atribuibles a la Empresa del Grupo o Subencargado en cuestión, o de hacer valer los medios de defensa pertinentes.

Indemnización al Cliente

12.6 En caso de incumplimiento de este Código, y con arreglo a los términos del Acuerdo de servicios, los Clientes tendrán derecho a una indemnización por daños directos según lo estipulado en el Acuerdo de servicios.

Apoyo mutuo

12.7 Todas las Empresas del Grupo deberán, según sea necesario, cooperar y prestar ayuda, en la medida que sea razonablemente posible, a fin de (a) atender una solicitud, queja o demanda presentada por un Cliente o un Empleado del Cliente o (b) cumplir con una investigación legal o una consulta de una autoridad gubernamental.

La Empresa del Grupo que reciba una solicitud de información de acuerdo con el artículo 6.1 o una reclamación o demanda de acuerdo con el artículo 12.2 o 12.3, tendrá la responsabilidad de atender todas las comunicaciones con el Cliente o el Empleado del Cliente referentes a dicha reclamación o demanda, a menos que lo impidan las circunstancias, o el Equipo internacional de privacidad y gestión de datos indique lo contrario.

Sugerencias y resoluciones vinculantes de la DPA

12.8 ADP deberá, de buena fe, cooperar y hacer todo lo posible por seguir el consejo de la DPA principal y la DPA competente en virtud del artículo 12.3 emitido en torno a la interpretación y aplicación de este Código. ADP deberá atenerse a las decisiones vinculantes de las DPA competentes.

Legislación aplicable a este Código

12.9 Este Código deberá regirse e interpretarse de conformidad con la legislación neerlandesa.

Artículo 13: Sanciones por incumplimiento

Incumplimiento **13.1** El incumplimiento de este Código por parte del Personal podría resultar en la aplicación de medidas disciplinarias o contractuales apropiadas de conformidad con la Legislación vigente y las políticas de ADP, incluyendo la posible terminación de empleo o de contrato.

Artículo 14: Conflictos entre este Código y la Legislación vigente con respecto al Encargado de los datos

Conflicto entre este Código y la Legislación **14.1** Siempre que exista un conflicto entre la Legislación vigente con respecto al Encargado de los datos y este Código, el Director responsable, o Representante de privacidad, deberá consultar con el Director internacional de privacidad, el/los miembro/s relevante/s de la Red de privacidad (según proceda) y el departamento jurídico de la unidad de negocio para determinar cómo cumplir con este Código y resolver el conflicto en la medida razonablemente viable, dados los requisitos legales aplicables a ADP.

Requisitos legales contradictorios nuevos **14.2** Los miembros del departamento jurídico, los representantes de seguridad comercial de ADP, el Equipo internacional de privacidad y gestión de datos y los Representantes de privacidad deberán informar con prontitud al Equipo internacional de privacidad y gestión de datos sobre cualquier requisito legal de los que tengan conocimiento que pudiera interferir con la capacidad de ADP de cumplir con este Código.

Los Representantes de privacidad pertinentes, previa consulta al departamento jurídico, deberán informar con prontitud a los Directores responsables de cualquier requisito legal que pudiera interferir con la capacidad de ADP de cumplir con este Código.

Informar a la DPA principal **14.3** Si ADP toma conocimiento de que la Legislación vigente con respecto al Encargado de los datos o cualquier otro cambio en la Legislación vigente con respecto al Encargado de los datos podría tener un efecto perjudicial considerable para la capacidad de ADP de cumplir con las obligaciones descritas en los apartados 3.1, 3.2 o 11.3, se lo notificará a la DPA principal.

Artículo 15: Cambios a este Código

Aprobación para realizar cmbios **15.1** Cualquier cambio importante de este Código requiere la aprobación previa del Director internacional de privacidad y del Departamento jurídico, así como la adopción por parte del Comité ejecutivo de ADP, y deberá comunicarse posteriormente a las Empresas del Grupo. No se efectuarán cambios importantes al Código sin la aprobación previa del Director internacional de privacidad. La Entidad delegada de ADP notificará, anualmente, a la DPA principal los cambios efectuados en este Código.

Siempre que un cambio efectuado en este Código tenga repercusiones significativas sobre las condiciones de Tratamiento de los Servicios al Cliente, ADP informará con prontitud a la DPA principal incluyendo una explicación breve sobre el cambio y también notificará al Cliente de dicho cambio. Durante los siguientes 30 días a la recepción de dicha notificación, el Cliente podrá oponerse a dicho cambio mediante una notificación por escrito dirigida a ADP. En el supuesto de que las partes no puedan llegar a un acuerdo mutuamente aceptable, ADP deberá facilitar una solución alternativa para la transferencia de datos. Si no fuera posible poner en marcha una solución alternativa de transferencia de datos, el Cliente tendrá derecho, amparado por este Código, a suspender la transferencia correspondiente de Datos del Cliente a ADP. En caso de que no fuera posible suspender la transferencia de datos, ADP deberá permitir que el Cliente cancele los Servicios al Cliente correspondientes de acuerdo con los términos del Acuerdo de servicios.

Fecha de entrada en vigor de los cambios **15.2** Cualquier cambio deberá entrar en vigor con efecto inmediato una vez que haya sido aprobado de conformidad con el artículo 15.1, publicado en el sitio web www.adp.com y comunicado a los Clientes.

Versiones previas **15.3** Toda solicitud, reclamación o queja de un Empleado del Cliente que implique a este Código deberá juzgarse teniendo en cuenta la versión de este Código tal cual está en vigor en el momento en el que se presenta la solicitud, reclamación o queja.

Artículo 16: Implementación de periodos de transición

Implementación **16.1** La implementación de este Código deberá ser supervisada por los Representantes de privacidad, con la asistencia del Equipo internacional de privacidad y gestión de datos. Salvo como se indica a continuación, deberá haber un periodo de transición de dieciocho meses a partir de la Fecha de entrada en vigor (tal y como se indica en el artículo 1.6) para el cumplimiento de este Código.

En consecuencia, salvo que se indique lo contrario, en un periodo de dieciocho meses a partir de la Fecha de entrada en vigor, todo Tratamiento de Datos del Cliente deberá realizarse de conformidad con este Código, y el Código deberá aplicarse íntegramente. Durante el periodo de transición, el Código deberá entrar en vigor para una Empresa del Grupo en cuanto dicha Empresa del Grupo complete las tareas necesarias para la implementación plena y dicha Empresa del Grupo haya proporcionado un aviso apropiado al Director internacional de privacidad.

Empresas del grupo nuevas

16.2 Cualquier entidad que se convierta en una Empresa del Grupo tras la Fecha de entrada en vigor deberá cumplir con este Código durante un periodo de dos años tras convertirse en una Empresa del Grupo.

Entidades enajenadas

16.3 Una Entidad enajenada permanecerá amparada por este Código tras su enajenación por el periodo de tiempo que requiera ADP a fin de delimitar el Tratamiento de Datos del Cliente relacionados con dicha Entidad enajenada.

Periodo de transición para acuerdos existentes

16.4 Cuando haya acuerdos existentes con Subencargados, u otras terceras partes, que se vean afectados por este Código, las disposiciones de los acuerdos prevalecerán hasta que los acuerdos se hayan renovado en el curso normal de la actividad siempre que, no obstante, dichos acuerdos estén formulados de conformidad con este Código en un periodo de dieciocho meses a partir de la Fecha de entrada en vigor.

Datos de contacto

Equipo internacional de privacidad y gestión de datos:
privacy@adp.com

Entidad delegada de ADP
ADP Nederland B.V.
Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
PAÍSES BAJOS

Interpretaciones

INTERPRETACIÓN DE ESTE CÓDIGO:

(i) Salvo que el contexto lo requiera de otro modo, todas las referencias a un artículo o anexo en particular serán referencias a ese artículo o anexo en o para este documento, tal y como puedan modificarse cada cierto tiempo.

(ii) Los encabezados se incluyen únicamente para facilitar su consulta y no deberán utilizarse en la interpretación de ninguna disposición de este Código.

(iii) Si se define una palabra o frase, sus otras formas gramaticales tendrán el significado correspondiente.

(iv) La forma masculina incluirá la forma femenina.

(v) Las palabras «incluyen», «incluye», «incluyendo» y cualquier palabra que las preceda deberá interpretarse sin limitar la generalidad de cualquier palabra o concepto anterior y viceversa.

(vi) La palabra «escrito» incluirá cualquier comunicación, escrito, contrato, registro electrónico, firma electrónica, facsímil u otro instrumento legalmente válido y exigible documentado independientemente de su formato.

(vii) Una referencia a un documento (incluyendo, sin límite, una referencia a este Código) se aplica al documento según sea modificado, variado, complementado o sustituido, salvo en la medida en que lo prohíba este Código o el documento al que se hace referencia.

(viii) Una referencia a la ley incluye cualquier requisito normativo, recomendación sectorial y mejores prácticas emitidas por las autoridades supervisoras nacionales e internacionales pertinentes u otros organismos.

ANEXO 1: Definiciones de las NCV

Actividades de apoyo al Cliente	ACTIVIDADES DE APOYO AL CLIENTE hace referencia a las actividades de Tratamiento llevadas a cabo por ADP para promover la entrega de sus productos y servicios. Las actividades de apoyo al Cliente pueden incluir, por ejemplo, formación de Profesionales, responder a preguntas sobre los servicios, abrir y solucionar solicitudes de asistencia, proporcionar información sobre productos y servicios (incluyendo actualizaciones y avisos de cumplimiento), control de calidad y supervisión, y actividades relacionadas que facilitan el uso eficiente de los productos y servicios de ADP.
ADP (Grupo ADP)	ADP (el GRUPO ADP) hace referencia, de manera colectiva, a Automatic Data Processing, Inc. (la empresa matriz) y las Empresas del Grupo, entre las que cabe mencionar ADP, Inc.
Archivo	ARCHIVO hace referencia a la recogida de Datos personales que ya no son necesarios para alcanzar los objetivos iniciales que llevaron a la recogida de dichos datos, o que ya no se usan para las actividades generales del negocio pero que pueden ser potencialmente útiles con fines meramente históricos, científicos o estadísticos, en la resolución de conflictos, para investigaciones o que cumplen una finalidad registral general. El acceso a un Archivo está limitado a los administradores del sistema y a otras personas cuyos trabajos requieren específicamente el acceso al archivo.
Asociado	ASOCIADO hace referencia a un Solicitante, a un empleado actual de ADP o a un antiguo empleado de ADP, con la excepción de Personas pluriempleadas. NOTA: por lo tanto, el Código de privacidad para el lugar de trabajo de ADP no se aplica al Tratamiento de Datos personales de Personas pluriempleadas.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. es la empresa matriz del Grupo ADP, y es una sociedad mercantil de Delaware (EE. UU.) con sede central en One ADP Boulevard, Roseland, New Jersey, 07068-1728 (EE. UU.).
Autoridad de protección de datos o DPA	AUTORIDAD DE PROTECCIÓN DE DATOS O DPA (por sus siglas en inglés) hace referencia a cualquier autoridad reguladora o de control que supervisa la protección y privacidad de los datos en el país en el que está establecida una Empresa del Grupo.
Categorías especiales de datos	CATEGORÍAS ESPECIALES DE DATOS hace referencia a Datos personales que revelan el origen étnico o racial de una persona, las preferencias políticas o afiliación a partidos políticos u organizaciones similares, las creencias religiosas o filosóficas, la pertenencia a

	organizaciones profesionales, comerciales o sindicales, el estado de salud física o mental, incluida cualquier opinión al respecto, discapacidades, código genético, adicciones, hábitos sexuales, delitos, antecedentes penales o procedimientos correspondientes a cualquier delito o comportamiento ilegal.
Cliente	CLIENTE hace referencia a cualquier Tercero que utilice uno o varios productos o servicios de ADP en el desarrollo de su propio negocio.
Código	CÓDIGO hace referencia (según corresponda) al Código de privacidad de ADP para datos empresariales, el Código de privacidad interno para el lugar de trabajo de ADP y el Código de privacidad para los servicios de tratamiento de datos de Clientes de ADP, denominados colectivamente como los Códigos.
Comité ejecutivo de ADP	COMITÉ EJECUTIVO DE ADP hace referencia al comité de directivos compuesto por (i) el director general de Automatic Data Processing, Inc. y (ii) aquellos directivos que rinden cuentas directamente al director general y que, de manera colectiva, son responsables de las operaciones del Grupo ADP.
Consejo directivo de privacidad	CONSEJO DIRECTIVO DE PRIVACIDAD hace referencia al consejo dirigido por el Director internacional de privacidad y compuesto por Representantes de privacidad, miembros de la Red de privacidad seleccionados por el Director internacional de privacidad y otras personas que pueden ser necesarias para ayudar a alcanzar el objetivo del Consejo.
Consumidor	CONSUMIDOR hace referencia a una Persona que interactúa directamente con ADP a título personal. Por ejemplo, Consumidores incluye a Personas que participan en programas de desarrollo del talento o que usan productos y servicios de ADP para su uso personal (es decir, al margen de una relación comercial con ADP o un Cliente de ADP).
Contrato de servicios	CONTRATO DE SERVICIOS hace referencia a cualquier contrato, acuerdo o condiciones por los que ADP presta Servicios al Cliente a un Cliente.
Contrato de subencargo	CONTRATO DE SUBENCARGO hace referencia a un acuerdo escrito o electrónico entre ADP y un Tercero Subencargado del Tratamiento con arreglo al artículo 7.1 del Código de privacidad para los servicios de tratamiento de datos de Clientes.
Contrato de tratamiento	CONTRATO DE TRATAMIENTO hace referencia a cualquier contrato para el Tratamiento de Datos personales celebrado por ADP y un

	Tercero Encargado del Tratamiento.
Datos de contacto profesionales	DATOS DE CONTACTO PROFESIONALES hace referencia a cualquier dato que corresponda a un Profesional como los que normalmente constan en una tarjeta de visita o al pie de un mensaje de correo electrónico.
Datos del Cliente	DATOS DEL CLIENTE hace referencia a los Datos personales que pertenecen a los empleados de los Clientes (incluidos los empleados potenciales, los antiguos empleados y las personas dependientes de los empleados) tratados por ADP en relación con la prestación de Servicios a los Clientes.
Datos personales o Datos	DATOS PERSONALES O DATOS hace referencia a cualquier información relacionada con una Persona identificada o identificable. Datos personales también puede hacer referencia a información personal relativa a políticas y estándares que ponen en práctica los Códigos.
Decisión de adecuación	DECISIÓN DE ADECUACIÓN hace referencia a una determinación dictada por una autoridad en protección de datos, o cualquier otra entidad competente, afirmando que un país, una región o el receptor de una transferencia de datos está capacitado para mantener el nivel adecuado de protección de los Datos personales. Las entidades amparadas por una Decisión de adecuación incluyen receptores que se hallen en países en los que, en virtud de la Legislación vigente, se les considere capacitados para proporcionar el nivel adecuado de protección de datos así como aquellos receptores que estén vinculados a otro instrumento normativo (como por ejemplo un conjunto de Normas corporativas vinculantes) que haya sido aprobado por la autoridad pertinente en protección de datos o por otro organismo competente. Por lo que respecta a los Estados Unidos, las empresas que obtengan certificación dentro de cualquier marco de privacidad de EE. UU.-EEE o EE. UU.-Suiza estarán cubiertas por una Decisión de adecuación.
Departamento jurídico	DEPARTAMENTO JURÍDICO hace referencia al Departamento jurídico de Automatic Data Processing, Inc.
Director responsable	DIRECTOR RESPONSABLE hace referencia al Director general de una Empresa del Grupo, o al director de una unidad de negocio o área funcional, que tiene el control presupuestario principal de la Empresa del Grupo, la unidad de negocio o el área funcional.

Director internacional de privacidad	DIRECTOR INTERNACIONAL DE PRIVACIDAD hace referencia al Asociado al que pertenece dicho cargo en Automatic Data Processing, Inc.
DPA principal	DPA PRINCIPAL hace referencia a la Autoridad de protección de datos de los Países Bajos.
EEE	EEE o ESPACIO ECONÓMICO EUROPEO hace referencia a todos los Estados miembros de la Unión Europea, junto con Noruega, Islandia y Liechtenstein y, a los efectos de los Códigos, Suiza y Reino Unido tras su salida de la Unión Europea. Por decisión del Departamento jurídico y siendo publicado en www.adp.com puede incluir otros países sujetos a leyes de protección de datos y restricciones de transferencia de datos similares a las restricciones de trasferencia de datos del EEE.
Empleado del Cliente	EMPLEADO DEL CLIENTE hace referencia a cualquier Persona cuyos Datos personales son tratados por ADP, en calidad de Encargado de los datos, para un Cliente con arreglo a un Acuerdo de servicios. Para mayor claridad, EMPLEADO DEL CLIENTE hace referencia a todas las Personas cuyos Datos personales son tratados por ADP en el desarrollo de los Servicios al Cliente (sin importar la naturaleza legal de la relación entre dicha Persona y el Cliente). No incluye a los profesionales cuyos Datos personales son tratados por ADP en conexión con la relación directa de ADP con el Cliente. Por ejemplo, ADP puede tratar los Datos personales de un Profesional de recursos humanos para celebrar un contrato con el Cliente. Estos Datos están sujetos al Código de privacidad para datos empresariales. Sin embargo, cuando ADP proporciona servicios de Tratamiento de nóminas al Cliente (por ej. emite nóminas salariales o proporciona asistencia en el uso de un sistema de ADP), los datos de la Persona se tratarán como Datos del Cliente.
Empresa del Grupo	EMPRESA DEL GRUPO hace referencia a cualquier entidad jurídica que se encuentre asociada a Automatic Data Processing, Inc. o a ADP, Inc., si cualquiera de las dos empresas, Automatic Data Processing, Inc. o ADP, Inc., posee, de manera directa o indirecta, más del 50 % del capital social emitido, cuenta con un 50 % o más del derecho de voto en las reuniones generales de accionistas, tiene la autoridad de nombrar a la mayoría de los directores o controla de otro modo las actividades de dicha entidad jurídica.
Encargado de los datos	ENCARGADO DE LOS DATOS hace referencia a la entidad o persona física que trata los Datos personales en nombre del Responsable del tratamiento.

Encargado interno	ENCARGADO INTERNO hace referencia a cualquier Empresa del Grupo que trata Datos personales a favor de otra de las Empresas del Grupo en calidad de Responsable del tratamiento.
Entidad contratante de ADP	ENTIDAD CONTRATANTE DE ADP hace referencia a la Empresa del Grupo que ha celebrado un contrato requerido por los Códigos, tales como un Contrato de servicios, un Contrato de subencargo o un acuerdo de transmisión de datos.
Entidad delegada de ADP	ENTIDAD DELEGADA DE ADP hace referencia a ADP Nederland, B.V., con sede registrada en Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL (Países Bajos).
Entidad enajenada	ENTIDAD ENAJENADA hace referencia a una Empresa del Grupo que como resultado de la venta de sus participaciones o activos o su enajenación, ya no pertenece a ADP por lo que no reúne los requisitos para ser Empresa del Grupo.
Equipo internacional de privacidad y gestión de datos	EQUIPO INTERNACIONAL DE PRIVACIDAD Y GESTIÓN DE DATOS hace referencia a la Oficina de privacidad y gestión de datos de ADP. La Oficina de privacidad y gestión de datos está dirigida por el Director internacional de privacidad y está compuesta por directivos, directores de privacidad y otros miembros del personal subordinados al Director internacional de privacidad o a los directivos y directores de privacidad.
Evaluación del impacto de la protección de datos (DPIA)	EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS (DPIA, por sus siglas en inglés) hará referencia a un procedimiento para llevar a cabo y documentar una valoración previa del impacto que puede tener un determinado Tratamiento en la protección de los Datos personales, en caso de que dicho Tratamiento sea susceptible de incurrir en altos riesgos de quebrantamiento de los derechos y libertades de las Personas, especialmente en los casos en los que se usen nuevas tecnologías. Una DPIA debe contener lo siguiente.

	(i) Una descripción de: (a) El alcance y el contexto del Tratamiento. (b) La Finalidad del negocio para la que se tratan los Datos personales. (c) Los fines específicos para los que se tratan las Categorías especiales de datos. (d) Categorías de Receptores de datos personales, incluidos aquellos receptores que no estén amparados bajo una Decisión de adecuación. (e) Plazos de tiempo del almacenamiento de los Datos personales. (ii) Una evaluación de: (a) La necesidad y proporcionalidad del Tratamiento. (b) Los riesgos para los derechos de privacidad de las Personas. Las medidas para mitigar esos riesgos, incluyendo garantías, medidas de seguridad y otros mecanismos (tales como privacidad por diseño) para garantizar la protección de los Datos personales.
Fecha de entrada en vigor	FECHA DE ENTRADA EN VIGOR hace referencia a la fecha en la que los Códigos entran en vigor tal y como se especifica en el artículo 1 de los Códigos.
Finalidad del negocio	FINALIDAD DEL NEGOCIO hace referencia a un objetivo legítimo para el Tratamiento de datos personales tal y como se especifica en los artículos 2, 3 o 4 de los Códigos de ADP, o para el Tratamiento de Categorías especiales de datos según lo especificado en el artículo 4 de los Códigos de ADP.
Infracción de la seguridad de los datos	INFRACCIÓN DE LA SEGURIDAD DE LOS DATOS hace referencia a cualquier incidente que repercuta en la confidencialidad, integridad o disponibilidad de los Datos personales, tales como el uso o la comunicación no autorizados de los Datos personales o el acceso no autorizado a los mismos, poniendo en peligro la privacidad o seguridad de dichos datos.
Interés primordial	INTERÉS PRIMORDIAL hace referencia a los intereses imperativos descritos en el artículo 13.1 del Código de privacidad para el lugar de trabajo de ADP y el Código de privacidad de ADP para datos empresariales, por los que las obligaciones de ADP o los derechos de las Personas, estipulados en los artículos 13.2 y 13.3 de los Códigos, pueden verse invalidados, en ciertas circunstancias particulares, si

	estos intereses imperativos prevalecen sobre los intereses de la Persona.
Legislación vigente	LEGISLACIÓN VIGENTE hace referencia a todas las leyes de privacidad y protección de datos que sean aplicables a cualquier actividad de tratamiento particular.
Legislación vigente con respecto al Encargado de los Datos	A efectos del Código de privacidad para los servicios de tratamiento de datos de Clientes, LEGISLACIÓN VIGENTE CON RESPECTO AL ENCARGADO DE LOS DATOS hace referencia a cualquier ley de privacidad o protección de datos que se aplique a ADP como Encargado de los datos en nombre de un Cliente que sea Responsable del tratamiento.
Legislación vigente con respecto al Responsable del Tratamiento	A efectos del Código de privacidad para los servicios de tratamiento de datos de Clientes, LEGISLACIÓN VIGENTE CON RESPECTO AL RESPONSABLE DEL TRATAMIENTO hace referencia a cualquier ley de privacidad o protección de datos que se aplique a un Cliente de ADP como Responsable del tratamiento de dichos Datos del Cliente.
Legislación vigente para el EEE	LEGISLACIÓN VIGENTE PARA EL EEE hace referencia a los requisitos, en virtud de la legislación vigente del EEE, que sean aplicables a los Datos personales recogidos inicialmente en el contexto de las actividades de una de las Empresas del Grupo establecidas en el EEE (también si estos son posteriormente transferidos a otra Empresa del Grupo establecida fuera del EEE).
Niños	A los efectos de recogida de datos y marketing de ADP, NIÑOS hace referencia a Personas con una edad menor a la establecida legalmente, por la legislación vigente, para poder otorgar el consentimiento para la recogida de dichos datos o el marketing.
Normas corporativas vinculantes	NORMAS CORPORATIVAS VINCULANTES hace referencia a la política de privacidad de un Grupo de empresas relacionadas de las que se espera un nivel adecuado de protección, en virtud de la Legislación vigente, para la transferencia de Datos personales entre las empresas de dicho Grupo.
Objetivo secundario	OBJETIVO SECUNDARIO hace referencia a cualquier objetivo, distinto al objetivo inicial, por el que se lleva a cabo un mayor tratamiento de los Datos personales.
Persona	PERSONA hace referencia a cualquier persona física identificada o identificable cuyos Datos personales son tratados por ADP, en calidad de Encargado de los datos o Responsable del tratamiento, exceptuando a Personas pluriempleadas. NOTA: por lo tanto, el

	Código de privacidad de ADP para datos empresariales y el Código de privacidad para el lugar de trabajo de ADP no se aplican al Tratamiento de los Datos personales de Personas pluriempleadas.
Persona dependiente	PERSONA DEPENDIENTE hace referencia al cónyuge, pareja, hijo o beneficiario de un Asociado, o a la persona de contacto para emergencias de un Asociado o Trabajador eventual.
Persona pluriempleada	PERSONA PLURIEMPLEADA hace referencia a un empleado de un Cliente de EE. UU. que está pluriempleado por una empresa subsidiaria indirecta de EE. UU. de Automatic Data Processing, Inc. como parte de la oferta de servicio de organización profesional de empleo en EE. UU.
Personal	PERSONAL hace referencia, de manera colectiva, a los Asociados actuales de ADP y los Trabajadores eventuales que trabajan para ADP en el presente.
Profesional	PROFESIONAL hace referencia a cualquier persona (con excepción de los empleados) que interactúa directamente con ADP en calidad de profesional o de negocio. Por ejemplo, Profesionales incluye al personal de recursos humanos del Cliente que se pone en contacto con ADP como usuarios de los productos o servicios de ADP. Profesionales también incluye a Clientes, Proveedores y representantes de cuentas de los Socios comerciales, contactos comerciales, contactos de asociaciones profesionales, reguladores, contactos de prensa y otras personas que interactúen con ADP en calidad comercial.
Proveedor	PROVEEDOR hace referencia a Terceros que proporcionan bienes o servicios a ADP (por ej. un proveedor de servicios, agente, Encargado de los datos, asesor o distribuidor).
Red de privacidad	RED DE PRIVACIDAD hace referencia a los miembros del Equipo internacional de privacidad y gestión de datos y otros miembros del departamento jurídico, incluyendo profesionales de cumplimiento y responsables de la protección de datos, encargados del cumplimiento en materia de privacidad en sus respectivas regiones, países, unidades de negocio o áreas funcionales.
Representante de privacidad	REPRESENTANTE DE PRIVACIDAD hace referencia a un ejecutivo de ADP que ha sido nombrado por un Director responsable o la Dirección ejecutiva de ADP para implementar y hacer cumplir los Códigos de privacidad en una Unidad de negocio de ADP.
Requisitos	REQUISITOS OBLIGATORIOS hará referencia a todas las

obligatorios	obligaciones que, en virtud de la Legislación vigente con respecto al Encargado de los datos, requieran el Tratamiento de Datos personales de (i) seguridad o defensa nacional, (ii) seguridad pública, (iii) prevención, investigación, detección o enjuiciamiento de delitos o infracciones éticas en profesiones con normativa regulativa, o (iv) la protección de cualquier Persona, o de sus derechos y libertades individuales.
Responsable del tratamiento	RESPONSABLE DEL TRATAMIENTO hace referencia a la entidad o persona física que, por sí misma, o en colaboración con otros, determina los objetivos y medios para el Tratamiento de los Datos personales.
Restricciones sobre la transferencia de datos en el EEE	RESTRICCIONES SOBRE LA TRANSFERENCIA DE DATOS EN EL EEE hace referencia a todas las restricciones en torno a las transferencias internacionales de Datos personales en virtud de las leyes de protección de datos de un país perteneciente al EEE.
Servicios al Cliente	SERVICIOS AL CLIENTE hace referencia a los servicios de gestión del capital humano proporcionados por ADP a los Clientes, tales como contratación, servicios de nómina y remuneración, prestaciones para empleados, gestión del talento, administración de recursos humanos, consultoría y análisis, y servicios de jubilación.
Socio comercial	SOCIO COMERCIAL hace referencia a todos los Terceros, con excepción de un Cliente o Proveedor que tenga, o haya tenido, una relación comercial o una alianza estratégica con ADP (por ej. un socio de comercialización conjunta, una empresa conjunta o un socio de desarrollo conjunto).
Solicitante	SOLICITANTE hace referencia a cualquier Persona que proporciona Datos personales a ADP en el contexto de una solicitud para un puesto en ADP como Asociado.
Subencargado de ADP	A efectos del Código de privacidad para los servicios de tratamiento de datos de Clientes, SUBENCARGADO DE ADP hace referencia a cualquier Empresa del Grupo contratada por otra Empresa del Grupo como Subencargada para datos de Clientes.
Subencargados	SUBENCARGADOS hace referencia, de manera colectiva, a los Subencargados de ADP y a los Terceros Subencargados del Tratamiento.
Tercero	Tercero hace referencia a cualquier persona, organización privada u organismo gubernamental que no sea una Empresa del Grupo.

Tercero Encargado del Tratamiento	TERCERO ENCARGADO DEL TRATAMIENTO hace referencia a un tercero que trata Datos personales en nombre de ADP, pero que no está bajo la autoridad directa de ADP.
Tercero Responsable	TERCERO RESPONSABLE hace referencia a un tercero que trata Datos personales y establece los objetivos y los medios del Tratamiento.
Tercero Subencargado del Tratamiento	TERCERTO SUBENCARGADO DEL TRATAMIENTO hace referencia a cualquier tercero que ADP contrate como Subencargado.
Trabajador eventual	TRABAJADOR EVENTUAL hace referencia a una Persona que presta servicios a ADP (y que está sujeta a la supervisión directa de ADP) de manera provisional o no permanente, tales como los trabajadores temporales, trabajadores contratados, contratistas independientes o asesores.
Tratamiento	TRATAMIENTO hace referencia a cualquier operación llevada a cabo con Datos personales, sea esta por medios manuales o automáticos, tales como la recogida, grabación, almacenamiento, organización, alteración, uso, comunicación (incluido el permiso de acceso remoto), transmisión o eliminación de Datos personales.

ANEXO 2: Medidas de seguridad

Presentado por:	ADP - Organización Global de Seguridad
Versión:	2.0
Publicado:	Septiembre 2019

Contenido

Sección 1 - Políticas de Seguridad de la Información 38

Sección 2 - Organización de la Seguridad de la Información 40

Sección 3 - Seguridad de Recursos Humanos 41

Sección 4 - Gestión de Activos 42

Sección 5 - Control de Accesos 43

Sección 6 - Criptografía 44

Sección 7 - Seguridad Física y Ambiental 45

Sección 8 - Operaciones de Seguridad 46

Sección 9 - Seguridad de las Comunicaciones 48

Sección 10 - Mantenimiento, Desarrollo y Adquisición de Sistemas 49

Sección 11 - Relaciones con proveedores 50

Sección 12 - Gestión de Incidentes de Seguridad de la Información 51

Sección 13 - Aspectos de la Seguridad de la Información de la Gestión de Resiliencia del Negocio. 52

Sección 14 - Conformidad 53

Términos y definiciones

Los siguientes términos pueden aparecer a lo largo del documento:

Término o Acrónimo usado	Definición
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Visión General

ADP mantiene un programa formal de seguridad de la información que contiene salvaguardas físicas, técnicas y administrativas para proteger la seguridad, confidencialidad e integridad de la información del cliente. Este programa está diseñado para (i) la salvaguarda de la seguridad y la confidencialidad de la información del cliente, (ii) proteger contra amenazas o daños la seguridad o integridad de la información, y (iii) proteger contra el acceso no autorizado y/o uso de la información.

Este documento contiene una visión general de las medidas y las prácticas de seguridad de ADP a la fecha de creación, y que se encuentran sujetas a cambios. Estos requerimientos y prácticas están diseñados para ser consistentes con los estándares de seguridad de la información ISO/IEC 27001:2013. ADP evalúa periódicamente sus políticas y estándares de seguridad. Nuestro objetivo es ayudar a asegurar que el programa de seguridad opere efectiva y eficientemente para proteger toda la información confiada a nosotros por parte de nuestros clientes y nuestros empleados.

Sección 1 - Políticas de Seguridad de la Información

Independencia de la función de Seguridad de la Información

El Chief Security Officer de ADP supervisa la Organización Global de Seguridad - Global Security Organization (GSO) de ADP, y reporta al General Counsel (Legal y Cumplimiento Normativo), en lugar de al Chief Information Officer, lo que proporciona a GSO una necesaria independencia de las tecnologías de la información (IT). GSO es un equipo de seguridad especializado que cuenta con una perspectiva multidisciplinar en seguridad y ciberseguridad de la información, conformidad, gestión del riesgo operacional, gestión de la seguridad del cliente, protección del personal, y resiliencia del negocio. La Dirección Senior de GSO, bajo nuestro Chief Security Officer, es responsable de gestionar las políticas, procedimientos y pautas principales de seguridad.

Definición formal de una política de seguridad de la Información

ADP ha desarrollado y documentado unas políticas formales de Seguridad de la Información que definen la perspectiva de ADP respecto a la seguridad de la información. Las áreas específicas cubiertas por estas políticas incluyen, entre otras, las siguientes:

- **Política de Gestión de la Seguridad –** Define la responsabilidad de la GSO y del Chief Security Officer (CSO), incluyendo las responsabilidades y controles de seguridad de la información durante el proceso de contratación, desde una perspectiva de seguridad.
- **Política Global de Privacidad –** Detalla la recolección de Información Personal, su acceso, exactitud, publicación y declaraciones de privacidad a los clientes.
- **Uso aceptable de comunicaciones electrónicas para empleados y Política de Protección de Datos** – Describe el uso aceptable, y las diferentes opciones de comunicaciones electrónicas, cifrado y gestión de llaves.
- **Política de Gestión de Información–** Proporciona los requerimientos para la clasificación de la información de ADP y establece controles de protección.
- **Política de Seguridad Física –** Define los requerimientos de seguridad de acceso a las instalaciones de ADP, y consecuentemente de los empleados y visitantes que trabajan en esas instalaciones.
- **Política de Gestión de las Operaciones de Seguridad –** Proporciona los controles mínimos para mantener los parches de sistemas, hacer frente de forma efectiva a las amenazas del malware y mantener copias y controles de seguridad de bases de datos.
- **Política de Supervisión de Seguridad –** Proporciona los controles para los Sistemas de Detección de Intrusión (IDS), logs, y Prevención de Pérdidas de Datos (DLP).
- **Política de Investigación y Gestión de Incidentes –** Define los estándares para la respuesta de incidentes, investigación electrónica, protección del empleado, y acceso a la información almacenada de los empleados.
- **Política de Acceso y Autenticación –** Define los requerimientos para la autenticación (por ejemplo usuarios y contraseñas), acceso remoto y accesos inalámbricos.
- **Política de Seguridad de Redes –** Arquitectura de seguridad de routers, firewalls, AD, DNS, servidores de mail, DMZ, servicios cloud, dispositivos de redes, web proxy y switched network technology.
- **Política de Riesgo Global de Terceros y Fusiones y Adquisiciones –** Define los controles mínimos de seguridad para contratar a cualquier tercero para asistir a ADP a lograr sus objetivos de negocio.
- **Política de Gestión de Aplicaciones –** Establece controles de seguridad apropiados en cada etapa del ciclo de vida de desarrollo de sistemas.
- **Política de Resiliencia de Negocio –** Rige sobre la protección, integridad y preservación de ADP estableciendo los requerimientos mínimos para documentar, implementar, mantener y mejorar continuamente el Programa de Resiliencia de Negocio.
- **Política de Gestión de Riesgos de Seguridad –** Identificación, supervisión, respuesta, análisis, supervisión y nuevas iniciativas de negocio.

Las políticas están publicadas en la Intranet de ADP y son accesibles a todos los empleados y contratados, desde dentro de la red de ADP.

Revisión de la Política de Seguridad de la Información

ADP realiza una revisión de su política de seguridad al menos una vez al año o bien cuando existan cambios relevantes que impacten al funcionamiento de los sistemas de ADP.

Sección 2 - Organización de la Seguridad de la Información

Roles y responsabilidades de la Seguridad de la Información

La GSO consiste en una serie de equipos de seguridad con una perspectiva multidisciplinar para estar en conformidad con los estándares de Seguridad de la Información y de Ciberseguridad, gestión del riesgo operacional, gestión de la seguridad del cliente, protección del empleado y resiliencia de negocio. Los roles y responsabilidades han sido formalmente definidos para todos los miembros de la GSO. La GSO es la encargada de diseñar, implementar y supervisar nuestro programa de seguridad de la información basándose en las políticas corporativas. Las actividades de la GSO son supervisadas por el Executive Security Committee, cuyos miembros incluyen al Chief Security Officer de ADP, así como a su Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer, y General Counsel.

Dispositivos móviles y Política de teletrabajo

ADP requiere que toda la información en dispositivos móviles se encuentre encriptada, para prevenir la fuga de datos como resultado de un robo o pérdida de un ordenador/dispositivo. Se requiere “Advanced end-point protection” y autenticación de dos factores sobre VPN para acceder a las redes corporativas de forma remota. Todos los dispositivos remotos deben encontrarse protegidos con contraseña. Los empleados de ADP están obligados a informar de pérdidas o robos de dispositivos de forma inmediata a través de un Proceso de Reporte de Incidentes de Seguridad.

Todos los empleados y contratados, como condición de trabajo con ADP, deben cumplir con las Políticas de Uso Aceptable de las Comunicaciones Electrónicas y Protección de Datos, como también con otras políticas relevantes.

Sección 3 - Seguridad de Recursos Humanos

Verificación de antecedentes

De forma consistente con los requerimientos legales aplicables a la jurisdicción de cada individuo, ADP realiza la verificación de antecedentes apropiada acorde a los deberes y responsabilidades de sus empleados, contratados y terceros. Estas verificaciones confirman la idoneidad del candidato para gestionar la información del cliente antes de hacer efectiva la contratación de los mismos.

La verificación de antecedentes puede incluir los siguientes componentes:

- Identidad/ Verificación de elegibilidad para el empleo
- Antecedentes laborales
- Historial académico y calificaciones profesionales
- Registros criminales (en lugares donde se encuentre legalmente autorizado y dependiendo de regulaciones locales).

Acuerdos de confidencialidad con empleados y contratados.

Los contratos de empleados y los contratos con contratistas contienen términos que indican las obligaciones y responsabilidades relacionadas con la información de los clientes a la cual tienen acceso. Todos los empleados de ADP y sus contratistas se encuentran ligados a obligaciones de confidencialidad.

Programa de Formación en Seguridad de la Información

Todos los empleados deben completar la formación en Seguridad de la Información como parte del proceso de entrada a la compañía. Además, ADP realiza una formación anual en Seguridad para recordar a los empleados de sus responsabilidades cuando se encuentran realizando sus tareas diarias.

Responsabilidades de los empleados y procesos disciplinarios

ADP ha publicado una política de seguridad que todos los empleados deben cumplir. Las violaciones a dichas políticas de seguridad pueden conducir a la revocación de privilegios de acceso y/o acciones disciplinarias que pueden derivar en la terminación de contratos de consultoría o empleo.

Terminación de las responsabilidades de empleo.

Las responsabilidades a la hora de la terminación de la relación de empleo han sido formalmente documentadas e incluyen, como mínimo:

- Retorno de toda la información y activos en posesión del empleado respectivo, cualquiera sea el medio donde se encuentre.
- Terminación de los derechos de acceso a las instalaciones de ADP, a su información y a sus sistemas.
- Cambio de contraseñas para cualquier cuenta compartida, si aplicase.
- Transferencia de conocimiento, si aplicase

Sección 4 - Gestión de Activos

Uso Aceptable de Activos

El Uso aceptable de activos se encuentra explicado en varias políticas aplicables a empleados de ADP y contratistas para ayudar a asegurar que la información de ADP, y de sus clientes no sea expuesta por el uso de dichos activos. Los ejemplos de las areas descritas en esas políticas son: uso de comunicaciones electrónicas, uso de equipos electrónicos y uso de activos de información.

Clasificación de la Información

La información adquirida, creada o mantenida por o en representación de ADP es asignada, según su aplicabilidad, a la siguiente clasificación de seguridad:

- Pública - Ejemplo: Folletos de Marketing, Reportes publicados anualmente
- Sólo Uso Interno de ADP: Ejemplo: Comunicaciones entre oficinas, procedimientos de operaciones.
- ADP Confidencial- Ejemplo: Información Personal y Personal Sensible.
- ADP Restringida- Ejemplo: Reportes financieros, Información estratégica.

Los requerimientos para la gestión de información se encuentran correlacionados directamente con la Clasificación de la Seguridad de la Información. Toda la información de nuestros clientes es clasificada como Confidencial.

Los empleados de ADP son responsables de gestionar y proteger los activos de información de acuerdo a su clasificación de nivel de seguridad, el cual proporciona protección de información y requerimientos aplicables de gestión para cada nivel de clasificación. La clasificación de confidencialidad de ADP se aplica a toda la información almacenada, transmitida o gestionada por terceros.

Eliminación de equipos y medios.

Cuando los equipos, documentos, archivos y medios de comunicación de ADP son eliminados o reusados, se toman las medidas apropiadas para prevenir la posterior recuperación de la información del cliente originalmente almacenada en ellos. Toda la información en ordenadores u otros dispositivos de almacenamiento electrónico, independientemente de su clasificación, es eliminada de forma segura, a menos que el dispositivo sea destruido, antes de abandonar las instalaciones de ADP o ser reusado. Los procedimientos para una destrucción segura/borrado de información de ADP almacenada en equipos, documentos, archivos y otros dispositivos se encuentra formalmente documentada.

Dispositivos físicos en tránsito

Distintas salvaguardas han sido implementadas para proteger los materiales impresos conteniendo la información del cliente contra los robos, pérdidas o accesos no autorizados/modificación (i) durante el tránsito, por ejemplo, en sobres cerrados, contenedores y entrega en mano a un usuario autorizado; y (ii) durante la revisión u otro proceso donde la información sea eliminada de su almacenamiento seguro.

Sección 5 - Control de Accesos

Requerimientos de Negocio para Control de Acceso

La Política de Control de Acceso de ADP está basada en requerimientos definidos por el negocio. Las políticas y estándares de control están articulados dentro de controles de acceso que se encuentran en todos los componentes de los servicios proporcionados y están basados en los principios de “menor privilegio” y “necesidad de conocer”.

Acceso a la Infraestructura – Gestión de Control de Acceso

Las demandas de Acceso para mover, agregar, crear y borrar son registrados, aprobados y revisados periódicamente.

Una revisión formal es realizada, como mínimo anualmente, para confirmar que los usuarios individuales corresponden con precisión a los roles importantes del negocio y que no continúen teniendo acceso después de un cambio de posición. Este proceso es auditado y documentado en un informe SOC1 Tipo II. Desde dentro de un sistema de gestión de identidades, un equipo dedicado de ADP es responsable de garantizar, denegar, cancelar, terminar y decomisar/desactivar los accesos a las instalaciones de ADP y sus sistemas de información. ADP usa una herramienta centralizada de Gestión de Accesos e identidades (IAM), la cual es gestionada de forma centralizada por un equipo dedicado de GETS. De acuerdo a los derechos de acceso solicitados a través de la herramienta centralizada de IAM, se inicia un flujo de validación y puede incluir al supervisor del usuario. El acceso se proporciona de forma provisional y existe un flujo de trabajo para prevenir que dicho acceso sea permanente. El acceso a las instalaciones por parte de los empleados se elimina inmediatamente después de su último día de trabajo, desactivando su tarjeta de acceso. Las cuentas del empleado se desactivan inmediatamente. Todos los activos del empleado son devueltos y chequeados por el Manager correspondiente y se comparan con la lista de activos de la base de datos de información de gestión de configuraciones. Después de un cambio de puesto de trabajo, o de cambios en la organización, los perfiles de usuarios o los derechos de acceso de los usuarios deben ser modificados por la Dirección de la Unidad de Negocio correspondientes y por el equipo de IAM. Adicionalmente, una revisión formal de derechos de acceso se realiza cada año para verificar que los derechos de acceso individuales corresponden con el rol de negocio y que no han quedado derechos de acceso irrelevantes posteriores al cambio de posición.

Política de Contraseñas

Las políticas de contraseñas de los empleados de ADP se encuentran en servidores, bases de datos y dispositivos de redes y aplicaciones, hasta el punto donde el dispositivo/aplicación lo permita. La complejidad de la contraseña deriva del análisis de riesgo de la información protegida y del contenido. Las políticas cumplen con estándares de la industria para fuerza y complejidad, incluyendo el uso de step-up, dos factores, autenticación biométrica donde sea apropiado.

Los requerimientos de autenticación de la aplicación cliente pueden variar de acuerdo al producto, y la federación de servicios (SAML 2.0) se encuentran disponibles en algunas aplicaciones específicas utilizando una red unificada y una capa de seguridad gestionada por GETS.

Session Timeouts

ADP refuerza los timeouts automáticos en todos los servidores, estaciones de trabajo, aplicaciones y conexiones de VPN basándose en un propuesta orientada al riesgo y consistente con los estándares de la industria. El restablecimiento de las sesiones solo puede tener lugar una vez que se haya provisto una contraseña válida.

Sección 6 - Criptografía

Controles criptográficos

ADP requiere que todos los intercambios de información sensible entre ADP y Terceros se realice de forma encriptada (o bien el canal de transporte debe estar encriptado) utilizando técnicas de encriptación aceptadas por la industria. Alternativamente, se puede utilizar una línea privada.

Gestión de llaves

ADP tiene un estándar de Seguridad de Encriptación que incluye un procedimiento de gestión y fideicomiso de llaves bien definido, que incluye tanto las formas simétricas como asimétricas de gestión de llaves. Las llaves de encriptación utilizadas son están siempre clasificadas como información confidencial. El acceso a dichas llaves se encuentra limitado estrictamente a aquellos que tienen la necesidad de conocerlas, o bien si se aprueba una excepción. Las llaves de encriptación y la gestión del ciclo de vida de las llaves siguen prácticas incluidas en los estándares de la industria.

Sección 7 - Seguridad Física y Ambiental

La propuesta de ADP a la seguridad física tiene dos objetivos – crear un entorno seguro de trabajo para los empleados de ADP y proteger la información personal almacenada en los Datacenters de ADP y en otras instalaciones estratégicas de ADP.

La política de Seguridad de ADP requiere que la Dirección de ADP identifique aquellas áreas donde se requiera un nivel especial de seguridad. El acceso a dichas áreas se proporciona sólamente a empleados autorizados y con fines específicos. Las áreas seguras de ADP emplean distintas herramientas de seguridad física, incluyendo el uso de videovigilancia, tarjetas de acceso de seguridad (acceso controlado por identidad) y guardias de seguridad ubicados en las entradas y salidas. Los visitantes pueden ser provistos de acceso cuando estén autorizados y son supervisados durante toda su estancia.

Sección 8 - Operaciones de Seguridad

Procedimientos de formalización de Operaciones de IT

GETS es la unidad de ADP responsable de la infraestructura de IT y de su mantenimiento. GETS mantiene formalmente y documenta las políticas y procedimientos de Operaciones de IT. Estos procedimientos incluyen, aunque no están limitados, a los siguiente:

- Gestión del Cambio
- Gestión de Back-up
- Gestión de errores de sistemas
- Reinicio y recuperación de sistemas
- Supervisión de Sistemas
- Establecimiento de tareas y supervisión.

Gestión del cambio en la Infraestructura

Un Change Advisory Board (CAB) periódico, incluyendo a representantes de una amplia variedad de equipos de ADP, es mantenido por GETS. Las reuniones de CAB discuten el impacto de las ventanas de desarrollo y promociones a entornos de producción, y también coordinar cualquier otro cambio en la infraestructura.

Plan de Capacidad de Sistema y Aceptación

Los requerimientos de capacidad son supervisados continuamente y revisados regularmente. Siguiendo con estas revisiones, los sistemas y redes son posteriormente escalados hacia arriba o hacia abajo. Cuando se realizan cambios significativos debido a un cambio en la capacidad o a una evolución tecnológica, el equipo de benchmarking de GETS puede realizar “pruebas de estrés” a los sistemas y aplicaciones relevantes. Al final de las mencionadas pruebas, el equipo proporciona un informe detallado de la evolución del rendimiento midiendo los cambios en (i) componentes, (ii) configuración y versiones de sistemas, y/o (iii) configuración y versión de middleware.

Protección contra códigos maliciosos

Tecnologías de protección de Endpoint están instaladas para proteger los activos de ADP de acuerdo a las mejores prácticas de la industria.

Política de Gestión de Back-Up

ADP cuenta con políticas que requieren que todas las operaciones de hosting realicen back-up de los datos de producción. El alcance y la frecuencia con que son ejecutados los back-ups está implementado de acuerdo a los requerimientos de negocio de los servicios relevantes de ADP, los requerimientos de seguridad de la información involucrada, y la criticidad de la información con respecto a su recuperación por desastre. La supervisión de la programación de los back-ups es realizada por GETS con el objetivo de detectar problemas y/o excepciones.

Seguridad de Logging y Supervisión

ADP ha implementado una infraestructura central de solo-lectura de logging (SIEM), y un Sistema de correlación y alerta de logs (TPSI). Las alertas son supervisadas y evaluadas en tiempo y forma por el CIRC.

Todos estos sistemas se encuentran sincronizados utilizando un Protocolo de Tiempo de Red NTP que se basa en referencias de reloj.

Cada log individual contiene, como mínimo:

- Marca de tiempo
- Quien (identidad del operador o administrador)
- Qué (Información sobre el evento)

Los pistas de auditoria y logging de Sistema para las aplicaciones de ADP están diseñados y configurados para rastrear la siguiente información:

- Acceso autorizado
- Operaciones Privilegiadas
- Intentos de acceso no autorizados
- Sistemas de alertas y errores
- Cambios en las configuraciones de seguridad de los sistemas, cuando los sistemas permiten esos logging.

Estos logs se encuentran disponibles solo para personal autorizado de ADP, y son enviados en tiempo real para prevenir que la información sea adulterada antes de ser almacenada en Dispositivos de registro seguro.

Sistemas de Infraestructura y Supervisión

ADP implementa las medidas apropiadas para proporcionar una supervisión de la infraestructura durante las 24 horas del día, 7 días a la semana. Las alertas de disrupción son gestionadas por distintos equipos de acuerdo a su nivel de criticidad y a las habilidades requeridas para resolverlas.

Las instalaciones de hosting de ADP utilizan aplicaciones de supervisión que se encuentran activadas de forma constante en todos los sistemas de procesamiento y en los componentes de red para proporcionar al personal de ADP una notificación proactiva de problemas y avisos en anticipación a posibles problemas.

Gestión de Vulnerabilidades Técnicas

Todos los equipos instalados en la infraestructura de hosting deben cumplir con la instalación de un sistema operativo protegido de seguridad (o proceso de compilación segura). Las operaciones emplean una configuración robusta, aprobada y estandarizada para cada tipo de servidor utilizado dentro de nuestra infraestructura. La implementación inmediata de los sistemas operativos está prohibida, ya que estas instalaciones pueden crear vulnerabilidades, como contraseñas genéricas de cuentas de sistema, que podrían presentar un riesgo de infraestructura. Estas configuraciones reducen la exposición de los equipos alojados que ejecutan servicios innecesarios que pueden provocar vulnerabilidades.

ADP cuenta con una metodología documentada para realizar evaluaciones periódicas de vulnerabilidad y revisiones de conformidad en las aplicaciones web y sus correspondientes componentes de infraestructura, que incluyen al menos a las 15 categorías primarias de pruebas. La metodología de evaluación está basada en mejores prácticas tanto internas como externas, incluyendo pero no limitándose, a Open Web Application Security Project (OWASP), SANS Institute and Web Application Security Consortium (WASC).

Sección 9 - Seguridad de las Comunicaciones

Gestión de la Seguridad de la Red

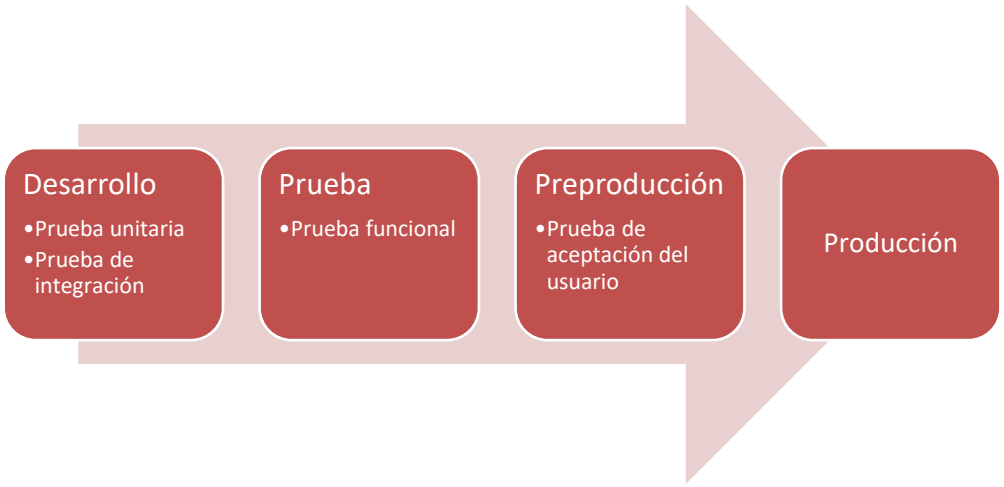
ADP emplea un Sistema de detección de intrusión basado en redes que supervisan el tráfico de la red a nivel de infraestructura (24 horas por día, 7 días a la semana) e identifica la actividad sospechosa y potenciales ataques.

Intercambio de Información

ADP implementa controles apropiados para que la información de ADP que es enviada a Terceros sea transferida entre sistemas de información y recursos autorizados y que sea solamente intercambiada a través de mecanismos seguros de transferencia de ADP.

Seguridad en Desarrollo y Procesos de Soporte

Durante el ciclo de desarrollo, se genera la documentación aplicable, y se crean planes de evaluación para la fase de prueba. Las diferentes etapas se definen para cada entorno con la aprobación correspondiente en cada fase.



- Para migrar del entorno de Pruebas a Pre-Producción, se requiere aprobación del equipo de calidad de ADP.
- Para migrar del entorno de Pre-Producción a Producción, se requiere la aprobación del equipo de Operaciones IT.

Los equipos de Desarrollo tienen que utilizar métodos de codificación segura. Los cambios en las aplicaciones son probados en entornos de desarrollo y regresión antes de llegar a los sistemas de Producción. Las pruebas realizadas se documentan. Una vez aprobados, los cambios son implementados en Producción. Un test de Intrusión (Penetration testing) es realizado una vez se han producido cambios significativos.

Un CAB periódico, incluyendo a representantes de una amplia variedad de equipos de ADP, es mantenido por GETS. Las reuniones de CAB tienen lugar periódicamente, y su objetivo es discutir impactos, acordar ventanas de desarrollo y aprobar la implementación de paquetes de software al entorno de Producción, como también informar sobre cualquier otro cambio en la infraestructura de Producción.

El equipo de Operaciones IT de ADP proporciona la aprobación final antes de la implementación de paquetes de software a entornos de Producción.

Seguridad en entornos de Desarrollo

Los entornos de Desarrollo y Producción se encuentran separados e independientes el uno del otro. Para reforzar la correcta segregación de tareas, los controles de acceso se implementan apropiadamente.

Información de Prueba

Por la política de Gestión de Aplicaciones de ADP, el uso de información real o “un-sanitized” en desarrollo y pruebas no está permitida, a menos que sea explícitamente solicitado y aprobado por el cliente.

Sección 11 - Relaciones con proveedores

Identificación de riesgo relacionados con Terceros

Las evaluaciones de Terceros que requieren acceso a ADP y/o a información del cliente se realizan periódicamente para determinar su conformidad con los requerimientos de seguridad de ADP para Terceros, y para identificar cualquier “gap” en los controles aplicados. Si se identifica un “gap”, se acuerdan nuevos controles con esos Terceros.

Acuerdos de Seguridad de la Información con Terceros

ADP tiene acuerdos con aquellos Terceros que incluyen compromisos apropiados de seguridad de acuerdo a los requerimientos de seguridad de ADP.

Sección 12 - Gestión de Incidentes de Seguridad de la Información

Gestión de Incidentes de Seguridad de la Información y mejoras

ADP cuenta con una metodología documentada para responder a incidentes de seguridad en tiempo y forma, de modo efectivo.

En caso de ocurrir un incidente, un equipo predefinido de empleados de ADP activa un plan de respuesta de incidentes que trabaja sobre áreas como las siguientes:

- Escaladas basadas en la clasificación del incidente o la severidad del mismo.
- Lista de contactos para reporte de incidente/escaladas
- Pautas para respuestas iniciales y de seguimiento con los clientes involucrados.
- Conformidad con las leyes aplicables de notificación de brechas de seguridad
- Log de Investigación
- Recuperación de Sistemas
- Resolución de problemas, informe y revisión
- Causa y remediación
- Lecciones aprendidas

Las políticas de ADP definen un incidente de seguridad, la gestión de incidentes, y todas las responsabilidades de los empleados en relación al reporte de incidentes de seguridad. Asimismo, ADP realiza regularmente formaciones con empleados y contratistas para asegurar el conocimiento de los requerimientos de reporte de incidentes. Esta formación está supervisada para asegurar que haya sido completada.

Sección 13 - Aspectos de la Seguridad de la Información de la Gestión de Resiliencia del Negocio.

Programa de Resiliencia de Negocio de ADP

ADP se encuentra comprometido a mantener nuestros servicios y operaciones funcionando fluidamente, de forma que podamos proporcionar a nuestros clientes con el mejor servicio posible. Es nuestra prioridad el identificar –y mitigar- los riesgos tecnológicos, ambientales y de salud que puedan interponerse en nuestra provisión de servicios. ADP ha creado un marco de trabajo integrado que establece los procesos de mitigación, preparación, respuesta y recuperación e incluye:

- Evaluación de Riesgo
- Análisis de amenaza de Riesgo
- Análisis de Impacto de Negocio
- Desarrollo de Plan
- Plan de Continuidad de Negocio
- Plan de Recuperación de Desastre
- Plan de Seguridad y Salud
- Respuesta de Mundo real
- Gestión de Crisis
- Respuesta de Emergencia
- Prueba y Validación
- Revisión
- Ejercicio

Sección 14 - Conformidad

Conformidad con estándares y Políticas de Seguridad

ADP emplea un proceso para realizar revisiones de conformidad de forma periódica. Adicionalmente, ADP realiza una auditoría SOC1 Tipo II de forma periódica. Estas auditorías son realizadas por una reconocida firma de auditorías, y sus informes están disponibles anualmente para nuestros clientes bajo pedido, en caso de ser aplicable.

Conformidad Técnica

Para reforzar la conformidad técnica con las mejores prácticas, ADP realiza de forma regular escaneos de vulnerabilidades de redes. Los resultados de dichos escaneos son priorizados y se desarrollan acciones correctivas con los equipos de hosting y su Dirección.

Los escaneos de vulnerabilidades se realizan de forma regular en entornos tanto internos como externos. Adicionalmente, se realizan escaneos de código fuente y pruebas de intrusión para cada producto. Utilizando herramientas especiales de escaneo de aplicaciones, se identifican vulnerabilidades a nivel de aplicaciones, que una vez identificadas son compartidas con los equipos de gestión de desarrollo de productos, e incorporados en los procesos de Quality Assurance para acciones correctivas. Los resultados son analizados, y se desarrollan y priorizan acciones correctivas.

Conservación de la Información

La política de ADP de retención en relación a la información del cliente ha sido diseñada conforme a las leyes aplicables. Al final de la relación contractual con nuestros clientes, ADP actúa de conformidad con sus obligaciones contractuales en relación a la información del cliente. ADP devolverá o permitirá al cliente recuperar (a través de descargas de información), toda la información requerida para la continuación de las actividades de negocio (en caso de no haber sido previamente solicitada). Luego, ADP procederá a destruir de forma segura cualquier remanente de información, a excepción de aquella requerida por la ley aplicable, autorizada por el cliente o requerida para la resolución de disputas.

ANEXO 3: Listado de las Empresas del Grupo sujetas al Código para Encargados de los datos

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Filipinas, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Suiza
ADP Brazil Ltda.	João Tibiriçá, 1112 - Vila Anastácio, São Paulo - SP, 05077-000, Brazil
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canadá
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Brussels, Bélgica
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, República Checa
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Alemania
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelona, España
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milan, Italia
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunis, Túnez
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, Francia
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, Francia
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Países Bajos
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, Francia
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 India
ADP International Services B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Países Bajos
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Rotterdam
ADP Outsourcing Italia SRL	Viale G. Richard 5/A – 20143 Milan, Italia
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Warsaw, Polonia

ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, India – 500082
ADP RPO UK Limited	22 Chancery Lane, London, Inglaterra, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, OH 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Eslovaquia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Turin, Italia
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Sverige AB	Östermalmstorg 1, 114 42 Stockholm, Suecia
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, Bucharest, Romania 020334
Automatic Data Processing Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australia
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62, Ubi Road 1, #11-07, Oxley Bizhub 2, Singapur 408734
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugal
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068