Medidas de segurança

Apresentado por:	**ADP - Organização de segurança global**
Versão:	**2.0**
Lançamento:	**setembro de 2019**

Índice

Seção 1 - Políticas de segurança da informação 4
Seção 2 - Organização da segurança da informação 6
Seção 3 - Segurança de recursos humanos 7
Seção 4 - Gestão de ativos 8
Seção 5 - Controle de acesso 9
Seção 6 - Criptografia 11
Seção 7 - Segurança física e do ambiente 12
Seção 8 - Segurança de operações 13
Seção 9 - Segurança de comunicações 15
Seção 10 - Aquisição, desenvolvimento e manutenção de sistemas 16
Seção 11 - Relações com fornecedores 17
Seção 12 - Gestão de incidentes de segurança da informação 18
Seção 13 - Aspectos de segurança da informação da gestão da resiliência corporativa 19
Seção 14 - Conformidade 20

Termos e definições

Os seguintes termos podem aparecer no documento:

Termo ou acrônimo usado	Definição
GETS	**Tecnologia e soluções corporativas globais**
GSO	**Organização de segurança global**
CAB	**Conselho de mudanças**
DRP	**Plano de recuperação de desastres**
CIRC	**Centro de resposta a incidentes críticos da GSO**
SIEM	**Gestão de segurança da informação e eventos**
IDS	**Sistema de detecção de invasão**
DNS	**Sistema de nomes de domínio**
NTP	**Protocolo de tempo de rede**
SOC	**Controles da organização de serviços**
TPSI	**Infraestrutura de segurança de plataforma de confiança**

Visão geral

A ADP possui um programa formal de segurança da informação que contém proteções administrativas, técnicas e físicas para salvaguardar a segurança, a confidencialidade e a integridade das informações do cliente. Esse programa foi projetado para, dentro da razoabilidade, (i) salvaguardar a segurança e a confidencialidade das informações do cliente, (ii) proteger contra ameaças ou riscos previstos à segurança ou integridade das informações e (iii) proteger contra acesso ou uso não autorizado das informações.

Esse documento contém uma visão geral das medidas e práticas de segurança da informação da ADP, a partir da data de lançamento, e que estão sujeitas a alterações pela ADP. Esses requisitos e práticas foram elaborados em conformidade com os padrões de segurança da informação ISO/IEC 27001:2013. A ADP avalia periodicamente suas políticas e padrões de segurança. Nosso objetivo é ajudar a garantir que o programa de segurança opere com eficiência e eficácia para proteger todas as informações que nos são confiadas por nossos clientes e seus funcionários.

Seção 1 - Políticas de segurança da informação

Independência da função de segurança da informação

O Diretor de Segurança da ADP supervisiona a Organização de segurança global (GSO) da ADP e se reporta ao Conselho Geral (GC), em vez do Diretor de Informação, o que dá à GSO a independência necessária da TI. A GSO é uma equipe de segurança convergente e interdepartamental que tem uma abordagem multidisciplinar à segurança cibernética e de informações, à conformidade, ao gerenciamento de risco operacional, ao gerenciamento de segurança do cliente, à proteção da força de trabalho e à resiliência empresarial. A alta gerência da GSO, sob o comando do nosso Diretor de Segurança, é responsável por gerenciar políticas, procedimentos e diretrizes de segurança.

Definição formal de uma política de segurança da informação

A ADP desenvolveu e documentou políticas formais de segurança da informação que definem a abordagem da ADP para gerenciar a segurança da informação. As áreas específicas cobertas por essa política incluem, entre outras:

- **Política de gestão de segurança –** Descreve as responsabilidades da Organização de segurança global (GSO) e do Diretor de Segurança (CSO), incluindo as responsabilidades de segurança da informação e os controles no processo de contratação de um ponto de vista da segurança.
- **Política de Privacidade Global –** Aborda a coleta de informações pessoais, o acesso a elas, a precisão delas, as divulgações e a declaração de privacidade para clientes.
- **Política de Uso Aceitável de Comunicações Eletrônicas e Proteção de Dados** – Descreve o uso aceitável, diferentes comunicações eletrônicas, criptografia e gerenciamento de chaves.
- **Política de Manuseio de Informações –** Fornece os requisitos para a classificação de informações da ADP e estabelece controles de proteção.
- **Política de Segurança Física –** Define os requisitos de segurança das instalações da ADP e, subsequentemente, dos nossos funcionários e visitantes que lá trabalham.
- **Política de Gestão de Operações de Segurança –** Fornece controles mínimos para a manutenção de correções de sistema, tratamento eficiente de ameaças de malware e manutenção de backups e controles de segurança de bancos de dados.
- **Política de Monitoramento de Segurança –** Fornece controles para sistemas de detecção de invasão (IDS), registros e prevenção de perda de dados (PPD).
- **Política de Gestão de Investigações e Incidentes –** Define padrões para resposta a incidentes, descoberta eletrônica, proteção da força de trabalho e acesso às informações armazenadas eletronicamente pelos funcionários.
- **Política de Acesso e Autenticação –** Descreve os requisitos para autenticação (por exemplo, ID de usuário e senha), acesso remoto e acesso sem fio.
- **Política de Segurança de Rede –** Arquitetura de segurança de roteadores, firewalls, AD, DNS, servidores de e-mail, DMZ, serviços de nuvem, dispositivos de rede, web proxy e tecnologia de rede comutada.
- **Política Global de Risco de Terceiros e Fusões e Aquisições –** Define controles mínimos de segurança para envolver terceiros a fim de auxiliar a ADP a atingir seus objetivos comerciais.
- **Política de Gestão de Aplicações –** Estabelece controles de segurança apropriados para cada estágio do ciclo de vida de desenvolvimento do sistema.
- **Política de Resiliência Corporativa –** Rege a proteção, integridade e preservação da ADP estabelecendo os requisitos mínimos para a documentação, implementação, manutenção e aprimoramento contínuo de Programas de Resiliência Corporativa
- **Política de Gestão de Riscos de Segurança Convergente –** Identificação, monitoramento, resposta, análise, governança e novas iniciativas corporativas.

As políticas são publicadas na intranet da ADP e podem ser acessadas por todos os funcionários e contratados dentro da rede da ADP.

Revisão da política de segurança da informação

A ADP revisa suas políticas de segurança da informação pelo menos uma vez por ano ou sempre que houver mudanças significativas que afetem o funcionamento dos sistemas de informação da ADP.

Seção 2 - Organização da segurança da informação

Responsabilidades e funções da segurança da informação

A GSO é composta por equipes de segurança interdepartamentais que utilizam uma abordagem multidisciplinar à conformidade com padrões de segurança cibernética e da informação, ao gerenciamento de risco operacional, ao gerenciamento de segurança do cliente, à proteção da força de trabalho e à resiliência empresarial. As funções e responsabilidades foram formalmente definidas para todos os membros da GSO. A GSO é responsável pelo design, pela implementação e pela supervisão do nosso programa de segurança da informação com base nas políticas corporativas. As atividades da GSO são supervisionadas pelo Comitê Executivo de Segurança, cujos membros incluem o Diretor de segurança, o Diretor Executivo, o Diretor Financeiro, o Diretor de Estratégia, o Diretor de Recursos Humanos e o Conselho Geral da ADP.

Política de computação móvel e teletrabalho

A ADP exige que todas as informações confidenciais sejam criptografadas em dispositivos móveis para evitar o vazamento de dados, o que pode resultar do roubo ou da perda de um computador/dispositivo. A proteção avançada de endpoint e a autenticação de dois fatores com o uso de VPN também são necessárias para acessar redes corporativas remotamente. Todos os dispositivos remotos devem ser protegidos por senha. Os funcionários da ADP têm o dever de informar dispositivos de computação remotos perdidos ou roubados imediatamente por meio de um Processo de Relato de Incidente de Segurança.

Como uma condição para o vínculo empregatício na ADP, todos os funcionários e contratados devem cumprir a Política de Uso Aceitável de Comunicações Eletrônicas e Proteção de Dados e outras políticas relevantes.

Seção 3 - Segurança de recursos humanos

Verificação de antecedentes

Conforme os requisitos legais aplicáveis na região de cada pessoa, a ADP realiza as devidas verificações de antecedentes, compatíveis com os deveres e as responsabilidades de seus funcionários, contratados e terceiros. Essas verificações confirmam a aptidão do candidato para lidar com as informações dos clientes antes de envolver ou contratar tais indivíduos.

A verificação de antecedentes pode incluir os seguintes componentes:

- Verificação de identidade/elegibilidade para trabalhar
- Histórico de trabalho
- Formação escolar/acadêmica e qualificações profissionais
- Antecedentes criminais (quando legalmente autorizado e dependendo das regulamentações locais do país)

Acordos de confidencialidade com funcionários e contratados

Os contratos de trabalho da ADP e os contratos com contratados contêm termos que indicam deveres e responsabilidades relacionados às informações do cliente às quais eles terão acesso. Todos os funcionários e contratados da ADP estão vinculados a deveres de confidencialidade.

Programa de treinamento de segurança da informação

Todos os funcionários devem concluir o treinamento de segurança da informação como parte do plano de integração. Além disso, a ADP oferece treinamento anual de segurança para relembrar os funcionários de suas responsabilidades ao executar tarefas diárias.

Responsabilidades dos funcionários e processos disciplinares

A ADP publicou uma política de segurança que todos os funcionários da ADP devem seguir. Violações das políticas de segurança podem levar à revogação de privilégios de acesso e/ou ações disciplinares, incluindo a rescisão de contratos de consultoria ou trabalho.

Término das responsabilidades de trabalho

As responsabilidades após o término do trabalho foram formalmente documentadas e incluem no mínimo:

- Devolver todas as informações e ativos da ADP em posse do funcionário em questão, em qualquer meio em que estejam armazenados
- Revogação dos direitos de acesso às instalações, informações e sistemas da ADP
- Alteração das senhas de contas compartilhadas ativas, se aplicável
- Transferência de conhecimento, se aplicável.

Seção 4 - Gestão de ativos

Uso aceitável de ativos

O uso aceitável de ativos é explicado em várias políticas, aplicáveis aos funcionários e contratados da ADP, para ajudar a garantir que as informações da ADP e dos clientes não sejam expostas pelo uso de tais ativos. Exemplos de áreas descritas nessas políticas são: uso de comunicações eletrônicas, uso de equipamentos eletrônicos e uso de ativos de informação.

Classificação de informações

As informações adquiridas, criadas ou mantidas pela ADP ou em seu nome recebem, conforme aplicável, uma classificação de segurança de:

- Público - Exemplo: folders de marketing, relatórios anuais publicados
- Somente para Uso Interno da ADP - Exemplo: comunicados entre unidades, procedimentos operacionais
- Confidencial da ADP - Exemplo: informações pessoais e informações pessoais sigilosas
- Restrito à ADP - Exemplo: previsões financeiras, informações de planejamento estratégico

Os requisitos para o tratamento de informações estão diretamente correlacionados à classificação de segurança da informação. Informações pessoais e informações pessoais sigilosas são sempre consideradas como algo Confidencial da ADP. Todas as informações do cliente são classificadas como confidenciais.

Os funcionários da ADP são responsáveis por proteger e manusear ativos de informação de acordo com seu nível de classificação de segurança, o que fornece proteção de informações e requisitos de manuseio aplicáveis para cada nível de classificação. A classificação de confidencialidade da ADP é aplicada a todas as informações armazenadas, transmitidas ou manipuladas por terceiros.

Descarte de equipamentos e mídias

Quando equipamentos, documentos, arquivos e mídias da ADP são descartados ou reutilizados, empreendem-se medidas apropriadas para evitar a recuperação subsequente de informações do cliente originalmente armazenadas neles. Antes de serem liberadas das instalações da ADP ou reaproveitadas, todas as informações em computadores ou mídias de armazenamento eletrônico, independentemente da classificação, são descartadas com segurança, a menos que a mídia seja fisicamente destruída. Os procedimentos para destruição/apagamento seguro de informações da ADP mantidas em equipamentos, documentos, arquivos e mídia são formalmente documentados.

Mídia física em trânsito

Implementamos medidas organizacionais para proteger materiais impressos contendo informações de clientes contra roubo, perda e/ou acesso/modificação não autorizados (i) durante o transporte, por exemplo, envelopes lacrados, contêineres e entrega em mãos ao usuário autorizado; e (ii) durante a análise, revisão ou outra atividade de tratamento de dados quando removidos do armazenamento seguro.

Seção 5 - Controle de acesso

Requisitos comerciais de controle de acesso

A Política de Controle de Acesso da ADP é baseada em requisitos definidos pela empresa. As políticas e padrões de controle são articulados em controles de acesso que são aplicados em todos os componentes do serviço fornecido e são baseados em um princípio de “privilégio mínimo” e “necessidade de ter conhecimento”.

Acesso à infraestrutura - Gestão de controle de acesso

As solicitações de acesso para mover, adicionar, criar e excluir são registradas, aprovadas e revisadas periodicamente.

Uma análise formal é realizada pelo menos uma vez por ano para confirmar se os usuários individuais correspondem com precisão à função comercial relevante e não terão acesso contínuo após uma mudança de cargo. Esse processo é auditado e documentado em um relatório SOC1[1] tipo II. Em um Sistema de Gerenciamento de Identidades, uma equipe da ADP dedicada é responsável por conceder, negar, cancelar, encerrar e descomissionar/desativar o acesso às instalações e aos sistemas de informação da ADP. A ADP usa uma ferramenta centralizada de gerenciamento de identidade e acesso (IAM) que é gerenciada centralmente por uma equipe GETS dedicada. De acordo com os direitos de acesso solicitados por meio da ferramenta IAM centralizada, um fluxo de trabalho de validação será acionado, podendo incluir a participação do supervisor dos usuários. O acesso é fornecido temporariamente e existem fluxos de trabalho para evitar que esse acesso seja permanente. O acesso de um funcionário a uma instalação é desativado imediatamente após o último dia de trabalho por meio da desativação do cartão de acesso (crachá do funcionário). Os IDs de usuário do funcionário são imediatamente desativados. Todos os ativos dos funcionários são devolvidos e verificados pela chefia de linha competente e são comparados com a lista de ativos no banco de dados de gerenciamento de configuração. Após uma mudança de cargo ou mudanças organizacionais, os perfis de usuário ou direitos de acesso do usuário devem ser modificados pela gerência da unidade comercial aplicável e pela equipe de IAM. Além disso, uma análise formal dos direitos de acesso é realizada todos os anos para verificar se os direitos dos usuários individuais correspondem à sua função comercial relevante e se não ficou algum direito de acesso irrelevante após uma transferência de cargo.

Política de senhas

As políticas de senhas de colaboradores da ADP são aplicadas em servidores, bancos de dados, dispositivos e aplicativos de rede, na medida em que o dispositivo/aplicativo permitir. A complexidade da senha é definida por uma análise que leva em conta o risco dos dados e conteúdos protegidos. As políticas atendem aos padrões vigentes do setor em termos de eficiência da segurança e complexidade, incluindo, entre outros, o uso de autenticação por etapas, multifator ou biométrica, quando apropriado.

Os requisitos de autenticação do aplicativo cliente variam de acordo com o produto, e os serviços federados (SAML 2.0) estão disponíveis em aplicativos específicos da ADP que utilizam uma rede unificada e uma camada de segurança gerenciada pela GETS.

[1] No caso de certos serviços dos EUA oferecidos pela ADP, isso é auditado em um relatório SOC 2 Tipo 2.

Tempos limite de sessão

A ADP aplica tempos limite automáticos a todos os servidores, estações de trabalho, aplicativos e conexões VPN com base em uma abordagem que leva em conta o risco consistente com os padrões do setor. O restabelecimento das sessões deve ocorrer somente após o usuário fornecer uma senha válida.

Seção 6 - Criptografia

Controles de criptografia

A ADP exige que informações confidenciais trocadas entre a ADP e terceiros da ADP sejam criptografadas (ou o canal de transferência seja criptografado) usando técnicas e níveis de criptografia aceitos pelo setor. Como alternativa, uma linha privada alugada pode ser usada.

Gerenciamento de chaves

A ADP tem um Padrão de Segurança de Criptografia interno que inclui procedimentos bem definidos de gerenciamento de chaves e custódia de chaves, incluindo gerenciamento de chaves simétricas e assimétricas.

As chaves de criptografia usadas para informações da ADP são sempre classificadas como informações confidenciais. O acesso a essas chaves é estritamente limitado àqueles que precisam ter conhecimento delas e exceções são permitidas somente mediante aprovação. As chaves de criptografia e o gerenciamento do ciclo de vida das chaves seguem práticas padrão do setor.

Seção 7 - Segurança física e do ambiente

A abordagem da ADP à segurança física tem dois objetivos: criar um ambiente de trabalho seguro para os colaboradores da ADP e proteger as Informações Pessoais mantidas nos data centers da ADP e outros locais estratégicos da ADP.

A política de segurança da ADP exige que a gerência da ADP identifique as áreas que requerem um nível específico de segurança física. O acesso a essas áreas é fornecido apenas a colaboradores autorizados e para fins autorizados. As áreas protegidas da ADP empregam várias proteções de segurança física, incluindo sistemas de vigilância por vídeo, uso de crachás de segurança (acesso controlado por identidade) e guardas de segurança posicionados nas entradas e saídas. Os visitantes só podem ter acesso quando autorizados e são supervisionados o tempo todo.

Seção 8 - Segurança de operações

Formalização de procedimentos de operações de TI

A GETS é a unidade da ADP responsável pelas operações e manutenção da infraestrutura de TI. A GETS mantém e documenta formalmente as políticas e os procedimentos de operações de TI. Esses procedimentos incluem o seguinte, entre outros:

- Gestão de mudanças
- Gestão de backup
- Solução de erros de sistemas
- Reinicialização e recuperação de sistemas
- Monitoramento de sistemas
- Agendamento e monitoramento de trabalhos

Gestão de mudanças de infraestrutura

Um Conselho de Mudanças (CAB) periódico, incluindo representantes de várias equipes da ADP, é organizado pela GETS. As reuniões do CAB abordam os impactos das janelas de implantação e promoções para produção, bem como coordenam qualquer outra mudança na infraestrutura de produção.

Planejamento e aceitação da capacidade do sistema

Os requisitos de capacidade são monitorados continuamente e revisados com frequência. Após essas revisões, os sistemas e redes são ampliados ou reduzidos conforme necessário. Quando mudanças significativas precisam ser feitas devido a uma mudança na capacidade ou uma evolução tecnológica, a equipe de análise comparativa da GETS pode realizar testes de estresse no aplicativo e/ou sistema relevante. Na conclusão do teste de estresse, a equipe fornece um relatório detalhado da evolução do desempenho avaliando as mudanças em (i) componentes, (ii) configuração ou versão do sistema ou (iii) configuração ou versão do middleware.

Proteção contra código malicioso

As tecnologias de proteção de endpoint padrão do setor são utilizadas para proteger ativos da ADP de acordo com as práticas padrão recomendadas do setor.

Política de gestão de backup

A ADP possui políticas que exigem que todas as operações de hospedagem de produção façam backup das informações de produção. O escopo e a frequência dos backups são definidos de acordo com os requisitos comerciais dos serviços relevantes da ADP, os requisitos de segurança das informações envolvidas e a criticidade das informações em relação à recuperação de desastres. O monitoramento de backups agendados é realizado pela GETS para identificar problemas ou exceções de backup.

Registro e monitoramento de segurança

A ADP implementou uma infraestrutura de registro central e somente leitura (SIEM) e um sistema de correlação e alerta de registro (TPSI). Os alertas de registro são monitorados e resolvidos em tempo hábil pelo CIRC.

Todos esses sistemas são sincronizados usando uma referência de relógio exclusiva baseada no protocolo de tempo de rede (NTP).

Cada registro individual contém no mínimo:

- Carimbo de data/hora
- Quem (identidade do operador ou administrador)
- O quê (informações sobre o evento)

Trilhas de auditoria e registros de sistema de aplicativos da ADP são elaborados e configurados para rastrear as seguintes informações:

- Acesso autorizado
- Operações privilegiadas
- Tentativas de acesso não autorizado
- Alertas ou falhas de sistemas
- Alterações nas configurações de segurança do sistema, quando o sistema permite tal registro

Esses registros estão disponíveis apenas para pessoal autorizado da ADP e são enviados em tempo real para evitar que os dados sejam adulterados antes de serem armazenados nos dispositivos de registro seguros.

Sistemas de infraestrutura e monitoramento

A ADP usa medidas adequadas para fornecer monitoramento de infraestrutura 24 horas por dia, 7 dias por semana. Os alertas de interrupção são gerenciados por diferentes equipes de acordo com seu nível de criticidade e as habilidades necessárias para resolvê-los.

As instalações do centro de hospedagem da ADP utilizam aplicativos de monitoramento que estão constantemente em execução em todos os sistemas de processamento relacionados e nos componentes de rede para fornecer à equipe da ADP notificações proativas sobre problemas e avisos que antecipam a ocorrência de possíveis problemas.

Gestão de vulnerabilidade técnica

Todos os computadores instalados na infraestrutura de hospedagem devem seguir a instalação de um sistema operacional especializado e de segurança reforçada (ou processo de compilação seguro). As operações hospedadas utilizam uma compilação reforçada, aprovada e padronizada para cada tipo de servidor usado em nossa infraestrutura. A instalação pronta para uso de sistemas operacionais é proibida, pois essas instalações podem criar vulnerabilidades, como senhas genéricas de contas de sistema, que introduziriam um risco de infraestrutura. Essas configurações reduzem a exposição de computadores hospedados que executam serviços desnecessários que podem apresentar vulnerabilidades.

A ADP tem uma metodologia documentada para conduzir avaliações periódicas e de vulnerabilidades de lançamento e revisões de conformidade de aplicativos baseados na Web voltados para a Internet e seus componentes de infraestrutura correspondentes, que incluem pelo menos 15 categorias principais de testes. A metodologia de avaliação é baseada nas melhores práticas internas e do setor, incluindo, entre outros, o projeto aberto de segurança em aplicações web (OWASP), o SANS Institute e o consórcio de segurança em aplicações web (WASC).

Seção 9 - Segurança de comunicações

Gestão de segurança de rede

A ADP utiliza um sistema de detecção de invasão baseado em rede que monitora o tráfego no nível da infraestrutura de rede (24 horas por dia, 7 dias por semana) e identifica atividades suspeitas ou possíveis ataques.

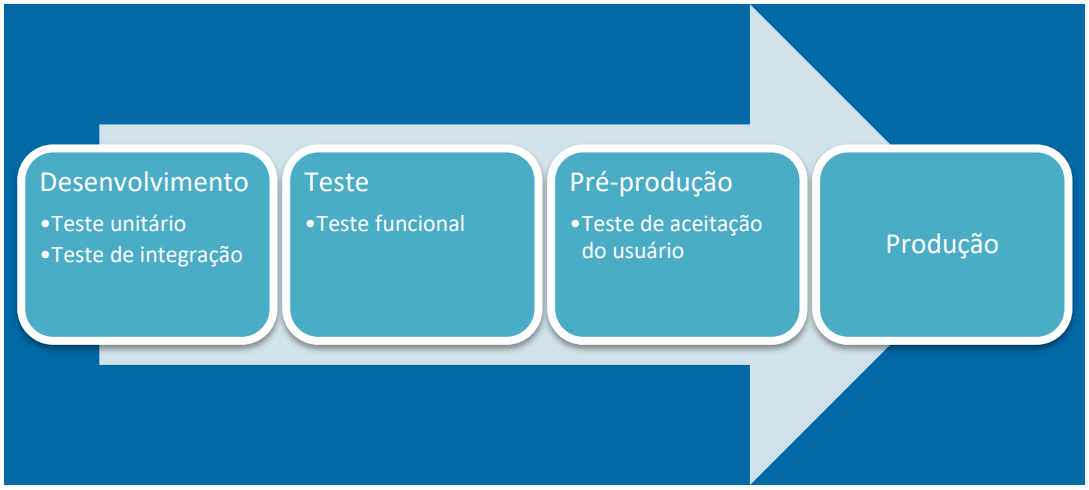
Troca de informações

A ADP implementa controles adequados para que as informações dos clientes da ADP enviadas a terceiros sejam transferidas apenas entre sistemas e recursos de informação autorizados e sejam trocadas apenas por meio dos mecanismos de transferência seguros e autorizados da ADP.

Seção 10 - Aquisição, desenvolvimento e manutenção de sistemas

Segurança nos processos de desenvolvimento e suporte

Durante o ciclo de desenvolvimento, a documentação aplicável é gerada e planos de teste são elaborados para a fase de teste. Para cada ambiente, são definidas diferentes etapas com aprovação relevante em cada fase:



- Para passar do ambiente de Teste para o ambiente de Pré-produção, é necessária a aprovação da equipe de Qualidade da ADP.
- Para passar da Pré-produção para a Produção, é necessária a aprovação das Operações de TI.

As equipes de desenvolvimento devem utilizar métodos de codificação seguros. As alterações de aplicativos são testadas em ambientes de desenvolvimento e regressão antes de chegarem aos sistemas de produção. Os testes são realizados e documentados. Após a aprovação, as alterações são implantadas na produção. O teste de penetração é realizado após mudanças significativas.

Um CAB periódico, incluindo representantes de várias equipes da ADP, é realizado pela GETS. As reuniões do CAB ocorrem regularmente e têm como objetivo discutir impactos, concordar com janelas de implantação e aprovar a promoção de pacotes de software para produção, bem como informar quaisquer outras alterações na infraestrutura de produção.

A equipe de Operações de TI da ADP fornece a aprovação final antes da promoção dos pacotes de software para o ambiente de produção.

Segurança em ambiente de desenvolvimento

Os ambientes de produção e desenvolvimento são segregados e independentes um do outro. Controles de acesso adequados são utilizados para impor a segregação adequada de funções. Os pacotes de software são acessíveis em cada estágio do processo de desenvolvimento e somente pelas equipes envolvidas naquele estágio.

Dados de testes

De acordo com a Política de Gestão de Aplicações da ADP, o uso de dados reais ou não higienizados em desenvolvimento e testes não é permitido, a menos que explicitamente solicitado e autorizado pelo cliente.

Seção 11 - Relações com fornecedores

Identificação de riscos relacionados a partes externas

As avaliações de risco de terceiros que exigem acesso à ADP e/ou às informações de clientes são realizadas periodicamente para determinar sua conformidade com os requisitos de segurança da ADP para terceiros e para identificar lacunas nos controles aplicados. Se uma lacuna de segurança for identificada, novos controles serão acordados com essas partes externas.

Acordos de segurança da informação com partes externas

A ADP celebra acordos com todos os terceiros que incluem compromissos de segurança apropriados para atender aos requisitos de segurança da ADP.

Seção 12 - Gestão de incidentes de segurança da informação

Gestão de incidentes de segurança da informação e melhorias

A ADP tem uma metodologia documentada para responder a incidentes de segurança de modo oportuno, consistente e eficaz.

Caso ocorra um incidente, uma equipe predefinida de funcionários da ADP ativa um plano formal de resposta a incidentes que aborda áreas como:

- Escalonamentos com base na classificação ou na gravidade do incidente
- Lista de contatos para relatórios/escalonamento de incidentes
- Diretrizes para respostas iniciais e acompanhamento com clientes envolvidos
- Conformidade com as leis aplicáveis de notificação de violação de segurança
- Registro de investigação
- Recuperação de sistemas
- Resolução de problemas, relatórios e revisão
- Causa raiz e remediação
- Lições aprendidas

As políticas da ADP definem o que é um incidente de segurança, o gerenciamento de incidentes e todas as responsabilidades dos funcionários em relação ao relato de incidentes de segurança. A ADP também realiza treinamentos regulares para funcionários e contratados da ADP para ajudar a garantir a conscientização sobre os requisitos de relatórios. O treinamento é monitorado para garantir a conclusão.

Seção 13 - Aspectos de segurança da informação da gestão da resiliência corporativa

Programa de resiliência corporativa da ADP

A ADP está comprometida em manter nossos serviços e operações funcionando continuamente sem interrupções para que possamos oferecer aos nossos clientes o melhor serviço possível. Nossa prioridade é identificar e mitigar os riscos tecnológicos, ambientais, de processo e de saúde que podem atrapalhar o fornecimento de nossos serviços comerciais. A ADP criou uma estrutura integrada que define nossos processos de mitigação, preparação, resposta e recuperação e inclui:

- Avaliação de risco
- Análise de ameaças de risco
- Análise de impacto nos negócios
- Desenvolvimento de planos
- Planejamento de continuidade dos negócios
- Planejamento de recuperação de desastres
- Planejamento de saúde e segurança
- Respostas baseadas no mundo real
- Gestão de crises
- Respostas emergenciais
- Teste e validação
- Analisar
- Revisar
- Executar

Seção 14 - Conformidade

Conformidade com as políticas e padrões de segurança

A ADP emprega um processo para realizar revisões de conformidade internamente em uma base periódica. Além disso, a ADP realiza uma auditoria SOC1[2] tipo II periodicamente. Essas auditorias são conduzidas por uma empresa de auditoria terceirizada bem conhecida e os relatórios de auditoria são disponibilizados anualmente aos clientes mediante solicitação, quando aplicável.

Conformidade técnica

Para garantir a conformidade técnica com as práticas recomendadas, a ADP realiza verificações de vulnerabilidades de rede programadas regularmente. Depois, os resultados da verificação são priorizados e desenvolvidos em planos de ação corretiva com as equipes de hospedagem e a gerência delas.

As verificações de vulnerabilidades são realizadas regularmente em ambientes internos e externos. Além disso, varreduras de código-fonte e testes de penetração são realizados em cada produto. Utilizando ferramentas especializadas de varredura de aplicativos, as vulnerabilidades no nível do aplicativo, se houver alguma, são identificadas, compartilhadas com as equipes de gerenciamento de desenvolvimento de produtos e incorporadas aos processos de garantia de qualidade para a realização de ações corretivas. Os resultados são analisados e planos de ação corretiva são desenvolvidos e priorizados.

Retenção de dados

A política de retenção de dados da ADP em relação às informações do cliente foi elaborada para cumprir as leis aplicáveis. No final de um contrato com o cliente, a ADP cumpre com suas obrigações contratuais relacionadas às informações do cliente. A ADP devolverá ou permitirá que o cliente recupere (por meio de download de dados) todas as informações do cliente necessárias para a continuidade das atividades comerciais do cliente (se não tiverem sido fornecidas anteriormente). Depois, a ADP destruirá com segurança as informações restantes do cliente, exceto conforme exigido pela lei aplicável, autorizado pelo cliente ou necessário para fins de resolução de conflitos.

[2] No caso de determinados serviços dos EUA oferecidos pela ADP, também haveria relatórios executivos SOC 2 Tipo II.