segurança da informação

Política de Segurança da Informação

VERSÃO 1.1

GreenCard

Histórico de Versões

Data	Versão	Descrição	Autor
13/08/2022	1.0	Criação do documento PR001 – Procedimentos de Segurança da Informação da Green Card.	Samira Fao de Oliveira
10/03/2023	1.1	Inclusão da Capa, Histórico de Versões, Sumário, Responsabilidade e Princípios. Alteração no texto do Escopo e Encarregado de Dados. Trocado o título “7. Responsabilidades” por “7. Responsabilidade das Áreas”. Inserido ao documento responsabilidades da “Área Jurídica”, “Gestores das Áreas” e "Todos os Colaboradores”. Inserido item “9. Responsáveis pelo desenvolvimento e aprovação”. Retirada do Glossário.	Carlos Mário Silveira Alviggi
31/03/2026	1.1	Revisão do documento	Leonardo Silva Vieira

Sumário

1. OBJETIVO

Esta política tem por finalidade apresentar os princípios básicos da Segurança da Informação, responsabilidades e penalidades caso as diretrizes desta política ou do procedimento de Segurança da Informação não sejam cumpridas.

2. RESPONSABILIDADE

Os Procedimentos listados nesse documento são de reponsabilidade do Departamento de Tecnologia da Informação. Qualquer mudança deve passar pelo parecer técnico do Diretor de TI e posteriormente ser aprovada pelo Comitê de Segurança da Informação da empresa. A Green Card tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação e privacidade de dados.

2. ESCOPO

Os princípios contidos nesta Política de Segurança da Informação deverão ser observados e cumpridos por todos os sócios, representantes comerciais, colaboradores, parceiros de negócio, fornecedores e terceiros que estejam se relacionando com a Green Card.

É dever de cada colaborador a leitura e manter-se atualizado em relação as políticas, procedimentos e normas adotadas pela Green Card, buscando orientação do seu gestor ou do departamento de TI sempre que não estiver absolutamente seguro quanto a conduta adequada a seguir no que diz respeito a segurança da informação.

3. PRINCÍPIOS

A Green Card observa as exigências da legislação que abordam aspectos da segurança da informação quando aplicável, bem como a legislação específica que trata da proteção de dados pessoais (lei 13709/18) dos seus clientes e colaboradores, e segue às normas da família ISO/IEC 27000 de Segurança da Informação.

4. SEGURANÇA DA INFORMAÇÃO

O processo de Segurança da Informação deve estabelecer diretrizes adequadas as necessidades da Green Card, visando manter a:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

5. PRINCIPIOS

- Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Green Card pertence à mesma. As exceções devem ser explícitas e formalizadas através de contrato entre as partes.
- Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais.
- Preservar e proteger as informações que estão sob responsabilidade da Green Card.
- Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação.
- Assegurar a confidencialidade, a integridade e a disponibilidade no desenvolvimento das atividades da empresa.
- Cumprir a legislação pertinente relacionada às atividades da Green Card no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

6. RESPONSABILIDADES DAS ÁREAS

7.1 Comitê de Segurança da Informação

A Green Card possui um comitê de Segurança da Informação, com o intuito de auxiliar na tomada de decisões relacionadas a ações de contenção de incidentes/eventos de segurança, implementação de novas melhorias, revisão de procedimentos e políticas, conforme descritas no PR002 - Procedimento do Comitê de Segurança da Informação.

7.2 Segurança a Informação

O processo de Segurança da Informação é responsável por:

- Elaborar, gerir, controlar e divulgar, de forma corporativa, a Política, Procedimentos e Manuais de Segurança da Informação para todos os colaboradores.
- Elaborar, participar e propor ao Comitê de Segurança da Informação ajustes e melhorias aos processos pertinentes à Segurança da Informação.
- Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.
- Disseminar a cultura de Segurança da Informação e melhoria contínua.
- Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

- Auditar processos sempre que necessário e apoiar os auditores internos e, eventualmente, externos.
- Analisar os riscos e oportunidades de melhorias pertinentes à segurança da informação utilizando métodos e ferramentas adequados.
- Realizar trabalhos de análise de vulnerabilidades, com intuito de assegurar o nível de segurança dos sistemas, de informações e dos demais ambientes em que armazenam, processam ou transmitem as informações.
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Solicitar informações às demais áreas da Green Card e realizar simulados de segurança, no intuito de verificar o cumprimento e aderência da Política de Segurança da Informação, sempre que necessário.
- Disponibilizar e gerenciar credenciais de acesso ao usuário.
- Treinar todos os colaboradores, referente as diretrizes e disseminar a cultura de Segurança da Informação.
- Comprometer-se com a conscientização e aplicação da melhoria contínua sempre que pertinente, não apenas só no processo de Segurança da Informação, mas com todos da empresa.

7.3 Área de TI

- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos no PR001 - Procedimento de Segurança da Informação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Green Card.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

7.4 Área de Recursos Humanos

- Solicitar para a área de TI os acessos aos sistemas da empresa para novos colaboradores.
- Solicitar para área de TI revogação e alteração de acessos sempre que colaboradores alterarem de área.
- Solicitar para a área de TI a inativação/bloqueio das credenciais de acessos nos sistemas sempre que um colaborador for desligado da empresa.
- Solicitar para a área de TI o bloqueio temporário das credenciais de acessos nos sistemas sempre que um colaborador entrar em férias da empresa. Cargos chaves o RH deve informar para a credencial não ser bloqueada.
- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento das diretrizes mencionadas no "FO001 - Termo de Confidencialidade e de Propriedade Intelectual, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações a Green Card.
- Solicitar aos colaboradores a assinatura do Termo de Compromisso e Ciência referente ao Código de Conduta Ética assumindo o dever de seguir as diretrizes estabelecidas.
- Obter a assinatura do Termo de Responsabilidade dos dispositivos móveis disponibilizados aos colaboradores e recolher o dispositivo no seu desligamento.

7.5 Área Jurídica

- Manter as áreas informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessárias cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da empresa;
- Participar previamente dos processos de contratação, validando as minutas que devem estar alinhadas aos controles de segurança da informação aplicáveis.

7.6 Gestores das Áreas

- Garantir e gerenciar o cumprimento desta Política de Segurança da Informação (PSI), Procedimentos de Segurança da Informação e demais documentos complementares pelos seus colaboradores.
- Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio.

- Garantir que os ativos de propriedade ou sob a responsabilidade da Green Card sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa.
- Identificar incidentes de segurança de informação ou qualquer ação duvidosa praticada por colaboradores, comunicando o Responsável por Segurança da Informação imediatamente.

7.7 Todos os Colaboradores

São responsabilidades e obrigações de todos os colaboradores da Green Card, independentemente do vínculo ou posição hierárquica:

- Estar ciente e manter-se atualizado com a Política de Segurança da informação (PSI), Procedimentos de Segurança da Informação e demais documentos complementares.
- Conhecer e assinar o "FO001 - Termo de Confidencialidade e de Propriedade Intelectual".
- Utilizar crachá de identificação nas dependências da empresa. Vindo a informar ao RH quando esquecer em casa ou em caso de perda.
- Utilizar os ativos de propriedade ou sob responsabilidade da Green Card somente para fins profissionais e autorizados, de forma ética e legal as informações e os ativos disponibilizados, respeitando os direitos e as permissões de uso concedidas.
- Cuidar da integridade, confidencialidade e disponibilidade dos dados, informações contidas nos sistemas, devendo comunicar por escrito à Green Card e a sua gerência imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes.
- Não revelar fora do âmbito profissional fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior.
- Não divulgar dados obtidos dos sistemas aos quais tenha acesso para outros colaboradores não envolvidos nos trabalhos executados, ciente de que este ato constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional.
- Ao utilizar os dados dos sistemas informatizados de acesso restrito, manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas.
- Não se ausentar da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros.
- Não revelar suas credenciais de acesso (usuário e senha) ao(s) sistema(s) a ninguém e tomar o máximo de cuidado para que permaneça somente em seu conhecimento.
- Responder por toda e qualquer atividade realizada nos Recursos de Tecnologia da Informação e Comunicação (TIC) do Green Card onde tenha sido feito o uso de suas credenciais de acesso.

- Entender que o usuário e senha de qualquer um dos sistemas disponibilizados pela Green Card é de uso pessoal e intransferível e não deve ser revelado a ninguém.
- Alterar a senha, sempre que obrigatório, ou sempre que haja suposição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas, respeitando as regras de senha segura exigidas pela empresa em seus sistemas.
- Proceder com cuidado na guarda e utilização de senha e não a emprestar a outro colaborador, ainda que habilitado. Ciente de que, sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, este ato constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares.
- Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na Green Card (tais como privilégio e direitos de acesso).
- Responder, em todas as instâncias, pelas consequências das ações ou omissões de sua parte ou dos usuários por você autorizados, que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha, ou das transações as quais tenha acesso.
- Utilizar as obras intelectuais, softwares, segredos industriais, marcas, identidade visual e qualquer outro sinal distintivo atual ou futuro da Green Card em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, somente de acordo com atividades profissionais e autorizadas pela empresa.
- Reportar formalmente ao Responsável pela Segurança da Informação quaisquer eventos relativos à violação ou possibilidade de violação de segurança de informação ou atividades suspeitas.
- Zelar pela imagem profissional, da Green Card, com uma conduta impecável, ciente de que constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano; bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente.
- Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais.

7.8 Encarregado de Dados

A Green Card nomeou seu Encarregado de Dados através do documento “NO001-Nomeação Encarregado de Dados”. Suas principais atividades são:

- Receber e aceitar reclamações e comunicações dos titulares;
- Realizar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;

- Orientar os colaboradores e os contratados da Green Card a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

7.9 Partes Interessadas

- **Direção:** Deve demonstrar apoio as políticas, procedimentos e controles relacionados à segurança da Informação e a melhoria contínua visando eficácia do sistema de gestão da segurança da informação. Assegurar através da análise crítica, que o sistema de gestão da Segurança da Informação está em conformidade com os requisitos da NBR ISO27001 e que está alinhado com as estratégias do negócio da empresa. E disponibilizar recursos necessários para a execução das diretrizes e aplicação de melhoria.
- **Alta gestão:** Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- **Colaboradores:** Será de inteira responsabilidade de cada colaborador todo prejuízo ou dano que vier impactar de forma direta e indireta a Green Card em decorrência da não obediência às diretrizes estabelecidas nesta política e nos procedimentos de Segurança da Informação.
- **Legislação:** Leis vigentes devem ser avaliadas pela Green Card e os requisitos pertinentes ao negócio da empresa deve ser atendido pelas áreas pertinentes.

8. DIRETRIZES

Visando atender a Lei 13.709/18 (LGPD) e as diretrizes pertinentes da ISO 27001, elaborou-se um procedimento com o objetivo de garantir a Segurança da Informação na Green Card, na qual contempla os seguintes itens:

- Classificação da Informação;
- Gestão de Senhas;
- Controle de Acesso Lógico;
- Controle de Acesso Físico;
- Gestão de Incidentes;
- Dispositivos moveis;
- Descarte da Informação;
- Mesa e Tela Limpa;
- Cópia de Segurança;
- Uso de Recursos de TI;

- Gestão de Vulnerabilidades;
- Lei geral de Proteção de Dados.

9. RESPONSÁVEIS PELO DESENVOLVIMENTO E APROVAÇÃO

Responsável	Descrição da Atividade
Analista de Segurança da informação	Responsável pelo desenvolvimento da Política de Segurança da Informação.
Diretor de TI	Responsável pelo parecer técnico da Política de Segurança da Informação.
Comitê de Segurança da Informação	Responsável pela aprovação da Política de Segurança da Informação.

10. PENALIDADES

As penalidades serão aplicadas para garantir que os usuários atuem sempre em conformidade com as diretrizes estabelecidas nesta política e nos procedimentos de Segurança da Informação, portanto não será admitido que qualquer usuário justifique violações ou o não cumprimento por desconhecimento deste. Os colaboradores e terceiros que, de alguma forma, violarem as diretrizes ou não cooperarem com as auditorias internas deverão responder em conformidade com o Código de Conduta Ética da Green Card.

APROVAÇÃO DO DOCUMENTO

Este documento é aprovado pelos participantes do Comitê de Segurança da Informação, eis que estão de acordo com as diretrizes descritas neste documento, os diretores e acionistas da Green Card.