Política de Segurança da Informação Carecode

Data	Nº Doc	Responsável	Versão
29/07/2024		Pedro Magalhães	2

1. Introdução

A política de segurança da informação da Carecode estabelece diretrizes e procedimentos para proteger os ativos de informação da empresa, incluindo dados confidenciais dos clientes, propriedade intelectual e sistemas de tecnologia da informação. Esta política se aplica a todos os funcionários, contratados e terceiros que tenham acesso aos recursos de informação da empresa.

2. Responsabilidades

2.1. Todos os funcionários são responsáveis por aderir e implementar as políticas de segurança da informação da Carecode.

2.2. O Departamento de Tecnologia da Informação (TI) é responsável por supervisionar e garantir a implementação das medidas de segurança da informação; monitorar continuamente o sistema para identificar e responder a ameaças de segurança, vulnerabilidades e incidentes; gerenciar os acessos aos sistemas e dados da Carecode, incluindo gestão de contas de usuário, privilégios e autenticação; realizar auditorias regulares com o intuito de proporcionar melhorias contínuas.

2.3. Encarregado de proteção de dados é o responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); orientar e fornecer treinamentos os

funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, conforme demanda

3. Acesso aos Sistemas e Dados

3.1. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

3.2. O acesso aos sistemas e dados da empresa é concedido com base no princípio do menor privilégio. Em outras palavras, os usuários devem ter apenas as permissões ou acesso necessários para realizar suas tarefas específicas, sem acesso desnecessário a recursos adicionais.

3.3. Os funcionários devem utilizar senhas fortes e ativar o segundo fator de autenticação em todas as contas e sistemas que ofereçam suporte a essa funcionalidade.

4. Gerenciamento de Dispositivos

4.1. Os computadores e dispositivos móveis fornecidos pela empresa devem ser protegidos com senhas fortes e/ou biometria. Uma senha forte pode conter qualquer combinação de letras, números e símbolos, entre 8 e 100 caracteres. As senhas são expiradas a cada 90 dias.

4.2. Os dispositivos devem ser atualizados regularmente com os patches de segurança mais recentes.

4.3. Em caso de perda ou roubo de dispositivos, os funcionários devem relatar imediatamente ao departamento de TI para que medidas de segurança adequadas possam ser tomadas.

4.4. Fica proibida a execução de programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

5. Uso Adequado dos Recursos de TI

5.1. Os recursos de TI da empresa devem ser utilizados apenas para fins comerciais legítimos.

5.2. A instalação de software não autorizado nos dispositivos da empresa é estritamente proibida.

5.3. Os funcionários devem estar cientes dos riscos associados ao phishing, engenharia social e outras ameaças cibernéticas, e devem relatar imediatamente qualquer atividade suspeita ao departamento de TI.

6. Recomendações sobre o uso de Email

6.1. Deve-se utilizar exclusivamente o correio eletrônico interno da Carecode.

6.2. Fica proibido o envio de mensagens que comprometam a imagem da empresa ou possam causar prejuízo moral ou financeiro.

6.3. Fica proibido o uso do e-mail da empresa para assuntos pessoais.

6.4. Fica proibido abrir ou executar arquivos anexados de remetentes desconhecidos ou suspeitos, especialmente com extensões como .bat, .exe, .src, .lnk e .com.

7. Proteção de Dados

7.1. Todos os dados pessoais devem ser tratados como confidenciais e protegidos contra acesso não autorizado, conforme os parâmetros indicados na Lei Geral de Proteção de Dados – LGPD (Lei n° 13.709/2018) e os regulamentos e publicações emitidos pela Autoridade Nacional de Proteção de Dados.

7.2. Os dados pessoais serão tratados apenas conforme a necessidade e em quantidade mínima possível para propósitos legítimos, específicos e em consonância com os demais princípios previstos na LGPD.

7.3. Os dados devem ser criptografados durante o armazenamento e a transmissão, conforme necessário.

7.4. Os backups dos dados devem ser realizados regularmente e armazenados de forma segura.

7.5. Os dados pessoais serão utilizados ainda conforme estabelecido em política(s) específica(s).

8. Recomendações no Uso do Google Workspace.

8.1. As recomendações presentes nesse tópico aplicam-se a todas as aplicações fornecidas pelo Google Workspace, incluindo e não se limitando ao Google Drive; ou que utilizem as funcionalidades Google Workspace para armazenamento, comunicação ou gerenciamento.

8.2. Acesso ao Google Workspace deve ser feito apenas através de credenciais de acesso com logins individuais, senhas fortes e segundo fator de autenticação ativado.

8.3. Somente dispositivos com endpoint corporativos disponibilizados pela CareCode poderão ser utilizados para conectar-se a qualquer aplicação que utilize o Google Workspace com credenciais disponibilizadas pela CareCode.

8.4. Como padrão, os usuários e contas com acesso ao Google Workspace disponibilizado pela CareCode estarão configurados para:

8.4.1. Exigir a verificação em duas etapas para efetuar-se login.

8.4.2. Impedir a reutilização de senhas;

8.4.3. Expiração de senhas em 90 dias.

8.5. Para evitar e corrigir o comprometimento de contas, a CareCode se compromete a:

8.5.1. Analisar regularmente relatórios de atividades para verificar o status das contas e administradores, além de detalhes da verificação em duas etapas.

8.5.2. Configurar alertas por e-mail do administrador para eventos como tentativas de login suspeitas, dispositivos móveis comprometidos ou alterações de configuração por outros administradores.

8.5.3. Implementar desafios de login para tentativas suspeitas, exigindo códigos de verificação ou respostas a desafios conhecidos apenas pelo proprietário da conta.

8.5.4. Identificar e suspender imediatamente contas comprometidas, investigando atividades mal-intencionadas e tomando medidas corretivas conforme necessário.

8.5.5. Revogar imediatamente o acesso de ex-funcionários aos dados da organização para prevenir vazamentos de informações sensíveis.

8.6. Em relação às aplicações utilizadas no Google Workspace, a CareCode se compromete a:

8.6.1. Analisar e aprovar apps de terceiros que acessam serviços principais como Gmail e Drive.

8.6.2. Controlar tanto apps internos quanto de terceiros que acessam os dados do Google Workspace.

8.6.3. Bloquear o acesso a apps menos seguros que não utilizam padrões modernos de segurança como OAuth.

8.6.4. Criar uma lista de permissões para apps de terceiros confiáveis que podem acessar os serviços principais do Google Workspace.

8.6.5. Controlar o acesso aos serviços principais do Google, como Gmail e Drive, com base em critérios como endereço IP, localização geográfica, políticas de segurança ou sistema operacional.

8.6.6. Adicionar criptografia do lado do cliente aos dados de apps como Gmail, Google Drive, Google Meet e Google Agenda, especialmente em ambientes com propriedade intelectual confidencial ou regulamentação rigorosa.

9. Classificação da Informação

Classificação	Descrição
Públicos	São informações que podem ser divulgadas a qualquer pessoa ou empresa interna ou externa.
Privada ou Uso Interno	São informações que podem ser de conhecimento geral dos colaboradores da CareCode, mas que não podem ser divulgadas a pessoas ou empresas externas.
Pessoais	Informações pessoais identificáveis (PII) de indivíduos, como nomes, números de identificação, endereços, etc.
Sensíveis	Informações sensíveis que precisam de proteção adicional, como informações de saúde e informações financeiras.
Confidencial	São informações confidenciais de acesso restrito a um grupo específico de pessoas e só podem ser divulgadas a pessoas ou empresas externas se expressamente autorizado pelo Encarregado, pelo Titular ou por contrato e desde que a pessoa ou empresa esteja vinculada a um contrato de não-divulgação (*non-disclosure agreement*) (NDA) assinado com CareCode. A divulgação indevida pode trazer severos prejuízos à empresa.

10. Conformidade Legal e Regulatória

10.1. A Carecode deve cumprir todas as leis e regulamentações aplicáveis relacionadas à segurança da informação, incluindo e não se limitando à Lei Geral de Proteção de Dados (LGPD) e aos regulamentos e publicações emitidos pela Autoridade Nacional de Proteção de Dados.

10.2. Todos os funcionários devem estar cientes das obrigações legais e regulatórias relacionadas à proteção de dados e colaborar com o departamento de TI para garantir o cumprimento.

11. Revisão e Atualização

11.1. Esta política será revisada e atualizada pelo menos anualmente pelo Comitê de Segurança da Informação.

11.2. Quaisquer alterações significativas na infraestrutura de TI ou nas ameaças à segurança da informação serão consideradas para atualização imediata desta política.

12. Violações da Política de Segurança da Informação e Sanções

12.1. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

12.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato