PSC - POLÍTICA DE SEGURANÇA CIBERNÉTICA

Resolução n° 4.658 do Banco Central do Brasil, de 26/04/2018.

A CAROL DTVM LTDA, apresenta a Política de Segurança Cibernética, em aderência à Resolução n° 4.658 do Banco Central do Brasil, de 26 de abril de 2018 que orienta e estabelece as diretrizes na qual a CAROL, se enquadra para a Segurança Cibernética e a prevenção de responsabilidade legal para todos os usuários.

OBJETIVO

Está Política foi desenvolvida, levando-se em conta, o tamanho, o perfil e o enquadramento da CAROL no S 5.

Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

Conscientizar, educar os colaboradores por meio desta política, normas e procedimentos internos aplicáveis as suas atividades diárias;

Proteger o valor e a reputação da empresa;

Garantir a continuidade de seus negócios, protegendo dos processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

Levando em conta o perfil da CAROL, estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

1. PRINCÍPIOS

A proteção e privacidade de dados dos clientes refletem os valores da CAROL e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de proteção de dados.

Informações – Determinações: São coletadas de forma ética e legal, para propósitos específicos e devidamente informados; Somente serão acessadas por pessoas autorizadas e capacitadas para seu uso adequado; Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados; As informações constantes de nossos cadastros, bem como outras solicitações que venha garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

2. DIRETRIZES

O cumprimento desta Política é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer as seguintes diretrizes:

Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;

Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;

Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela CAROL;

Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;

Garantir a continuidade do processamento das informações críticas de negócios;

Atender as leis que regulamentam as atividades da CAROL e seu mercado de atuação;

Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;

Comunicar imediatamente o Setor de T.I a respeito de quaisquer descumprimentos desta Política.

3. AMBIENTE – SEGURANÇA FÍSICA E LÓGICA

Controle de responsabilidade na gestão e operação de recursos no processamento das informações, com garantia na segurança de redes locais e internet, com monitoramento no tratamento de respostas aos incidentes, minimizando o risco de falhas e administração segura da rede de comunicações. Equipamentos e instalações de processamento, são mantidos em área segura, visando sua integridade e disponibilidade.

4. CONTINUIDADE DE NEGÓCIOS

A gestão de segurança é feita no sentido de mitigar riscos, minimizar os impactos e, se necessário, recuperar perdas de ativos da informação, após incidentes, através de requisitos, tais como: funcionários chaves, análise de impacto nos negócios e testes periódicos de recuperação, com linhas diversas de web.

Para a devida garantia da continuidade de negócios, a Carol DTVM, possui práticas que visam garantir os três pilares da segurança da informação:

Confidencialidade: Ações tomadas para assegurar que informações confidenciais e críticas não sejam acessadas ou roubadas por pessoas desautorizadas.

Integridade: Ações para manutenção da consistência, confiabilidade e veracidade das informações e sistemas pela empresa ao longo dos processos ou de seu ciclo de vida, garantindo que os mesmos sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los, comprometê-los ou danificá-los.

Disponibilidade: Garantir a acessibilidade que se tem dos dados e sistemas da empresa e prover métodos e procedimentos que evitem ou reduzam ao máximo interrupções das operações da empresa como um todo.

5. MEDIDAS DE CONFIDENCIALIDADE, INTEGRIDADE e DISPONIBILIDADE

O controle de acesso às informações, são restringidos à menor permissão e privilégios possíveis, com revisão periódica e com a aprovação do gestor responsável da

informação, que são cancelados ao término do contrato de trabalho do colaborador ou prestador se serviço.

6. Classificação de Dados Sensíveis

Os ativos de informação gerados e utilizados na operação da Carol DTVM, incluindo planilhas, documentos e dados de sistemas são classificados de acordo com a relevância do impacto que o vazamento deste pode causar à Carol DTVM, sob o ponto de vista de imagem, operacional, legal e financeiro.

Estes ativos são classificados em 3 pesos diferentes e a partir desta divisão são definidos os devidos acessos e autorizações conforme abaixo:

- Restrito: Utilizado por um grupo restrito com pessoas pré-determinadas pela Diretoria Carol DTVM;
- Privado: Uso exclusivamente interno na Carol DTVM;
- Público: Informação que pode ser divulgada externamente;

7. Regras de Acesso Ao Recurso Computacional

Todos os recursos computacionais na Carol DTVM são acessados por meio login de usuário e senhas concedidos após autorização do Gestor do usuário ou, em caso de terceiros, pelo funcionário responsável pelo prestador de serviços.

Cada usuário possui o seu próprio login e senha, sendo esta, sua assinatura eletrônica pessoal e intransferível.

A Carol DTVM recomenda e realiza a configuração de seus serviços e sistemas para que sejam permitidos apenas senhas fortes.

Os seguintes critérios são utilizados para criação de senhas fortes:

- Duração máxima da senha: A senha deve ser alterada a cada 60 dias.
- Histórico de senhas: O mesmo usuário não pode repetir as últimas 4 senhas utilizadas
- Tamanho mínimo da senha
  - Mínimo de 6 caracteres para usuários da área de negócios e administrativa
  - Mínimo de 8 caracteres para usuários administradores

- Complexidade
  - As senhas devem ser compostas por no mínimo três das Regras abaixo:
    - Caracteres maiúsculos (A, B, C...) ○ Caracteres minúsculos (a, b, c...) ○ Numerais (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
    - Caracteres especiais (@ # &)

- Números de tentativas inválidas de logon: Em caso de 3 tentativas inválidas o login deve ser bloqueado.

- Desbloqueio: Desbloqueio deve ser solicitado para área de TI por telefone, presencialmente ou por e-mail corporativo

- Exclusão de conta por inatividade de uso
  - Com exceção de contas de serviços de sistemas, as contas dos usuários sem acesso há mais de 60 dias serão inativadas automaticamente, com exe.

8. Proteção Contra Software Malicioso

Todos os computadores da rede da Carol DTVM, bem como os servidores em nuvem, deverão estar protegidos por antivírus, software de firewall e as últimas atualizações de sistema operacional.

9. Mecanismos de Rastreabilidade

Todos os sistemas Contratados pela Carol DTVM, deverão rastrear as inclusões, alterações e exclusões de informações realizadas pelos usuários (logs) para que seja possível realizar auditorias e investigações internas e externas relacionadas às informações geradas.

Todos os documentos, planilhas e apresentações, considerados críticos para o funcionamento do negócio, são armazenados em serviços que permitem controlar a versão e alterações realizadas pelos usuários.

10. Controle de Gestão de Mudança de Sistemas (GMUD)

A fim de se evitar incidentes e garantir que a qualidade caminhe em conjunto com as constantes evoluções sistêmicas da operação, adotamos um conjunto de

procedimentos e ações necessárias para detectar, implementar e controlar as mudanças e aprimoramentos necessários.

Utilizamos ambientes distintos de sistemas para realização de testes de homologação e operação em produção. Desta forma, podemos nos certificar que todas as novas implementações sejam previamente testadas, homologadas e aceitas pelos colaboradores, antes de implantar em ambiente produtivo, evitando assim incidentes que impactam a operação.

Após aceita uma nova versão pelo usuário responsável, a mesma é sempre publicada em horário não útil para evitar interrupções e instabilidades no sistema produtivo.

11. Cópias de Segurança

Diariamente são realizadas cópias de segurança dos sistemas e dos arquivos documentos críticos para eventual restauração em caso de incidentes.

12. Redundância de Acessos

Operamos com dois links de Internet contratados de empresas distintas, para que, em caso de queda de serviço de um link, o acesso seja realizado por outro sem gerar impacto à operação.

13. POLÍTICAS PARA CONTINUIDADE DE NEGÓCIOS

13.1 Regras para Tratamento de Incidentes

São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento dos princípios de confidencialidade, integridade ou disponibilidade, colocando o negócio e seus objetivos em risco.

Todos os colaboradores da Carol DTVM, devem ter a capacidade de identificar e reportar incidentes sempre que presenciarem.

Todos os eventos que gerem interrupções, mau funcionamento, imprecisão ou vazamento de informação nos sistemas da empresa deve ser notificado o quanto antes para a área de Compliance, que irá registrar em um repositório único o evento ocorrido, bem como sua característica e nível de severidade.

Para cada evento registrado, após a sua detecção e registro, devem ser realizados os seguintes passos:

- **Comunicação:** comunicação do incidente às partes envolvidas e caso necessário entidades externas;
- **Comunicação**: imediata ao setor de Compliance;
- **Resposta:** Tratamento do incidente, identificação e endereçamento de solução da causa raiz;
- **Finalização:** encerramento formal e análise para identificação de possíveis melhorias em processos e controles.

14. Procedimentos em Caso de Interrupção de Serviços Relevantes

Produto CAROL DTVM LTDA:
-Operações de Ouro Ativo Financeiro, Via WEB Sistema operacional de operações de Compra e Venda de OURO.
-STR BACEN VIA WEB.
Para os produtos acima, temos dois Provedores de Internet, caso um pare de funcionar; temos outro.

O intuito é minimizar ao máximo o risco de incidentes para os serviços críticos, porém, se ainda assim, houver uma interrupção, o reestabelecimento do serviço ou de sua contingência será agilizado uma vez que a equipe está ciente dos passos a serem seguidos.
Periodicamente, de acordo com o tempo estabelecido por serviço, são realizados testes de recuperação e contingência, que visam assegurar o funcionamento da operação em cenários de contingência e garantir o conhecimento das pessoas envolvidas neste cenário.

15. Cenários de Incidentes

A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação:

- Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;
- Indisponibilidade do ambiente tecnológico em virtude de ataque maliciosos interno e externo;

- Vazamento de informações confidenciais (informações de clientes, informações estratégicas, outros);
- Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- Compartilhamento de senhas

16. REGRAS PARA CONTRATAÇÃO DE SERVIÇOS NA NUVEM

Partindo da premissa que atualmente as hospedagens em nuvem permitem a utilização das mais novas tecnologias, com possibilidade de escalabilidade e ferramentas de segurança com constantes atualizações que possibilitam uma gestão da segurança mais econômica e eficaz que um data center privado local. A administração da Carol DTVM, permite a contratação de serviços na nuvem de empresas no Brasil ou no Exterior, porém com a exigência de procedimentos de segurança e de parâmetros de contratação destes serviços.

Para que os serviços na nuvem sejam contratados evitando prejuízos ao regular funcionamento da operação, são estabelecidos os seguintes parâmetros para a prestadora de serviços:

- Comprovação de idoneidade e de cumprimento da legislação e da regulamentação vigentes;
- Que a Carol DTVM tenha acesso garantido aos dados processados e/ou armazenados na empresa contratada;
- Estabelecimento de processos para assegurar a confidencialidade, integridade, disponibilidade e recuperação dos dados processados e/ou armazenados na empresa contratada, considerando a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados;
- Comprovação de capacidade técnica da contratada e experiência prévia na prestação deste serviço;
- Acesso às informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- Segregação dos dados dos clientes da Carol DTVM por meio de controles físicos ou lógicos;
- Qualidade dos controles de acesso voltados à proteção dos

dados e das informações dos clientes da instituição.

- Na contratação de aplicativos e sistemas na nuvem, o fornecedor deverá adotar controles de gestão de mudança (GMUD) de modo a mitigar os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

17. COMUNICAÇÃO E TRANSPARÊNCIA DA CONTRATAÇÃO EM NUVEM

Para assegurar que a prestação dos serviços a serem contratados não causem prejuízos ao seu regular funcionamento das nossas operações, nem embaraço à atuação do Banco Central do Brasil, a Carol DTVM proverá:

Acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

Comunicação todos os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem previamente ao Banco Central do Brasil;

Obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

18. RESPONSABILIDADE

A Alta Administração da CAROL DTVM LTDA, é incentivadora e comprometida com a melhoria contínua desta Política.

19. COMUNICAÇÃO

Esta Política, é divulgada a todos os funcionários e colaboradores da CAROL e está disponível na rede interna. Qualquer irregularidade no cumprimento desta Política será alvo de investigação interna e deverá ser comunicada imediatamente para o endereço de e-mail: CAROLDTVM@CAROLDTVM.COM.BR.

CAROL DTVM LTA

Arnaldo Robles Filho

Diretor

ARNALDO ROBLES FILHO:81371560897

Assinado de forma digital por ARNALDO ROBLES FILHO:81371560897
Dados: 2024.08.20 11:09:01 -03'00'

Atualização Agosto /2024