1. Objetivo

Este documento tem por objetivo constituir um compromisso e postura claros por parte da alta direção da SKY no que tange à Segurança Cibernética, em conformidade com as políticas, normas e procedimentos da companhia, leis em vigor e regulamentações emitidas pelos órgãos regulatórios, contra os riscos de destruição, perda, divulgação, falha na gestão e não disponibilidade de rede.

2. Área Responsável

Segurança da Informação

3. Informações Gerais

3.1. Premissas

Estabelecer um conjunto adequado de controles, a fim de proteger a integridade, disponibilidade e confidencialidade da informação através de:

- ✓ Mecanismos implementados para suportar o processamento das operações da SKY;

- ✓ Avaliação de riscos na companhia onde sejam identificadas ameaças, vulnerabilidades e o potencial impacto nos ativos da informação caso o risco seja concretizado;
- ✓ Identificação dos requisitos legais, regulamentares e contratuais que devem ser cumpridos.

Tais ações poderão ser refletidas na documentação de políticas, normas, procedimentos e padrões sobre o correto uso e manejo dos recursos de TI enquadrados sob regulamentações nacionais e padrões internacionais.

3.2. Definições

Confidencialidade: Assegurar que as informações sensíveis e críticas não sejam disponibilizadas sem autorização, exceto quando requisitadas por autoridade judicial competente.

Integridade: Está relacionada com a precisão e completitude da informação, bem como com sua validação de acordo com os valores e expectativas do negócio.

Disponibilidade: Está relacionada com a disponibilização da informação quando requerida pelos processos do negócio, a qualquer momento.

Efetividade: Está relacionada com a relevância e pertinência da informação aos processos do negócio, sendo que a informação deve ser fornecida de uma maneira oportuna, correta, consistente e utilizável.

Eficiência: Está relacionada à otimização de recursos para gerar informação (produtividade e economia).

Confiabilidade: Possuir mecanismos de checagem para garantir o fornecimento de informação confiável e íntegra.

Cumprimento: Refere-se à obediência a leis, regulamentos e acordos contratuais aos quais está submetido o processo de negócio, tanto as impostas externamente quanto as políticas internas.

3.3. Responsabilidades

O Diretor de Segurança da Informação (CISO) é responsável por manter a política e seu quadro normativo, providenciando colaboração e recomendações em geral, inclusive durante sua implementação.

Todos os Diretores e Gerentes são diretamente responsáveis por implementar a política e o quadro normativo, garantindo que seus dependentes cumpram com o mesmo.

Todas as pessoas que acessam ativos da informação da SKY são responsáveis pela compreensão e cumprimento da política e seu quadro normativo.

4. Diretrizes

A Alta Direção reconhece que a informação tem um papel muito importante em qualquer organização, uma vez que permite a formação de um conjunto de táticas, estratégias e atividades em prol do cumprimento dos objetivos estabelecidos. Este processo ocorre através de diferentes meios e formas (correio eletrônico, Internet, papel, meios magnéticos, etc.), os quais devem ser protegidos adequadamente.

Portanto, a SKY assegura que:

- ✓ Serão avaliados os riscos da informação e serão estabelecidas, em consequência, medidas de proteção adequadas.
- ✓ A informação será protegida contra acessos não autorizados.
- ✓ A confidencialidade da informação ficará assegurada.
- ✓ A integridade da informação será preservada.
- ✓ A disponibilidade da informação para os processos de negócios será sustentada.
- ✓ Serão observados os cumprimentos dos requisitos da Organização, Legais e Regulatórios que sejam aplicáveis.
- ✓ Será estabelecida uma estrutura organizacional apropriada para a gestão da Segurança da Informação.
- ✓ Serão avaliados, desenvolvidos, mantidos e testados os planos de continuidade e recuperação do negócio.

- ✓ Serão identificados e desenvolvidos temas de sensibilização e capacitação em matéria de Segurança da Informação.
- ✓ Todos os incidentes de segurança da informação, reais ou supostos, serão averiguados, comunicados, pesquisados e documentados pelo Comitê de Incidentes de Segurança da Informação, que responde ao CISO da SKY.
- ✓ Toda informação deverá estar classificada em virtude de sua importância para a organização e deve ser tratada segundo tal classificação, de acordo com o disposto nas normas de Proteção de Dados Privados da companhia.
- ✓ Os sistemas de informação serão submetidos periodicamente a auditorias internas ou externas com a finalidade de verificar o correto funcionamento dos planos de segurança, determinando graus de cumprimento e recomendando medidas corretivas.
- ✓ Serão realizadas revisões anuais sobre os controles mínimos de segurança para Terceiras Partes que acessem, capturem, transfiram, processem e/ou armazenem Dados Privados.
- ✓ Existirá um quadro normativo composto por normas, procedimentos, padrões, instrutivos e/ou recomendações que irá acompanhar a política e irá aprofundar os temas específicos de Segurança da Informação.
- ✓ A presente política e o quadro normativo de segurança da informação deverão ser de obrigatório cumprimento para todos os funcionários que trabalham na companhia, incluindo terceiros e fornecedores ligados à mesma.
- ✓ Ações de conscientização e educação sobre temas de Segurança da Informação e Segurança Cibernética devem ser realizadas periodicamente

para garantir que todos os colaboradores estejam alinhados com as diretrizes da empresa.

5. Processos de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, os seguintes processos são adotados:

- **Gestão de Ativos da Informação:** os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados;

- **Classificação da Informação:** as informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações;

- **Gestão de Acessos:** as concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos determinados pela SKY. Os acessos podem ser rastreáveis, a fim de garantir que todas as ações passiveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações;

- **Gestão de Riscos:** os riscos podem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da SKY, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de Segurança Cibernética são escalonados nos fóruns apropriados, para decisão;

- **Gestão de Fornecedores:** a SKY realiza a Avaliação de Fornecedores dos serviços prestados com transferência ou compartilhamento de informações;

- **Gestão de Logs de Acesso:** garantir a rastreabilidade das ações executadas por usuários e sistemas em todos os sistemas e ambientes computacionais, monitorando a fim de detectar ações impróprias, garantindo a confidencialidade das informações;

- **Gestão de Vulnerabilidade e aplicação de Patches:** a gestão visa a redução de falhas e fragilidade dos sistemas, aplicando correções de segurança e evitando o comprometimento das informações e serviços;

- **Tratamento de Incidentes de Segurança da Informação:** os incidentes de Segurança da Informação devem ser reportados ao CISO SKY e discutidos em Comitê;

- **Conscientização:** a SKY promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação;

6. Notificações de Incidentes de Segurança

O Diretor de Segurança da Informação (CISO) é responsável por averiguar, pesquisar e classificar os incidentes de segurança, além de comunicar a Alta Direção da empresa em caso de ocorrência de incidentes.

O DPO, quando houver um incidente de segurança que envolva dados pessoais, deverá comunicar todos os usuários afetados e aos Órgãos Reguladores.

7. Conscientização do usuário

Na página **https://www.sky.com.br/dicas-de-seguranca** estão disponíveis dicas e procedimentos aos usuários para navegação mais segura e proteção dos dados.

8. Vigência e Revisão

A política de Segurança da Informação e Segurança Cibernética da SKY entra em vigor na data de sua publicação oficial.

A política de Segurança da Informação e Segurança Cibernética será atualizada anualmente e/ou quando ocorrerem mudanças significativas, tendências de ameaças e vulnerabilidades ou melhorias, ou quando necessário em razão de questões legais relativas ao negócio.

A política de Segurança da Informação e Segurança Cibernética da SKY não altera e/ou revoga as demais políticas atualmente em vigor.

9. Dados de Contato

Se você tiver questionamentos ou dúvidas em relação a esta política, ao tratamento de dados realizado pela SKY ou ao exercício de seus direitos relacionados a dados pessoais, por favor, entre em contato conosco através do link “Entenda a proteção de dados na SKY”, disponível no site www.sky.com.br.

10. Aprovadores

CISO/DPO e Alta Direção da SKY

11. Normas, padrões e boas práticas adotadas

ABNT NBR ISSO/IEC 27001:2013 Tecnologia da Informação

Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018