POLÍTICA DE
SEGURANÇA DA INFORMAÇÃO

Um time que transforma sempre caminha junto

Introdução

A Digivox possui um programa de Segurança da Informação que é a base das atividades de todas as empresas do Grupo. Está direcionado à Alta administração: Presidente, Diretores, Executivos; aos Colaboradores: funcionários, estagiários, aprendizes, dirigentes e empregados de empresas contratadas; e todos os demais que estejam atuando ou prestando serviços em nome das empresas ou para o Grupo Digivox.

Para orientação do programa, foram criadas políticas e procedimentos de segurança. Dentre eles, a Política de Segurança da Informação que tem como objetivo transmitir para os colaboradores o compromisso que a Digivox possui com a manutenção da segurança das informações de nossos ativos, clientes, parceiros, funcionários, colaboradores e fornecedores, além de estabelecer os meios necessários com intuito de prover segurança da informação em nosso meio de trabalho.

Assim, para todos os funcionários e colaboradores que fazem parte da Digivox, é importante que seja reconhecido que dentro de uma perspectiva de segurança da informação um dos principais ativos da Digivox é a informação. Pois, entende-se que, uma vez que nossa empresa provê oportunidades de negócio e empreendimentos, que são idealizados mediante diversas informações coletadas de clientes, do mercado e entre outros.

Quanto mais seguras forem as informações que nós obtemos, mantemos e utilizamos, menor será o nosso prejuízo com fraudes, naturalmente. Quanto mais seguras estiverem as informações em nossa posse, mais confiança teremos do mercado para estreitar cada vez mais nossos relacionamentos, buscando sempre expandir o que tem feito da Digivox uma grande empresa.

Além dos aspectos éticos e morais relacionados à segurança da informação, estamos atentos também aos aspectos legais e regulamentares, que estão se modernizando e exigindo que as empresas possuam um compromisso cada vez mais forte com a segurança das informações daqueles que são de maior importância para nós, os clientes, funcionários e parceiros.

É notável que o nosso mercado ainda tem muito que evoluir em termos de proteção de dados, visto que muitas vezes os consumidores são assediados através de fraudes e perturbações que ocorrem devido ao vazamentos de suas informações, que podem ocorrer devido a ações intencionais ou não, e que podem ocorrer dentro da própria Digivox ou ativada por algum agente externo.

Entretanto, salientamos que a Digivox está na busca da obtenção da conformidade com os requisitos regulatórios de segurança da informação do mercado e sobretudo no que diz respeito à Lei Geral de Proteção de Dados. E atua em diversas vertentes, tais como jurídica e processual e não apenas revisando conceitos técnicos. Nesse sentido, nossa empresa tem investido esforços e recursos na criação e adoção de novas estratégias e técnicas mais seguras de condução do negócio. Buscando assegurar Políticas e procedimentos que garanta que as informações dos clientes, colaboradores e parceiros estejam íntegras, seguras e disponíveis através da modernização dos processos, inteligência artificial e também ferramentas de segurança de última geração. Mas, essa responsabilidade e desejo não podem ficar restritos às equipes de tecnologia. Pois é necessário que sejam conduzidos esforços de segurança da informação em todas as áreas da empresa, com o objetivo de estabelecer regras, processos e constante auditoria das atividades. A fim de que nos tornemos cada vez melhores no que fazemos, melhorando nossos processos e investindo em nosso pessoal como um todo, para que esses aprendam cada vez mais e ajudem a Digivox em seu objetivo de ser referência por suas soluções inovadoras de alto valor agregado.

Dito isso, criamos não só um projeto. Mas um Programa de Segurança da Informação que consiste basicamente em um agregado de projetos que estão sendo executados simultaneamente e que visam um objetivo em comum, em nosso caso, a segurança das informações da Digivox. Assim sendo, o Sistema de Gestão de Segurança da Informação é um sistema que cuida do planejamento, implementação, revisão e gerenciamento da Segurança da Informação.

1. Palavra da Diretoria

Para todos os membros da diretoria, é de suma importância a manutenção não somente das conformidades com as exigências da Lei Geral de Proteção de Dados e da Legislação vigente no Brasil, como também a preservação das relações com os que nos confiam suas informações, isto é, todos os colaboradores, os parceiros e os clientes.

Nesse sentido, precisamos que um esforço mútuo seja conduzido para que alcancemos o objetivo, não só por parte da diretoria, mas de todos de nossa organização. Sendo assim, fez-se necessário a elaboração desta Política de Segurança da Informação. Solicitamos a todos que pertencem ao público destinado, leiam com atenção e cumpram o que for cabível a sua função.

2. Terminologia básica de Segurança da Informação

Seguro ou inseguro são os estados nos quais uma informação pode se encontrar dentro do escopo de segurança da informação. Sendo que uma informação segura é toda aquela que se encontra **confidencial, íntegra e autêntica.** Então, quando nos perguntarem se uma determinada informação está segura, devemos nos perguntar se ela preserva esses três princípios.

A **confidencialidade** é a qualidade de toda informação que não é pública, isto é, uma informação que é de propriedade específica de uma pessoa ou organização. Quando compartilhamos ou obtemos uma informação de propriedade alheia sem autorização nós estamos colocando essa informação em um estado de insegurança, quebrando assim sua confidencialidade.

A **integridade** diz respeito à informação permanecer em seu estado tal como fora concebida ou idealizada, sem alterações não autorizadas. A partir do momento em que um terceiro, sem a devida autorização, é capaz de interceptar e alterar uma informação está fazendo com que a informação não seja mais íntegra. Logo, ela não está mais em um estado de segurança.

A **disponibilidade** remete ao objetivo básico da transmissão de uma informação, que é fazer saber. Logo, se desejamos que alguém saiba de algo essa informação deve estar disponível para as partes a serem comunicadas. Uma vez que a informação está ou pode ser indisponibilizada ela não está mais em um estado de segurança.

Observando isso, podemos dizer que **Segurança da Informação** é a preservação da confidencialidade, integridade e disponibilidade da informação.

Já o Sistema de Gestão da Segurança da Informação é a parte do sistema que cuida do planejamento, implementação, manutenção, revisão e aprimoramento da segurança da informação.

3. Sistema de Gestão de Segurança da Informação

Para que a empresa faça observância às mudanças legais, tecnológicas e também às normas internacionais de segurança da informação de forma eficaz, reunimos uma equipe multidisciplinar dedicada, com capacidade técnica exemplar e a responsabilidade de auxiliar os demais setores e auditar suas atividades. A fim de medir o grau de comprometimento, exposição de cada setor, e continuamente delegar ações para aumentar o grau de segurança da informação de cada um dos setores que somados fazem a Digivox. Para condução dessas atividades, foi designado como responsável pela área de Segurança da Informação, o colaborador Paulo Montenegro. Que, juntamente com sua equipe composta por: Fernanda de Albuquerque; Gerente do projeto, e representantes das áreas de DHO, Comunicação, Desenvolvimento de software e de Infraestrutura; planejam e conduzem as atividades de Segurança da Informação em parceria com cada setor da empresa.

Podendo este delegar tarefas no âmbito de segurança da informação para os colaboradores da empresa, a fim de assegurar por meio destes os objetivos de segurança da Digivox aqui expressos previamente e posteriormente. As atribuições da área de Segurança da Informação serão: avaliar os setores, definir projetos, coordenar a execução dos projetos, monitorar e auditar a segurança dos sistemas e também dos processos estabelecidos dentro da empresa. Sendo importante que este setor esteja presente durante as atividades de planejamento estratégico e tomadas de decisões que possam de alguma forma comprometer os objetivos de segurança da informação da empresa.

4. O que diz nossa Política de Segurança da Informação

A Política de Segurança da Informação é o primeiro entregável de nosso Sistema de Gestão de Segurança da Informação, que tem como objetivo expressar o comprometimento e apoio da direção relacionados à segurança da informação de forma pública para toda a organização. Objetivando definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação.

O estabelecimento dessa política é o primeiro passo para que prossigamos para sua implantação a fim de assegurar a execução e auditabilidade dos processos. A Digivox se compromete a satisfazer todos os requisitos aplicáveis relacionado à segurança, incluindo leis, regulamentos e diretrizes garantindo a continuidade do negócio com melhoria contínua do sistema de gestão implementado Dentre as finalidades desta política, estão: a direção, os princípios e as regras básicas de gestão da segurança da informação. Os usuários do documento recebem-o na íntegra e são funcionários e colaboradores da Digivox, assim como as partes externas relevantes: clientes e parceiros de negócios.

Para embasamento, os documentos analisados como referência da Política de Segurança da Digivox são:

- Norma ISO/IEC 27001, cláusulas 2 e 5.3;
- Documento sobre o escopo do SGSI;
- Metodologia de avaliação e tratamento de riscos;
- Declaração de aplicabilidade;
- Lista de Obrigações Legais, regulamentares e contratuais.

Esta política aplica-se a todo Sistema de Gestão de Segurança da Informação, como definido no próprio documento de escopo do SGSI.

4.1 Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação são os seguintes:

- Fortalecer a imagem no mercado através da proteção dos nossos dados, dos dados do cliente e dos dados do cliente do nosso cliente;
- Treinar, Conscientizar e capacitar o time de colaboradores;
- Preservar os nossos ativos de informação: pessoas, equipamentos, serviços, softwares, infraestrutura.

Os objetivos serão monitorados e medidos mensalmente e revisados anualmente junto com a Política. Os resultados serão utilizados como materiais de entrada para a análise crítica feita pela alta administração.

4.2 Requisitos de segurança da informação

A Política de Segurança da Informação e todo o Sistema de Gestão de Segurança da Informação deve estar em conformidade com os requisitos legais e regulamentares

4.3 Controles da segurança da informação

Os procedimentos para identificação e avaliação de riscos e oportunidades estão definidos na metodologia de avaliação de riscos e de tratamento do risco. Os controles selecionados e seu status de implementação estão listados na declaração de aplicabilidade.

4.4. Continuidade de negócios

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

4.5 Responsabilidades do SGSI

As responsabilidades básicas para o Sistema de Gestão de Segurança da Informação são:

1. O CEO é responsável por garantir que o SGSI seja implementado de acordo com esta Política.

2. O Comitê é responsável pela coordenação operacional do SGSI.

3. A alta administração deve analisar o SGSI pelo menos uma vez por ano ou sempre que ocorrer uma mudança importante e elaborar minutas sobre a reunião.

4. O Setor de Desenvolvimento Humano Organizacional implementa o programa de conscientização e treinamentos sobre segurança da informação para os funcionários.

5. A proteção da integridade, disponibilidade, e confidencialidade é responsabilidade do proprietário de cada ativo.

6. A área de Comunicação do Setor Comercial & Marketing irá definir quais informações relativas a segurança da informação serão comunicadas para qual parte interessa (internamente e externamente), por quem e quando.

7. O setor de Desenvolvimento Humano Organizacional é responsável por avaliar e implementar o plano de treinamento e conscientização que se aplica a todas as pessoas que têm uma função na gestão de segurança da informação.

4.6 Ambiente de Desenvolvimento

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

4.7 Violações

O não cumprimento dos requisitos previstos na Política de Segurança da Informação e nas normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

4.8 Comunicação da Política

A área de Comunicação do Setor Comercial & Marketing deve garantir que todos os funcionários da Digivox, bem como todas as partes externas apropriadas conheçam a Política de Segurança da Informação.

5. Responsabilidades gerais

Agora, devemos expressar claramente que é responsabilidade de todo colaborador da **Digivox**. Fazendo observância às normas expedidas pelo Comitê de Segurança da Informação em relação aos procedimentos e requisitos e zelar pela confidencialidade, integridade e disponibilidade das informações que estiverem em sua posse.

Sendo assim, de modo geral, é dever de todo colaborador da empresa:

I. Comunicar ao Comitê de Segurança da Informação, através de **soc@digivox.com.br** sobre qualquer incidente ou violação dos princípios de segurança: confidencialidade, integridade e disponibilidade. Independentemente de a violação ter ocorrido por colaborador interno, externo, terceirizado, hierarquicamente superior ou inferior (ou através da plataforma de Sistemas Internos onde deve ser aberto incidente a respeito).

II. Fazer observância à legislação vigente não somente como colaborador, mas de forma primária como cidadão de nossa República Federativa do Brasil, comunicando para ao Núcleo de Segurança da Informação qualquer violação da legislação vigente seguindo os mesmos critérios informados anteriormente.

III. Aderir aos programas de treinamento ofertados pela empresa, assim como as boas práticas de Segurança da Informação, com o objetivo de aprender como zelar de forma mais eficiente pela manutenção da segurança das informações da empresa e informações pessoais das quais a empresa é titular, e evitar qualquer tipo de incidente que por ventura venha a ocorrer por conduta indevida na utilização dos recursos computacionais.

IV. Fazer observância às normas emitidas pelo Comitê de Segurança da Informação uma vez que sua função esteja delimitada no escopo observado pela norma e também comunicar qualquer dificuldade ou impossibilidade de acatar a norma para que o devido suporte seja fornecido.

V. Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;

VI. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

VII. Realizar o descarte adequado de documentos de acordo com seu grau de classificação, utilizando recursos como fragmentadoras de papel.

6. Validade e Gestão de Documentos

Este documento é válido a partir de 22 de novembro de 2021.

GRUPO DIGIVOX
0800 724 8181

Digivox - João Pessoa
Av. Paulino Pinto, 1500 | João Pessoa, PB - Brasil

Digivox - Miami
1953 NW 93rd Avenue | Miami, FL - USA

DIGI SOLUÇÕES DE COMUNICAÇÃO LTDA.
CNPJ 06.126.611/0001-67