Qonta

POLÍTICA DE SEGURANÇA CIBERNÉTICA DA QONTA

CONTROLE DE ATUALIZAÇÕES E VERSÕES				
Versão	**Data**	**Responsável**	**Aprovado Por**	**Detalhamento da Alteração**
1.0	11/2025	Henrique B.	Conselho Administrativo	Versão inicial da Política de Segurança Cibernética da Qonta

1. Objetivo

Esta Política de Segurança da Informação e Cibersegurança estabelece as diretrizes gerais adotadas pela Qonta Serviços de Tecnologia Ltda. ("Qonta") para a proteção das informações, ativos tecnológicos, sistemas e ambientes digitais sob sua responsabilidade, bem como para a mitigação de riscos relacionados a incidentes de segurança, incluindo acessos não autorizados, indisponibilidade de sistemas, comprometimento de aplicações e outros eventos de natureza similar.

Esta Política possui caráter institucional e orientativo, não descrevendo controles técnicos específicos, os quais estão detalhados no Anexo Técnico de Cybersegurança da Qonta, que a complementa.

2. Escopo e Aplicação

Esta Política aplica-se a todos os sistemas, plataformas, aplicações, APIs e ambientes tecnológicos sob responsabilidade direta da Qonta, bem como às pessoas físicas ou jurídicas que, direta ou indiretamente, tenham acesso a tais ambientes no contexto da prestação de serviços, incluindo colaboradores, prestadores de serviços, parceiros e fornecedores.

A Qonta opera segundo um modelo integralmente digital (digital first), não mantendo instalações físicas próprias destinadas à execução de suas atividades operacionais. Assim, esta Política limita-se a ambientes digitais e tecnológicos.

Esta Política não se aplica a sistemas, infraestruturas ou ambientes que estejam sob controle exclusivo de terceiros parceiros, os quais permanecem sujeitos às suas próprias políticas, controles e obrigações legais e regulatórias, sem prejuízo das responsabilidades assumidas contratualmente perante a Qonta.

3. Princípios de Segurança da Informação

As diretrizes de cibersegurança da Qonta são orientadas pelos seguintes princípios:

- **Confidencialidade**, assegurando que informações sejam acessadas apenas por pessoas, sistemas ou processos devidamente autorizados;
- **Integridade**, garantindo que informações não sejam alteradas, corrompidas ou destruídas de forma indevida;

- **Disponibilidade**, garantindo que sistemas e informações estejam acessíveis quando necessário;

- **Rastreabilidade e responsabilização**, assegurando o registro e o monitoramento de eventos relevantes de segurança.

4. Classificação da Informação

A Qonta adota diretrizes para classificação das informações sob sua responsabilidade, com o objetivo de assegurar que dados e informações recebam níveis de proteção compatíveis com sua criticidade, sensibilidade e requisitos legais ou contratuais.

As informações podem ser classificadas, de forma não exaustiva, nos seguintes níveis:

• Pública: informações cujo acesso é livre ou autorizado para divulgação externa;

• Interna: informações de uso interno da Qonta, não destinadas à divulgação pública;

• Confidencial: informações cujo acesso é restrito a pessoas ou sistemas autorizados, podendo causar impacto relevante em caso de divulgação não autorizada;

• Sensível ou Restrita: informações críticas, incluindo dados pessoais sensíveis, segredos de negócio ou informações protegidas por obrigações legais, regulatórias ou contratuais.

Os critérios detalhados de classificação, manuseio, armazenamento, compartilhamento e descarte das informações são definidos em normas e procedimentos internos complementares.

5. Modelo Operacional e Infraestrutura de Terceiros

A Qonta presta seus serviços por meio de integrações tecnológicas e do uso de infraestruturas operadas por terceiros, incluindo provedores de tecnologia e instituições de pagamento reguladas.

Entre esses parceiros, destaca-se a Celcoin Instituição de Pagamento S.A. (CNPJ nº 13.935.893/0001-09), responsável pelos controles de segurança, continuidade e resiliência dos ambientes sob seu controle, nos termos da legislação aplicável e dos contratos firmados.

Os controles de segurança cibernética, continuidade de negócios e recuperação de desastres relativos a ambientes operados por terceiros são de responsabilidade desses parceiros. A Qonta adota medidas técnicas, organizacionais e contratuais razoáveis para assegurar que as integrações ocorram de forma segura, sem que isso implique assunção de responsabilidade integral por eventos ocorridos fora de seu controle direto.

6. Governança, Responsabilidade e Conscientização

A Qonta mantém governança interna voltada à segurança da informação e cibersegurança, responsável por definir diretrizes gerais, supervisionar controles aplicáveis e avaliar riscos relevantes associados à sua operação tecnológica.

A Qonta promove ações de conscientização e treinamento em segurança da informação e cibersegurança, proporcionais ao porte da organização, ao modelo operacional e às funções exercidas por colaboradores e prestadores de serviços, com o objetivo de reduzir riscos associados a erro humano, uso indevido de credenciais e práticas inseguras.

O responsável pelo tema de segurança da informação, cibersegurança e proteção de dados no âmbito da Qonta é:

Felipe S.

E-mail de contato: **dpo@qonta.com.br**

Este canal destina-se a comunicações relacionadas à segurança cibernética e proteção de dados no contexto das atividades da Qonta.

7. Gestão de Riscos de Segurança da Informação

A Qonta realiza avaliações periódicas de riscos de segurança da informação e cibersegurança, considerando ameaças, vulnerabilidades, impactos potenciais e dependência de infraestruturas de terceiros.

Os resultados dessas avaliações são utilizados como subsídio para:

• Priorização de controles técnicos e organizacionais;

• Definição de planos de mitigação e tratamento de riscos;

• Apoio à tomada de decisão pela governança interna;

• Revisão e aprimoramento contínuo das práticas de segurança.

A metodologia, periodicidade e critérios de aceitação de riscos são definidos em procedimentos internos, observadas as limitações do modelo operacional e o princípio da proporcionalidade

8. Diretrizes Gerais de Segurança Cibernética

A Qonta adota um conjunto de diretrizes gerais de segurança cibernética alinhadas às melhores práticas de mercado, com o objetivo de reduzir riscos, proteger seus ativos tecnológicos e assegurar a resiliência de seus serviços, avaliando riscos de segurança cibernética de forma proporcional ao seu modelo operacional, utilizando essas avaliações como subsídio para priorização de controles e tratamento de incidentes.

Essas diretrizes incluem, entre outras:

- **Controle de acesso lógico**, com concessão de acessos baseada em necessidade de negócio, segregação de funções e princípio do menor privilégio, incluindo revisão periódica de perfis de acesso;

- **Gestão de identidades e credenciais**, contemplando mecanismos de autenticação adequados à criticidade dos sistemas e ambientes;

- **Proteção criptográfica**, com uso de criptografia para dados em trânsito e em repouso, quando aplicável;
- **Monitoramento e registro de eventos**, com geração de logs e trilhas de auditoria para fins de segurança, rastreabilidade e investigação de incidentes;
- **Gestão de vulnerabilidades**, incluindo identificação, priorização e tratamento de falhas de segurança em sistemas e aplicações;
- **Desenvolvimento seguro**, com incorporação de práticas de segurança ao longo do ciclo de vida de desenvolvimento de software;
- **Proteção de ambientes**, incluindo segregação entre ambientes de desenvolvimento, teste e produção.

Os controles técnicos e operacionais específicos que materializam essas diretrizes encontram-se descritos no Anexo Técnico de Cybersegurança da Qonta, não fazendo parte do escopo desta Política.

9. Segregação Lógica e Arquitetura Multi-Tenant

A Qonta adota arquitetura tecnológica que privilegia a segregação lógica de dados, contas e recursos, de modo a reduzir riscos de acesso indevido, vazamento de informações ou exposição entre clientes distintos.

Os mecanismos de segregação lógica são implementados considerando:

- identificação inequívoca de contextos, contas e clientes;
- validações de acesso em nível de aplicação e infraestrutura;
- controles que impeçam consultas ou operações cruzadas entre diferentes clientes.

A segregação adotada é de natureza lógica, compatível com ambientes compartilhados e em nuvem, não havendo segregação física dedicada por cliente.

A Qonta adota medidas voltadas à proteção de dados ao longo de todo o seu ciclo de vida, incluindo armazenamento, processamento, transmissão e descarte, observadas as diretrizes estabelecidas nesta Política e no Anexo Técnico.

10. Continuidade de Negócios e Recuperação de Desastres (Infraestrutura)

A Qonta mantém práticas voltadas à continuidade da infraestrutura tecnológica sob sua responsabilidade, com foco na preservação da disponibilidade mínima necessária à prestação de seus serviços digitais.

Essas práticas incluem, de forma proporcional ao porte e ao modelo operacional da Qonta:

- realização de backups periódicos de dados e configurações relevantes;

- utilização de infraestrutura em nuvem e serviços gerenciados, que incorporam mecanismos de redundância, alta disponibilidade e recuperação;
- definição de procedimentos internos para restauração de ambientes e serviços em caso de falhas relevantes;
- priorização da recuperação de componentes considerados críticos para a operação.

A Qonta não estabelece garantias públicas de tempo máximo de recuperação ou disponibilidade contínua, uma vez que parte relevante da operação depende de infraestruturas operadas por terceiros parceiros, incluindo instituições de pagamento e provedores de tecnologia, cujos planos de continuidade e recuperação são de sua exclusiva responsabilidade.

11. Gestão de Incidentes de Segurança Cibernética

A Qonta mantém procedimentos para identificação, registro, análise, tratamento e encerramento de incidentes de segurança cibernética que afetem sistemas ou ambientes sob sua responsabilidade.

Para fins desta Política, considera-se incidente de segurança qualquer evento que resulte ou possa resultar em:

- acesso não autorizado a sistemas, aplicações ou informações;
- indisponibilidade relevante de serviços ou funcionalidades;
- comprometimento da integridade de aplicações ou ambientes;
- falhas relevantes de segurança que possam afetar a operação.

Os incidentes são classificados de acordo com sua criticidade operacional e tratados observando-se os níveis de severidade e prazos de início de atendimento definidos pela Qonta em sua política interna de SLAs, incluindo:

- **Crítico**: início do atendimento em até duas horas corridas;
- **Alta severidade**: início do atendimento entre quatro e seis horas;
- **Média severidade**: início do atendimento entre oito e doze horas;
- **Baixa severidade**: início do atendimento entre doze e vinte e quatro horas;
- **Bug**: registro por meio de abertura de ticket para tratamento conforme priorização técnica.

Os prazos referem-se exclusivamente ao início do atendimento e da análise, não constituindo garantia de resolução definitiva dentro desses períodos.

12. Acessos Indevidos, Uso Irregular e Incidentes de Segurança

A Qonta adota medidas para prevenir, detectar e tratar situações de acesso indevido, uso irregular de sistemas ou tentativas de violação de seus ambientes tecnológicos, incluindo:

- acessos não autorizados por terceiros;
- uso indevido de credenciais legítimas;
- tentativas de exploração de vulnerabilidades;
- falhas de configuração que resultem em exposição de sistemas ou dados.

Esses eventos são tratados como incidentes de segurança cibernética e seguem os procedimentos de gestão de incidentes previstos nesta Política.

Quando tais incidentes envolverem dados pessoais, seu tratamento observará adicionalmente a Política de Privacidade da Qonta e a legislação aplicável, sem prejuízo das medidas de segurança e contenção adotadas no âmbito cibernético.

13. Comunicação e Compartilhamento de Informações

A Qonta poderá comunicar clientes, parceiros, fornecedores ou autoridades competentes acerca de incidentes de segurança cibernética que impactem de forma relevante seus serviços, sempre que tal comunicação for necessária ou legalmente exigida.

O compartilhamento de informações relacionadas a incidentes observará, cumulativamente:

- o princípio da necessidade e proporcionalidade;
- os deveres de sigilo e confidencialidade;
- a utilização de canais seguros;
- a preservação da integridade de investigações em curso.

Quando o incidente envolver infraestruturas de terceiros parceiros, a Qonta poderá atuar de forma coordenada com esses parceiros, respeitados os limites contratuais e técnicos aplicáveis.

14. Portabilidade de Dados e Continuidade em Caso de Insolvência

Na hipótese de descontinuidade das atividades da Qonta, poderá ser viabilizada, quando tecnicamente possível, a exportação de dados que não estejam protegidos por sigilo legal, regulatório ou contratual.

A portabilidade observará:

- os limites da legislação aplicável;
- as obrigações contratuais vigentes;
- as responsabilidades e limitações técnicas dos parceiros de infraestrutura envolvidos.

A Qonta não garante a preservação ou migração integral de dados em todos os cenários, especialmente quando houver dependência de infraestruturas operadas por terceiros.

15. Limitações e Não Garantia

As medidas de cibersegurança adotadas pela Qonta visam reduzir riscos, mas não eliminam completamente a possibilidade de incidentes de segurança, falhas técnicas ou eventos adversos, especialmente em ambientes digitais complexos e integrados a terceiros.

16. Documento Relacionado

Esta Política deve ser lida em conjunto com o seguinte documento complementar:

- Anexo I – Anexo Técnico de Cybersegurança da Qonta
- Anexo II – Gestão de Incidentes de Segurança Cibernética

Qonta

Anexo I – Anexo Técnico de Cybersegurança da Qonta

1. Objetivo

Este anexo técnico tem como objetivo descrever os controles técnicos, operacionais e de segurança adotados na plataforma, fornecendo subsídios para processos de due diligence, auditoria, avaliação de riscos e compliance regulatório. Os controles descritos neste Anexo refletem a arquitetura e ferramentas atualmente adotadas pela Qonta e podem ser ajustados ao longo do tempo, sem prejuízo das diretrizes gerais estabelecidas na Política.

2. Autenticação

A plataforma utiliza o AWS Cognito como serviço central de autenticação. Todas as APIs são validadas nativamente na AWS antes de atingir o ambiente de aplicação, assegurando que apenas requisições autenticadas sejam processadas.

As políticas de autenticação seguem boas práticas de mercado, incluindo requisitos de senha forte, expiração e renovação controlada de tokens, bem como uso de refresh tokens com tempo de vida limitado.

3. Autorização e controle de acesso

O controle de acesso foi projetado para mitigar riscos de acesso indevido, incluindo cenários associados ao controle de acesso quebrado (Broken Access Control).

Existe um mecanismo próprio de autorização aplicado a todos os usuários autenticados, responsável por validar permissões em nível de recurso e ação.

O modelo de autorização é baseado em ações internas, atualmente com mais de 400 ações cadastradas (exemplos: consulta de saldo, simulação de empréstimo, consulta de dict). Cada API está vinculada a uma ação específica, permitindo segregação e controle granular de permissões.

Todas as rotas de API exigem obrigatoriamente o tenantId e, quando aplicável, o número da conta, seguindo o padrão:

/api/tenant/{tenantId}/account/{accountNumber}/recurso

No processamento da requisição, são realizadas validações cruzadas, incluindo:

- Validação das informações de identidade exclusivamente por meio do JWT emitido pelo Cognito, garantindo imutabilidade dos dados ao longo do fluxo.

- Conferência de atributos definidos no momento da emissão do token, incluindo tenantId e identificadores do usuário.

- Verificação de correspondência entre o tenantId presente na requisição e o tenantId contido no JWT.

- Validação do canal de acesso autorizado para o perfil do usuário (exemplo: restrição de usuários de back office a canais específicos).

- Verificação de vínculo entre usuário e conta, existência da conta, permissões do perfil para execução da ação solicitada e status do usuário.

4. Arquitetura multi-tenant

A solução foi desenvolvida com abordagem multi-tenant desde sua concepção. Todos os dados armazenados possuem associação obrigatória ao tenantId, impedindo consultas ou operações sem a correta identificação do tenant.

Rotas, serviços internos, APIs e bases de dados utilizam o tenantId como parte da chave primária ou identificador lógico, promovendo segregação de dados e reduzindo riscos de exposição entre tenants.

5. Infraestrutura e isolamento de ambientes

A plataforma não utiliza servidores gerenciados manualmente. Toda a infraestrutura é provisionada via infraestrutura como código, utilizando AWS CloudFormation, com versionamento em repositórios Git e pipelines automatizados de deploy via GitHub Actions.

Os ambientes de desenvolvimento e produção estão isolados em VPCs e VPNs, sem acesso direto externo. O tráfego ocorre exclusivamente por aplicações executadas na AWS, como funções Lambda, expostas por APIs protegidas pelo AWS API Gateway com autenticação integrada ao Cognito.

6. Gerenciamento de patches e atualizações

Toda a arquitetura de aplicação é baseada em serviços serverless, eliminando a necessidade de gerenciamento direto de sistemas operacionais. A AWS é responsável pela aplicação de patches de segurança, atualizações e manutenção da infraestrutura subjacente.

Os bancos de dados relacionais utilizam serviços gerenciados da AWS, com aplicação automática de patches para versões LTS estáveis, executada em janelas programadas.

7. Integrações máquina a máquina

As integrações máquina a máquina em ambiente de produção utilizam controle de acesso por whitelist de endereços IP, configurada por tenant, autenticação via API Key e aplicação das mesmas camadas de autorização e validação utilizadas nos demais canais.

8. PIN transacional

O PIN transacional é implementado utilizando recursos do AWS Cognito. Internamente, é criado um usuário dedicado no Cognito com prefixo interno, sendo o PIN representado pelas quatro últimas letras de uma senha, também com prefixo interno.

A validação do PIN ocorre por meio de middleware que autentica esse usuário dedicado. Esse modelo garante que o armazenamento das credenciais seja realizado de forma segura pelo Cognito, não permitindo recuperação ou listagem de senhas, apenas redefinição.

O controle permanece sob serviços gerenciados da AWS, protegidos por camadas de firewall e políticas de acesso IAM.

9. Relacionamento entre usuários e contas

A plataforma mantém um mecanismo interno de vinculação entre usuários e contas, suportando cenários como múltiplas contas por usuário, permissões delegadas (por exemplo, contadores) e acessos ampliados para usuários internos de back office.

10. Limites transacionais

Existe um módulo centralizado de gestão de limites transacionais desenvolvido internamente.

Cada transação é validada online, com base no histórico recente de movimentações do cliente, para decisão de aprovação ou rejeição.

Esse módulo é utilizado de forma transversal por todos os fluxos transacionais da plataforma.

11. Validações de liveness

Validações de liveness são exigidas em fluxos considerados críticos, incluindo criação de conta, troca de senha, troca de dispositivo e outras operações sensíveis.

12. Autenticação adicional (OTP)

A plataforma utiliza códigos de uso único (OTP) como fator adicional de autenticação em diversos fluxos. Os canais suportados incluem WhatsApp, SMS e e-mail.

13. Controle de dispositivos

Existe controle por device ID autorizado para cada conta. Caso um novo dispositivo tente realizar transações, é obrigatória a execução de um novo processo de liveness para liberação, reduzindo riscos de clonagem ou uso não autorizado.

14. Autenticação multifator (TOTP)

Há integração com mecanismos de autenticação baseada em TOTP, como Google Authenticator. Esse fator é obrigatório para o canal de internet banking. As sessões autenticadas possuem validade de uma hora.

15. Criptografia

Todos os dados em trânsito utilizam criptografia TLS 1.2.

Os dados em repouso são criptografados por meio do AWS KMS.

Determinadas informações sensíveis recebem camada adicional de criptografia antes de

serem persistidas em banco de dados.

16. Firewall e proteção perimetral

A plataforma utiliza os serviços de firewall gerenciados da AWS para proteção de front-end e back-end, incluindo mitigação de DDoS, controle de tráfego automatizado, limitação de requisições, proteção contra bots e outros vetores de ataque conhecidos.

O ambiente opera em modo de bloqueio automático para atividades suspeitas, incluindo tráfego originado de países sujeitos a sanções. As regras são majoritariamente gerenciadas pela própria AWS.

17. Backups e recuperação

São realizados backups diários de 100% dos recursos, com retenção atual de 35 dias.

Existe planejamento para ampliação do período de retenção para atender exigências regulatórias futuras, com previsão mínima de cinco anos.

18. Gerenciamento de segredos

Todas as credenciais, chaves e segredos são armazenados no AWS Secrets Manager, com controle de acesso baseado em políticas IAM e registro de uso.

19. Monitoramento e alertas

A plataforma possui monitoramento transacional contínuo, incluindo abertura de contas e análise de valores de transações de entrada e saída, considerando o perfil de consumo dos clientes.

São utilizadas ferramentas de monitoramento e observabilidade, como Datadog e serviços nativos da AWS.

Alertas específicos são configurados para eventos críticos, como tentativas de desembolso

de empréstimos sem saldo disponível.

20. Monitoramento de erros e incidentes

Existe monitoramento ativo de erros, timeouts e eventos anômalos em ciclos de cinco minutos.

Ocorrências geram notificações automáticas em canais internos de comunicação. A operação segue política de tratamento imediato de incidentes, evitando recorrência e normalização de falhas.

Qonta

Anexo II - Gestão de Incidentes de Segurança Cibernética

1. Objetivo

Este Anexo tem por objetivo estabelecer diretrizes operacionais para a gestão de incidentes de segurança cibernética relacionados aos sistemas, aplicações e ambientes tecnológicos sob responsabilidade da Qonta, incluindo procedimentos de identificação, classificação, tratamento, comunicação e encerramento.

Este Anexo complementa a Política de Cibersegurança da Qonta e não descreve controles técnicos específicos, os quais permanecem detalhados no Anexo Técnico de Cybersegurança.

2. Escopo

Este Anexo aplica-se exclusivamente a incidentes de segurança cibernética que afetem:

- sistemas, plataformas e aplicações sob responsabilidade direta da Qonta;
- integrações tecnológicas operadas pela Qonta;
- dados e informações processados nos ambientes controlados pela Qonta.

Incidentes ocorridos em infraestruturas operadas por terceiros parceiros seguem os procedimentos e políticas desses parceiros, cabendo à Qonta atuação coordenada nos limites de sua responsabilidade.

3. Definição de Incidente de Segurança

Para fins deste Anexo, considera-se incidente de segurança cibernética qualquer evento confirmado ou suspeito que resulte ou possa resultar em:

- acesso não autorizado a sistemas, aplicações ou informações;
- uso indevido de credenciais, perfis de acesso ou privilégios;
- indisponibilidade relevante de sistemas ou serviços;
- comprometimento da integridade de aplicações, dados ou ambientes;
- exposição indevida de informações;
- falhas relevantes de segurança que afetem a operação.

4. Classificação de Severidade

Os incidentes são classificados de acordo com sua criticidade operacional, considerando impacto, urgência e abrangência, nos seguintes níveis:

- **Crítico**
- **Alta Severidade**

- **Média Severidade**
- **Baixa Severidade**
- **Bug**

A classificação orienta a priorização do atendimento e o prazo de início das ações.

5. Prazos de Início de Atendimento (SLAs)

Os prazos para início do atendimento e da análise dos incidentes seguem os níveis definidos pela Qonta:

- **Crítico**: até **duas horas corridas**;
- **Alta severidade**: entre **quatro e seis horas**;
- **Média severidade**: entre **oito e doze horas**;
- **Baixa severidade**: entre **doze e vinte e quatro horas**;
- **Bug**: registro por meio de abertura de ticket para tratamento conforme priorização técnica.

Os prazos acima não constituem garantia de resolução definitiva, servindo exclusivamente como referência para início do atendimento.

6. Fluxo de Gestão de Incidentes

De forma geral, a gestão de incidentes segue as seguintes etapas:

1. **Identificação**
   Detecção do evento por monitoramento, reporte interno ou comunicação de terceiros.
2. **Registro**
   Registro do incidente em sistema interno, com descrição inicial e evidências disponíveis.
3. **Classificação**
   Avaliação da severidade e definição da prioridade de atendimento.
4. **Início do Atendimento**
   Adoção das primeiras medidas técnicas conforme o SLA aplicável.
5. **Mitigação**
   Ações destinadas a conter o incidente e reduzir seus impactos operacionais.
6. **Encerramento**
   Encerramento do incidente após estabilização do ambiente, com registro das ações realizadas.

7. Acessos Indevidos e Uso Irregular

Eventos relacionados a acessos indevidos, uso irregular de sistemas, tentativas de exploração de vulnerabilidades ou uso abusivo de credenciais são tratados como incidentes de segurança cibernética e seguem integralmente o fluxo definido neste Anexo.

A Qonta poderá adotar medidas adicionais de contenção, incluindo bloqueio de acessos, suspensão de credenciais ou restrição temporária de funcionalidades, quando necessário para preservação da segurança.

8. Incidentes Envolvendo Dados Pessoais

Incidentes de segurança cibernética podem ou não envolver dados pessoais.

Quando um incidente envolver dados pessoais, sua avaliação, tratamento e eventual comunicação observarão, adicionalmente, as disposições da Política de Privacidade da Qonta e da legislação aplicável, sem prejuízo das medidas técnicas adotadas no âmbito da segurança cibernética.

9. Comunicação de Incidentes

A comunicação de incidentes poderá ocorrer quando:

- houver impacto relevante sobre os serviços prestados;
- houver obrigação legal ou regulatória;
- a comunicação for necessária para mitigação de riscos.

A Qonta observará os princípios da necessidade, proporcionalidade e confidencialidade, bem como a preservação de investigações técnicas em curso.

10. Incidentes em Infraestrutura de Terceiros

Quando o incidente ocorrer em ambientes operados por terceiros parceiros, a atuação da Qonta limitar-se-á a:

- coordenação com o parceiro responsável;
- acompanhamento das ações corretivas;
- comunicação aos clientes, quando aplicável.

A Qonta não controla diretamente os procedimentos internos, prazos ou decisões técnicas desses terceiros.

11. Registro e Evidências

A Qonta mantém registros dos incidentes tratados, contendo informações suficientes para fins de acompanhamento interno, auditoria e melhoria contínua, observadas as limitações legais, técnicas e contratuais de retenção.

Quando aplicável, incidentes relevantes podem ser objeto de análise posterior com foco em prevenção de recorrência e aprimoramento dos controles existentes

12. Limitações

Este Anexo não estabelece garantias de disponibilidade, continuidade, tempo máximo de recuperação ou ausência de incidentes, nem amplia as responsabilidades da Qonta além daquelas previstas na Política de Cibersegurança, nos contratos aplicáveis e na legislação vigente.