Medidas de seguridad

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

Contenido

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.

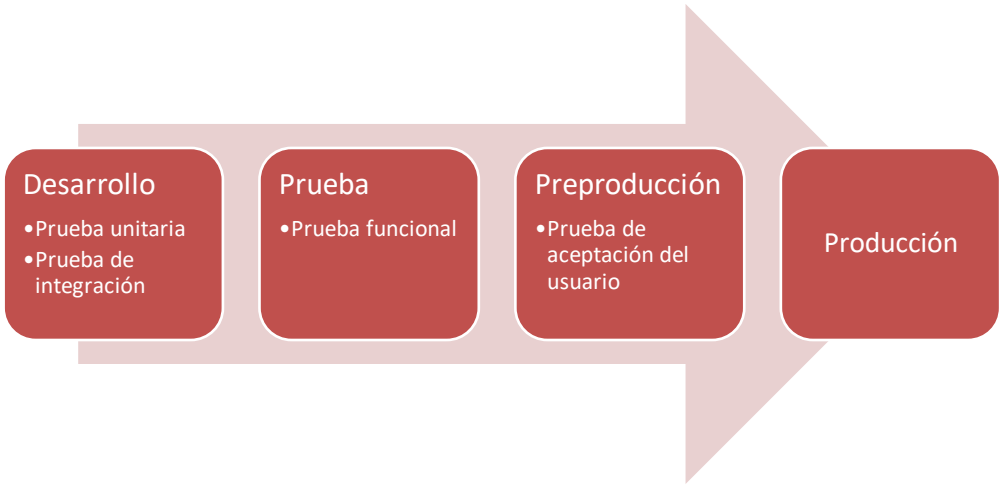
Intercambio de Información

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.

Sección 10 - Mantenimiento, Desarrollo y Adquisición de Sistemas

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.