02.03.2021

C6 BANK

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

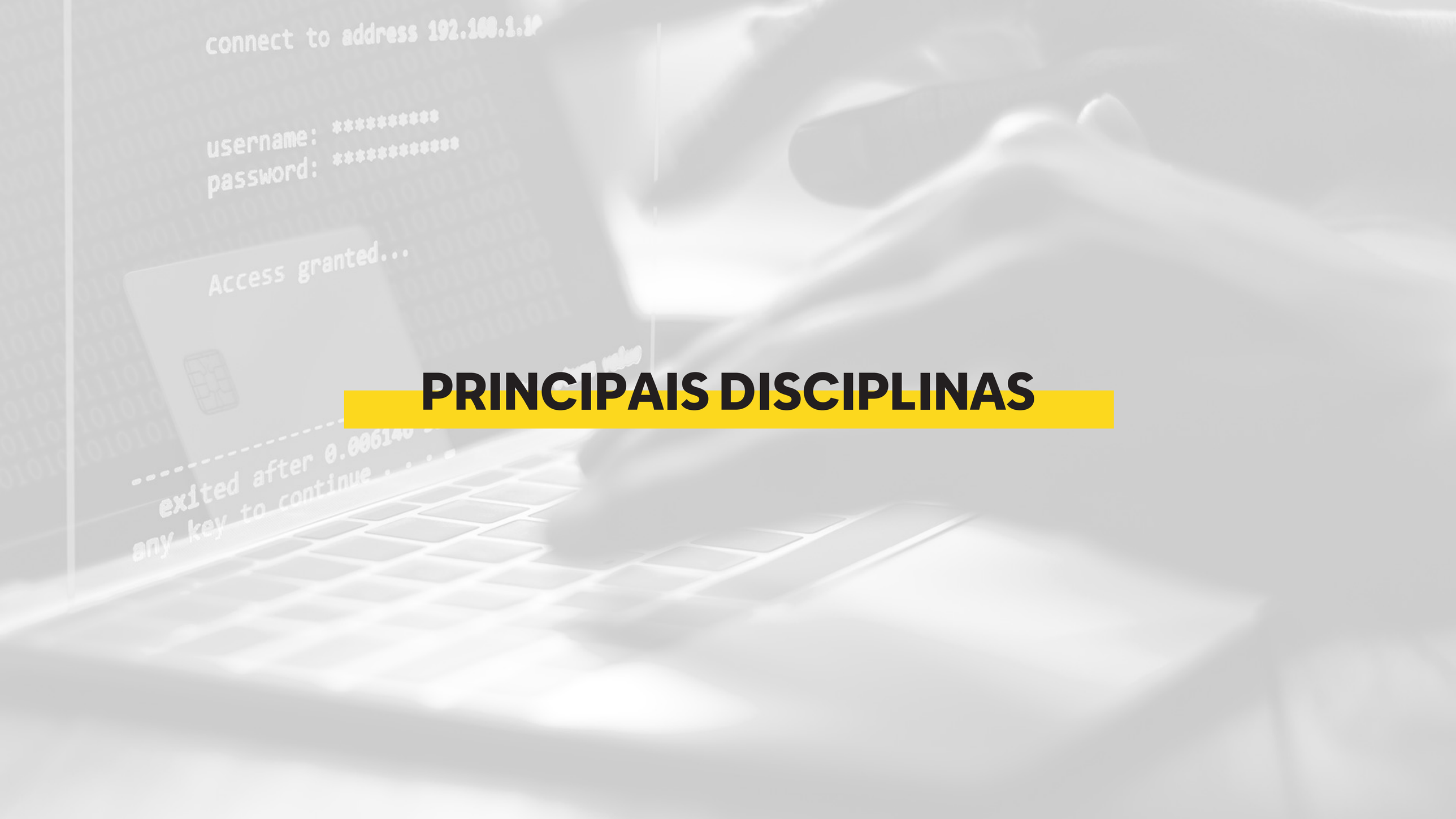
A Política de Segurança da Informação e Cibernética estabelece as diretrizes de segurança e proteção das informações que devem ser aplicadas nos ambientes de computação e de escritório do C6 Bank e da Carbon Holding e seus parceiros, pensando na melhoria da nossa segurança cibernética e dos dados e transações de nossos clientes.

Ela foi criada com base nas melhores práticas, leis e regulamentações do mercado, incluindo as regras da Lei Geral de Proteção de Dados Pessoais (LGPD), e está constantemente sendo revista e atualizada.

Objetivos & Estratégia

- A Diretoria da Carbon Holding está, desde a sua fundação, comprometida na melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

- O objetivo de Segurança na Carbon Holding é garantir a confidencialidade, integridade, disponibilidade, autenticidade, legalidade, não-repúdio e privacidade das informações por meio da prevenção, detecção, redução das vulnerabilidades e contenção de incidentes relacionados com o ambiente cibernético.



PRINCIPAIS DISCIPLINAS

Criptografia

- Os recursos de criptografia são utilizados para assegurar a confidencialidade, integridade, a autenticidade e o não repúdio das informações.

- São utilizadas a criptografia de chave simétrica para garantia da confidencialidade, e a criptografia de chave assimétrica para garantia da confidencialidade, integridade e não repúdio das informações. As funções de resumo (hash) são utilizadas para garantia da integridade de arquivos ou gerar assinaturas digitais.

Prevenção e detecção de intrusão

- Os incidentes de segurança podem causar impactos negativos financeiros, de imagem, operacionais ou que afetem diretamente a estratégia da Carbon Holding.

- Para evitar a ocorrência destes eventos, a Carbon Holding utiliza recursos tecnológicos para as atividades de monitoramento, identificação e bloqueio de qualquer comportamento ou tráfego de rede suspeito que pode indicar atividades potencialmente maliciosas, como uma tentativa de ataque ou uma exploração de vulnerabilidade.

- Os contratos com empresas terceiras e prestadores de serviço devem estabelecer a responsabilidade de colaboração ante a um incidente de segurança.

Classificação da informação

- A classificação das informações tem por objetivo identificar a criticidade, rotular e tratar as informações utilizando os controles aplicáveis de acordo com sua sensibilidade.

- O nível de sensibilidade das informações deve ser indicado através do uso de marcas e tarjas nos documentos e e-mails, classificando-as como Públicas, Internas, Restritas ou Confidenciais.

- É responsabilidade de todos os colaboradores e prestadores de serviço assegurar que as informações são classificadas corretamente e são compartilhadas por meios compatíveis com seu nível de confidencialidade.

Gestão de vulnerabilidades

- O processo de gestão de vulnerabilidades tem por objetivo identificar constantemente as fragilidades no ambiente tecnológico e avaliar o potencial risco para o negócio, desde a identificação até as atividades de remediação.

- São utilizados recursos de varredura (scan) de vulnerabilidades em redes, computadores, infraestrutura e aplicações, testes de intrusão simulando ataques externos, acompanhamento de notificações de fornecedores e contatos com entidades externas de segurança.

Cópias de segurança

- São realizadas cópias de segurança (Backups) e testes de recuperação (Restore) das informações corporativas e de clientes que são relevantes ao negócio, com tempo de retenção em linha com as leis e regulações aplicáveis ao segmento financeiro.

- A estratégia do Plano de Backup é consoante com a criticidade das informações à continuidade do negócio, e as rotinas e modalidades de Backup devem ser aplicadas conforme o cenário, considerando o plano tático de maior eficiência operacional.

- Nos casos onde as atividades de Backup e Restore são operadas por terceiros, as especificações devem estar previstas nos acordos entre as partes.

Gestão de identidade e acesso

- Para evitarmos todo e qualquer tipo de risco cibernético, seguimos uma metodologia de acesso que ajuda na identificação de cada usuário, controlando os sistemas e as respectivas senhas, verificando se elas seguem um padrão de segurança e utilizando recursos de autenticação em duas etapas sempre que possível.

- Trabalhamos com o princípio de menor privilégio, o que significa que você só tem acesso às funcionalidades necessárias para desempenhar o seu trabalho. Cada usuário tem um perfil que garante que todos os processos sejam feitos de maneira correta, permitindo o monitoramento dos acessos pelo sistema e a prevenção a acessos não autorizados.

Responsabilidade no uso da senha

- Todos os colaboradores são responsáveis por zelar por suas informações de autenticação.

- As senhas não devem ser compartilhadas ou armazenadas em locais inseguros e devem atender aos padrões mínimos exigidos pela Carbon Holding.

- As senhas são confidenciais e secretas, portanto, não devem ser compartilhadas com outras pessoas.

Uso de recursos tecnológicos

- O Conglomerado C6 disponibiliza aos usuários diversos recursos tecnológicos com propósito exclusivo de apoiar o desenvolvimento das atividades inerentes a função dos colaboradores e prestadores de serviço.

- Para proteger as informações são aplicados parâmetros e controles de segurança como antivírus, anti malware, DLP, entre outros. Tais recursos são passíveis de monitoramento.

- Não é permitida a instalação de Softwares e Hardwares não autorizados nos recursos tecnológicos da organização.

- Atitudes em dissonância com os valores estabelecidos na Carbon Holding não são toleradas.

Cultura e conscientização de segurança

- A estratégia de Segurança da Informação inclui estimular a cultura, conscientização e educação dos colaboradores e parceiros sobre a segurança da informação e prevenção a fraudes.

- Possuímos um programa contínuo de treinamentos, comunicações e diversas ações para conscientizar todos os colaboradores sobre o papel fundamental que cada um de nós tem na proteção de informações e dados da Carbon Holding.

- Realizamos interação com comunidades, comunicações periódicas via canais oficiais da Carbon Holding, mantemos um portal dedicado para instrução de clientes e realizamos diversas ações com o propósito de elevar a consciência de todo o público sobre o seu papel fundamental na proteção das informações.

Relacionamento com fornecedores e prestadores de serviço

- O time de Segurança possui a responsabilidade de avaliar os aspectos de segurança no relacionamento com fornecedores e prestadores de serviço cujo escopo de trabalho contemple o tratamento de informações de propriedade intelectual da Carbon Holding.

- São admitidas avaliações pela área de segurança, contemplando auditorias externas e, eventualmente, a realização de testes de intrusão (pentests) quando pertinente ao contexto e mediante consentimento do proprietário da informação.

Prevenção, identificação e tratamento de incidentes de segurança

- A Carbon Holding adota uma estrutura para prevenção, identificação e tratamento de incidentes de segurança em seu ambiente e em parceria com os provedores de serviço, inclusive aqueles alocados em nuvem.

- Os incidentes de segurança são classificados de acordo com seus impactos financeiros, de imagem, operacionais, ou que afetem diretamente a estratégia da organização, podendo ser classificados desde baixo até críticos.

- As equipes de tratamento de incidentes cibernéticos podem ser acionadas por e-mail através dos canais security@c6bank.com ou csirt@c6bank.com.

Privacidade dos titulares

- A Carbon Holding preza pela privacidade dos titulares de dados pessoais independentemente do seu vínculo com a empresa.

- Todos os produtos, projetos, processos, sistemas e controles são desenhados e executados sempre observando o tratamento de dados pessoais de forma adequada, alinhado junto aos titulares e de forma transparente e responsável.

- São exigidos os mesmos compromissos com a privacidade junto aos prestadores de serviços, parceiros e fornecedores.

- Os titulares dos dados pessoais podem entrar em contato com a Carbon Holding para obter entendimento sobre o tratamento de seus dados, quais dados são utilizados e quais são as respectivas justificativas para tais ações.

Segurança de aplicações e novas tecnologias

- Quando a Carbon Holding identificar a necessidade de desenvolver, adquirir, substituir ou incrementar suas ferramentas, sistemas, aplicativos ou tecnologias vigentes, deverão ser realizadas análises para observar a capacidade dos mesmos para cumprir com os requisitos mínimos de segurança.

- O C6 Bank estabeleceu um programa de recompensas para pesquisadores independentes que reportarem bugs e problemas de segurança em nossas aplicações (Bug Bounty), reforçando valores como o frescobol, transparência e ética.

Prevenção à fraudes

- Durante a execução de todos os processos de negócio, principalmente na criação de produtos e utilização de novas tecnologias, a área de Prevenção à Fraude pode estabelecer controles e monitorar comportamentos suspeitos que indiquem uma possível ação fraudulenta.

- A Carbon Holding compartilha conteúdo de conscientização para que clientes consigam distinguir ações legítimas das atividades de fraudadores.

- O C6 Bank disponibiliza uma cartilha especial com diversas recomendações em nosso site: https://www.c6bank.com.br/seguranca.

Sanções

- O não cumprimento das diretrizes declaradas nesta Política Corporativa está sujeito a sanções por parte da Carbon Holding.

- Os processos de gestão de consequências são tratados sob sigilo e zelando pela privacidade dos envolvidos.

Veja também outras dicas e recomendações de segurança que compartilhamos em nosso site: https://www.c6bank.com.br/seguranca.

SIGA OS CANAIS OFICIAIS DE COMUNICAÇÃO DO C6 BANK

- **Instagram**: instagram.com/c6bank/
- **Facebook**: facebook.com/C6bank
- **LinkedIn**: linkedin.com/company/c6-bank/
- **TikTok**: tiktok.com/@c6bank
- **Twitter**: twitter.com/C6Bank
- **YouTube**: youtube.com/c/C6BankOficial
- **Medium**: medium.com/c6banknoticias
- **C6 Pay**: instagram.com/c6pay/

02.03.2021

C6 BANK