Política de Segurança da Informação

19/08/2022

Introdução

A informação é um ativo muito valioso para a Apex Group, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.
A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, WEB, FTP, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc e pode estar armazenada localmente (em servidores no Data Center Local, estações de trabalho, mídias eletrônicas, etc) ou no ambiente de computação em Nuvem (Servidores em Data Center remoto – VPC Amazon, localizado em São Paulo).

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

1. **Confidencialidade**: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
2. **Integridade**: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.
3. **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três pilares, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

A proteção da informação não é uma tarefa trivial. Em geral, o sucesso da Política de Segurança da Informação adotada por uma instituição depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e a maneira pela qual são implantados e monitorados,os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de todos os colaboradores, independente do nível hierárquico.

Objetivo da Política de Segurança da Informação

A Política de Segurança da Informação da APEX GROUP é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas pela APEX GROUP no que diz respeito à adoção de procedimentose mecanismos relacionados à segurança da informação.

As diretrizes e controles implementados e utilizados na APEX GROUP se estendem ao ambiente de computação em Nuvem, de forma que venha garantir a prevenção, detecção e mitigação dosriscos de incidentes de segurança.

Estrutura Normativa da Segurança da Informação

Definição

A estrutura normativa da Segurança da Informação da APEX GROUP é composta por umconjuntode documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política de Segurança da Informação (Política)**: constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- **Normas de Segurança da Informação (Normas)**: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- **Procedimentos de Segurança da Informação (Procedimentos)**: instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da APEX GROUP.

Divulgação e Acesso à Estrutura Normativa

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores e fornecedores da APEX GROUP e publicada no site corporativo, na área Compliance, seção Políticas e Manuais, de maneira que seu conteúdo esteja público e permita consulta a qualquer momento.
No A**nexo 4** deste documento, encontra-se a minuta do Termo de Recebimento, Ciência e Adesão a este documento, que deve ser preenchida e assinada por fornecedores, prestadores de serviço e/ou empresas terceirizadas que possuam relações comerciais com a Apex Group e necessidades legítimas de negócio para tal.
Os Procedimentos de Segurança da Informação são restritos ao ambiente de Tecnologia da Informação e devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

Aprovação e Revisão

Os documentos integrantes da estrutura normativa da Segurança da Informação da APEX GROUPdeverão ser aprovados e revisados conforme os seguintes critérios:

- Política-- Nível de Aprovação: Diretor Responsável pela Segurança da Informação
  - Periodicidade de Revisão: Anual
- Normas-- Nível de Aprovação: Security Officer ou Diretor Responsável pela Segurança da Informação
  - Periodicidade de Revisão: Anual
- Procedimentos-- Nível de Aprovação: Security Officer ou Gestor responsável pela área envolvida
  - Periodicidade de Revisão: Anual

Atribuições e Responsabilidades na Gestão de Segurança da Informação

Cabe a **todos os colaboradores (funcionários, estagiários e prestadores de serviços)** da APEX GROUP:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da APEX GROUP;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

- Formalizar a ciência através da assinatura do Contrato de Confidencialidade no momento da contratação e do aceite da Política e das Normas de Segurança da Informação, assumindo responsabilidade por seu cumprimento;

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela APEX GROUP;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela APEX GROUP;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à área de Tecnologia da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

Gestores e suas Responsabilidades

Os gestores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da APEX GROUP, cabendo a eles verificar se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

A área de Tecnologia da Informação poderá realizar auditorias periódicas internas sobre o acesso dos usuários às informações e sua retenção, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

Área de Tecnologia da Informação (Tecnologia da Informação - TI)

- É responsabilidade da área de TI estabelecer, publicar, manter e disseminar normas e políticas de segurança da informação relevantes;
- Medidas estruturais como plano de comunicação, auto avaliação e revisões de auditoria deverão assegurar e monitorar a conformidade com as políticas de segurança;
- Devem ser desenvolvidos padrões e procedimentos para suportar as políticas onde for apropriado;
- As políticas e materiais de conscientização devem ser revisados e publicados anualmente ou sempre que houver mudanças significativas;
- As políticas de segurança da informação são restritas à empresa e devem ser reveladas somente aos colaboradores da APEX GROUP e a terceiros que tenham a necessidade legítima de negócio para conhecê-las;
- Exceções às políticas serão tratadas caso a caso pela área de Tecnologia da Informação. Todas as exceções, caso sejam aprovadas, devem ser documentadas, arquivadas e revisadas anualmente. Para aprovação de exceções serão requeridas justificativas de negócio completas e dependendo da exceção requerida, a aprovação final deve ser apenas fornecida pela diretoria;
- Dar ciência a todos os funcionários e prestadores de serviço que os ambientes, sistemas, recursos computacionais e as redes da empresa poderão ser monitorados.

Penalidades

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, multa, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

Documentos Vinculados

Fazem parte desta Política as seguintes normas que definem as regras e restrições para funcionamento dos serviços:

i. Norma de Uso de e-mail Corporativo;
ii. Norma de Uso de Software;
iii. Norma de Gestão de Acessos;
iv. Norma de Classificação da Informação;
v. Norma de Uso da Internet;
vi. Norma de Acesso Físico;
vii. Norma de Utilização de Senhas;
viii. Norma de Uso Aceitável de Estações de Trabalho, Notebooks e Demais Dispositivos;
ix. Norma de Backup;
x. Norma de Gestão de Incidentes de Segurança;
xi. Norma de Criptografia e Gestão de Chaves
xii. Norma de Desenvolvimento de Sistemas
xiii. Norma para Gerenciamento de Vulnerabilidades
xiv. Norma de Serviços de Computação em Nuvem
xv. Norma de Acesso Remoto via VPN
xvi. Norma de Hardening
xvii. Norma de Reutilização e Descarte Seguro

Aprovações da Política

Este documento foi aprovado pela Diretoria da APEX GROUP, no Comitê de Compliance e RiscosOperacionais.
A via original encontra-se armazenado junto a área de Compliance / Segurança da Informação.
A cópia da via de aprovação é apresentada no Anexo 1.

Norma de Uso do E-mail Corporativo

1. Objetivo

O objetivo desta norma é estabelecer regras e requisitos de segurança para o uso do e-mail corporativo da APEX GROUP.

2. Definição

O e-mail é a ferramenta de comunicação interna e externa necessária para realização dos negócios da APEX GROUP.

3. Utilização do E-mail

1. As mensagens enviadas devem ser escritas em linguagem profissional de forma que não comprometa a imagem da empresa, não viole a legislação vigente, os princípios éticos e valores da APEX GROUP.
2. A utilização do e-mail é individual, sendo o usuário responsável pelo conteúdo enviado através dele. A utilização do e-mail deve ser feita apenas para fins profissionais.
3. Não devem ser enviados e-mails com mensagens ou imagens que:
    1. Possam prejudicar a imagem da APEX GROUP, de seus colaboradores ou dequalquer outra organização;
    2. Contenham declarações difamatórias ou ofensivas de qualquer natureza;
    3. Contenham informações preconceituosas com qualquer classe, como raça, sexo, idade, religião, condição física, etc.;
    4. Contenham informações pornográficas, obscena ou qualquer outra inadequada para um ambiente profissional;
    5. Que incentivem atividades ilegais;
    6. Sejam classificadas como SPAM, correntes, etc..
4. Não deve ser reproduzido ou divulgado material que infrinja direitos autorais, sem a permissão do autor.
5. Não devem ser enviadas mensagens em nome da APEX GROUP que contenhamopiniões pessoais.
6. Uma mensagem eletrônica é considerada um documento formal da empresa.
7. O conteúdo do e-mail de cada usuário pode ser auditado pela empresa com o objetivo de garantir a segurança e integridade de seu negócio. O acesso ocorrerá a critério da empresa mediante comunicação ao superior imediato e à área de Tecnologia da Informação.
8. Mensagens recebidas de origens desconhecidas ou suspeitas devem ser removidas da caixa de entrada imediatamente desde que não sejam necessárias para análise e/ou registro de incidente de segurança.
9. Ao enviar uma mensagem, procure incluir apenas os destinatários interessados no assunto. Cópias desnecessárias sobrecarregam os recursos e causam excesso de conteúdo nas caixas de entradas.
10. Caso o colaborador cometa o equívoco de relacionar destinatários que não deveriam ter acesso ao conteúdo da mensagem, este deve notificar imediatamente seu gestor direto e, quando necessário, as áreas de Compliance e Segurança de Informação que a tomada das devidas providências.
11. Ao enviar uma mensagem de correio eletrônico, ela está restrita a você e ao (s) destinatário (s). Porém, no caso de informações que exijam um maior sigilo, você deve indicar na primeira linha da mensagem o nível de classificação dessa informação, dentre os níveis de confidencialidade descritos na Política de Segurança - Classificação da informação.
12. É proibida a edição e adulteração de e-mails ou cabeçalhos de e-mail, de forma que seja preservada a mensagem original em casos de resposta e encaminhamento.
13. Caso receba uma mensagem enviada por engano, proceder da seguinte maneira:
    1. caso seja uma mensagem do domínio ***apexgroup.com***, informe ao remetente

oocorrido e remova a mensagem da sua caixa;

2. caso não seja do domínio *apexgroup.com*, simplesmente remova a mensagemda sua caixa.

Arquivos em anexo

1. Enviar arquivos anexados somente quando for imprescindível. Cuidado quando estiver repassando (Encaminhar/Forward) mensagens para não repassar desnecessariamente arquivos anexados.
2. Garantir que cada um dos arquivos anexados possua o seu nível de confidencialidade da informação de acordo com a Política de Segurança – Norma de Classificação da Informação.
3. Arquivos recebidos de remetentes desconhecidos não devem ser abertos e a mensagem deve ser removida. Salvo exceções de equipes capacitadas e autorizadas àanálise. Acionar a Área de Tecnologia da Informação caso necessário.

Gestão do Correio Eletrônico

1. Não compartilhe a sua senha de acesso ao ambiente de rede e ao correio eletrônico com nenhum outro usuário.

4. Conclusão

O não cumprimento das regras descritas nesta norma constitui falta grave e o usuário está sujeito a penalidades administrativas e/ou contratuais.
Situações não previstas e sugestões devem ser encaminhadas à área de Tecnologia da Informação.

Norma de Uso de Softwares

1. Objetivo

O objetivo desta norma é definir um padrão para utilização de programas de computador de forma legal e segura dentro da APEX GROUP.

2. Abrangência

Esta norma se aplica a todos os usuários (colaboradores e prestadores de serviço) que utilizam tanto localmente e quanto remotamente o ambiente computacional da APEX GROUP.

3. Definições

Direito autoral - Referente ao rol de direitos aos autores de suas obras intelectuais. **Licença de software** - É uma definição de ações autorizadas ou proibidas, no âmbito do direitode autor de um programador de software de computador concedidas ou impostas ao usuário deste software.
Disco Virtual - Ferramenta online para armazenamento de arquivos em nuvens, ou seja, em um ambiente *Web* acessível por qualquer computador, de qualquer local.

4. Utilização de Programas

1. Todos os direitos autorais devem ser respeitados e jamais violados.
2. Todos os programas de computador devem estar devidamente licenciados e as mídias originais devem ser devidamente protegidas contra cópia.
3. A instalação somente poderá ser feita pelos analistas da área de Tecnologia da Informação da APEX GROUP, salvo as exceções autorizadas pelo gestor.
4. As estações de trabalho disponibilizadas para uso dos colaboradores ou prestadores de serviço serão auditadas e monitoradas conforme as premissas de segurança. Os equipamentos que não estiverem de acordo serão retirados da rede.
5. A utilização, para fins profissionais, de ferramentas online para armazenamento,colaboração e compartilhamento de informações em nuvem (discos virtuais), deverá ser feita com cuidado e apenas pelo período de tempo necessário. A informação deverá ser removida imediatamente após seu uso ou compartilhamento. Observar e respeitar a Política de Classificação da Informação.

5. Uso de Antivírus

Todo arquivo em mídia proveniente de entidade externa a Apex Group deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente WEB, FTP, HD Externo/PenDrive, e similares deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pela área de Tecnologia da Informação.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

6. Software Desenvolvido Dentro da Apex Group

Todo software, componente ou artefato de software produzido dentro da Apex Group é de propriedade da empresa.

7. Conclusão

O não cumprimento das regras descritas nesta Norma constitui falta grave e o usuário está sujeito a penalidades administrativas e/ou contratuais.
Situações não previstas e sugestões devem ser encaminhadas à área de Tecnologia da Informação.

Norma de Gestão de Acessos

1. Objetivo

Esta norma tem como objetivo definir o processo de gestão de acessos de funcionários, estagiários e prestadores de serviços aos sistemas da APEX GROUP, além de estabelecer padrões para gerenciamento de contas e senhas.

2. Abrangência

Esta norma se aplica a todos os usuários da APEX GROUP.

3. Responsabilidade

A gestão de acessos ao ambiente e sistemas da Apex Group é de responsabilidade da área de TI.Exceções deverão ser analisadas e documentadas.

4. Controle de Acessos Baseado em Função - RBAC

Os acessos serão concedidos baseados na Matriz de Controle de Acessos Baseado emFunção (RBAC).

Na matriz são definidas as funções existentes na área e os perfis de acesso e transações previamente autorizadas a sistemas, pastas de rede e demais recursos sistêmicos e computacionais pertinentes à função. As permissões de acesso, transações e perfis declaradas na Matriz RBAC são definidas pelo Gestor da área.

Qualquer alteração nas permissões de acesso definidas deve ser autorizada pelo gestor responsável pela função. Novos perfis só podem ser definidos e implantados mediante autorização do gestor.

Caso a área não possua a Matriz de Controle de Acessos Baseado em Função definida, os acessos a sistemas e recursos deverão ser solicitados e aprovados pelo gestor.

5. Concessão e Revogação de Acessos

5.1 Admissão e Movimentação Funcional de Funcionários / Estagiários / Prestadores de Serviços

A área de Recrutamento e Seleção de Pessoal da empresa ou o gestor responsável pela contratação deverá informar a área de Tecnologia da Informação, através de registro de chamado, toda e qualquer contratação, ausência, férias ou movimentação funcional (transferência de área) de funcionários, estagiários e/ou prestadores de serviços. Deverá ser informado o nome do funcionário, estagiário ou prestador de serviço, a área onde o mesmo irá desempenhar suas atividades, a função que o mesmo irá exercer, a data de início na função.

Os acessos serão atribuídos conforme definições da Matriz de Controle de Acessos Baseado em Função (RBAC).

De posse dessas informações, a área de Tecnologia da Informação irá fazer a concessão dos acessos atribuídos à função ou solicitados e repassar as credenciais de acesso ao colaborador.

Nos casos de movimentação funcional, os acessos serão ajustados de acordo com a nova função desempenhada. Os acessos que não forem mais necessários para exercer a nova função serão revogados.

No caso de prestadores de serviços deverá também ser informado o tempo em que o mesmo prestará serviço á Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

Cabe a área de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação.

5.2. Desligamento de Funcionários / Estagiários / Prestadores de Serviços

No caso de desligamento ou afastamento de funcionários, a área de Recursos Humanos ou o gestor responsável pelo funcionário, estagiário ou prestador de serviço deverá comunicar o fato o mais rapidamente possível a área de Tecnologia da Informação, para que os acessosinternos e externos à APEX GROUP sejam revogados de maneira tempestiva. E caso seja necessário auditoria posterior caberá ao gestor responsável solicitá-lo.

6. Acesso a VPN

O acesso a VPN será autorizado e liberado para que os colaboradores possam acessar de maneira remota o ambiente da APEX GROUP.

Todas as solicitações devem ser efetuadas pelo Gestor da área solicitante para a área de Tecnologia da Informação via sistema de Help Desk, informando o *login*, cargo ou função e a justificativa/necessidade.

Os acessos serão concedidos após análise da área de Tecnologia da Informação.

A área de Tecnologia da Informação irá orientar o usuário sobre os procedimentos necessários para utilização da VPN para acesso remoto do ambiente da empresa.

Norma de Classificação da Informação

1. Objetivo

Esta norma tem como objetivo definir requisitos para classificação da informação de forma a assegurar que as informações da APEX GROUP recebam um nível adequado de proteção.

2. Escopo

Todos os usuários da informação da APEX GROUP.

3. Definições

Classificação da informação - Processo através do qual o proprietário da informação atribui um grau de sigilo às informações.
Grau de sigilo – Graduação atribuída a ativos de informação considerados sigilosos em decorrência da sua natureza ou conteúdo.
Informação - Recursos de informação são definidos como qualquer dado criado, coletado, comunicado, usado ou observado por qualquer usuário de informação durante o seu período empregatício ou relacionamento com a APEX GROUP.
Sigilo - Segredo de conhecimento restrito a pessoas credenciadas, proteção contra revelação não autorizada.

4. Introdução

Toda informação, independente da forma como seja apresentada: arquivos eletrônicos, mensagens eletrônicas, WEB, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo (não se limitando apenas a estes), manipuladas no ambiente do escritório deverão indicar o nível de classificação da informação.
Toda e qualquer outra forma de exposição da informação da APEX GROUP deve ser classificadae ter explícito o seu nível de confidencialidade.

5. Gestor da informação

1. Todas as informações e ativos associados aos recursos de processamento da informação devem ter um gestor que será responsável pela segurança dos mesmos.
2. É responsabilidade do gestor definir a classificação das informações e dos sistemas sob sua responsabilidade, realizar revisões periódicas e efetuar reclassificações quando necessário de forma a assegurar que os recursos de informação estejam no nível de classificação adequado.
3. As tarefas de rotina do gestor podem ser delegadas, por exemplo, para um custodiante que cuide do ativo/informação no dia-a-dia, porém a responsabilidade pela informação permanece com o gestor.

6. Níveis de classificação da informação

O grau de sigilo para os negócios da APEX GROUP considera os níveis descritos a seguir:

Níveis de classificação	Definição
Confidencial	É o mais alto grau de sigilo e deve ser aplicado a informações estratégicas que somente devem ser de conhecimento de um grupo específico de pessoas. São considerados originariamente restritos, e devem ser classificados como tal, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco, dano, dificuldade ou penalidade significativa para a APEX GROUP, seus clientes, parceiros comerciais ou funcionários. Ex: Informações financeiras, planos estratégicos, informações jurídicas, dados de portadores de cartão, etc.
Interna	São informações de uso interno, com circulação exclusiva dentro da empresa. Estas informações podem estar disponíveis a alguns ou a todos empregados, terceiros, prestadores de serviço e parceiros comerciais a serviço da APEX GROUP. Exemplo: Documentos de serviços e produtos, ocatálogo telefônico da empresa, procedimentos operacionais, alguns anúncios de emprego, organogramas, memorandos e manuais gerais internos são restritos ao uso exclusivo da empresa. **Qualquer informação não rotulada deve ser considerada como "Proprietária".**
Pública	São passíveis de classificação Pública informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança com relação a acesso ou guarda. O sigilo da informação não é vital para a empresa. Exemplo: Informações de marketing, notícias, site corporativo, relatórios anuais, etc. Material de propaganda e informativos, relatórios e outros devem ser considerados confidenciais até o momento de sua divulgação.

7. Mesa Limpa

A Mesa Limpa é um programa que estabelece que todos os colaboradores tem responsabilidades ao manusear as informações da APEX GROUP. Por isso, nenhuma informação da APEX GROUP deve ser exposta sem cuidados especiais dentro ou fora do ambiente de trabalho, seja ela eletrônica ou em papel.

Todos os funcionários, estagiários e prestadores de serviços da APEX GROUP devem assegurar que as informações internas restritas não sejam acessadas por pessoas não autorizadas.

Documentos contendo informações classificadas como Confidenciais ou Restritas devem permanecer dentro de gavetas ou armários trancados, evitando serem deixados sobre as mesas quando o funcionário, estagiário ou prestador de serviço se ausentar por períodos longos. Documentos que forem enviados para serem impressos nas impressoras devem ser recolhidos imediatamente por quem originou a impressão.

Da mesma forma, dispositivos de armazenamento de dados devem estar trancados em local seguro quando não estiverem em uso. Qualquer violação da política deve ser relata imediatamente ao superior.

O acesso à tela do monitor e o acesso ao microcomputador deve ser bloqueado sempre quando o funcionário se ausentar de sua mesa. Automaticamente após algum tempo o sistema operacional é bloqueado sendo necessário entrar com o *login* para desbloquear.

8. Compartilhamento de Informações

Não é permitido o compartilhamento de pastas locais dos micros dos funcionários da APEX GROUP. Todos os dados deverão ser armazenados nos Servidores da Rede, e o controle de acessos e credenciais é gerenciado pelo Servidor "AD"(Controlador de Domínio - *Active Directory*).

A área de Tecnologia da Informação verifica periodicamente todos os compartilhamentos locais existentes nas estações de trabalho a fim de garantir que dados considerados confidenciais e/ou restritos deixem de estar armazenados na rede.

O uso das multifuncionais deve estar sujeito às autorizações de acesso gerenciadas pelo sistema proprietário do fabricante associado ao AD e limitados a cada área.

9. Descarte das Informações

As informações armazenadas em arquivos e diretórios e que não serão mais utilizadas deverão ser apagadas e removidas das lixeiras do sistema operacional.
Mídias contendo informações confidenciais ou sensíveis que não devam ser mantidas por mais tempo devem ser descartadas de forma segura, conforme disposto abaixo:

- Discos rígidos: formatação segura (no mínimo 7 passagens) ou inviabilizar fisicamente a utilização do disco.
- Discos magnéticos flexíveis: desintegrar, incinerar, triturar ou derreter.
- Fita magnética: desmagnetizar, triturar, incinerar, pulverizar ou derreter.
- USB "thumb" drives, smart cards, e mídia digital: incinerar, pulverizar ou derreter.
- Discos óticos (CDs e DVDs): destruir a superfície ótica, incinerar, pulverizar, triturar ou derreter.
- Cópias impressas (recibos de papel, relatórios e faxes): fragmentação, fragmentação cruzada, incineração ou transformação em polpa.

10. Conclusão

As situações específicas devem ser registradas junto à Área de Tecnologia da Informação da APEX GROUP.
Fica estabelecido que qualquer informação de cliente será sempre classificada como confidencial e só poderá ser divulgada, mesmo para pessoas da APEX GROUP, com expressa autorização.
Informações da APEX GROUP que não estejam em áreas públicas devem, da mesma maneira, serem tratadas como informação confidencial e somente podem ser divulgadas, com expressa autorização do detentor da informação.

Norma de Uso da Internet

1. Objetivo

Definir os requisitos e as regras de segurança para o uso da Internet no ambiente da APEX GROUP.

2. Abrangência

Esta norma se aplica a todos os usuários (funcionários, prestadores de serviço e estagiários) que utilizam o ambiente de tecnologia da APEX GROUP.

3. Proteção da informação

O ambiente de internet deve ser usado para desempenhar as atividades profissionais do usuário para a APEX GROUP. Os acessos realizados nesse ambiente são monitorados pela APEX GROUP com o objetivo de garantir o cumprimento dessa política.

Os recursos de tecnologia da APEX GROUP, disponibilizados para os usuários, tem comoobjetivo a realização de atividades profissionais. A utilização dos recursos de tecnologia com finalidade pessoal é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança da APEX GROUP.

4. Regras para os usuários

1. O usuário não deve alterar a configuração do navegador da sua máquina no que diz respeito aos parâmetros de segurança.
2. Quando estiver acessando a internet o usuário não deve acessar sites ou executar ações que possam infringir direitos autorais, marcas, licença de software ou patentes existentes.
3. Nenhum material com nível de sigilo "Confidencial" pode ser disponibilizado fora do ambiente monitorado da APEX GROUP.
4. Nenhum material ofensivo ou hostil pode ser disponibilizado no ambiente da APEX GROUP.
5. É proibido e considerado abuso:
    1. A visualização, compartilhamento, *streaming*, cópia e acesso WEB de conteúdos que não estejam relacionados à atividade profissional, tais quais:
        1. de cunho sexual, pornográfico e de pedofilia;
        2. que defendam atividades ilegais;
        3. que menosprezem, depreciem e incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, religião, nacionalidade.
    2. A transferência ou cópia de grandes quantidades de arquivos de vídeo, som, ou gráficos não relacionados aos interesses de negócios da companhia. Este tipo de ação afeta diretamente os recursos de rede.
    3. Participação em:
        1. qualquer discussão pública sobre os negócios da companhia, através do uso de salas de chat, comunidades virtuais, grupos de discussão, ou qualquer outro tipo de fórum público, a menos que autorizado pela Diretoria.
    4. Distribuição de informações confidenciais da APEX GROUP.
    5. Transferência e compartilhamento (downloads/uploads) de arquivos e programas ilegais.

5. Conclusão

O não cumprimento das regras descritas nesta Norma constitui em falta grave e o usuário está sujeito a penalidades administrativas e/ou contratuais.
Situações não previstas e sugestões devem ser encaminhadas à área de Tecnologia da Informação.

Norma de Acesso Físico

1. Objetivo

Esta norma tem como objetivo definir regras para prevenir acesso físico não autorizado, danos e interferência nas instalações e informações da APEX GROUP.

2. Abrangência

Esta norma se aplica a todos os colaboradores e visitantes.

3. Definições

Colaborador: Refere a funcionários e estagiários em tempo integral ou meio período, empregados temporários e prestadores de serviços que estejam residentes nas dependências da APEX GROUP.
Visitante: É definido como um fornecedor, convidado de um colaborador, pessoal de serviços ou qualquer um que necessite entrar nas dependências da APEX GROUP por um curto período detempo, normalmente não mais que um dia.

4. Perímetro de segurança física

1. O acesso às dependências da APEX GROUP deve ser restrito somente ao pessoalautorizado.
2. Os visitantes, durante permanência no ambiente do escritório, deverão estar acompanhados de um funcionário.

5. Controle de Acesso Físico

O ambiente físico da APEX GROUP possui controle de acesso através de Cartão de Proximidade e código, onde a leitora conta com um gerenciador embutido (*Stand Alone*), com exceção do *Datacenter*. Este também com acesso por cartão de proximidade tem gerenciador de acesso separado da leitora com registro epossibilidade de auditoria.

Cada funcionário possui um cartão de proximidade com identidade única e cada ambiente controlado possui o seu controle de acesso.

A configuração das permissões é realizada pelo departamento de Tecnologia da Informação, onde somente os funcionários deste tem permissão para configurar os dispositivos de controle, mediante a liberação pela Diretoria Executiva.

O controle e mapeamento dos cartões de proximidade e acessos é efetuado na planilha "***ControleDeAcessoECracha_Apex.xlsx***". A planilha é atualizada sempre que aconteceuma contratação, movimentação funcional ou desligamento de funcionário.

6. Acesso ao Data Center

O acesso ao Data Center é permitido apenas a funcionários previamente autorizados.

Os funcionários da área de Tecnologia da Informação estão autorizados a acessar o Data Center. Além deles, o Gestor da área Administrativa também tem autorização para acessar o Data Center em situações excepcionais.

Os visitantes somente podem ter acesso ao Data Center mediante autorização da área de Tecnologia da Informação. A visita deverá ser acompanhada durante toda a

permanência do visitante por funcionário da Área de Tecnologia da Informação. O registro contendo os dados do visitante, bem como data e horários de entrada e saída, devem ser feito na Planilha de Visitante do Data Center.

7. Segurança de equipamentos

1. Os locais de armazenagem de informações confidenciais devem ser protegidos a fim de evitar o acesso não autorizado.
2. Não é permitido comer, beber ou usar ferramentas que possa produzir fumaça dentro das instalações do Data Center ou em salas que suportam a infraestrutura da APEX GROUP.
3. Caso se ausente do seu local de trabalho, o colaborador deve bloquear o acesso a sua estação de trabalho ou terminal, evitando que outras pessoas possam utilizá-lo em seu lugar.
4. O cabeamento de redes deve ser protegido contra interceptação não autorizada ou danos, por exemplo, pelo uso de conduítes ou evitando trajetos que passem por áreas públicas.
5. Dispositivos de segurança concedidos a Colaboradores são de uso individual e intransferível e devem sempre estar em posse do seu portador.

8. Remoção de propriedade

1. Equipamentos, informações ou softwares não devem ser movidos ou retirados do local sem prévia autorização.
2. Os funcionários e/ou fornecedores que tenham autoridade para permitir a remoção de ativos devem ser claramente identificados.
3. Devem ser estabelecidos limites de tempo para retirada de equipamentos do local e a devolução deve ser controlada.
4. Deve ser feito um registro da retirada e da devolução de equipamentos, quando do seu retorno.

9. Circuito fechado de TV (CFTV)

1. Existe, no escritório, um sistema de circuito fechado de televisão (CFTV) para monitorar todas as dependências da APEX GROUP com gravação de imagens em 24x7.
2. Os arquivos ou cópias destes, com imagens gravadas somente poderão ser entregues a autoridades mediante ordem judicial, ou a quem requisitar após autorização do gestor da informação.

10. Gravação telefônica

1. Todos os ramais da APEX GROUP são gravados através do sistema automático degravação.
2. Os arquivos com as gravações telefônicas devem ser guardadas em local com controle de acesso e livre de agentes que possam causar danos as mesmas.
3. A liberação ou reprodução de qualquer mídia deve ser aprovada pelo diretor da área envolvida ou substituto aprovado mediante solicitação formal justificada.

11. Conclusão

O não cumprimento das regras descritas nesta Norma constitui em falta grave e o usuário está sujeito a penalidades administrativas e/ou contratuais.
Situações não previstas e sugestões devem ser encaminhadas à área de Tecnologia da Informação.

Norma de Utilização de Senhas

1. Objetivo

Esta norma tem como objetivo definir regras para uso de *login* e senhas para acesso a sistemas da APEX GROUP.

2. Abrangência

Esta norma se aplica a todos os funcionários, estagiários e prestadores de serviços com acessos autorizados a sistemas e ambientes computacionais e de rede da APEX GROUP

3. Credenciais para acesso a sistemas e ambiente de rede

As contas devem ser únicas, nominais e de uso individual e não devem ser compartilhadas em hipótese alguma.

As senhas são confidenciais e não devem ser divulgadas a nenhuma pessoa, seja ela da APEX GROUP ou não. Nenhum funcionário está autorizado a solicitar ou divulgar senhas de acesso de outras pessoas ou suas. Caso isso ocorra, será necessária comunicação ao Gestor.

Recomenda-se a utilização de senhas complexas, ou seja, utilizar, pelo menos, três das quatro opções: letras maiúsculas, minúsculas, caractere especial e ou número. As senhas utilizadas em outros locais, como bancos e sites específicos não devem ser reutilizadas na APEX GROUP, além disso, não devem ser utilizadas senhas com informações pessoais, como datas ou nomes conhecidos.

A senha deve ter no mínimo 8 caracteres.

Toda senha deve ser trocada periodicamente.

Sistemas de autenticação deverão expirar as senhas periodicamente (60 dias).

As senhas que forem armazenadas em qualquer ferramenta de gestão de senhas, devem ser criptografadas. A senha jamais deve estar disponível para a leitura de outras pessoas.

A criação de uma conta privilegiada para tarefas administrativas deve ser aprovada pelo time responsável pelo sistema.

As senhas administrativas ou de usuários com privilégios elevados (*root*, *admin*, etc.) não devem ser armazenadas de forma insegura. São considerados exemplos de forma insegura de armazenamento (não se limitando a eles): arquivos texto, arquivos que não estejam criptografados, de forma escrita, etc. Recomenda-se usar gerenciador de senhas com senha mestra.

A sessão da estação ou servidor deverá ser bloqueada assim que o usuário ou administrador se ausentar do local, independente do tempo.

O titular da conta será o único e exclusivo responsável por qualquer ocorrência que envolva o servidor.

Contas de usuários desligados devem ser imediatamente bloqueadas.

Novas senhas (iniciais ou reinicializadas) devem ser transmitidas de maneira segura, utilizando-se ferramentas ou métodos que garantam o sigilo das mesmas.

4. Conclusão

Qualquer tentativa de executar operações não permitidas poderá ser tipificada ou caracterizada como violação da Política de Segurança da Informação.

Norma de Uso Aceitável de Estações de Trabalho, Notebooks e Demais Dispositivos

1. Objetivo

Esta norma tem como objetivo definir as regras para uso dos recursos de computação oferecidos pela APEX GROUP a seus funcionários, estabelecer padrões de uso de Software (Programas, Sistemas) e Hardware (Estações de Trabalho e Notebooks).

2. Utilização de Equipamentos – Estações de Trabalho e Notebooks

Os usuários de computadores (desktops, notebook e/ou dispositivos móveis), ou qualquer outro equipamento computacional, de propriedade da APEX GROUP, devem estar cientes que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido sem autorização e/ou acompanhamento da área de Tecnologia da Informação.

Alguns cuidados devem ser observados:

Fora do escritório (com ou sem acesso remoto a rede interna da Apex Group):

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Não solicitar ajuda de estranhos;
- Manter sempre o equipamento com acesso bloqueado caso não esteja distante ou não utilizando o equipamento, mesmo que temporariamente;
- Atenção ao transportar o equipamento na rua.

Em caso de furto ou perda

- (Furto) Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e a área de Tecnologia da Informação;
- (Furto) Envie uma cópia da ocorrência para as áreas de Tecnologia da Informação e Administrativo.

Utilização de Dispositivos Pessoais

É proibida a utilização de dispositivos pessoais (notebooks, laptops, celulares, entre outros) no ambiente computacional da Apex Group (conectar os dispositivos na rede privativa).

Norma de Backup

1. Objetivo

Definir as diretrizes sobre backup de dados e informações da APEX GROUP.

2. Diretrizes

Todos os dados da APEX GROUP deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da área de Tecnologia da Informação e deverão ser feitas diariamente.Todos os backups além de serem guardados internamente (Servidor de Backup) também são enviados para o serviço de armazenamento em Cloud da *Amazon Glacier* (*Amazon*) fora da estrutura internada APEX GROUP.

Os backups só podem ser acessados e restaurados pela área de Tecnologia da Informação, através de *login* e senha, para evitar que pessoas não autorizadas, dentro e fora da APEX GROUP,tenham acesso a estes dados em caso de perda ou roubo da mídia.

Deverá haver permanentemente um conjunto completo de sistema de backup capaz de restaurar todos os dados da APEX GROUP em caso de sinistro.

Para o servidor de arquivos diariamente é realizado um backup Diferencial dos dados do servidor de arquivos e guardados devidamente no servidor interno de backup.

O acesso a estes arquivos é direto, sem necessidade de descompactação. Somente a área de Tecnologia da Informação tem permissão de acesso aos arquivos de backup para fazer restauração e testes.

O processo de backup é aplicável para todas as informações do ambiente.

Cópia de Segurança de Arquivos em Desktops

Não é política da APEX GROUP o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento diretamente em rede. Nestes e em outros casos, o setor de Tecnologia da Informação deverá alertar ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente ou enviar os mesmos para o servidor de arquivos da APEX GROUP.

Há casos em que existe a necessidade de se fazer backups de e-mails de gerenciadores de e-mails com caixas de correio antigas do tipo POP.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da APEX GROUP.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da APEX GROUP o Setor de Tecnologia da Informação disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup.

Segurança e Integridade de Dados

O gerenciamento dos bancos de dados, incluindo *backup*, restauração e sincronização é responsabilidade exclusiva do setor de Tecnologia da Informação, mais precisamente de seu DBA, assim como a manutenção, alteração e atualização de equipamentos e programas.

Ao longo do dia, um ou mais, ***BACKUPs* DIFERENCIAIS** serão realizados e armazenados pelo período de 24 horas nas mesmas condições de segurança do ***BACKUP* COMPLETO.**

Para os bancos de dados que armazenarem informações de alta relevância operacional e ou informações de terceiros deverão sofrer, **BACKUP INCREMENTAL** que ocorrerá por padrão de hora em hora, mas poderá ser ajustado segundo as necessidades de segurança da informação da aplicação.

Todos os BACKUPS deverão estar catalogados, armazenados em mídias criptografadas e serão administrados segundo o modelo GFS (*Granfather, Father and Son*) de rotação de BACKUPS.

O acesso aos arquivos de BACKUP será restrito apenas ao DBA responsável e ao Administrador de Sistemas.

3. Campo de Aplicação

Este regulamento se aplica aos servidores indicados para realização de backup, de acordo com criticidade e relevância das informações contratualmente exigidas entre APEX GROUP e cliente.
Exemplos de itens aplicáveis:

- Arquivos dos Sistemas Operacionais;
- Servidores Storage;
- Bancos de Dados;
- Máquinas Virtuais (imagens);
- Servidores de E-mail.

4. DEFINIÇÕES

Backup Diferencial: Armazenamento feito a partir do conteúdo alterado desde a realização do último backup full.
Backup Incremental: Armazenamento que faz a inclusão de todos os arquivos novos e modificados desde o último backup full, diferencial ou outro incremental.
Backup Full/Completo: Armazenamento integral de todo o conteúdo selecionado para o processo de backup.
Fileserver: Servidor destinado ao armazenamento de arquivos.

5. REFERÊNCIAS

POP 082 - Acionar Suporte Técnico
REG 004 - Manutenção e Suporte
REG 007 - Controle de Documentos

6. Procedimento de Backup

6.1. Responsabilidades

O gerenciamento dos bancos de dados, incluindo backup, restauração e sincronização é responsabilidade exclusiva do setor de Tecnologia da Informação, mais precisamente de seu DBA, assim como a manutenção, alteração e atualização de equipamentos e programas.

A Diretoria de TI é encarregada dos procedimentos de backup documentados nesta política e, consequentemente, responsável por executar a restauração quando necessário. Além disso, também se responsabiliza por manter o bom funcionamento das mídias de backup e armazená-las sob condições indicadas pelos respectivos fabricantes.

É dever da Diretoria de TI realizar pesquisas frequentes para identificar atualizações de correção do sistema de gestão de backups, assim como novas versões do produto, sugestões de melhorias, entre outros. A equipe deve monitorar

também o tempo de vida e uso das mídias de backup, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

A equipe responsável pelo procedimento de backup também deverá definir quais servidores e respectivos diretórios e arquivos serão incluídos para o armazenamento. Observa-se a prioridade para:

- Arquivos de log dos sistemas;
- Dados e configurações de bancos de dados;
- Arquivos relacionados a serviços de alta criticidade ao negócio;
- Fileservers.

6.2. Procedimento de Backup

Os backups são executados conforme abaixo:

- **Backup Full (Completo)**: Abrange todas as aplicações e é realizado anualmente, com período de retenção de 5 anos, mensalmente, com período de retenção de 1 ano, e semanalmente, com período de retenção de 1 mês;
- **Backup Diferencial:** Abrange todas as alterações e incrementações de dados realizadas desde o último backup full, e é realizado com periodicidade relativa a cada particularidade do servidor, com período de retenção de 1 semana; Ao longo do dia, um ou mais, BACKUPs DIFERENCIAIS serão realizados e armazenados pelo período de 24 horas nas mesmas condições de segurança do BACKUP COMPLETO.
- **Backup Incremental:** Para os bancos de dados que armazenarem informações de alta relevância operacional e ou informações de terceiros deverão sofrer BACKUP INCREMENTAL que ocorrerá por padrão de hora em hora, mas poderá ser ajustado segundo as necessidades de segurança da informação e da aplicação.
- Todos os BACKUPS deverão estar catalogados, armazenados em mídias criptografadas e serão administrados segundo o modelo GFS (Granfather, Father and Son) de rotação de BACKUPS.
- O acesso aos arquivos de BACKUP será restrito apenas ao DBA responsável e ao Administrador de Sistemas.

6.3. Armazenamento dos Dados

Os dados ficam armazenados em servidores storage gerenciados, dentro do período de 1 ano, e após esse prazo o armazenamento é feito em fita magnética e guardado fisicamente em cofres antichamas pelo prazo definido por contrato.

Caso ocorra a limitação física decorrente da capacidade máxima do cofre, a APEX GROUP é responsável por provisionarum novo local igualmente seguro, para que não ocorra interrupções neste processo.

6.4. Descarte de Mídias

As mídias deverão ser inutilizadas de acordo com as recomendações do fabricante (observando as condições de uso), além da necessidade de que o descarte deve ser documentado e registrado através de um método de controle, utilizando preferencialmente as boas práticas propostas pela ABNT NBR ISO/IEC 27002:2013.

O estoque de mídias extras (além das utilizadas no momento) deve ser constantemente mantido, de forma a ser utilizado para qualquer uso emergencial.

6.5. Procedimento de Restauração e Testes Periódicos

Testes de restauração de qualquer tipo de backup devem ser executados pelos seus responsáveis periodicamente e devidamente documentados. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restaurações, é utilizado um formulário de controle rígido de execução dessas rotinas, o qual deve ser preenchido pelos responsáveis e auditado pelo coordenador responsável.

6.6. Ações a Serem Evitadas

Dentre as ações que devem ser evitadas, destacam-se os itens abaixo elencados:

- Descarte de qualquer mídia sem sua inutilização sem as práticas adotadas e sugeridas no capítulo 5.4 deste documento;
- Reutilização de mídias utilizadas por outros softwares de gerenciamento de backup sem a devida formatação.

Norma de Gestão de Incidentes de Segurança

1. Objetivo

Esta norma tem como objetivo definir regras para a gestão de incidentes de segurança da informação de forma que eles sejam identificados, filtrados, analisados e respondidos em tempo hábil e que medidas apropriadas sejam tomadas para que estes incidentes não ocorram novamente.

2. Definições

Incidente de segurança - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou de redes que tragam riscos para nossos ativos e os ativos de nossos clientes.
Vulnerabilidade - Falha no projeto, implementação ou configuração de uma aplicação ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança.

3. Registro e Notificação de Incidentes

1. O gerenciamento de incidentes de Segurança da informação deve incluir, mas não se limitar aos seguintes eventos:
    1. Vazamento de Informações;
    2. Fraude;
    3. Comportamento anormal de sistemas (ex. reinicialização não programada do sistema, mensagens inesperadas, erros anormais em arquivos de log do sistema ou em terminais)
    4. Compartilhamento de senha;
    5. Notificações sobre eventos de segurança (ex. alertas de integridade de arquivos, alarmes de detecção de intrusos, alertas de antivírus, alarmes de segurança física).
    6. Uso indevido de recursos de tecnologia;
    7. Detecção de redes wireless no ambiente da APEX GROUP, etc.

2. O processo de registro e escalonamento de incidentes de segurança deve considerar, mas não se limitar a:
    1. Estabelecimento de processo adequado de registro de incidentes e descrição detalhada de todas as ações para solução de cada incidente de segurança, através do formulário de Registro de Ocorrências(RRO), disponível na seção Compliance em nossa intranet ;
    2. Análise e identificação da causa do incidente;
    3. Notificação do incidente aos membros do comitê de risco operacional e alta diretoria para avaliação de instauração de sala de guerra para tratativas da ocorrência.
    4. A comunicação a clientes, entidades externas e órgãos reguladores, quando aplicável, ficará sob responsabilidade da área de Compliance.;
    5. Notificação da ação para os envolvidos;
    6. Definição e divulgação do comportamento correto a ser tomado;

4. Comunicação de Incidentes de Segurança

1. A área de TI deve estabelecer um ponto de contato que seja conhecido de toda a organização e esteja disponível em regime 24x7 e em condições de assegurar uma resposta adequada e oportuna para os incidentes de segurança.

2. Um processo deve ser estabelecido para identificar vulnerabilidades recentemente descobertas. Procedimentos e padrões devem ser atualizados para endereçar as novas vulnerabilidades se necessário.
3. Procedimentos e padrões devem ser implementados especificando quando, por quem, as autoridades e as agencias regulatórias que devem ser notificadas em caso de incidentes ou vulnerabilidades.
4. Todos os colaboradores devem ser conscientizados sobre os procedimentos para notificação dos diferentes tipos de eventos e vulnerabilidades que possam causar incidentes de segurança.
5. É esperado que os colaboradores permaneçam vigilantes a respeito de possíveis atividades fraudulentas.
6. Todos os incidentes e/ou vulnerabilidades de segurança devem ser imediatamente reportados ao ponto de contato designado na área de TI.
7. Quaisquer erros de software descobertos ou suspeitas de vulnerabilidades em sistemas devem ser reportados imediatamente para o gestor do sistema e também para o responsável pela segurança da informação.
8. Deve ser estabelecido procedimento formal de registro e escalonamentoestabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação.
9. Informações relacionadas a incidentes de segurança devem ser divulgadas somente por pessoas autorizadas.

5. Tratamento de Incidentes de Segurança

1. Devem ser estabelecidos procedimentos que limitem o tempo de exposição de dados de clientes no caso de perda, roubo ou uso indevido.
2. Pessoal treinado e qualificado deve investigar incidentes/vulnerabilidades pesquisando a natureza e escopo dos mesmos e identificando que sistemas de informações sensíveis e tipos de informações sensíveis foram acessados ou usados indevidamente. Este pessoal deve tomar passos apropriados para conter e controlar o incidente e prevenir mais acessos não autorizados ou uso de informações sensíveis.
3. Incidentes de segurança gerados por falhas de sistema devem ser investigados por técnicos competentes.
4. Os colaboradores responsáveis pelo gerenciamento de incidentes devem sersuportados pelo gerenciamento em todas as solicitações razoáveis de assistência e ferramentas de forma a responder efetivamente a incidentes / vulnerabilidades.
5. O responsável pela Segurança da Informação deve responder de forma rápida e cautelosa aos incidentes de segurança significantes.
6. Caso seja constatada a possibilidade de processo jurídico quando um evento de segurança da informação for detectado, deve-se envolver o departamento jurídico imediatamente para obter consultoria sobre as evidências necessárias.
7. Informações específicas sobre incidentes de segurança, como, por exemplo, detalhes de uma invasão recente de sistema, não devem ser compartilhados com pessoas que não tiverem necessidade de saber justificável.

6. Coleta de Evidências

1. Devem-se estabelecer processos para coleta de evidências relacionadas a vulnerabilidades e incidentes.
2. Evidências relacionadas a suspeitas de vulnerabilidades devem ser registradas e tratadas de acordo com procedimentos de segurança estabelecidos.
3. A divulgação e/ou armazenamento de evidências só poderá ser feito por pessoas autorizadas.

Norma de Criptografia e Gerenciamento de Chaves

1. Objetivo

Esta norma tem como objetivo definir meios criptográficos para proteger a confidencialidade, autenticidade e a integridade das informações da APEX GROUP.

2. Definições

Algoritmo de criptografia - É um conjunto de funções matemáticas que, executadas em um texto, determinam de que forma a mensagem será cifrada.
Criptografia - Métodos de proteção de informações pelos quais apenas os detentores de um determinado segredo denominado "chave", têm acesso a elas. Informações criptografadas, mesmo quando capturadas em trânsito pela rede, não podem ser lidas por quem não conhece a chave necessária.
Chave de criptografia - É um parâmetro que controla a operação do algoritmo de criptografia. A chave especifica a transformação do texto aberto em texto cifrado ou a transformação do texto cifrado em texto aberto.
Confidencial (informação) - Informação que não pode estar disponível ou ser divulgada a indivíduos, entidades ou processos sem autorização.

3. Gerenciamento de Chaves

1. Chaves de criptografia são confidenciais e devem receber tratamento adequado de acordo com o as regras de manuseio, armazenamento e transmissão de informações.
2. Chaves de criptografia não devem ser reveladas para consultores, contratantes ou outros terceiros.
3. Deve haver cópias de backup das Chaves de criptografia.
4. Se for utilizada criptografia para proteger dados sensíveis armazenados em mídia, as chaves criptográficas e os materiais usados no processo de criptografia não devem ser armazenados em qualquer local desta mídia de armazenamento.

4. Geração e armazenamento de chaves

1. As chaves de criptografia devem preferencialmente ser geradas por um software homologado pela organização e quando forem geradas manualmente, devem ser manuseadas por um grupo restrito de pessoas.
2. O uso de algoritmos proprietários de criptografia não é permitido, a menos que seja explicitamente aprovado pela Segurança da Informação.
3. As chaves armazenadas nos dispositivos de criptografia não devem ser mostradas em texto aberto.
4. Os equipamentos utilizados para gerar, armazenar e guardar as chaves devem ser fisicamente protegidos.
5. As chaves de criptografia devem ser armazenadas em local seguro no menor número de localidades possível.

5. Custódia e distribuição de chaves

1. Acesso a chaves de criptografia deve ser limitado a aqueles que tenham necessidade de negócio comprovada.
2. Antes de ter acesso a uma chave de criptografia, o custodiante deve assinar um termo de responsabilidade fornecido pela APEX GROUP declarando comprometimento com a confidencialidade das referidas informações.
3. A distribuição de chaves deve ser realizada preferencialmente de maneira automatizada.

6. Revogação, substituição e recuperação de chaves

1. Toda vez que um novo certificado digital for gerado, o certificado antigo correspondente deve ser revogado.
2. Chaves criptográficas que tenham sido comprometidas ou reveladas devem ser imediatamente revogadas ou substituídas.

Norma de Desenvolvimento de Sistemas

1. Objetivo

Esta norma tem como objetivo definir mecanismos de segurança para o desenvolvimento seguro dos sistemas da APEX GROUP.

2. Abrangência

Esta norma se aplica a todos os sistemas desenvolvidos pela Apex Group ou os sistemasdesenvolvidos para a APEX GROUP por prestadores de serviços de terceiros.

3. Definições

Alta disponibilidade - Técnicas de aumento da resistência a falhas em sistemas, visando aumentar sua disponibilidade.

4. Desenvolvimento e Manutenção de Sistemas

1. Todas as atividades de desenvolvimento e manutenção de sistemas executadas por pessoal interno estão sujeitas às políticas, padrões, procedimentos e outras convenções de desenvolvimento;
2. Princípios de desenvolvimento seguro e práticas específicas e atualizadas pelo gerenciamento devem ser usados para todos os sistemas desenvolvidos ou mantidos internamente.
3. Para todo sistema utilizado por clientes devem ser implementados métodos de alta disponibilidade.
4. Todos os sistemas desenvolvidos internamente ou desenvolvidos para atender a APEX GROUP deverão, em sua fase de homologação, passar por uma avaliação de segurança com o objetivo de identificar possíveis vulnerabilidades ou desvios dos controles de segurança.
5. Para sistemas já existentes antes da publicação desta política, deve ser feita uma análise de custo e de risco para avaliar quais itens devem ser aplicados.
6. Nenhum processo de desenvolvimento de sistemas deve alterar informações dos ambientes de produção. Os dados utilizados em ambiente de testes devem ser mascarados ou fictícios.
7. Dados confidenciais de produção (ex: números válidos de cartão de crédito, CPF, RG, endereço) não devem ser usados para testes ou desenvolvimento. Nos casos onde houver necessidade incontornável de utilização de dados de produção no ambiente de testes, será necessário obter aprovação formal do gestor da informação antes da utilização dos dados.
8. Solicitações de regra no firewall deverão ser avaliadas e autorizadas pela área de TI.
9. Os critérios para seleção de softwares de terceiros ou desenvolvimento terceirizado de software devem incluir os controles de segurança da Política e do Padrão de Desenvolvimento de Sistemas, bem como seguir as determinações da Norma de Uso de Software da APEX GROUP. Exceções devem ser analisadas pela Área de TI.
10. Não é permitida a publicação de sistemas no ambiente de produção que não tenham passado por todas as fases do processo de homologação e análise da área de Segurança. Entende-se por ambiente de produção sistemas acessíveis de uma rede externa e/ou com dados reais.

5. Segregação de Ambientes e Controle de Mudanças

1. Mudanças em sistemas de produção devem ser executadas apenas por administradores de sistemas autorizados.
2. Devem ser implementados controles apropriados para garantir a inexistência de conflito de funções quando do desenvolvimento, manutenção e promoção de sistemas para o ambiente de produção. Para tanto, os colaboradores das áreas de desenvolvimento, homologação e produção não podem executar funções em duas dessas três áreas ao mesmo tempo. Isto somente estará autorizado, caso o colaborador mude oficialmente de área e após a certificação de que este colaborador não carrega nenhum acesso da antiga área.
3. Os ambientes de desenvolvimento e produção devem ser segregados por um ambiente de testes, de forma que as aplicações desenvolvidas ou adquiridas não entrem em produção sem estar devidamente testadas e documentadas.
4. Sistemas em fase de desenvolvimento ou homologação não deverão ser hospedados em ambiente público. No caso de desenvolvimento por terceiros, o ambiente deve ser limitado via firewall.

6. Código Fonte

1. Todos os sistemas desenvolvidos internamente deverão ter um repositório no servidor oficial da APEX GROUP.
2. Consultores e prestadores de serviço terão acesso restrito no repositório oficial da APEX GROUP, devendo ter permissão para acessar única e exclusivamente os repositórios dosprojetos em que estejam alocados.

7. Licença

1. Os códigos de programação desenvolvidos por funcionários ou colaboradores contratadores são de propriedade da APEX GROUP e cabe ao gestor responsável definir o tipo de licença e condições de uso.

Norma para Gerenciamento de Vulnerabilidades

1. Objetivo

Esta norma tem como objetivo estabelecer um processo periódico de identificação, análise e correção de vulnerabilidades.

2. Definições

Ambiente de produção - Infraestrutura ligada diretamente aos produtos e serviços oferecidos aos clientes.
Baseline de Segurança - São determinações de segurança que devem ser aplicadas aos elementos de infraestrutura para garantir que não estejam vulneráveis a ameaças.
Evidência de falso-positivo - É a prova que uma determinada vulnerabilidade não existe para o alvo específico.
Vulnerabilidade - Falha no projeto, implementação ou configuração de um software, aplicação ou sistema operacional que, quando explorada por um atacante, resulta na violação de segurança de um computador.

3. Responsabilidades

TI

1. Executar periodicamente "scan de vulnerabilidades" no ambiente de produção.
2. Gerar relatório de vulnerabilidades.
3. Analisar as evidências para as vulnerabilidades consideradas como falso-positivos.
4. Definir / negociar prazos para correção do ambiente de acordo com sua criticidade.
5. Monitorar a execução das atualizações de acordo com o SLA definido.
6. Avaliar o impacto da mudança para os clientes.
7. Elaborar estratégias para realização das correções de segurança com mínimo impacto para clientes - idealmente, sem nenhum impacto.
8. Executar as correções de segurança nos ambientes sob sua responsabilidade.
9. Organização de planos de ação para descontinuidade de produtos ou funcionalidades legados.
10. Garantir que os baselines definidos estejam aplicados no ambiente.

Todos os colaboradores

1. Notificar imediatamente a área de TI caso identifique vulnerabilidades em qualquer ativo da empresa.

Norma de Serviços de Computação em Nuvem

1. Objetivo

Esta norma tem como objetivo definir conceitos e regras para a gestão dos serviços em Nuvem utilizados pela APEX GROUP, garantindo que todos as diretrizes da Política de Segurança da Informação da APEX GROUP sejam aplicadas e estendidas a esse ambiente.

Os controles implementados e utilizados na APEX GROUP garantem também no ambiente em Nuvem a prevenção, detecção e mitigação dos riscos de incidentes de segurança.

2. Descrição dos Serviços de Computação em Nuvem

Utilizamos um VPC (Virtual Private Cloud) da AWS (Amazon), localizado em São Paulo.

O acesso é restrito por VPN Site-Host.

A definição do prestador de serviço (Amazon) foi baseada nos critérios descritos a seguir:

- A infraestrutura em Nuvem da Amazon possui controles robustos de segurança e proteção de dados;
- Conformidade com as principais regulamentações, normas e práticas de mercado;
- Garantia da Confidencialidade, Integridade e Disponibilidade da Informação;
- Reconhecimento da qualidade dos serviços prestados por todo o mercado.

3. Procedimentos

O gerenciamento dos serviços de computação em Nuvem abrange, não se limitando:

1. Gerenciamento dos servidores e outros ativos já ativos;
2. Provisionamento de novos servidores para atender novas demandas;
3. Gestão de Incidentes de Segurança no Ambiente em Nuvem;
4. Implementação e Gestão de Controles de Segurança da Informação, de forma aimpedir, prevenir, detectar ou mitigar eventuais vulnerabilidades que possam causar incidentes de segurança;
5. Gerenciamento de Billing;
6. Comunicação com Órgãos Reguladores.

4. Comunicação ao BACEN

A contratação de serviços **relevantes** de processamento e armazenamento de dados em nuvem ou alterações contratuais relevantes devem ser previamente comunicadas ao BACEN.

Devem ser indicados nessa comunicação:

1. Nome da empresa contratada;
2. Serviços que estão sendo contratados;
3. Indicação da localidade (País, estado, cidade) onde o serviço será prestado;
4. Alterações contratuais (quando aplicável).

A comunicação deverá ser realizada no prazo máximo de 10 (dez) dias após a contratação ou alteração contratual do serviço.

5. Segurança e Compliance – Amazon

A Amazon fornece papers onde são descritos, de forma ampla, seus principais controles que garantem segurança, privacidade, disponibilidade conformidade.

Os papers estão disponíveis através dos links a seguir:

Compliance: http://aws.amazon.com/pt/compliance/

Segurança: http://aws.amazon.com/pt/security/

O conteúdo dos papers está disponível nos anexos dessa Política.

Norma de Acesso Remoto via VPN

1. Objetivo

Esta norma tem como objetivo definir as diretrizes para acesso remoto via VPN..

2. Diretrizes

Todas as solicitações devem ser efetuadas pelo Gestor da área solicitante para a área de Tecnologia da Informação via sistema de Help Desk, informando o *login*, cargo ou função e a justificativa/necessidade.

Os acessos serão concedidos após análise da área de Tecnologia da Informação.

O acesso a VPN será autorizado e liberado para que os colaboradores possam acessar de maneira remota o ambiente da APEX GROUP.

O acesso remoto poderá ser utilizado quando houver necessidade de trabalho via Home Office, quando houver impossibilidade de acessar o escritório, durante exercícios de contingência (Plano de Continuidade de Negócios) ou em outras situações não citadas e que gerem esta necessidade.

A área de Tecnologia da Informação irá orientar o usuário sobre os procedimentos necessários para utilização da VPN para acesso remoto do ambiente da empresa, de modo a garantir a segurança dos dados da instituição.

Norma de Hardening

1. Objetivo

Esta norma tem como objetivo implementar o processo constante de blindagem (*hardening*), ou seja, mapeando ameaças, mitigando riscos e executando atividades preventivas, a fim de antecipar ataques que possam vir a impactar ativos/serviços de informação ou recursos computacionais.

2. Definições

Ameaça – Causa potencial de um incidente.
Ativo – Tudo aquilo que possui valor para a organização.
Hardening – Processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque
Risco – Efeito da incerteza sobre os objetivos de segurança da informação da Apex Group.
Segurança da informação (SI) – Conjunto de boas práticas que visam a preservação das propriedades de confidencialidade, integridade e disponibilidade das informações.
Usuários – Empregados com vínculo empregatício de qualquer área da Apex Group, ou terceiros alocados na prestação de serviços da organização, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a acessar, utilizar ou manipular qualquer ativo de informação da Apex Group para o desempenho de suas atividades profissionais.

3. Diretrizes

Este documento visa descrever as configurações e procedimentos que devem ser adotados em ativos das instalações da Apex Group, como dispositivos conectados em uma rede específica, incluindo dispositivos de rede, estações de trabalho, servidores, controladores de domínio, etc. Todos os passos aqui descritos devem ser aplicados em tais ativos, e qualquer desvio do padrão aqui estabelecido deve ser justificado à Alta Direção, além de ser devidamente documentado.

a. Atualizações do Sistema e Software Adicional

Ao fazer uma nova instalação do sistema operacional em um equipamento, todas as atualizações críticas e de segurança disponibilizadas pelo desenvolvedor, a um prazo máximo de 30 dias, devem ser aplicadas. Para as instalações atuais do sistema operacional, o processo de atualização de correções deve garantir que todas as atualizações críticas e de segurança disponibilizadas pelo desenvolvedor ou fabricante sejam, da mesma forma, aplicadas em no máximo 90 dias a partir de sua data de liberação.

b. Conexões de Rede Sem Fio em Servidores

Uma conexão sem fio, principalmente em âmbito corporativo, torna-se uma porta de entrada fácil para agentes mal intencionados. Portanto, deve-se garantir que todos os servidores corporativos estejam conectados à rede de forma cabeada. Caso o servidor possua qualquer tipo de placa de rede wireless, deve-se garantir que esta esteja desabilitada.

c. Política de Senhas Local

A política de senhas local, assim como explicitado na **Norma de Utilização de Senhas** presente nesta Política de Segurança da Informação, utiliza os seguintes parâmetros elencados na tabela a seguir:

Parâmetro	Valor
Maximum Password Age	60 days
Minimum Password Age	0 days
Minimum Password Lenght	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Not Defined

d. Instalação do Antivírus

As estações de trabalho e sistemas devem possuir um antivírus instalado. A instalação do software de antivírus deve ser realizada através do procedimento disponibilizado pelo fabricante ou pela administração da rede, mantendo o padrão de instalação e configuração do software. Deve-se assegurar que a atualização automática do banco de dados do antivírus esteja habilitada, de forma a atuar contra malwares descobertos recentemente.

e. Configuração de Firewall

Para garantir a segurança dos servidores e demais ativos, é recomendado que estejam abertas somente as portas necessárias para o funcionamento dos sistemas, a partir dos protocolos utilizados, de forma a evitar o risco de clientes anônimos se comunicarem em outras portas.
Caso algum servidor da rede possua funções como área de trabalho remota para gerenciamento, estas só devem estar disponíveis por meio de uma conexão VPN, garantindo que agentes mal intencionados e não autorizados não tenham acesso à rede e aos ativos.
O processo de instalação de qualquer dispositivo de rede é embasado através de pontos de qualidade e controle orientados através das melhores práticas dos fabricantes e estão contidos em uma base de dados compartilhada.

f. Checklist de Aplicação de Hardening

Com a finalidade de desenvolver uma ação organizada para executar a atividade de hardening é recomendável que a organização obtenha uma lista contendo todas as etapas necessárias para execução dessa tarefa em seus ativos e sistemas, seja esta proveniente do próprio fabricante, ou utilizando configurações definidas e padronizadas pela própria Apex Group, que estejam de acordo com as boas práticas de hardening.
A lista de verificação precisa estar de acordo com a infraestrutura, configurações de segurança e aplicativos contidos na Apex Group, tomando como base o inventário de ativos.

g. Registro de Logs e Monitoramento

Com a finalidade de garantir a rastreabilidade das ações executadas no ambiente da

Apex Group, devem ser capturados registros de logs dos sistemas de informação, para que seja possível o monitoramento de atividades e, no caso de problemas, a sua mitigação de formaágil.

Devem ser estipulados métodos de proteção para impossibilitar a adulteração e acesso não

autorizado desses registros, inclusive por parte dos administradores do sistema. É preciso garantir que o monitoramento de logs esteja configurado e capturando os dados desejados. O espaço em disco deve ser alocado durante as compilações do servidor para registro. Os registros devem ser armazenados em backup de acordo com as políticas de retenção da Apex Group e, em seguida, liberados para abrir espaço para eventos mais atuais.
Itens como espaço em disco disponível, uso de processador e memória, atividade de rede e até mesmo temperatura devem ser constantemente analisados e registrados para que as anomalias possam ser facilmente identificadas e tratadas.

Norma de Reutilização e Descarte Seguro

1 - Objetivos

A Apex Group, mediante a elaboração e publicação de sua Política de Reutilização e Descarte Seguros de Informações, visa estabelecer maior controle e proteção no gerenciamento do descarte ou reutilização de forma segura das mídias e equipamentos da Apex Group que contenham informações da organização ou sob sua responsabilidade, evitando a perda ou vazamento de informações.

2 -Escopo

Essa política se aplica às mídias (removíveis ou não) e qualquer tipo de equipamento que armazene informações no ambiente da Apex Group, estejam as informações em estado físico ou digital, e deve ser observada por todos aqueles que deles se utilizem de alguma forma no desempenho de suas atividades, tais como empregados, parceiros, prestadores de serviço, colaboradores, fornecedores, estagiários, dentre outros.

3 - Diretrizes Gerais

3.1. A reutilização de mídias e/ou equipamentos, e seu descarte, quando não mais necessários, que contenham informações da organização ou que estejam sob sua responsabilidade, depende de rotinas/procedimentos formais que garantam sua destruição segura e protegida;

3.2. Informações corporativas armazenadas em qualquer tipo de mídia e/ou equipamento em processo de reutilização ou descarte, devem possuir processo específico para tais atividades, em conformidade com as normas e procedimentos aplicáveis;

3.3. Os itens desta norma e a realização dos procedimentos dela decorrentes se sujeitam a fiscalização e/ou monitoramento por parte da área da Segurança da Informação;

3.4. Cada usuário é responsável por todos os atos praticados e ações realizadas a partir da utilização de credenciais de acesso disponibilizadas para seu uso;

3.5. O descarte de itens sensíveis deve ser registrado, sempre que possível, a fim de manter uma trilha de auditoria.

4 - Reutilização e Descarte Seguros

4.1. A inclusão de mídias e/ou equipamentos no processo de reutilização e descarte seguro e protegido deve ser precedido de autorização da área de Segurança da Informação.

4.2. Todas as atividades realizadas pela área responsável pelo descarte/preparação para reutilização mídias e equipamentos, incluindo falhas relacionadas ao processo de acordo com procedimento específico, devem ser registradas.

4.3. Dispositivos de armazenamento (discos rígidos, mídias removíveis etc.) que contenham informação confidencial devem possuir procedimento específico de formatação com processo seguro (Wipe).

4.4. Dispositivos defeituosos cuja formatação não seja possível devem passar por procedimento

para a destruição física, tais como, triturar, desmagnetizar, incinerar ou amassar.

4.5. Documentos físicos

4.5.1. Devem ser disponibilizados nos espaços físicos do ambiente da Apex Group repositórios específicos para descarte de documentos físicos, em locais em que possam ser monitorados;

4.5.2. Os repositórios devem ser verificados e esvaziados, ao menos, uma vez ao dia, pelo responsável do setor designado para o descarte do material.

4.6. Mídias Eletrônicas (Pendrive, CD, DVD, cartões de memória, discos rígidos e outros)

4.6.1. Os dispositivos de mídias a serem reutilizados devem seguir procedimentos pré-estabelecidos que garantam a proteção, segurança e remoção absoluta de seu conteúdo, sem possibilidade de restauração;

4.6.2. Mídias contendo informações corporativas devem ser precedidas da inutilização da informação nela contida antes de seu descarte/destruição, que também deve ser feito de maneira irreversível, como, por exemplo, por meio de trituração;

4.6.3. A remoção dos dados deve ser efetuada com diligência, dentro da própria organização, bem como os procedimentos de destruição lógica e destruição física, de maneira a inibir qualquer possibilidade de restauração.

4.7. Equipamentos de qualquer natureza

4.7.1. Equipamentos que armazenem informações da organização ou que estejam sob sua responsabilidade, para que possam ser locados, transferidos de área, enviados para reparos, destruídos e/ou colocados à disposição da corporação, devem sofrer a prévia inutilização da informação neles contida, seguindo o item anterior;
4.7.2. Equipamentos contendo dados sensíveis que venham a sofrer danos deve-se avaliar os riscos e a pertinência de enviá-los para reparo ou optar pelo descarte e destruição seguros.

5 - Papéis e responsabilidades

5.1. É responsabilidade do colaborador da Apex Group destinar o documento, mídia, equipamento sob sua guarda ou utilização para os repositórios e/ou áreas de descarte.

5.2. Deve haver um ou mais responsáveis por verificar os repositórios e destinar as mídias, equipamentos e documentos para o processo de descarte ou preparo para reutilização.

5.3. Cada setor deve controlar e monitorar qualquer tipo de acesso indevido a informações destinadas para descarte, levando o assunto ao conhecimento dos superiores, quando necessário.

5.4. Aqueles que acessarem sem autorização informações destinadas a descarte podem ser responsabilizados.

6 - Sanções e Punições

6.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política e/ou demais normas e procedimentos de segurança, sãopassíveis decorreções e/oupenalidades, a depender da gravidade da violação;

6.2. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a Apex Group, o infrator será responsabilizado pelos prejuízos, cabendo, ainda, aplicação dasmedidas judiciais pertinentes.

7 - Revisões

Essa Norma deve ser revisada com periodicidade de, no mínimo, um ano ou conforme houver

mudanças que impacte ou para assegurar a eficácia no descarte segura das informações.

Anexo 1 – Aprovações da Política

As vias originais das atas do Comitê de Compliance e Riscos Operacionais (e respectiva aprovação da Política de Segurança da Informação) estão armazenadas junto a área de Compliance e de Segurança da Informação.

Anexo 2 – Amazon - Compliance

http://aws.amazon.com/pt/compliance/

Conformidade com a AWS

O AWS Compliance permite que nossos clientes compreendam os controles robustos estabelecidos na AWS para manter a segurança e a proteção de dados. Como você está construindo sistemas sobre a infraestrutura de nuvem da AWS, as responsabilidades de conformidade serão compartilhadas: o AWS Compliance garante a infraestrutura adjacente e sua empresa se responsabiliza pelas iniciativas de conformidade relacionadas a tudo o que for colocado na infraestrutura da AWS. As informações fornecidas pelo AWS Compliance ajudam você a entender nossa postura de conformidade e a avaliar a conformidade da sua empresa com os requisitos do setor e/ou governo.

Programas de garantias da AWS

A infraestrutura de nuvem da AWS foi projetada e gerenciada de acordo com regulamentações, normas e práticas recomendadas, incluindo:

- HIPAA
- SOC 1/SSAE 16/ISAE 3402 (antiga SAS70)
- SOC 2
- SOC 3
- PCI DSS, nível 1
- ISO 27001
- FedRAMP (SM)
- DIACAP e FISMA
- ITAR
- FIPS 140-2
- CSA
- MPAA

Os clientes podem solicitar relatórios e certificações produzidos por nossos auditores terceirizados que atestam a eficácia do projeto e da operação do ambiente da AWS. As solicitações de relatórios e certificações podem ser feitas através do representante de conta da AWS. Se você não souber quem é seu representante de contas da AWS ou se quiser ser alinhado a um representante, entre em contato com o Desenvolvimento de Negócios e Vendas da AWS para solicitar ajuda.

Para obter mais informações sobre o AWS Compliance, consulte o whitepaper AWS Risk and Compliance. Este whitepaper fornece informações para auxiliar os clientes da AWS a integrar a AWS à estrutura de controle existente, que oferece suporte ao seu ambiente de TI.

Fórum de conformidade da AWS

O Fórum de conformidade da AWS oferece aos clientes da AWS um fórum de comunidade exclusivo, onde você pode entrar em contato com colegas clientes da AWS, interagir com especialistas de conformidade da AWS e acessar facilitadores especializados do setor e educação. Esse fórum pode oferecer a você suporte nos seus esforços para atingir e manter garantia de segurança e conformidade durante o uso da AWS. Não há cobrança adicional para se tornar membro do Fórum de conformidade da AWS – o único requisito é participar de uma rápida pesquisa inicial, para que o conteúdo e as discussões do fórum possam ser adaptados ao seu setor, à sua região e aos seus interesses.

Participe da pesquisa para juntar-se ao fórum agora » Pesquisa de entrada no Fórum de conformidade da AWS

Whitepapers de conformidade da AWS

- Whitepaper Risco e conformidade da AWS. Este whitepaper fornece informações para auxiliar os clientes da AWS a integrar a AWS à estrutura de controle existente, que oferece suporte ao seu ambiente de TI.
- Whitepaper Auditoria de lista de verificação de segurança para uso da AWS. Este whitepaper oferece uma lista de verificação para ajudar a projetar e executar uma avaliação de segurança do uso da AWS por uma organização, que pode ser necessário de acordo com o setor ou normas regulatórias.

Estudos de caso de conformidade da AWS

Cognia

Saiba como a Cognia atingiu uma conformidade PCI DSS de nível 1 com a AWS. Leia a história »

Atestados, relatórios e certificações de terceiros

HIPAA

A AWS permite que entidades cobertas e seus associados de negócios sujeitos ao U.S. Health Insurance Portability and Accountability Act (HIPAA – Lei de responsabilidade e portabilidade de seguro-saúde dos Estados Unidos) aproveitem o ambiente seguro da AWS para processar, manter e armazenar informações de saúde confidenciais. A AWS assinará acordos de associados de negócios com tais clientes.

A AWS também oferece um whitepaper sobre a HIPAA para os clientes interessados em saber mais sobre como podem aproveitar a AWS para o processamento e armazenamento de informações de saúde. O whitepaper Creating HIPAA-Compliant Medical Data Applications with AWS descreve como as empresas podem usar a AWS para processar sistemas que facilitam a conformidade com a HIPAA e a HITECH. Para obter mais informações sobre o programa de conformidade AWS HIPAA, entre em contato com o Desenvolvimento de vendas e negócios da AWS.

Para saber mais sobre a conformidade com o HIPAA da AWS, acesse

Perguntas Frequentes do HIPAA da AWS »

SOC 1/SSAE 16/ISAE 3402

A Amazon Web Services agora publica um relatório de controles organizacionais de serviço 1 (SOC 1), tipo II. A auditoria para esse relatório é realizada de acordo com a declaração sobre normas para comprovação de contratos nº 16 (SSAE 16) e as Normas internacionais para contratos de garantia nº 3402 (ISAE 3402).

Essa auditoria é a substituição do relatório de auditoria da Declaração sobre normas de auditoria nº 70 (SAS 70), tipo II. Este relatório padrão duplo pode atender a uma ampla variedade de requisitos de auditoria dos Estados Unidos e de órgãos de auditoria internacionais.

A auditoria do relatório SOC 1 declara que os objetivos de controle da AWS foram devidamente desenvolvidos e que os controles definidos para proteger os dados do cliente funcionam com eficácia. O relatório SOC 1 da AWS inclui todos os datacenters da AWS no mundo que suportam serviços no escopo.

Para saber mais sobre a conformidade com o SOC 1 da AWS, acesse

Perguntas Frequentes do SOC da AWS »

SOC 2

Além do relatório SOC 1, a AWS publica um relatório de controles organizacionais de serviço 2 (SOC 2), tipo II. Semelhante ao SOC 1 na avaliação de controles, o relatórioSOC 2 é um relatório de comprovação que expande a avaliação de controles para os critérios definidos pelos princípios de serviços de confiança do American Institute of Certified Public Accountants (AICPA). . Esses princípios definem controles de prática líderes pertinentes à segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade aplicáveis a organizações de serviços, como a AWS. O SOC 2 da AWS é uma avaliação do design e eficácia operacional de controles queatendem aos critérios para o princípio de segurança definido nos critérios de princípios de serviços de segurança do AICPA. Esse relatório fornece transparência adicional na segurança da AWS com base em um padrão do setor definido e demonstra ainda mais o compromisso da AWS em proteger dados de clientes. O relatório SOC 2 da AWS inclui todos os datacenters da AWS no mundo que suportam serviços no escopo.

Para saber mais sobre a conformidade com o SOC 2 da AWS, acesse

Perguntas Frequentes do SOC da AWS »

SOC 3

A AWS publica um relatório de controles de empresas de serviços 3 (SOC 3). O relatório SOC 3 é um resumo disponível ao público do relatório SOC 2 da AWS e oferece o Selo de segurança SysTrust da AICPA.

O relatório inclui a opinião do auditor externo da operação de controles (com base nosPrincípios de confiança de segurança do AICPA incluídos no relatório SOC 2), a declaração do gerenciamento da AWS em relação à efetividade dos controles e uma visão geral da infraestrutura e serviços da AWS. O relatório SOC 3 da AWS inclui todos os datacenters da AWS no mundo que suportam serviços no escopo. Este é um excelente recurso para os clientes validarem que a AWS obteve garantia de um auditor externo sem passar pelo processo de solicitação de um relatório SOC 2. Veja o relatório SOC 3 da AWS.

Para saber mais sobre a conformidade com o SOC 2 da AWS, acesse

Perguntas Frequentes do SOC da AWS »

PCI DSS, nível 1

A AWS tem conformidade nível 1 com o Padrão de segurança de dados (DSS) da Indústria de cartões de pagamento (PCI). Os clientes podem executar aplicativos em nossa infraestrutura de tecnologia em conformidade com a PCI para armazenar, processar e transmitir informações de cartão de crédito na nuvem. Em fevereiro de 2013, o Conselho do padrão de segurança de dados da PCI publicou as Diretrizes de computação em nuvem do DSS da PCI. Essas diretrizes fornecem aos clientes que administram um ambiente de dados de proprietários de cartões de crédito considerações para manter os controles do DSS da PCI na nuvem. A AWS incorporou as Diretrizes de computação em nuvem do DSS da PCI no Pacote de conformidade com a PCI da AWS para os clientes. O Pacote de conformidade com a PCI da AWS inclui o Atestado de conformidade com a PCI (AoC) da AWS, que mostra que a AWS recebeu validação em relação às normas aplicáveis a um provedor de serviços de nível 1 no DSS da PCI versão 2.0 e o Resumo de responsabilidade quanto à PCI da AWS, que explica como as responsabilidades de conformidade são compartilhadas entre a AWS e nossos clientes na nuvem. A certificação de nível 1 no DSS da PCI da AWS inclui todos os datacenters da AWS no mundo que suportam serviços no escopo.

Para saber mais sobre a conformidade com o PCI DSS da AWS, acesse

Perguntas frequentes sobre PCI DSS Nível 1 »

ISO 27001

A AWS tem certificação ISO 27001 segundo a norma 27001 da International Organization for Standard (ISO). A certificação ISO 27001 é uma norma de segurança mundialmente adotada que descreve os requisitos para os sistemas de gerenciamento de segurança de informação. Ela oferece uma abordagem sistemática para gerenciar informações das empresas e dos clientes com base em avaliações de risco periódicas. Para obter a certificação, uma empresa deve demonstrar que tem uma abordagem constante e sistemática para gerenciar os riscos de segurança das informações que afetam a confidencialidade, a integridade e a disponibilidade das informações da empresa e do cliente.

A AWS criou um programa formal para manter a certificação. A certificação reforça o compromisso da Amazon de proporcionar transparência nos seus controles e práticas de segurança. A certificação ISO 27001 da AWS inclui todos os datacenters da AWS no mundo que suportam serviços no escopo.

Para obter mais informações sobre a conformidade com ISO 27001 da AWS, acesse

Perguntas frequentes sobre ISO 27001 »

FedRAMP (SM)

A AWS conquistou duas Authority to Operate (ATOs) para agências do Programa federal de gerenciamento de autorização e risco (FedRAMP) em nível de impacto moderado. O FedRAMP é um programa governamental que fornece uma abordagem padronizada de avaliação, autorização e monitoramento contínuo da segurança para produtos e serviços de nuvem até o nível moderado.

Todas as agências do governo americano podem aproveitar os pacotes de ATO para agências da AWS armazenados no repositório do FedRAMP para avaliar a AWS em relação aos seus aplicativos e cargas de trabalho, fornecer autorizações para usar a AWSe fazer a transição de cargas de trabalho dentro do ambiente da AWS.

Para saber mais sobre a conformidade com o FedRAMP da AWS, acesse

Perguntas frequentes sobre FedRAMP »

DIACAP e FISMA

A AWS permite que os órgãos governamentais dos EUA alcancem e mantenham a conformidade com a Lei federal de gestão de segurança da informação (FISMA). A infraestrutura da AWS foi avaliada por assessores independentes para diversos sistemas governamentais, como parte do processo de aprovação dos proprietários desses sistemas. Várias organizações civis e do Departamento de defesa (DoD) conseguiram autorizações de segurança para sistemas hospedados na AWS, de acordo com o processo de Estrutura de gerenciamento de riscos (RMF) definido na NIST 800-37 e no Processo de certificação e credenciamento de garantia da informação do DoD (DIACAP). A infraestrutura segura da AWS ajudou órgãos federais a ampliar os casos de uso de computação em nuvem e implementar dados e aplicativos confidenciais do governo na nuvem, sem deixar de cumprir os rigorosos requisitos de segurança das normas federais. Para solicitar mais

informações sobre o DIACAP e/ou a FISMA da AWS, entre em contato com o Desenvolvimento de vendas e negócios da AWS.

ITAR

A região AWS GovCloud (EUA) oferece suporte ao cumprimento dos regulamentos do tráfego internacional de armas (ITAR). Como parte do gerenciamento de um abrangente programa de conformidade com o ITAR, empresas sujeitas a regulamentações de exportação do ITAR devem controlar as exportações não intencionais restringindo o acesso a dados protegidos de cidadãos americanos e restringindo a localização física dos dados ao território dos EUA. O AWS GovCloud (EUA) fornece um ambiente fisicamente localizado nos EUA no qual o acesso por parte do pessoal da AWS é limitado aoscidadãos americanos, permitindo que empresas qualificadas transmitam, processem e armazenem artigos e dados sujeitos às restrições do ITAR. O ambiente AWS GovCloud (EUA) foi auditado por um terceiro independente para validar que os controles apropriados estão em vigor para apoiar programas de conformidade de exportação do cliente paraesse requisito.

FIPS 140-2

A publicação Norma de processamento de informações federal (FIPS) 140-2 é uma norma de segurança do governo dos EUA que especifica os requisitos de segurança para módulos criptográficos que protegem informações confidenciais. Para oferecer suporte a clientes com requisitos FIPS 140-2, os endpoints da VPN da Amazon Virtual Private Cloud e terminações SSL no AWS GovCloud (EUA) operam usando o hardware validado pela FIPS 140-2. A AWS trabalha com clientes do AWS GovCloud (US) para fornecer as informações necessárias para ajudar a gerenciar a conformidade ao usar o ambiente AWS GovCloud (EUA).

Outras iniciativas de conformidade

A flexibilidade e o controle que a plataforma da AWS oferece aos clientes permitem implementar soluções que atendam aos padrões específicos do setor, incluindo:

- CSA: o Cloud Security Alliance (CSA – Aliança de segurança da nuvem) com sua iniciativa de Security, Trust & Assurance Registry (STAR – Segurança, confiança e registro de seguro) incentiva a transparência nas práticas de segurança dentro dos provedores de nuvem. O CSA STAR é um registro gratuito, acessível ao público, que documenta os controles de segurança fornecidos por várias ofertas de computação em nuvem, ajudando os usuários a avaliarem a segurança dos provedores de nuvem que utilizam atualmente ou que estão considerando contratar. A AWS é registrada pelo CSA STAR e concluiu o CSA Consensus Assessments Initiative Questionnaire (CAIQ – Questionário de iniciativa de avaliações de consenso do CSA). Esse questionário (CAIQ) publicado pela CSA fornece uma forma de consultar e documentar quais controles existem nas ofertas de Infraestrutura como serviço da AWS. O CAIQ tem um conjunto de mais de 140 perguntas que um auditor de nuvem e cliente de nuvem podem querer fazer a um provedor de nuvem. Os clientes podem encontrar o questionário completo no Apêndice A do whitepaper AWS Risk and Compliance.

- MPAA: o Motion Picture Association of America (MPAA – Associação de cinematografia da América) estabeleceu um conjunto de práticas recomendadas para armazenar, processar e fornecer com segurança conteúdo e mídia protegida. As empresas de mídia usam essas práticas recomendadas como forma de avaliar o risco e a segurança do seu conteúdo e infraestrutura. A AWS demonstrou alinhamento com as práticas recomendadas da MPAA e a infraestrutura da AWS é compatível com todos os controles de infraestrutura aplicáveis da MPAA. Embora a MPAA não ofereça uma "certificação", os clientes do setor de mídia podem solicitar documentação para aprimorar sua avaliação de riscos e do conteúdo do tipo MPAA na AWS.

Contato com a AWS sobre relatórios e certificações de conformidade

Você pode solicitar relatórios e certificações produzidos por nossos auditores terceirizados que atestam a eficácia do projeto e da operação do ambiente da AWS. As solicitações de relatórios e certificações podem ser feitas através do representante de conta da AWS. Se você não souber quem é seu representante de contas da AWS ou se quiser ser alinhado a um representante, entre em contato com o Desenvolvimento de Negócios e Vendas da AWS para solicitar ajuda.

Anexo 3 – Amazon - Segurança

http://aws.amazon.com/pt/security/

Centro de Segurança da AWS

A infraestrutura de nuvem da AWS foi projetada para ser um dos ambientes de computação em nuvem mais flexíveis e seguros atualmente disponíveis. Ela oferece uma plataforma extremamente escalável e altamente confiável, que permite que os clientes implementem aplicativos e dados de forma rápida e segura.

Proteção de classe mundial

Com a nuvem da AWS, não são apenas as dores de cabeça que desaparecem, mas também muitos dos problemas de segurança relacionados à infraestrutura. Os datacentersde nível mundial e altamente seguros da AWS utilizam vigilância eletrônica e sistemas de controle de acesso multifator de última geração. Os datacenters são protegidos 24 horas por dia, 7 dias por semana por seguranças treinados e o acesso é autorizado estritamente com base no menor privilégio possível. Os sistemas ambientais são projetados paradiminuir o impacto das interrupções nas operações. E várias regiões e zonas de disponibilidade permitem que você permaneça resiliente diante da maioria dos modos de falha, inclusive desastres naturais ou falhas do sistema.

A infraestrutura virtual da AWS foi projetada para oferecer excelente disponibilidade e para garantir privacidade e separação total de clientes. Para obter uma lista completa de todas as medidas de segurança criadas na infraestrutura, plataformas e serviços da nuvem da AWS, leia nosso whitepaper Overview of Security Processes.

Recursos de segurança integrados

Seus aplicativos e dados não precisam apenas ser protegidos por instalações e infraestrutura altamente seguras, eles também precisam ser protegidos por amplos sistemas de monitoramento de segurança e de rede. Esses sistemas oferecem medidas de segurança básicas, mas importantes, como a proteção distribuída de negação de serviço (DDoS) e detecção de tentativa de acesso de senha por força bruta nas contas da AWS. As medidas de segurança adicionais incluem:

- Acesso seguro – Os pontos de acesso do cliente, também chamados de endpoints de API, permitem acesso via HTTP seguro (HTTPS) para que você possa estabelecer sessões de comunicação seguras com seus serviços da AWS usando SSL.

- Firewalls integrados – Você pode controlar o nível de acessibilidade às suas instâncias configurando regras integradas de firewall – de totalmente públicas a completamente privadas, ou algo entre os dois. E quando suas instâncias residirem dentro de uma sub-rede da Virtual Private Cloud (VPC), você pode controlar tanto a saída quanto a entrada.

- Usuários exclusivos – A ferramenta AWS Identity and Access Management(IAM) permite que você controle o nível de acesso que seus próprios usuários terão aosAWS infrastructure services. Com o AWS IAM, cada usuário pode ter credenciaisexclusivas de segurança, eliminando a necessidade de senhas ou chaves compartilhadas e permitindo o uso das práticas recomendadas de segurança de separação de funções e menor privilégio.

- Autenticação multifator (MFA) – A AWS oferece suporte integrado à Autenticação multifator (MFA) para uso com contas da AWS e contas de usuários individuais do IAM.

- Sub-redes privadas – O serviço AWS Virtual Private Cloud (VPC) permite que você adicione uma camada adicional de segurança de rede às suas instâncias criando sub-redes privadas e até adicionando um túnel VPN IPsec entre sua rede doméstica e sua VPC AWS.

- Armazenamento de dados criptografas – Os clientes podem ter os dados e objetos que armazenam no Amazon S3, Glacier, Redshift e Oracle RDS criptografados automaticamente usando o Advanced Encryption Standard (AES) 256, um padrão de criptografia de chave simétrica que utiliza chaves de criptografia de 256 bits.

- Opção de conexão dedicada– O serviço AWS Direct Connect permite estabelecer uma conexão de rede dedicada entre suas instalações locais e a AWS. Usando VLANs 802.1q padrão do setor, essa conexão dedicada pode ser particionada em várias

conexões lógicas para permitir o acesso a ambientes de IP públicos e privados dentro da sua nuvem da AWS.

- GovCloud isolado – Para clientes que precisam de medidas adicionais para atender às regulamentações US ITAR, a AWS oferece uma região totalmente separada chamada AWS GovCloud (US), que oferece um ambiente onde os clientes podem executar aplicativos compatíveis com o ITAR e oferece endpoints especiais que utilizamapenas criptografia FIPS 140-2.

- Opção de armazenamento de chave de criptografia dedicada e baseada em hardware – Para clientes que precisam usar dispositivos Hardware Security Module (HSM) para armazenamento de chave criptográfica, o AWS CloudHSM oferece uma forma altamente segura e conveniente de armazenar e gerenciar chaves.

- Trusted Advisor– Fornecido automaticamente quando você se cadastra para o suporte premium, o serviço Trusted Advisor é uma forma conveniente de você ver onde poderia aplicar um pouco mais de segurança. Ele monitora os recursos da AWS e alerta você quanto a falhas de configuração de segurança, como acesso excessivamente permissivo a certas portas de instância do EC2 e buckets de armazenamento do S3,uso mínimo de separação de funções usando o IAM e políticas fracas de senha.

Como a infraestrutura da nuvem da AWS oferece tantos recursos de segurança integrados, você pode simplesmente focalizar a segurança do seu SO convidado e aplicativos. Os engenheiros de segurança e arquitetos de solução da AWS desenvolveramwhitepapers e checklists operacionais para ajudá-lo a selecionar as melhores opções para suas necessidades e práticas recomendadas de segurança, como oarmazenamento de chaves secretas e senhas de forma segura e rotativa ou alterando-as com frequência.

Verificar nossa segurança

Sabemos que é importante que você entenda as medidas de proteção usadas paradefender a infraestrutura de nuvem da AWS. Mas, como você não pode tocar fisicamente os servidores nem caminhar pelos datacenters, como você pode ter a certeza de que pode contar com os controles de segurança corretos?

A resposta está nas certificações e avaliações de terceiros pelas quais a AWS passa. A AWS obteve a certificação ISO 27001 e foi validada como provedor de serviços de nível 1 no Padrão de Segurança de Dados (DSS) da Indústria de Cartões de Pagamento (PCI).

Passamos por auditorias SOC 1 anuais e fomos avaliados positivamente no nível moderado para os sistemas do governo federal, bem como no nível 2 DIACAP para sistemas do DoD.

Cada certificação significa que um auditor verificou que os controles de segurança específicos estão disponíveis e operando conforme pretendido. Você pode ter acesso aos relatórios de conformidade aplicáveis entrando em contato com seu representante de conta da AWS. Para obter mais informações sobre os regulamentos e padrões de segurança com os quais a AWS está em conformidade, veja a página da web Conformidade com a AWS ou o whitepaper AWS Risk and Compliance.

Compartilhar a responsabilidade de segurança

Como você está construindo sistemas sobre a infraestrutura da nuvem da AWS, as responsabilidades de segurança serão compartilhadas: a AWS protegeu a infraestrutura subjacente, mas você deve proteger tudo o que colocar na infraestrutura. Isso inclui suas instâncias do EC2 da AWS e tudo o que você instalar nelas, todas as contas que acessem suas instâncias, o grupo de segurança que permite acesso externo às suas instâncias, a sub-rede da VPC em que as instâncias residem se você tiver selecionado essa opção, o acesso externo aos seus buckets S3, etc.

Isso significa que há várias decisões de segurança que você precisa tomar e controles que você precisa configurar. Para obter informações sobre como configurar um serviço específico da AWS, consulte a documentação do serviço. Para obter mais dicas sobre as melhores práticas de segurança para recursos da AWS, veja a seção Recursos de segurança da nossa página da web.

Como entrar em contato com a segurança da AWS

A Equipe de segurança da AWS incentiva a comunicação com o cliente. Estabelecemos processos para:

- Obter permissão para realizar testes de penetração/varredura
- Relatar vulnerabilidades de segurança
- Relatar e-mails suspeitos
- Relatar abuso dos recursos da AWS

Chave PGP pública da AWS

Criamos uma chave PGP assinada para comunicações confidenciais que você queira enviar. Você pode acessá-lo aqui.

Anexo 4 – Minuta do Termo de Recebimento, Ciência e Adesão

TERMO DE RECEBIMENTO, CIÊNCIA E ADESÃO
A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA APEX GROUP

[NOME DA EMPRESA OU FORNECEDOR], inscrita(o) no [CNPJ OU CPF]....., por meio do seu representante devidamente constituído, [IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DA EMPRESA OU FORNECEDOR], DECLARA, sob as penas da lei, em complemento às condições estabelecidas do [CONTRATO],datado de [data] de [mês] de [ano], que:

1. Recebeu uma cópia integral da Política de Segurança da Informação da Apex Group ("POLÍTICA"); A POLÍTICA também encontra-se atualizada e publicada no site corporativo da Apex Group, na área Compliance, seção Políticas e Manuais.
2. Tomou conhecimento de todos os seus termos e se compromete a cumpri-los integralmente;
3. Compartilhará as condutas contidas nesta POLÍTICA com seus empregados, colaboradores, parceiros, suarespectiva cadeia produtiva e seus subcontratados, quando for o caso;
4. Não tem conhecimento de qualquer violação ou indício de violação a esta POLÍTICA ou à legislaçãoanticorrupção;
5. Se compromete a informar à APEX GROUP caso venha a tomar conhecimento de qualquer violação ou indíciode violação a esta POLÍTICA ou à legislação anticorrupção; e
6. Tem conhecimento de que a manutenção da relação contratual com a APEX GROUP implica na concordância emseguir esta POLÍTICA e suas eventuais alterações, aditamentos ou revisões futuras.

[Local], [Dia], [Mes] de [Ano]

Nome: _____

ANEXO 5 - POLÍTICA DE SEGURANÇA CIBERNÉTICA

(INTERNO)

ÍNDICE

1. OBJETIVO

A Política de Segurança Cibernética **do Apex Group** visa prover a metodologia necessária para instituir processos**, procedimentos** e controles para prevenir, **detectar, tratar** e reduzir as vulnerabilidades **e incidentes**, garantindo a proteção dos ativos **da informação** associados aos negócios críticos **da organização contra ameaças internas e externas**, **acessos indevidos e modificações não autorizadas, reduzindo a exposição a perdas e danos decorrentes de falhas de cibersegurança, garantindo a confidencialidade, disponibilidade e integridade das informações e recursos para continuidade das operações do negócio,** definindo processos para o tratamento de incidentes cibernéticos e para avaliação de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem para garantir a segurança das operações, **visando minizar impactos sobre as atividades, além de promover entre seus colaboradores a conscientização da cultura de segurança cibernética. Esta política tem ainda por objetivo atender os requisitos para a contratação de serviços relevantes de processamento de dados e de computação em nuvem, estando em conformidade com o cumprimento da Resolução CMN 4.893/2021 do Banco Central do Brasil.**

As definições relacionadas à instituição, contidas na política de segurança cibernética, são compatíveis com: definição de porte e modelo da instituição, perfil de risco da instituição, natureza e complexidade de suas operações, serviços e processos assim como a sensibilidade dos dados tratados pela instituição.

2. DEFINIÇÕES

Colaborador: funcionários de quaisquer cargos, estagiários, sócios, diretores e prestadores de serviços.

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas. **Somente usuários autorizados podem visualizar a informação entre sua origem e destino, sem interceptação de terceiros.**

Disponibilidade: garantir que as informações estejam disponíveis **e acessíveis a todo momento, sem interrupções**, a todas as pessoas autorizadas a tratá-las. **A informação é acessível por usuários autorizados sempre que solicitada.**

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais. **Somente usuários autorizados podem alterar a informação.**

Normas de Segurança da Informação: especificam os processos e controles que devem ser

implementados para o alcance dos objetivos de segurança da informação definidos nesta política.

Prestadores de serviços: pessoa jurídica ou física que mantenha contrato de prestação de serviço com o Apex Group.

Segurança Cibernética: é um conjunto de práticas que visam proteger os sistemas conectados à Internet, incluindo hardware, software e dados de ataques cibernéticos. **Trata-se da proteção das informações no meio digital, prevenindo, detectando e respondendo às ameaças, ataques e vulnerabilidades, a fim de resguardar a Confidencialidade, Integridade e Disponibilidade dos ativos da organização.**

Incidente de segurança: qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação.

Incidente de segurança da informação e privacidade: Um ou mais eventos de segurança da informação e privacidade indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Riscos cibernéticos:

SOC: *Security Operations Center* em português Centro de Operações de Segurança, é uma equipe com objetivo de prestar serviços de detecção e reação a incidentes de segurança.

3. PAPÉIS E RESPONSABILIDADES

Compete ao Colaborador:

I. Cumprir as diretrizes estabelecidas nesta Política;

II. Estar ciente e atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de Segurança da Informação sempre que estiver com dúvidas;

III. Comunicar à área de Segurança da Informação quaisquer incidentes identificados relacionados à segurança da informação.

Compete à área de Segurança da Informação:

I. Promover a atualização, definição e **análise crítica** das versões da Política de Segurança Cibernética**, apreciadas e aprovadas pela Alta Direção e pelo Comitê Gestor de Segurança da Informação**, **em intervalos planejados, para assegurar sua contínua pertinência, adequação e eficácia**;

II. Implantar e testar a eficácia dos **procedimentos e** controles utilizados;

III. Analisar criticamente incidentes em conjunto com o Diretor de Segurança da Informação e do **Comitê Gestor de Segurança Cibernética e da Informação**;

IV. Monitorar e analisar os alertas e informações relacionadas à segurança das informações;

V. Implementar melhorias no tratamento de incidentes de segurança da informação;

VI. Identificar eventos de Segurança Cibernética, estabelecendo ações de detecção, tratamento e prevenção de incidentes;

VII. Atender aos requisitos legais e regulamentares;

VIII. Conscientizar, educar e treinar os colaboradores nas suas atividades diárias com foco na Segurança Cibernética;

IX. Conscientizar os clientes em relação ao tema de segurança da informação;

X. Estabelecer o plano de ação e resposta a incidentes, aprovado pela Alta Direção, visando à implementação desta política de segurança cibernética e elaborar o relatório anual sobre a implementação do plano de ação e resposta a incidentes com data-base de 31 de dezembro (arts. 6º e 8º da Res. CMN 4.893/2021).

Compete ao Gerente de Segurança da Informação:

I. Reportar ao diretor responsável pela Segurança Cibernética nº 4.893/2021 os incidentes de Segurança da Informação que causem impactos de criticidade alta;

II. Apoiar sempre que necessário ou escalonar as necessidades decorrentes ao tratamento dos incidentes.

Compete ao Comitê Gestor de Segurança Cibernética e da Informação:

I. Deliberar sobre assuntos relativos à Segurança Cibernética e da Informação;

II. Aprovar e revisar anualmente, ou sempre que necessário, a política de segurança da informação e cibernética, incluindo as demais normas relacionadas aos controles, o processo de segurança da informação e o processo de gerenciamento de incidentes de segurança da informação, em harmonia com os regulatórios do BACEN, PQO, CMN, CVM, bem como as normas ISO 27001 e 27002 e boas práticas de segurança da informação mundialmente reconhecidas;

III. **Aprovar ações periódicas de conscientização, educação e capacitação em segurança da informação em todas as áreas da APEX GROUP;**

IV. **Aprimorar continuamente propostas de normas e políticas de uso dos recursos da TI referentes à Segurança da informação, tais como: gerenciamento de identidades e controle de acesso lógico e físico; controle de acesso à internet; utilização de e-mail, utilização de equipamentos e aplicações de TI de forma segura, em observância às políticas da APEX GROUP;**

V. **Tomar decisões sobre questões de segurança da informação não contempladas na política de segurança da informação e normas relacionadas;**

VI. **Receber e analisar as comunicações de descumprimento das normas referentes à política de segurança cibernética e da informação da APEX GROUP, apresentando parecer às autoridades/orgãos compentes para sua apreciação;**

VII. **Aprovar o plano de continuidade de negócios (BCP e DR).**

VIII. **Para maiores detalhes verificar pág. 3 da Política de Segurança da Informação**

4. ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores e empresas da Apex GroupAPEX GROUP, o qual abrange: a MAF Distribuidora de Títulos e Valores Mobiliários S.A. (“MAF DTVM”), Modal Asset Management Ltda. (“MAM”) e Modal Administração de Recursos Ltda. (“MAR”).
Para maiores detalhes verificar pág. 3 da Política de Segurança da Informação.

5. DIRETRIZES GERAIS

As diretrizes de Segurança Cibernética do Apex Group têm os seguintes objetivos principais:

a) Estar em conformidade com a Resolução ~~**Resoluções CMN nº 4.658/2018**~~ nº 4.893/2021 que dispõe sobre a política de segurança cibernética **e requisitos para a contratação de serviços de processsamento e armazenamento de dados e de computação em nuvem a serem observados pela instituições autorizadas a funcionar pelo BACEN**;

b) Atender ao programa de Segurança Cibernética exigidas na Resolução CVM 35;

c) Assegurar que os procedimentos contenham no mínimo a descrição dos controles referentes à segurança **cibernética**;

d) Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, colaboradores e proteger os dados e os sistemas da informação, contra acessos

indevidos, pessoas e alterações não autorizadas;

e) Definir procedimento para prevenção, identificação e tratamento de incidentes de Segurança Cibernética;

f) Definir mecanismos de manutenções e atualizações técnicas e de segurança dos sistemas;

g) Comunicar de forma tempestiva os reguladores das ocorrências de incidentes de segurança cibernética relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pelo Apex Group, bem como das providências para o reinício das atividades;

h) Definir procedimentos e controles voltados à prevenção, e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços às empresas do Apex Group que manuseiem dados ou informações sensíveis, ou que sejam relevantes para a condução das atividades operacionais da instituição;

i) Definir procedimentos e controles voltados ao descarte e manutenção segura de dados e equipamentos;

j) Definir os parâmetros para classificação de dados e as informações quanto à relevância;

k) Monitorar serviços contratados;

l) Adotar práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

m) Criar programas de conscientização e treinamento para os colaboradores e prepostos sobre a segurança das informações.

6. MONITORAMENTO DE CIBERSEGURANÇA

Para garantir a segurança do ambiente cibernético da instituição foram adotadas ferramentas de controle de perímetro, monitoração e bloqueio de conteúdo, assim como ferramentas para garantir a rastreabilidade e prevenção a vazamento e possíveis incidentes de dados sensíveis.

7. GESTÃO DE IDENTIDADE DE ACESSOS

Os controles lógicos de sistema relevantes possuem gerenciamento na autenticação, validação segura de qualquer entrada de dados e manutenção de acordo com a metodologia interna, realização de testes visando identificação de vulnerabilidades controles contra softwares maliciosos, acesso controlado e monitorado a ambientes de produção, testes de penetração, controle de patches, bem como manter as cópias de segurança de dados e das informações

atualizadas.

Os acessos e a sua revisão são regidos de acordo com os normativos de acessos disponibilizados na intranet do Apex Group e suas segregações de funções, distribuição e controle de acessos físicos e/ou lógicos que possam conter informações das empresas do Apex Group bem como possuir controles para proteger as informações, utilizando as melhores práticas do mercado. Para mais detalhes verificar pág. 13 Norma de gestão de acessos e pág. 20 Norma de Acesso Físico da política de Segurança da Informação.

8. GOVERNANÇA, RISCOS E CONFORMIDADE

Devem ser estabelecidos e continuamente aprimorados os controles de segurança cibernética, a fim de certificar que as informações sejam monitoradas e/ou os recursos de tecnologia sejam inspecionados nas dependências de fornecedores relevantes e que atendam o mínimo dos requisitos referentes a segurança cibernética, tais como: a localização de onde os dados estão hospedados, continuidade, medidas de segurança para transferir e armazenar os dados, manutenção e proteção das informações de clientes na segregação de dados e dos controles de acesso físicos e lógicos e que os dados transferidos estejam íntegros e disponíveis na transferência de dados, bem como dados excluídos totalmente, quando solicitado.

Em caso de incidentes em fornecedores relevantes que envolvam informações de responsabilidade do Apex Group, o mesmo deverá comunicar à área de Segurança da Informação de forma tempestiva e observando a razoabilidade de tempo aceitável, após a detecção, assim como comunicar as medidas que serão adotadas para a minimização do impacto do incidente, quais titulares de dados, informações e sistemas foram afetados e, após isso, apresentar as evidências da mitigação do risco, assim como garantias da mitigação.

9. CLASSIFICAÇÃO DA INFORMAÇÃO

Assegurar que as informações sejam classificadas, preservadas e guardadas conforme diretrizes institucionais e em conformidade com a Norma de Classificação da Informação **(documento anexo)**, o Apex Group, seus colaboradores e seus prestadores de serviço tem a missão de estar em conformidade com as leis sancionadas a fim de proteger as informações de seus clientes.

As informações sensíveis devem ser tratadas e armazenadas de forma segura e íntegra, bem como com os métodos de criptografia adequados e a proteção contra o vazamento de informações.

O descarte de informações e ativos devem ser realizados de forma segura, com a utilização de equipamentos apropriados, como fragmentadoras, de acordo com as boas práticas internas

garantindo, assim, confidencialidade dos dados. Para mais detalhes verificar pág. 15 da palitica de Segurança da Informação.

10. RESPOSTA A INCIDENTES

A resolução de incidentes cibernéticos consiste na definição dos critérios e procedimentos para mitigar riscos relacionados à segurança garantindo a detecção, classificação, registro, análise, tratamento e monitoração, onde são registradas todas as fases, contendo, inclusive, análise da causa e impacto. A resposta de incidentes deve ser administrada de acordo com os requisitos específicos adotados e estabelecer critérios de avaliação e relevância de um incidente.

A tratativa de incidentes de segurança será realizada prioritariamente pela equipe ~~do SOC~~ **de Segurança Cibernética e da Informação**, sendo esta a única proprietária do processo de tratamento, porém, durante o ciclo de vida do incidente, pode haver acionamento de equipes necessariamente envolvidas no processo, bem como acionamento de fornecedores e parceiros de acordo com sua necessidade para apoiarno tratamento de incidentes.

Os colaboradores poderão reportar incidentes de Segurança da Informação por meio do canal de reporte de incidentes: sec.info_BRA@apexgroup.com

Os incidentes reportados serão classificados segundo o risco que representam para a APEX GROUP e o impacto na continuidade dos negócios. Além disso, devem ser devidamente registrados, tratados e comunicados.

O Apex Group adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

Procedimento em caso de incidente:

Toda ocorrência, bem como as informações recebidas de terceiros, deverá ser avaliada pela equipe de Segurança da Informação para a determinação da criticidade e impacto causados nas operações. Uma vez que a equipe de Segurança da Informação tenha sido acionada devido a um potencial incidente, este deverá convocar Comitê Gestor de Segurança Cibernética e da Informação.

Avaliação inicial:

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo

decidir pela formalização ou não do incidente.

Incidente caracterizado:

Se for caracterizado um incidente, os membros do Comitê de Segurança deverão tomar as medidas imediatas que poderão abranger a comunicação aos órgãos reguladores, comunicação interna ou externa, em especial ao investidor que tenha sido afetado.

Plano de ação e resposta a incidentes:

O processo de tratamento dos incidentes consta no Plano de Resposta a Incidentes, visando a implementação das práticas aqui dispostas e dispõe de um Plano de Ação, o qual abrange:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética;

- Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes.

- Comunicar prontamente os reguladores sobre incidentes definidos como críticos e, em caso de necessidade, compartilhar as informações dos incidentes com as instituições do mesmo ramo, e, se necessário, informar aos clientes e/ou fornecedores envolvidos no incidente.
- **O Apex Group deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, contendo:**
  - **(i) a efetividade da implementação das ações desenvolvidas para adequar a estrutura organizacional e operacional da instituição financeira aos princípios e às diretrizes da política de segurança cibernética;**
  - **(ii) o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta política;**
  - **(iii) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e**
  - **(iv) os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes (art. 8, § 1º Resolução 4.893/2021);**
- **O relatório deve ser submetido ao Comitê de Risco e apresentado ao Conselho de Administração até 31 de março do ano seguinte ao da data-base (art. 8, § 2º, incisos I e II da Resolução 4.893/2021);**

- **A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo anualmente, e aprovados pela diretoria da APEX GROUP, após apreciação do Comitê Gestor de Segurança Cibernética e da Informação (art. 9 da Resolução 4.893/2021);**
- **Para mais detalhes verificar pág. 31 da Política de segurança da Informação**

11. USO ACEITÁVEL DE ATIVOS

Os ativos corporativos são geridos de acordo com os requisitos especificados na Norma de Uso Aceitável de Ativos, que estabelece as regras para utilização, proteção das informações e garantia que todos os usuários usem os recursos de computação da empresa de maneira eficaz, eficiente, ética e lícita. Para mais detalhes verificar pág. 24 da Política de Segurança da Informação.

12. GESTÃO DE VULNERABILIDADES

A área de Segurança da Informação atua na identificação, estabelecimento, avaliação, classificação, solução, redução e documentação das vulnerabilidades relevantes nos sistemas internos e expostos na Internet continuamente, bem como no monitoramento das configurações básicas de segurança, a fim de verificar aplicabilidade adequada conforme procedimento interno.

As avaliações das práticas de segurança fazem parte do processo de desenvolvimento de sistemas relevantes, tornando o processo de concepção dos sistemas construídos dentro do Apex Group mais confiável, contendo trilhas de auditoria, estável e protegido contra ameaças, atendendo os requisitos e metodologia interna, bem como assegurando que as informações processadas sejam protegidas. Para mais detalhes verificar pág. 38 da Política de Segurança da Informação.

13. CONSCIENTIZAÇÃO CIBERNÉTICA

O plano de conscientização de segurança cibernética abrange campanhas, termos de ciência e treinamentos periódicos; visando a disseminação de conhecimento para com os colaboradores do Apex Group, de modo que todos tenham um nível adequado de conhecimento e responsabilidade na proteção dos ativos de informações. Este plano estabelece maneiras de zelar, minimizar e mitigar danos de segurança cibernética com o comprometimento da Alta Administração tencionando a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

A área de Segurança da Informação manterá um plano de conscientização aos clientes, abordando temas para proteção das informações e sobre a eficácia da segurança das plataformas do Apex Group. Para mais detalhes verificar o PSAP.

14. CONTINUIDADE DE NEGÓCIOS

O plano de continuidade de negócios estabelece, implementa e mantém procedimentos documentados para gerenciar interrupções, **minimizar impactos e recuperar perdas de ativos da informação após um incidente crítico, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres, incluindo-se no processo a continuidade dos serviços contratatados em nuvem e os testes previstos para os cenários de ataques cibernéticos, de modo a resguardar a continuidade das** atividades com base em objetivos de recuperação identificados em um tempo mínimo aceitável, dentro do prazo acordado, garantindo que os procedimentos sejam testados com resultados satisfatórios para atendimento do negócio.

Cenários de incidentes devem ser considerados nos testes de continuidade de negócios. **Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para cenários de ataques cibernéticos (art. 3, V, letra "a" e art. 19, III da Resolução 4.893/2021).**

Fornecedores devem atender os requisitos de continuidade de negócios, contemplando os testes em caso de interrupção de serviços críticos prestados ao Apex Group de processamento, armazenamento de dados e de computação em nuvem, bem como o reestabelecimento da operação normal da Instituição. Para mais detalhes verificar o PCN.

15. PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a APEX GROUP deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- **A adoção de serviços hospedados em nuvem privada, pública, híbrida ou em ambiente de parceiros e/ou fornecedores, respeitam sempre a premissa da confidencialidade, integridade e disponibilidades das informações;**

- **Os serviços devem respeitar a legislação e localidades, que estejam dentro dos acordos estabelecidos pelas autarquias responsáveis pela regulação e fiscalização de nosso mercado e atuação;**
- **A sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;**
- **O acesso pela APEX GROUP aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados (art. 12, letra "e" da Resolução 4893);**
- **O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;**
- **A identificação e a segregação dos dados dos usuários da APEX GROUP por meio de controles físicos ou lógicos; e**
- **A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários da APEX GROUP.**

Na avaliação da relevância do serviço a ser contratado, a APEX GROUP DTVM também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

16. CONTRATAÇÃO DE PRESTAÇÃO DE SERVIÇOS DE ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A APEX GROUP DTVM deve assegurar que os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem contemplem (art. 17 da Res. 4.893/2021):

- **A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;**
- **A adoção de medidas de segurança para a transmissão e armazenamento dos dados;**
- **A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;**
- **Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à APEX GROUP DTVM, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;**
- **O acesso da APEX GROUP DTVM às informações fornecidas pela empresa contratada bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;**

- **A obrigação da empresa contratada notificar a APEX GROUP DTVM sobre a subcontratação de serviços relevantes para a APEX GROUP DTVM;**
- **A permissão de acesso do Banco Central do Brasil aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;**
- **A adoção de medidas pela APEX GROUP DTVM, em decorrência de determinação do Banco Central do Brasil;**
- **A obrigação de a empresa contratada manter a APEX GROUP DTVM permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.**

Em caso de decretação de regime de resolução da APEX GROUP DTVM pelo Banco Central do Brasil, o contrato de prestação de serviços deve prever:

- **A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;**
- **A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços;**

A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:

- **A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;**
- **A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.**

17. COMUNICAÇÃO AO BANCO CENTRAL DO BRASIL

A comunicação da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil até 10 (dez) dias após a contratação dos serviços e deve conter as seguintes informações (art. 15 da Res. 4.893/2021):

- **A denominação da empresa contratada;**
- **Os serviços relevantes a serem contratados; e**
- **A indicação dos países e das regiões onde os serviços poderão ser prestados e os dados armazenados, processados e gerenciados.**

Caso haja alterações contratuais que impliquem modificação das informações, a comunicação ao Banco Central deve ser efetivada até 10 (dez) dias após a alteração contratual.

18. DOCUMENTOS RELACIONADOS

Os documentos relacionados a essa Política estão publicados na Intranet, sendo eles:

a) **Política de Segurança da Informação;**

b) Plano de Continuidade de Negócios;

c) Norma de Plano de Resposta a Incidentes de Segurança da Informação;

d) Norma de Uso Aceitáveis de Ativos; e

e) Normas de Controle de Acessos (Físico e Lógico).

19. DESCUMPRIMENTO DESTA POLÍTICA

Na hipótese de violação desta Política, as sanções administrativas serão aplicadas de acordo com o Normativo Interno de Matriz de Consequência disponibilizada na Intranet.

FOLHA DE CONTROLE

Informações Gerais

Título	Política de Segurança Cibernética
Versão do Documento	1.3
Área Proprietária da Política	Segurança da Informação
Legislação relacionada	~~Resolução CMN Nº 4.658/2018~~ Resolução CMN Nº 4.893/2021 Resolução CVM 35
Classificação da Informação	Interna

Histórico de Versões

Versão	Motivo da alteração	Data de início
1.0	Elaboração	Outubro/2021
1.1	Revisão	Outubro/2021
1.2	Revisão por Anderson de Aguiar Gomes	Março/2022
1.3	Revisão Raphael Colvara	Maio/2023
1.4	Vitoria Guarino Ferreira	Julho/2023

Aprovação

Aprovado por:	Eduardo Soluri	

Original assinado sob custódia da área de Compliance Institucional. Pode ser disponibilizado sempre que necessário.

Cargo:

Controle de Revisões da Política

Versão	Data	Descrição	Responsável
00	01/09/2012	Primeira versão do documento	Alexandre Maciel
01	23/10/2012	Segunda versão do documento	Alexandre Maciel
02	17/11/2012	Terceira versão do documento	Alexandre Maciel
03	11/10/2013	Revisão anual do documento	Alexandre Maciel
04	10/10/2014	Revisão anual do documento	Alexandre Maciel
05	10/10/2015	Revisão anual do documento	Wanderley Cabral
06	31/03/2016	Revisão de ortografia e fontes	Wanderley Cabral
07	04/07/2016	Revisão do documento	Wanderley Cabral
08	25/07/2017	Revisão do documento	Wanderley Cabral
09	27/08/2018	Revisão do documento	Wanderley Cabral
10	22/10/2018	Revisão do documento	Eduardo Soluri
11	30/04/2019	Revisão do Documento	Wanderley Cabral
12	02/05/2019	Aprovação do Documento	Eduardo Soluri
13	15/07/2020	Aprovação do Documento	Eduardo Soluri
14	06/08/2021	Revisão do Documento	Raphael Greco
15	03/09/2021	Aprovação do Documento	Eduardo Soluri
16	15/08/2022	Revisão do Documento	Richard Nunes
17	19/08/2022	Aprovação do Documento	Eduardo Soluri
18	30/05/2023	Aprovação do Documento	Raphael Colvara