Política de Segurança da Informação

A presente política atribui à área de Segurança da Informação a responsabilidade pela proteção dos recursos tecnológicos da SUMICITY TELECOMUNICAÇÕES S.A., ou simplesmente SUMICITY, pelo desenvolvimento, disseminação e a manutenção dessa política, normativas e procedimentos complementares.

Essa política estabelece diretrizes e responsabilidades com base nas melhores práticas de mercado, além da norma ABNT NBR ISO/IEC 27002, com o objetivo de proteger as informações da SUMICITY TELECOMUNICAÇÕES S.A. contra perdas, danos ou uso inapropriado. Refere-se às informações obtidas, criadas, armazenadas, processadas, transportadas ou descartadas nos sistemas e ambiente da SUMICITY ou de terceiros que sejam relacionados a SUMICITY.

OBJETIVO

Estabelecer diretrizes, controles e responsabilidades para assegurar que as informações estejam protegidas contra perdas, danos ou uso inapropriado. Estabelecer e regulamentar a política de segurança para uso de e-mail, uso de dados, acesso à rede de computadores e disponibilização de recursos de TI, aplicada na SUMICITY e observando a preservação da confidencialidade, da integridade e da disponibilidade da informação.

Orientar os colaboradores, parceiros, fornecedores, clientes, terceiros, governo e demais entidades externas quanto às suas responsabilidades na segurança e proteção da informação de modo a garantir a continuidade das atividades da SUMICITY.

TERMOS E DEFINIÇÕES

Acesso remoto: forma de acesso às redes corporativas por usuários autorizados por meio da internet.

Ativo de Informação: –qualquer informação, dispositivo ou outro componente do ambiente que seja utilizado para a entrega de serviços e objetivos do negócio SUMICITY. Usualmente os ativos são recursos tecnológicos, processos, software, documentos e informações.

Autenticidade: princípio pelo qual uma informação é identificada como autêntica, legítima e verdadeira, garantindo sua origem ou procedência.

Base autoritativa: referência primária para consultas e atualizações de perfis de acesso com base nos cargos, nível hierárquico e atribuições entre outros, para colaboradores, parceiros, fornecedores, clientes e terceiros.

Colaborador: funcionários e estagiários contratados para trabalhar na SUMICITY.

Confidencialidade: princípio que limita o acesso à informação apenas às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Criptografia: forma de codificar uma informação de maneira que apenas usuários autorizados tenham acesso à informação original.

Custodiante: área de Tecnologia da informação ou empresa contratada, que realiza a guarda e proteção das informações e recursos computacionais da SUMICITY.

Disponibilidade: princípio que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Equipamentos de TI: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação e de acesso, estações de trabalho, notebooks, monitores, teclados, mouse, servidores de rede, equipamentos de conectividade e infraestrutura, equipamentos de videoconferência, chips, celulares, tablets e/ou qualquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada;

Gestor da Informação: delegado pelo proprietário da Informação, para administrar, armazenar, processar, transportar e destruir informações sob sua responsabilidade.

Governo e demais Entidades Externas: fazem parte deste grupo os funcionários de empresas privadas, governos, instituições não governamentais, entre outros.

Incidentes de Segurança da Informação: qualquer ocorrência de evento que viole os princípios de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade).

Informação: todo e qualquer conteúdo de conhecimento (em meio digital ou não) que trate de assuntos relacionados a SUMICITY.

Integridade: princípio que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do

seu ciclo de vida (criação, obtenção, armazenamento, processamento, transporte e descarte).

LGPD: Lei Geral de Proteção de Dados, a Lei nº 13.709, de 14 de agosto de 2018, regulamenta qualquer atividade que envolva utilização de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, no território nacional ou em países onde estejam localizados os dados.

Parceiros/fornecedores: empresas parceiras ou fornecedores que complementam a força de trabalho.

Proprietário da Informação: gestores das áreas funcionais da SUMICITY responsáveis pela classificação de um conjunto específico de informações, determinando os acessos e os requerimentos de proteção.

Risco de Segurança da Informação: possibilidade de que eventos não desejados ocorram com as informações ou com os sistemas de informação.

Segurança da Informação (SI): competência que visa proteger a informação contra ameaças e vulnerabilidades buscando garantir a continuidade do negócio e minimização de riscos, alinhado com os objetivos estratégicos de negócio. Adicionalmente, zela pelos princípios de confidencialidade, integridade, disponibilidade e autenticidade. Sistemas de Informação: sistemas desenvolvidos internamente e/ou adquiridos, softwares e aplicações utilizados para criar, obter, armazenar, processar, transportar e destruir informação.

Terceiros: empresas/funcionários terceirizados contratados para trabalhar na SUMICITY.

TI: área de Tecnologia da Informação da SUMICITY;

Usuário: colaboradores, parceiros, consultores, auditores, fornecedores, clientes, terceiros, governo e demais entidades externas da SUMICITY, que tenha acesso a qualquer informação relacionada a SUMICITY, seja em ambiente próprio ou terceirizado, localizado dentro ou fora das instalações da SUMICITY.

DIRETRIZES

3.1 Descrições Gerais

As informações, sistemas e redes da SUMICITY devem ser classificados, protegidos e utilizados de maneira responsável, de forma a manter os princípios de confidencialidade, autenticidade, integridade e disponibilidade.

É obrigação de todos zelar pela segurança, integridade e preservação das informações e dados tratados pela SUMICITY para garantir a continuidade dos negócios, minimizando riscos e maximizando o retorno dos investimentos e as oportunidades de negócio.

As informações e recursos tecnológicos da SUMICITY devem somente ser utilizados pelos usuários autorizados, para execução de suas funções e atribuições profissionais. É permitido o uso para fins pessoais desde que não causem impacto em recursos tecnológicos ou na segurança da informação da SUMICITY.

Para acessos e privilégios, os usuários devem ter apenas o essencialmente necessário para a execução de suas funções respeitando, portanto, o princípio do mínimo privilégio.

Todo ambiente deve ser monitorado, auditado, e as informações obtidas podem ser utilizadas para procedimentos disciplinares ou legais.

É explicitamente proibido o uso dos recursos tecnológicos disponibilizados para acessar, transmitir, obter, apresentar, publicar, divulgar ou requerer os seguintes tipos de conteúdo:

- Pornografia e Pedofilia;
- Que viole direitos autorais ou licenciamento;
- Que promova, incite ou oriente crimes, violência e danos à propriedade; Que viole leis, regulamentações ou contratos de uso;
- Que ameace, difame ou ofenda pessoas, grupos ou entidades;
- Que dificulte, viole ou impossibilite a implementação de políticas e controles de segurança definidas;
- Que resulte em qualquer tipo de impacto negativo ou danos à imagem e aos recursos computacionais da SUMICITY;

3.2 Suprimentos

A base autoritativa de fornecedores, parceiros e terceiros deverá ser mantida em base centralizada pela área de Suprimentos e deve ser a referência primária para informações de parceiros, fornecedores e terceiros em processos, sistemas e recursos computacionais.

O parceiro/ fornecedor devolverá os ativos de TI por ele utilizados nas mesmas condições que recebeu, observado o desgaste natural decorrente do uso, ao final do seu contrato com SUMICITY, mediante baixa do Termo de Responsabilidade, Uso e Cautela de Ativos de TI na área de Suprimentos e/ou TI.

3.3 Segurança Física e do Ambiente

Independentemente da forma que a informação se apresente (impressa, escrita, armazenada eletronicamente, transmitida por correio ou meios eletrônicos, imagens ou áudios), seu compartilhamento, integridade, armazenamento e até o descarte devem ser devidamente protegidos por todos os colaboradores.

Caso seja identificado o acesso ou presença de indivíduos não autorizados, sem identificação ou em atividade que viole os padrões de segurança da informação, comportamento ou mesmo que exponha outros e os equipamentos a riscos, deve ser imediatamente reportado às equipes de segurança patrimonial ou segurança da informação.

3.4 Gestão das Operações e Comunicações

Toda comunicação eletrônica, que ocorra fora de ambientes controlados pela SUMICITY ou utilizando meios externos, deve permitir a implementação de recursos e ferramentas que possibilitem a segurança destas informações de forma a não depender de iniciativas de terceiros. O responsável pela segurança da informação deverá apoiar na definição e implementação desses recursos.

Toda disponibilização ou implantação de acesso remoto, seja individual ou dedicado, deve estar em conformidade com todos os requisitos de segurança definidos. No caso de funcionários, deverá ser autorizada pelo responsável de Segurança da Informação e pelo gestor da área funcional. Para fornecedores, terceiros ou parceiros é necessária, além das aprovações mencionadas anteriormente, a aprovação do gestor do contrato.

Todo serviço de suporte contratado, deverá disponibilizar recursos de acesso remoto supervisionado via internet pelo custodiante, sem a necessidade de liberação de acessos remotos adicionais.

3.5 Gestão de Identidades

Devem existir mecanismos formais de controle de acesso às informações, recursos tecnológicos e dependências físicas da SUMICITY, que sejam capazes de identificar, autenticar, autorizar e rastrear as atividades de usuários legítimos ou não.

Todos os privilégios de acessos concedidos, alterados ou revogados devem ocorrer de forma controlada e formalizada, conforme os princípios de mínimo privilégio, segregação de funções e estando devidamente autorizado, de acordo com as funções definidas a cada indivíduo.

São definidos três níveis de identidades, conforme listado abaixo:

- Contas individuais – Todo usuário possuirá uma identificação única, não podendo ser compartilhada com outros usuários. Subdivide-se em contas de colaboradores, contas de terceiros, contas de parceiros ou fornecedores e contas de visitantes.
- Contas de administração – São contas com privilégios administrativos ou especiais, utilizadas apenas por pessoas formalmente autorizadas.
- Contas de serviço – São contas utilizadas exclusivamente para execuções sistêmicas e equipamentos, não podendo ser utilizadas por qualquer usuário.

O responsável pela Segurança da Informação é o responsável pela gestão de contas de administração e de serviços.

3.6 Classificação das Informações

Todas as informações devem ser classificadas e protegidas de acordo com seus requisitos específicos durante o ciclo de vida da informação (criação, obtenção, processamento, armazenamento, transporte e destruição), conforme Política de Classificação, Rotulação e Tratamento da Informação. O Encarregado deve avaliar de forma criteriosa toda classificação que envolvam dados pessoais.

Toda informação classificada em qualquer nível diferente de pública, que venha a ser disponibilizada, armazenada ou acessada por outros ambientes que não os de produção, deverá impreterivelmente ter os dados envolvidos mascarados e descaracterizados de forma a preservar a confidencialidade destas.

É de extrema importância evitar que qualquer tipo de informação, principalmente as confidenciais fiquem expostas ou de fácil acesso para o uso indevido. A SUMICITY preza pelo conceito de tela e mesa limpa ao fim do seu expediente como boa prática para assegurar que a informação, tanto em formato digital quanto físico (anotações em papel e impressos), e equipamentos (notebooks, celulares corporativos, tablets etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso ou o responsável esteja ausente.

3.7 Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Todas as aplicações, sistemas e recursos tecnológicos deverão ser avaliados pela área de Segurança da Informação quanto a controles e impactos em segurança e em tempo de projeto, permitindo a implantação

de ajustes e correções que se façam necessárias antes da entrada em produção.

Os sistemas desenvolvidos ou adquiridos devem ser analisados em relação ao impacto à LGPD e a Segurança da Informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas em que a SUMICITY julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela SUMICITY ou por terceiros.

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

3.8 Gestão de Incidentes de Segurança da Informação e Privacidade de Dados

Um incidente de segurança pode ser definido um simples ou uma série de eventos de segurança da informação indesejados ou inesperados que tenham capacidade de comprometer as operações do negócio e ameaçar a segurança da informação. Em geral, indica uma possível violação desta Política, falha de controles ou uma situação anteriormente desconhecida que possa ter efeito adverso para a segurança da informação.

O responsável pela Segurança da Informação deve viabilizar a metodologia para a resposta a incidentes de segurança da informação, contemplando procedimentos para a preparação, detecção, resposta, contenção, correção e avaliação posterior de incidentes de segurança. Além disso, também deve definir diretrizes para a custódia de evidências e planos de comunicação.

O responsável de Segurança da Informação poderá intervir sem aviso prévio, em casos de incidentes que comprometam a disponibilidade, autenticidade, integridade e confidencialidade dos ativos da SUMICITY e posteriormente notificar os gestores da informação e encarregado.

Todos os incidentes que afetem a segurança deverão ser comunicados à Gerência de Infraestrutura de TI, tais como, mas não limitados a:

- Acesso não autorizado;
- Denial of Service (negativa de acesso) com o intuito de tornar os recursos de um sistema indisponíveis para seus Usuários, impactando a disponibilidade da informação;
- Vírus e outros códigos maliciosos;
- Uso impróprio (quando o Usuário viola essa Política) Comportamento anormal do computador;
- Vazamento de dados, intencional ou não;
- Suspeita de comprometimento de senhas;
- Recebimento de mensagens de extorsão etc.

3.9 Análise de Segurança da Informação

Devem ser testados os principais recursos tecnológicos da SUMICITY para assegurar que os controles de segurança continuem refletindo um ambiente seguro e que suporte seu crescimento.

Todos os sistemas sob a responsabilidade ou contratados pela SUMICITY estão sujeitos a testes de segurança sem aviso prévio. A equipe de segurança da informação ou parceiro apontado por essa é responsável pela realização de testes periódicos dos recursos tecnológicos da SUMICITY.

3.10 Continuidade do Negócio

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.

3.11 Desvios

Os desvios à política devem ser notificados ao responsável de Segurança da Informação. Após análise inicial, o responsável pelo desvio deve apresentar justificativa documentada e que necessita ser aprovada e assinada pelo proprietário da informação/gestor da área funcional. Os desvios devem ser endereçados ao Comitê de Segurança da Informação e Governança de Dados, para que sejam tomadas as medidas cabíveis.

No interesse de investigações conduzidas pela Comissão de Ética da SUMICITY, estão previamente autorizadas, independentemente da aprovação do CEO, (i) a análise de todo e qualquer arquivo contido em Equipamento de TI fornecido pela SUMICITY; (ii) a análise de imagens de circuito interno de segurança; e (iii) a realização de entrevistas pessoais com os envolvidos ou com quaisquer outros

Usuários, inclusive terceiros, conforme necessário, que possam auxiliar na apuração dos relatos. Portanto, os Usuários não devem ter expectativa de privacidade no que se refere a assuntos tratados através de e-mails corporativos e/ou armazenados em Equipamentos de TI da SUMICITY.

4.CONSIDERAÇÕES FINAIS

A violação a qualquer termo ou disposição dessa Política sujeitará o(a) infrator(a) a medidas corretivas, incluindo a possibilidade de suspensão não remunerada do emprego, rescisão do contrato de trabalho, sem prejuízo de eventuais medidas cabíveis nas esferas administrativa, cível ou criminal.

Além das penalidades previstas nesta Política, na hipótese de as infrações configurarem crime, a SUMICITY poderá cientificar as autoridades competentes ou adotar as medidas administrativas ou judiciais cabíveis. Aplicam-se a essa Política as normas previstas no Código da Ética SUMICITY.

5.LEGISLAÇÃO RELACIONADA

- Lei nº 8.078 de 11 de setembro de 1990, o Código de Defesa do Consumidor;
- Lei nº 9.296 de 1996, que trata sobre a interceptação das comunicações telefônicas;
- Lei nº 12.737 de 30 de novembro de 2012, dispõe sobre a tipificação de delitos informáticos; Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet;
- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;

6.BIBLIOGRAFIA

- ISO/IEC 27001
- NBR ISO/IEC
- 27002:2005 ISO 27701
- ITIL® Foundation, ITIL 4 edition