POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE CYBER SEGURANÇA

1. Objetivo

Esta Política estabelece as diretrizes de governança relacionadas à Segurança da Informação e de Cyber Segurança adotadas pela ConectCar, visando a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), conforme orientações da norma ABNT NBR ISO/IEC 27001 e regulamentações aplicáveis. Tem como objetivo orientar os colaboradores, os contratados e os prestadores de serviço da CONECTCAR sobre suas responsabilidades, atribuições e ações necessárias na condução do SGSI e para reduzir ou mitigar riscos e assegurar a confidencialidade, a integridade e a disponibilidade das informações existentes ou geradas durante o desempenho de suas atribuições.

---

2. Público-alvo

As disposições desta política aplicam-se: (i) a todos os funcionários, estagiários e aprendizes, doravante denominados "colaboradores"; (ii) às entidades e aos órgãos que possuam acesso às informações da CONECTCAR; e (iii) aos prestadores de serviços, pessoas físicas ou jurídicas, que possuam acesso aos dados ou informações sensíveis necessários para a condução das atividades operacionais da organização.

---

3. Princípios da segurança da informação

O processo de Segurança da Informação e de Cyber Segurança da CONECTCAR, cujo objetivo é proteger as informações do negócio e clientes, é pautado pelos princípios fundamentais de:

- *Confidencialidade:* quando o acesso à informação deve ser disponibilizado apenas para as entidades ou pessoas devidamente autorizadas pelo proprietário ou dono da informação;
- *Integridade*: fato de manter a informação armazenada e trafegada com todas as suas características originais ao longo do seu ciclo de vida estabelecidas pelo proprietário ou dono da informação;
- *Disponibilidade*: garantir que a informação esteja disponível para uso sempre que entidades ou pessoas autorizadas necessitarem.

---

4. Diretrizes

As diretrizes estabelecem um programa de prevenção, detecção e redução de vulnerabilidades e impactos relacionados aos incidentes de segurança da informação e de Cyber Segurança.

4.1. Informação: importância e proteção
Classificação da informação e Governança
A informação é um importante ativo da CONECTCAR e deve ser preservada e salvaguardada em conformidade com suas políticas, normas, procedimentos e controles, bem como, com as leis e regulamentos sobre o tema.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE CYBER SEGURANÇA

Proteção de dados e privacidade
A CONECTCAR tem o compromisso de promover a aderência às leis de privacidade de dados e de proteção financeira de seus clientes, sendo este compromisso transmitido aos seus colaboradores, contratados e prestadores de serviço.

4.2. Gestão de identidades e de acessos
A gestão e revisão das identidades e dos acessos aos recursos computacionais da CONECTCAR são realizados em conformidade com os requisitos descritos em Norma específica, garantindo a definição de: (i) recursos; (ii) mínimos privilégios; (iii) operações que podem ser executadas; (iv) componentes autorizados; (v) e devida rastreabilidade de acessos realizados.

4.3 Controles dos dispositivos de tecnologia
Os recursos de tecnologia disponibilizados pela CONECTCAR para uso dos funcionários são protegidos por controles contra-ataques cibernéticos, infecções e prevenção ao vazamento de dados.

4.4 Desenvolvimento de sistemas e garantia de qualidade
A avaliação dos aspectos de segurança deve ser parte integrante no desenvolvimento de sistemas relevantes. Controles de segurança devem ser estabelecidos ao longo de toda a vida útil desses sistemas para assegurar que as informações processadas estejam protegidas, de acordo com sua classificação e exposição a risco.

4.5 Segurança e monitoramento da infraestrutura, redes e sistemas
As redes e sistemas corporativos relevantes devem ser administrados, monitorados e protegidos em consonância com as exigências e requisitos de Segurança da Informação da CONECTCAR. Devem também ser protegidos contra acessos não autorizados por meio de tecnologias de rede devidamente atualizadas, revisadas e testadas periodicamente, de forma independente.

4.6. Registro e respostas de incidentes de segurança
Os incidentes de segurança da informação relevantes são registrados e destes decorrem a devida análise das referidas causas e impactos. No caso da ocorrência de incidentes relevantes, devem ser realizadas as avaliações de adequabilidade dos controles existentes e de necessidade de criação de novos controles, bem como, a contenção dos efeitos do incidente para as atividades da CONECTCAR.

4.7. Continuidade do negócio e recuperação de incidentes
O planejamento de continuidade do negócio é administrado de acordo com os requisitos estabelecidos na Política de Continuidade de Negócios e do Plano de Continuidade de Negócio de TI, que contempla cenários de incidentes relevantes a serem considerados nos testes de continuidade de negócios.

4.8. Gestão dos prestadores de serviços relevantes
Devem ser estabelecidos e continuamente aprimorados os controles de segurança cibernética destinados a assegurar que as informações tratadas pelos seus fornecedores estejam devidamente protegidas.

4.9. Avaliação de riscos de produtos ou serviços
Os riscos de segurança da informação devem ser avaliados e administrados de acordo com os requisitos definidos em Norma específica e nos controles de proteção. Após o registro e a análise devem ser executadas as respostas proporcionais aos riscos identificados.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE CYBER SEGURANÇA

4.10. Backup de dados
A CONECTCAR deve zelar pelo processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes, a fim de atender aos requisitos operacionais e legais, assegurar a continuidade do negócio em caso de falhas ou incidentes, além de auxiliar em sua ágil recuperação.

4.11. Conscientização de colaboradores, clientes e fornecedores
A CONECTCAR mantém um plano anual de conscientização direcionado ao desenvolvimento e à manutenção das habilidades dos funcionários em relação à segurança da informação.

---

5. Violações de segurança
As violações das regras definidas nesta Política poderão ensejar a aplicação de medidas disciplinares, conforme determinam as normas internas e o Código de Conduta da CONECTCAR.

---

6. Canal de comunicação
No caso de alertas de segurança, incidentes ou suspeitas sobre desvio de políticas, procedimentos e/ou regulamentações, as notificações devem ser enviadas para os canais de comunicação a seguir: security@conectcar.com e/ou para o Canal de Ética da CONECTCAR https://canalconfidencial.com.br/conectcar/

****