Vonquér

Política de Segurança da Informação e de Segurança Cibernética Vonquér

VONQUÉR GESTORA DE RECURSOS LTDA.

Segurança da Informação

1. Introdução

A Política de Segurança da Informação ("Política") visa o adequado gerenciamento das informações de posse temporária ou de propriedade da Vonquér Gestora de Recursos Ltda. ("Vonquér" ou "Gestora"). Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A responsabilidade em relação à segurança da informação deve ser comunicada no início do vínculo com a Gestora, devendo os mesmos assinar o Termo de Compromisso atestando conhecimento e comprometimento com as normas internas, e a que esteja sujeita a Gestora, no caso de colaboradores, ou atender ao modelo de diligência do Anexo I desta Política, no caso de prestadores de serviço.

A área de *Compliance* realizará a revisão e atualização desta Política periodicamente ou sempre que algum fato relevante ou evento justifique sua revisão antecipada, conforme análise e decisão do Diretor de *Compliance*.

2. Confidencialidade

Por "Informação Confidencial", entende-se: informação resguardada contra a revelação pública não autorizada, ou seja, toda a informação eletrônica, escrita ou falada da qual o Colaborador tiver acesso dentro da Gestora, incluindo: dados da Vonquér, seus sócios, diretores, clientes e Colaboradores em geral, bem como de relatórios de órgãos reguladores, autorreguladores e do poder público, dados de inspeções e fiscalizações, materiais de marketing e demais informações de propriedade da Gestora.

3. Controles de Acesso a Informações Confidenciais

Todo acesso a diretórios e sistemas de informações da Gestora deve ser controlado. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pelo Diretor de *Compliance*.

O controle do acesso a sistemas de informações da Gestora levará em conta as seguintes premissas:

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil; e
- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora.

4. Barreira de Controle de Informações

Os Colaboradores detentores de Informações Confidenciais ou Privilegiadas, em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

- Os Colaboradores devem evitar circular em ambientes externos à Gestora com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;

- O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;
- As informações que possibilitem a identificação de um cliente da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da Gestora ou do próprio cliente;
- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc; e
- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

5. Identificação dos Detentores da Informação, Manutenção de Registros e *Logs*

O Diretor de *Compliance* deve manter o registro dos Colaboradores que detenham Informações Confidenciais, com a indicação do tipo de informação detida, devendo informar aos demais Diretores da Gestora todas as Informações Confidenciais que estejam em poder dos Colaboradores que possam significar restrição nas operações da Gestora.

Será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que os usuários (*login*) individuais de Colaboradores internos serão de responsabilidade do próprio e os usuários (*login*) de terceiros serão de responsabilidade do diretor da área contratante. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

Com relação ao monitoramento e auditoria do ambiente, os Notebooks possuem sistema de arquivamento de Logs. A informação gerada por esse sistema poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

A Gestora informa, ainda, que poderá tomar as seguintes medidas:

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Diretor de *Compliance*;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; ou
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da Gestora e sujeitará o usuário às sanções administrativas e legais cabíveis.

Para fins de ilustração, segue uma lista não exaustiva de eventuais exemplos que podem ocasionar sanções: uso ilegal de software; introdução (intencional ou não) de vírus de informática; tentativas de acesso não autorizado a dados e sistemas; ou divulgação de informações sensíveis da Gestora.

6. Proteção da Base de Dados

Os recursos computacionais da Gestora devem ser: (i) protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora atue em mercado regulado.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (*backups*) e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases deve ser limitado somente a pessoas autorizadas pela área de *Compliance.*

7. Vazamento de Informações Confidenciais

Os Colaboradores deverão comunicar à área de *Compliance* quaisquer casos de violações às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Em caso de vazamento de informação confidencial, o Diretor de *Compliance* julgará qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos.

8. Testes e Treinamento de Segurança da Informação

A Gestora realizará testes periódicos de segurança para os sistemas de informações (sem se limitar a, mas em especial, para os meios eletrônicos), no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. O treinamento sobre segurança de informação fará parte do treinamento inicial e periódico da Gestora, o qual deverá considerar, dentre outros, assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos.

SEGURANÇA CIBERNÉTICA

1. Objetivo

A Política de Segurança Cibernética (“Política”) tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política segue práticas de mercado, bem como está de acordo com as leis, regulamentação e autorregulação aplicáveis, incluindo o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e o Guia de Cibersegurança de dez/2017.

2. Princípios

O objetivo desta Política é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Gestora devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Gestora.

Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Gestora poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

A Vonquér exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

3. Responsabilidade

3.1. Responsável pela Segurança Cibernética

O Sr. Carlos Eduardo Lopes Carvalho é o responsável por esta Política, sendo o principal responsável dentro da Gestora para tratar e responder questões de segurança cibernética ("Responsável pela Segurança Cibernética"), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Seguem abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

• Testar a eficácia dos controles utilizados e identificar os riscos residuais.

• Configurar os equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

• Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

• Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

• Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Gestora, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Gestora.

• Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Gestora.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética.

3.3. Responsabilidade Geral

Caberá a todos os Colaboradores conhecer e adotar as disposições da presente Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da Gestora, o Colaborador deverá comunicar imediatamente ao Responsável pela Segurança Cibernética, diretamente ou por meio do canal apropriado. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

4. Identificação/Avaliação de Riscos (*risk assessment*)

A Gestora periodicamente, no mínimo anualmente, deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pelo Responsável pela Segurança Cibernética e pelo responsável pela área de gestão da Vonquér, o qual deverá ser documentado pelo Responsável pela Segurança Cibernética com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Gestora. A Gestora poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança Cibernética julgue necessário.

Após a condução do referido processo, o Responsável pela Segurança Cibernética avaliará as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Gestora, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade de o evento acontecer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar

  vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”);

- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
- Vazamento de informações durante tráfego de dados não criptografados.

Periodicamente, no mínimo anualmente, deverá a Gestora revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

5. Ações de Prevenção e Proteção

A Gestora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Internet, e-mail e computadores

A Vonquér oferece a seus Colaboradores uma completa estrutura material e tecnológica para o exercício das atividades. É de responsabilidade do Colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

Os Colaboradores da Vonquér deverão zelar pela conservação do computador utilizado, devendo para tanto realizar periodicamente a verificação da existência de vírus, bem como a manutenção do antivírus atualizado. Sendo constatada a presença de vírus ou qualquer anomalia, o Colaborador da Vonquér deverá comunicá-la imediatamente ao responsável da área.

Além disso, o Colaborador é responsável pela proteção de seu banco de dados, seja ele composto por planilhas, e-mails e/ou conversas telefônicas contendo dados confidenciais de clientes e/ou da Vonquér, dentre outros.

- Os equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Vonquér e sob nenhuma hipótese servirão de instrumento à discriminação em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei;
- A utilização de equipamentos para fins particulares não é permitida;
- A instalação de cópias de arquivos e programas, ou downloads de arquivos e programas de qualquer natureza, obtidos de forma gratuita ou remunerada, em computadores da Vonquér, depende de autorização expressa do Responsável pela Segurança Cibernética e deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes, bem como os bons costumes, sendo vedada a cópia de softwares que promovam discriminação de qualquer tipo ou espécie;
- Periodicamente e sem aviso prévio serão realizadas inspeções nos computadores para averiguação de *downloads* impróprios não autorizados ou gravados em local indevido;
- O correio eletrônico disponibilizado pela Vonquér caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo de utilização exclusiva para alcançar os fins comerciais aos quais se destina;
- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (os “Email’s Corporativos”), seus respectivos anexos, e a navegação através da rede mundial de computadores (a “Internet”) através de equipamentos da Vonquér poderão ser monitoradas. A navegação pela Internet deverá ser feita observando as melhores práticas de boa conduta da

Vonquér. A Vonquér se reserva ao direito de bloquear sites da Internet inapropriados ou que firam as morais e bons costumes. Toda a navegação na Internet poderá ser monitorada pela Vonquér;

- Os E-mail's Corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem;
- Nos equipamentos e computadores disponibilizados pela Vonquér não é autorizado o uso de e-mails públicos (*webmails*) ou qualquer outro tipo de correio eletrônico que não seja o correio corporativo da Vonquér.

Senhas

Senhas de caráter sigiloso, pessoal e intransferível serão fornecidas aos Colaboradores para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas deverão ser transmitidas a pessoas que não sejam Colaboradores, sendo os Colaboradores responsáveis pela manutenção de cada senha com suas características.

Monitoramento Telefônico

As conversas telefônicas poderão ser monitoradas e gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política, inclusive no âmbito judicial.

5.1. Procedimentos de Segurança Cibernética de Terceiros

Os Colaboradores externos da Vonquér, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de Colaboradores externos, envolve determinados riscos que devem ser levados em conta pela Gestora, demandando certos cuidados proporcionais a esta identificação de ameaças.

5.1.1. Avaliação dos Terceiros Contratados

Nesse sentido, a área de *Compliance* da Gestora deverá verificar o conteúdo mínimo de *compliance* em segurança cibernética de terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (links) com a Gestora ou (iv) qualquer outros que a área de *Compliance* julgue que por qualquer motivo possa gerar risco de cibersegurança à Gestora, previamente à sua contratação, na forma do Anexo I a esta Política.

O resultado será usado pelo Responsável de Segurança Cibernética para avaliação da capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

5.1.2. Requisitos de Segurança da Informação nos Contratos com Terceiros

A Gestora deverá incluir em contratos com Colaboradores externos requisitos de segurança da informação nos contratos de prestação de serviços, bem como verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

6. Monitoramento e Testes

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; e (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

Para garantir as regras mencionadas nesta Política, a Gestora deverá:

- Implantar sistemas de monitoramento nas estações de trabalho. A informação gerada poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Para os riscos associados a *Phishing*, conduzir treinamentos e campanhas periódicas;
- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso o Responsável pela Segurança Cibernética julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

7. Plano de Resposta a Incidente

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios (“Plano”), considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos.

Os Colaboradores poderão reportar incidentes diretamente ao Responsável pela Segurança Cibernética ou por meio do canal de reporte de incidentes: compliance@vonquer.com.

7.1. Procedimento em Caso de Incidente

Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá dar início ao Procedimento de Contingência a seguir:

Avaliação Inicial

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Responsável pela Segurança Cibernética e tomadas após o incidente. O foco deverá ser 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, deve o Responsável pela Segurança Cibernética tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à CVM, ANBIMA ou mais alguma autoridade, (iI) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial a Investidor que tenha sido afetado; e (iv) houve prejuízo para a Gestora, algum veículo de investimento ou investidor específico. Além disso, o Responsável pela Segurança Cibernética, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um call diário ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pelo Responsável pela Segurança Cibernética, com um sumário elaborado pelo mesmo contendo as medidas a serem tomadas, responsabilidades e prazos.

Também deverá se avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, enquanto o Diretor de Gestão verificará se todas as informações necessárias ao portfólio estão seguras e a área de gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados ao Responsável pela Segurança Cibernética. Colaboradores externos relevantes deverão ser mantidos atualizados.

Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao *full compliance*, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de *Compliance* deverá registrar o histórico em local adequado.

8. Reciclagem e Revisão

A Gestora deverá manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em cibersegurança, com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações, como parte de suas responsabilidades.

O Responsável pela Segurança Cibernética, realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou

evento motive sua revisão antecipada, conforme análise e decisão do Responsável pela Segurança Cibernética.

Anexo I - Modelo de Diligência de Cibersegurança com Terceiros

Conteúdo mínimo de Compliance em segurança cibernética a ser verificado:

1. A empresa tem políticas, programa e procedimentos formais relativos à segurança da informação e cibersegurança? a. Se sim, é objeto de teste ou auditoria periódica? b. Se não, está em fase de elaboração? Qual é o prazo de finalização dele para devido envio à instituição contratante?

2. A empresa apresenta plano de resposta a incidentes de cibersegurança?

3. A empresa apresenta ações de conscientização, educação e formação de segurança da informação junto a seus funcionários?

4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados transacionados com a empresa contratante?

5. Quais são as práticas aplicadas para detectar atividade não autorizadas nos sistemas utilizados? Solicitar também designação de responsável por detectar tais atividades e a quem se reporta.

6. Na eventualidade de detecção de incidente de cibersegurança, o relato é feito por meio de canais de gestão apropriadas o mais rápido possível? Há comunicação a clientes e/ou reguladores (quando aplicável)?

Favor disponibilizar os seguintes documentos:

- Programa de segurança cibernética: se a organização segue políticas, programa e procedimentos formais relativos à segurança da informação e cibersegurança, recomenda-se solicitar envio da documentação à empresa contratante para avaliação e arquivamento. Solicitar também o último relatório de teste/auditoria periódica.
- Certificações: solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço.