← Voltar

Política de Segurança da Informação

01. **OBJETIVO**

A **PALADIUM CORP. DESENVOLVIMENTO DE TECNOLOGIA LTDA.** ("**PALADIUM**" ou "Companhia") reconhece a importância e trata como prioridade a Segurança dos seus clientes, funcionários e dados corporativos comerciais. Considerando a relevância das Informações, a PALADIUM resolveu estabelecer esta **Política Interna de Segurança da Informação** ("Política"), com a finalidade de estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das Informações da **PALADIUM** ou sob a sua guarda. A Política visa

garantir a Confidencialidade, Integridade, Disponibilidade e Autenticidade das Informações, assegurando o seu uso adequado e a mitigação de riscos à Segurança da Informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD), suas normas reguladores, e de outras normas vigentes.

2. ESCOPO

Esta Política se aplica a todos os ativos de Informação da **PALADIUM**, incluindo dados, sistemas, aplicativos, dispositivos e redes. Esta Política se aplica a todos os empregados, funcionários, prestadores de serviço, fornecedores, parceiros e quaisquer terceiros (comumente, “Colaboradores”) que acessam ou processam as Informações da **PALADIUM.**

3. DEFINIÇÕES

As definições a seguir visam esclarecer os termos-chave utilizados nesta Política para alinhar seu entendimento às normas aplicáveis:

- **Autenticidade:** propriedade pela qual se assegura que a Informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.
- **Confidencialidade:** propriedade pela qual se assegura que a Informação não esteja Disponível ou não seja revelada a pessoas, empresas, sistemas, órgãos ou entidades não autorizados.
- **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável.

- **Dado Pessoal Sensível:** Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Disponibilidade:** propriedade pela qual se assegura que a Informação esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados.
- **Incidente de Segurança ("Incidente"):** violação de quaisquer das propriedades da Segurança da Informação.
- **Identificação Biométrica:** método que envolve o reconhecimento de características físicas, fisiológicas e comportamentais humanas, com o propósito de identificar um indivíduo.
- **Informação:** dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
- **Integridade:** propriedade pela qual se assegura que a Informação não foi modificada ou destruída de maneira não autorizada ou acidental.
- **Monitoramento Eletrônico**: uso de sistemas de câmeras de vigilância e dispositivos de captura de imagens para monitorar áreas públicas
- **Segurança da Informação:** ações que objetivam viabilizar e assegurar as propriedades de Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade das Informações.
- **Titular:** pessoa natural a quem se referem os Dados Pessoais que são objeto de tratamento.

3. PRINCÍPIOS

As normas, diretrizes e procedimentos adotados pela **PALADIUM** no âmbito da Segurança da Informação se baseiam nos seguintes princípios:

- **Confidencialidade** de todas as Informações, garantindo que elas estejam disponíveis ou sejam reveladas apenas a pessoas, sistemas e entidades

autorizados e credenciados;

- **Integridade** de todas as Informações, garantindo que elas são completas, perfeitas e intactas, assegurando-se que elas não sejam modificadas ou destruídas de maneira não autorizada ou acidental;
- **Disponibilidade** das Informações, garantindo que elas se encontrarão disponíveis e utilizáveis para a pessoa autorizada, sistema ou entidade, quando houver necessidade e for solicitado o acesso à Informação para atendimento dos interesses do negócio;
- **Autenticidade** das Informações, garantindo que ações relevantes sobre as Informações tenham sua autoria preservada e comprovada.
- **Resiliência**, garantindo o retorno ágil das operações em caso de Incidentes que gerem qualquer tipo de instabilidade; e
- **Conformidade** com a legislação e regulamentos aplicáveis, observando as melhores práticas de Segurança da Informação, e respeitando o acesso à Informação, à proteção de Dados Pessoais e à proteção da privacidade.

5. DIRETRIZES DA PALADIUM

Abaixo, constam as diretrizes básicas de Segurança da Informação que deverão ser observadas por todos os Colaboradores que tenham acesso a Informações internas confidenciais e Dados Pessoais em posse da **PALADIUM**:

a. Treinamento e Conscientização

A **PALADIUM** realiza treinamentos e campanhas de conscientização periódicas sobre Segurança da Informação para seus Colaboradores, de modo que estejam sempre cientes de suas responsabilidades organizacionais para a manutenção da Segurança dos ativos e recursos informacionais da Companhia.

b. Prestadores de Serviços

Prestadores de Serviço que se utilizem ou mantenham recursos informacionais da **PALADIUM** estão sujeitos a obrigações contratuais de Segurança da Informação adequadas aos riscos representados pela atividade, incluindo obrigações de Confidencialidade.

Todos os fornecedores e operadores contratados pela **PALADIUM** são submetidos à diligência prévia conduzida pelo time de Cibersegurança, que verifica sua adequação às exigências técnicas e organizacionais de proteção de dados e Segurança da Informação.

Sem prejuízos de medidas gerais de Segurança, Fornecedores envolvidos em soluções de Identificação Biométrica, deverão garantir, considerando o seu papel e a aplicabilidade destas medidas, que:

- A transmissão de dados, especialmente de dados biométricos, se opera de forma criptografada;
- O armazenamento de dados biométricos se opera de forma criptografada;
- Os dados biométricos são resguardados por controles de acesso robustos; e
- O fornecedor realiza testes periódicos para identificação e correção de vulnerabilidades.

c. Controle de Acesso

A**PALADIUM** se compromete a implementar controles de acesso apropriados e robustos para garantir que os usuários apenas tenham acesso às Informações que, em acordo com as necessidades de suas funções, precisem acessar.

Para tanto, adota controles de autenticação internos e práticas de Segurança para evitar acessos não autorizados a todos os recursos de Informação da Companhia, como:

- Controles técnicos que (a) demandem senhas robustas; (b) obriguem a troca de senhas-padrão fornecidas após o primeiro acesso do usuário; (c) requeiram a mudança periódica de senhas; e (d) impossibilitem a reutilização de senhas antigas;
- Mecanismos de múltiplos fatores de autenticação para acesso a recursos sensíveis, como o repositório de imagens coletadas, equipamentos do sistema de vigilância e templates biométricos;
- Bloqueio de acesso imediato após comunicação de desligamento de Colaborador;

- Adoção de procedimento formal para concessão e remoção de acesso físico ou lógico aos sistemas de Monitoramento Eletrônico ou que tratem dados biométricos. Com a concessão de acesso devendo se operar por meio de autorização da respectiva alçada de competência, com permissões limitada ao efetivamente necessário para o exercício das funções do Colaborador e periodicamente revistas; e
- Garantir o registro de logs das ações executadas, em especial, os acessos realizados, e quaisquer ações executadas nos sistemas que tratem dados biométricos ou que realizem o Monitoramento Eletrônico.

d. Gerenciamento de Vulnerabilidades

A PALADIUM aplica esforços para detecção, análise e contenção de malwares e outras vulnerabilidades cibernéticas que ameacem os sistemas de informação da Companhia. Isso inclui práticas de gerenciamento de riscos e vulnerabilidades de Segurança da Informação, como:

- Atualização periódica de seus sistemas e aplicativos, instalando os patches de Segurança disponibilizados pelos fornecedores;
- Utilização de softwares antivírus e/ou antimalware, mantendo-os atualizados;
- Realização de varreduras periódicas em seus sistemas, utilizando-se dos softwares antivírus;
- Adoção e apropriada configuração de firewalls para proteção de todos os ativos de Informação conectados à rede pública;
- Adoção de controles técnicos para prevenir ataques contra a Disponibilidade de seus serviços e operações crítica;
- Bloqueio de equipamentos que detenham acesso aos templates biométricos para inserção de dispositivos removíveis não autorizados, como pendrives ou outros dispositivos de armazenamento externo;
- Monitoramento constante dos sistemas de Monitoramento Eletrônico para detecção de falhas em seu funcionamento e, na medida que sejam de responsabilidade da PALADIUM, adoção de medidas corretivas ou comunicação aos respectivos responsáveis;
- Condução de testes regulares de Segurança em sistemas e aplicativos para identificar e corrigir falhas antes que sejam exploradas, especialmente naqueles envolvidos em Monitoramento Eletrônico ou Identificação Biométrica; e
- Implementação de um plano de continuidade de negócios, possibilitando a rápida restituição dos sistemas e operações em caso de Incidentes de

Segurança, com ações preventivas e procedimentos de recuperação que minimizem os impactos de interrupções.

e. Proteção de Dados Pessoais Armazenados

A **PALADIUM** limitará o tratamento de Dados Pessoais ao estritamente necessário para a persecução de suas finalidades.

Quando proceder o tratamento de Dados Pessoais, especialmente dados biométricos, a Companhia se compromete a utilizar criptografia no armazenamento dessas Informações, no mínimo, do lado do servidor ou, em caso de uso de servidores on-premise, de disco.

Especificamente em relação a templates biométricos, a PALADIUM envidará esforços razoáveis para que, sempre que possível, que seu armazenamento se opere garantindo-se a criptografia a nível de coluna.

Ademais, de forma prévia ao descarte de mídias físicas, a PALADIUM garantirá sua formatação e sobrescrição – não sendo possível a sobrescrição e contendo, a mídia, Dados Pessoais, esta deverá ser destruída. Caso o descarte de mídias físicas seja executado por um prestador de serviço, o contrato com este prestador deverá prever o dever de registro da destruição/descarte.

f. Cópias de Segurança (*Backups*)

A **PALADIUM** realiza cópias de Segurança dos dados e Informações em sua posse de forma periódica, em acordo com a necessidade e sensibilidade de cada ativo.

As cópias de Segurança devem ser armazenadas de forma criptografada, em ambiente físico ou lógico segregado do original, e acessível apenas aos profissionais responsáveis por realizar as cópias e/ou restaurá-las.

g. Segurança Física

A **PALADIUM** aplica medidas de Segurança físicas para proteger os recursos informacionais e dados sob a sua guarda contra acessos não autorizados e situações acidentais ou ilícitas de alteração ou destruição.

Para tanto a **PALADIUM** garantirá que suas instalações que permitam acesso aos sistemas de Monitoramento Eletrônico, dados biométricos ou outras Informações Confidenciais, possuam acesso físico restrito, considerando a necessidade de acesso a essas informações.

Ademais, todos os Colaboradores da **PALADIUM** devem seguir práticas de "Tela Limpa, Mesa Limpa", não deixando documentos ou quaisquer outras anotações com informação confidencial em local visível ou desprotegido, bem como não devendo se distanciar do computador ou do dispositivo móvel que tenha lhe sido confiado sem bloqueá-lo.

h. Segurança das Comunicações

A **PALADIUM** garantirá que as comunicações envolvendo Dados Pessoais e outras Informações Confidenciais se operem por canais criptografados, especialmente em se tratando de dados biométricos ou decorrentes de Monitoramento Eletrônico. A **PALADIUM** deverá, ainda, garantir a adequada instalação e configuração de um sistema de firewall em suas máquinas e adoção de ferramentas AntiSpam, filtros de e-mail ao sistema de correio eletrônico, inclusive, integrando o antivírus ao mesmo.

i. Segurança de Dispositivos Móveis

A **PALADIUM** fornecerá aos seus Colaboradores os equipamentos necessários e adequados para o desempenho de suas funções, sendo vedado a utilização de equipamentos pessoais para fins institucionais.

A **PALADIUM** realizará a configuração de Segurança dos aparelhos fornecidos aos seus colaboradores, bem como instalará todos os programas de computador necessários ao exercício de suas funções- sendo estritamente vedado a burla de quaisquer desses controles de Segurança ou a instalação de quaisquer programas de computador de fontes ilegítimas ou sem expressa autorização da **PALADIUM**.

Considerando a sua sensibilidade, a **PALADIUM** adotará medidas apropriadas para prevenir o acesso às informações confidenciais acessíveis a partir dos dispositivos móveis, incluindo controles de autenticação multifator e a implementação de funcionalidades que permitam apagar remotamente os dados e Informações armazenados, em caso de perda do dispositivo.

j. Serviços em nuvem

Em caso de contratação de serviços de processamento ou armazenamento de dados em nuvem, a **PALADIUM** adotará medidas apropriadas para o seu gerenciamento, de modo a garantir que a contratação destes serviços não reduza o nível de Segurança previsto nesta Política. Dentre as medidas a serem adotadas, incluem-se:

- A implementação de cláusulas contratuais adequadas, inclusive, sempre que possível, um contrato de acordo de nível de serviço com o provedor de serviços em nuvem;
- A prévia avaliação da conformidade do serviço a ser contratado com os requisitos de Segurança da Informação estabelecidos nesta Política; e
- A adoção de controles de acesso apropriados aos serviços em nuvem relacionados a Dados Pessoais, garantido, sempre que possível, a autenticação multifator para acesso aos serviços em nuvem relacionados a Dados Pessoais.

6. **USO ACEITÁVEL**

Todos os usuários dos ativos informacionais disponibilizados pela **PALADIUM** devem utilizar sistemas, aplicações, programas e acessar Informações sempre para finalidades legítimas de negócio, dentro de parâmetros éticos e em conformidade a todas as políticas, normas e diretrizes da **PALADIUM**, protegendo assim, os ativos físicos e as Informações da Companhia, seus clientes, Colaboradores e parceiros comerciais.

Em qualquer caso é **proibido** aos Colaboradores da **PALADIUM**:

- Compartilhar as suas credenciais de acesso (ex. login e senha), inclusive com colegas de trabalho;
- Desativar, ignorar ou, de qualquer outro modo, burlar, as configurações de Segurança em suas estações de trabalho;
- Utilizar dispositivos de armazenamento externos, como pendrives e discos rígidos externos;
- Utilizar dispositivos pessoais para fins de trabalho.

7. **RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

A **PALADIUM** adota o seguinte procedimento para a resposta à Incidentes de Segurança da Informação:

- **Detecção**: é dever de todos os Colaboradores monitorarem o cumprimento e atendimento desta Política, devendo notificar a área de Tecnologia da Informação tão logo detectem qualquer indício de sua violação ou qualquer outra situação que suspeitem tratar-se de um Incidente. Ademais, é dever da área de Tecnologia da Informação monitorar ativamente os sistemas da Companhia para a detecção de potenciais Incidentes de Segurança da Informação.
- **Investigação**: uma vez que tome conhecimento de um Incidente, a área de Tecnologia deverá adotar as medidas necessárias para investigá-lo e verificá-lo e, caso se caracterizem como Incidente envolvendo Dados Pessoais, comunicar ao Encarregado sua ocorrência, prestando todas as Informações necessárias.
- **Contenção e Erradicação:** confirmada a ocorrência do Incidente, a área de Tecnologia, com apoio do Encarregado, se necessário, adotará as medidas necessárias e possíveis para mitigar os seus efeitos e encerrá-lo.
- **Comunicação**: em paralelo, o Encarregado, com apoio da área de Tecnologia da Informação e outras áreas que se façam relevante, se o caso, deverá avaliar os impactos do Incidente nos direitos e liberdades dos Titulares e, se adequado, comunicá-los e à ANPD.
- **Correção**: a área de Tecnologia da Informação deverá adotar as ações necessárias e possíveis para evitar a recorrência do Incidente, corrigindo as falhas e causas raízes identificadas que possibilitaram a sua ocorrência.
- **Registro**: a área de Tecnologia da Informação, em conjunto com o Encarregado, deverá manter registro dos Incidentes identificados, especialmente àqueles envolvendo Dados Pessoais.

8. CONSIDERAÇÕES FINAIS

Esta Política entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

O cumprimento desta Política é obrigatório e é um dever de todos observá-la. Seu descumprimento poderá implicar na aplicação das sanções contratuais e legais aplicáveis. Caso identifique uma não conformidade com esta Política, é obrigação de todos os Colaboradores reportá-la imediatamente através do endereço de e-mail compliance@paladium.ai

← Voltar

Plano de resposta a incidentes

INTRODUÇÃO

O presente Plano de Resposta a Incidentes de Segurança ("Plano de Resposta" ou "Plano") foi desenvolvido para orientar o gerenciamento célere e eficiente de qualquer incidente ou suspeita de incidente que afete a **PALADIUM CORP. DESENVOLVIMENTO DE TECNOLOGIA LTDA.** ("Paladium").

Um "incidente" pode ser definido como qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de uma informação, tal como acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Um incidente pode envolver dados pessoais e/ou informações confidenciais da Paladium e/ou de terceiros.

Para fins deste Plano, "informação confidencial" contempla informações referentes ao negócio ou aos produtos e serviços, softwares, sistemas, planos de negócio, *know-how*, informações técnicas, comerciais, financeiras, parceiros, clientes, marcadas ou não como confidenciais, ou que, devido às circunstâncias ou à própria natureza das informações, devam ser consideradas como confidenciais. Por sua vez, "Dados Pessoais" são informações relacionadas a uma pessoa natural identificada ou identificável, nos termos da legislação vigente.

Exemplos de possíveis incidentes incluem, mas não se limitam a, **(i)** extravio (perda, furto ou roubo) de um dispositivo corporativo contendo informações de qualquer natureza; **(ii)** envio de e-mail para o destinatário errado; **(iii)** exposição de dados e informações em diretório aberto da internet, sem controles de acesso; **(iv)** vulnerabilidades de segurança que permitem o acesso não autorizado a informações em sistemas próprios ou de terceiros; **(v)** ataques maliciosos de *hackers* aos servidores da Paladium ou **(vi)** indisponibilidade dos dados (caso sejam criptografados por um *ransomware*, por exemplo).

O Plano não necessariamente é capaz de atender a todas as particularidades de determinados incidentes, mas traz diretrizes relevantes para que eventuais incidentes sejam contidos e os seus impactos mitigados de forma eficiente.

Todos os envolvidos na execução do Plano deverão manter o incidente sob o mais absoluto sigilo, salvo nos casos em que houver decisão conjunta de comunicação do incidente pelas áreas e colaboradores legitimados, nas hipóteses previstas por este Plano.

I. PROCESSO DE RESPOSTA

A correta e pronta resposta a um incidente é fundamental para minimização dos danos causados aos titulares dos dados afetados, no caso de incidente envolvendo dados pessoais, bem como à Paladium em qualquer tipo de incidente.

Em regra, o procedimento de resposta passa pelas seguintes etapas:

1. Detecção e Avaliação do Incidente

Qualquer colaborador que tenha conhecimento ou suspeita de que um incidente tenha ocorrido deverá reportar a situação imediatamente, com o máximo de detalhes, para a área técnica, por meio do endereço de e-mail compliance@paladium.ai. Caso o colaborador já tenha detectado que o incidente envolve dados pessoais, o Encarregado deverá ser notificado, por meio do endereço de e-mail compliance@paladium.ai. Caso a área técnica não tenha sido envolvida até este momento, o Encarregado deve notificar a área imediatamente.

A área técnica deverá acionar o Diretor responsável pela área técnica, que deverá coordenar a coleta das informações iniciais que julgar apropriadas para uma avaliação preliminar do escopo e identificação do risco do potencial incidente. Quando o incidente envolver dados pessoais, o Encarregado deverá estar envolvido.

Na medida do que seja possível levantar em um momento inicial, as informações devem incluir:

- Quais sistemas, equipamentos, arquivos e demais fontes digitais foram comprometidas;
- Tipo de vulnerabilidade/ataque (por exemplo, erro de configuração, *malware* usado etc.);
- Se o evento é interno ou externo e se alguma empresa, afiliada ou parceira parece ter sido afetada;
- Se o incidente envolve dados pessoais ou dados pessoais sensíveis[1].

Durante toda a resposta ao incidente, desde a avaliação e coleta de informações iniciais, deve-se **documentar** todas as informações recebidas, passos e ações tomadas de uma maneira que tais sejam preservadas como

potencial evidência. Além das informações acima, é importante que se registre **(i)** quem identificou o incidente; **(ii)** quem reportou; **(iii)** para quem foi reportado; e **(iv)** quem tem ciência do incidente, bem como a data e a hora das comunicações.

2. **Contenção da vulnerabilidade e início da mitigação de danos**

2.1 **Correção e Contenção**

Feita a avaliação inicial e identificada gravidade do risco, devem ser tomadas medidas imediatas para conter o incidente e evitar possíveis comprometimentos adicionais e/ou a continuidade de uma eventual vulnerabilidade. Essas medidas podem incluir, mas não se limitar a:

- Correção técnica de eventuais vulnerabilidades sistêmicas e falhas técnicas que podem ter dado origem ao incidente;
- Contato com fornecedores ou prestadores de serviço cujo sistema pode ter dado origem ao incidente para que possam corrigir a vulnerabilidade;
- Isolamento do perímetro do incidente, limitando o acesso a sistemas, equipamentos e ambientes, se necessário;
- Após os passos acima, monitoramento dos servidores para garantir que a falha técnica foi corrigida;
- Reprodução e redundância do ambiente cuja vulnerabilidade foi identificada para permitir a realização de análise dos fatos e evidências;
- Aquisição de uma imagem forense através do disco rígido dos computadores identificados;
- Coleta de informações e registro de todos os acessos que ocorreram durante o período de exposição e seu IP relacionado;
- Checagem dos IPs de maior acesso ao local da vulnerabilidade nos últimos dias para verificar se há algum comportamento estranho, bem como para identificar o local de onde o acesso está ocorrendo.

Nem todas as medidas listadas acima serão aplicáveis a todos os incidentes. Cabe à área técnica verificar aquelas que são apropriadas, bem como sugerir novas ações, conforme o caso.

2.2 **Engajamento do Grupo de Trabalho (GT)**

Em paralelo à correção e contenção do incidente, o Diretor responsável pela área técnica deverá convocar um grupo de gestão de crise ("GT"), que terá composição multidisciplinar, necessária para gerenciar todos os problemas associados a incidentes.

O GT incluirá, ao menos, o Encarregado de Proteção de Dados e/ou um membro do Encarregado para averiguar se o incidente envolve Dados Pessoais, e os representantes da área técnica, do Jurídico e o CEO. A depender da natureza do incidente, representantes de outras áreas podem ser incluídos no GT (por exemplo, se o incidente envolver dados de empregados, representantes da área de Recursos Humanos podem ser envolvidos).

O Diretor responsável pela área técnica nomeará o coordenador do GT, cujas responsabilidades incluirão: **(i)** convocar reuniões do GT; **(ii)** preparar relatos sobre as discussões; **(iii)** preparar atas de reuniões; **(iv)** organizar os prazos e acompanhar pendências de cada uma das áreas e pessoas responsáveis. O GT permanecerá ativo até que o incidente seja totalmente gerenciado de forma satisfatória. Ao longo de todo o procedimento de resposta, o GT será responsável por[2]:

- Coordenar a avaliação do incidente;
- Avaliar a necessidade de realizar as comunicações aos titulares de dados, às autoridades competentes, como a Autoridade Nacional de Proteção de Dados (ANPD), e à imprensa, em função da gravidade do incidente, nos termos da Resolução CD/ANPD nº 15/2024;
- Garantir a preservação de evidências dos fatos e a produção de ambiente de redundância para viabilizar futuras análises;
- Definir todas as ações corretivas e outras que sejam consideradas relevantes para tratar o incidente e suas implicações, incluindo as medidas jurídicas, regulatórias, societárias ou de relações públicas;
- Avaliar a necessidade de suporte de terceiros (como a contratação de peritos especializados, assessoria jurídica externa, agência de comunicação etc.);
- Avaliar a existência de seguros para cobrir eventuais danos causados pelo incidente e a necessidade de acionamento deles.

As responsabilidades acima são do GT como um todo, mas elas devem ser designadas para as pessoas do GT mais aptas para lidar com cada uma das tarefas.

A contratação de aconselhamento de especialistas internos e externos garante imparcialidade nas análises. Em caso de incidente de maior gravidade, é recomendável que isso seja feito tão logo possível.

3. **Avaliação das obrigações legais**

No caso de incidente envolvendo dados pessoais:

3.1. **Avaliação da obrigação de notificação nos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou LGPD) e da Resolução CD/ANPD nº 15/2024**

A LGPD estabelece que o controlador dos dados deverá comunicar à ANPD e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48) e a Resolução CD/ANPD nº 15/2024 estabelece critérios para que o controlador avalie quando um incidente pode acarretar risco ou dano relevante aos titulares.

A Paladium será considerada "controladora" quando tiver o poder e liberdade para decidir sobre como os dados pessoais devem ser tratados.

Caso o incidente envolva Dados Pessoais, o Encarregado, em conjunto com o GT, deve analisar as informações conhecidas sobre o incidente até o momento para identificar **(i)** quais titulares estão envolvidos; e **(ii)** se os Dados Pessoais que foram acessados, divulgados, destruídos ou atingidos de outra forma tem o potencial de causar algum dano ou acarretar risco relevante aos titulares dos dados.

Caso a conclusão seja que o incidente se enquadra em tal critério ou caso a Paladium esteja na dúvida sobre tal enquadramento, é necessário iniciar a preparação de uma notificação à ANPD e outra aos titulares, a partir dos templates de notificação disponibilizados pela ANPD. Para isso, a Paladium deverá reunir as informações exigidas pela Resolução CD/ANPD nº 15/2024, mais especificamente aquelas indicadas no § 2º do art. 6º para a comunicação à ANPD e no art. 9º para a comunicação aos titulares.

Após o GT reunir tais informações, o CEO deverá avaliar o conteúdo da mensagem e abordagem antes do envio à ANPD e aos titulares. A comunicação deverá ser realizada no prazo de três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais.

No caso de incidente que envolva ou não dados pessoais:

3.2 **Avaliação das obrigações legais e contratuais**

Nessa etapa, o GT, com o auxílio do Jurídico, deverá:

- Refinar a avaliação inicial do nível de risco do incidente e identificar, em mais detalhes, os dados afetados (como dados técnicos, dados corporativos estratégicos, dados relacionados à propriedade intelectual da Paladium ou de terceiros, segredos de negócio etc.);
- Avaliar eventuais obrigações legais de reporte;
- Revisar os contratos com clientes e outros parceiros comerciais para identificar a existência de obrigações contratuais de notificação para tais terceiros;
- Avaliar a necessidade ou viabilidade de adotar medidas cíveis ou criminais contra terceiros, relacionadas ao incidente; e
- No caso da existência de seguro cibernético, analisar a apólice de seguros cibernéticos para verificar a cobertura e dever de comunicação de sinistro.

4. **Elaboração e manutenção de um Registro do Incidente**

Após a identificação, correção, contenção do incidente e definição de um plano de ação, o GT deverá trabalhar na elaboração de um Registro completo com as informações sobre o incidente.

A Paladium deve manter o Registro do incidente, inclusive daquele não comunicado à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

Conforme exigido pela Resolução CD/ANPD nº 15/2024, o Registro deverá conter, no mínimo:

- A data de conhecimento do incidente;
- A descrição geral das circunstâncias em que o incidente ocorreu;
- A natureza e a categoria de dados afetados;
- O número de titulares afetados;
- A avaliação do risco e os possíveis danos aos titulares;
- As medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
- A forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
- Os motivos da ausência de comunicação, quando for o caso.

5. **Comunicação**

Se o GT não for formado nas primeiras horas após a detecção do incidente, o Diretor responsável pela área técnica deve solicitar à área responsável que verifique se alguma medida emergencial em termos de comunicação interna, ao público e/ou autoridades competentes deve ser tomada. Para auxiliar na tomada de decisão da área responsável, todas as informações disponíveis serão fornecidas pelo Diretor responsável pela área técnica.

A partir da sua formação, o GT deverá definir, com o auxílio do Jurídico e do CEO, a estratégia, a abordagem e o conteúdo da comunicação para os seguintes destinatários, conforme aplicável: o público interno, as autoridades, órgãos reguladores, parceiros comerciais, clientes e imprensa. No caso de incidente envolvendo dados pessoais, o Encarregado deve auxiliar em tais definições em relação ao titular dos dados e à ANPD, se necessário.

Assim, o GT, em conjunto com as áreas acima, deverá:

- Preparar as comunicações e notificações necessárias;
- Avaliar caso a caso como responder as demandas da imprensa, corrigir ou atualizar matérias com informações relevantes para o negócio;
- Avaliar como calibrar o volume da resposta com relação à repercussão do assunto na mídia e em redes sociais;
- Monitorar comunicações na mídia de forma eficaz e até que o incidente seja solucionado;
- Monitorar os canais de atendimento a clientes e parceiros durante o período de resposta ao incidente e alinhar o *script* utilizado em caso de questionamentos relacionadas ao incidente;
- Avaliar se é o caso de mobilizar porta-voz. Caso seja identificada a necessidade de mobilizar porta-voz para atender demandas de imprensa, deve-se assegurar que estejam capacitados tecnicamente e alinhados com as mensagens do negócio.

II. CLASSIFICAÇÃO DO INCIDENTE

A classificação dos riscos do incidente deverá ser feita preliminarmente pelo Diretor responsável pela área técnica em conjunto com o Jurídico e, se houver

dados pessoais, com o Encarregado. Tal classificação deverá ser sujeita à validação do GT a partir do momento da sua formação.

É atribuição do GT validar a classificação dos riscos, bem como atuar, após sua classificação, de acordo com as diretrizes deste Plano. O Diretor responsável pela área técnica e o Encarregado, se aplicável, bem como o GT em momento posterior, devem considerar os critérios previstos na Resolução CD/ANPD nº 15/2024 para a tomada de decisões quanto à classificação da gravidade do incidente e à condução deste Plano.

CONSIDERAÇÕES FINAIS

Este Plano entrará em vigor na data de sua aprovação e divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

O cumprimento do Plano é obrigatório e é um dever de todos observá-la. Seu descumprimento poderá implicar na aplicação das sanções contratuais e legais aplicáveis. Caso algum colaborador identifique uma não conformidade com este Plano, é sua obrigação reportá-la imediatamente através do endereço de e-mail compliance@paladium.ai.

© 2025 Paladium. All rights reserved.