Política de Segurança da Informação

Responsável:
Comitê da LGPD.

Emissão: 14/11/2023

Revisão: 3

Av. Presidente Wilson, 231 sala 902 – CEP 20030-905 – Rio de Janeiro – RJ
www.logum.com.br

Sumário

1. Objetivo 3
2. Definições Gerais 3
3. Abrangência 5
4. Diretrizes da Segurança da Informação 6
5. Segurança do Ambiente Físico 8
6. Segurança do Ambiente Lógico 9
7. Gerenciamento de Senhas e Autenticação 11
8. Correio Eletrônico (*e-mail*) 12
9. Acesso à Rede Corporativa 16
10. Acesso à Internet 17
11. Retenção de Dados 18
12. Gestão de Incidentes 18
13. Gestão de Mudança 22
14. Proteção de Dados e Auditoria 22
15. Papéis e Responsabilidades 22
16. Violação da Política de Segurança da Informação 24
17. Boas Práticas 24
18. Controles implementados 25
19. Canais de Comunicação 25

Anexo I - Termo de Recebimento e Adesão às Políticas da Logum Logística S.A. 26

Anexo II – Contrato de Comodato 27

Anexo III – Termo de Responsabilidade para Acesso de e-mails de Terceiros 28

Av. Presidente Wilson, 231 – 9º andar – CEP 20030-905 – Rio de Janeiro – RJ
www.logum.com.br

1. Objetivo

A **Política de Segurança da Informação** ("**Política**") reúne um conjunto de diretrizes relacionadas à Segurança da Informação (SI) e utilização dos ativos de Tecnologia da Informação e Comunicação (TIC).

São objetivos desta **Política:**

- Endereçar os tópicos relacionados a utilização de *e-mail*, Internet, acesso à rede LOGUM, sistemas corporativos, ativos de TI de uso individual e coletivo;
- Garantir a conformidade com os requisitos de integridade, legalidade, disponibilidade, confiabilidade, confidencialidade e segurança dos ativos de informação da LOGUM, assim como a Lei Geral de Proteção de dados (LGPD – Lei 13.709/18);
- Estabelecer responsabilidades e limites de atuação dos Colaboradores e Terceiros da LOGUM em relação à segurança da informação e a promoção e disseminação da cultura de conformidade em segurança da informação no ambiente interno e/ou externo da Companhia;
- Estabelecer os requisitos mínimos para a gestão de eventuais registros relacionados a incidentes envolvendo "**dados pessoais".**

A presente **Política** deve ser lida em conjunto com as obrigações previstas nos documentos abaixo relacionados, que versam sobre informações em geral, e a complementam quando aplicável:

i. Contratos de trabalho de funcionários da Logum e outros documentos comparáveis, que dispõem sobre obrigações de confidencialidade em relação às informações mantidas pela empresa;
ii. Política de Privacidade e Proteção de Dados Pessoais, Política de Trabalho Híbrido – Home Office e Presencial, Política de Atribuição e Uso de Telefonia Móvel e Código de Ética e Conduta;
iii. Todas as normas internas a respeito da proteção de **dados pessoais** que vierem a ser elaboradas e atualizadas, de tempos em tempos

2. Definições Gerais

AMBIENTE FÍSICO: engloba os ativos da empresa, como instalações e equipamentos;

AMBIENTE LÓGICO: conjunto de sistemas, dados e programas da empresa;

ANPD: a Autoridade Nacional de Proteção de Dados;

ANTISPAM: ferramenta utilizada para bloquear mensagens indesejadas de correio eletrônico (Spams);

ATIVOS DE TIC: estações de Trabalho (Desktop/Notebook), celulares, servidores, softwares, arquivos, correio eletrônico, Dispositivos de Autenticação, equipamentos de rede e quaisquer equipamentos eletrônicos ou sistemas relacionados à tecnologia da informação e comunicação;

AUTENTICAÇÃO: processo de verificação da identidade de um usuário ou sistema, necessário para autorizar a utilização de recursos corporativos de TIC e ao acesso das informações de propriedade da LOGUM. Tal processo tem como objetivo confirmar a identidade do usuário ou entidade que está tentando acessar a informação;

BACKUP: cópia de dados ou arquivos digitais, de um dispositivo de armazenamento para outro, de forma que os dados ou o sistema possa ser restaurado em caso de perda dos dados originais;

CATÁLOGO DE ENDEREÇOS: agenda de endereços eletrônicos existente na aplicação de correio eletrônico;

CFTV: Circuito Fechado de Televisão, ou seja, consiste em sistema de monitoramento de ambientes através de visualização e gravação de imagens capturadas por câmeras. O sistema de CFTV pode transmitir as imagens gravadas ou em tempo real para monitores de vídeo;

CONFIDENCIALIDADE: garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada; princípio cujo objetivo é limitar o acesso à informação tão somente a pessoas, entidades e processos autorizados pelo titular da informação;

CONTA DE USUÁRIO: credencial de Acesso aos Recursos da Rede Corporativa que identifica o Usuário que a utiliza. Seu uso é pessoal, intransferível e de responsabilidade do próprio Usuário. É identificado pelo termo "Login" nos Recursos da Rede Corporativa;

CREDENCIAL DE ACESSO: conjunto de informações (login e senha) utilizadas no processo de Autenticação de sistemas, como: SAP, Mastersaf, Portal de Agendamento, etc

CRIPTOGRAFIA: mecanismo com objetivo de impedir que as informações trocadas sejam lidas indevidamente por pessoas não autorizadas;

DATA CENTER: ambiente projetado para abrigar equipamentos de TI (servidores, firewalls, etc.). O objetivo principal de um *Data Center* é garantir a alta disponibilidade dos sistemas hospedados;

DISPONIBILIDADE: princípio cujo objetivo é garantir que a informação esteja sempre acessível e utilizável pelas pessoas, entidades e processos autorizados, sempre que estes necessitarem;

DISPOSITIVOS DE ARMAZENAMENTO MÓVEL: incluem, entre outros, pen-drive, disco removível e HD externo;

E-mail: forma reduzida para E(lectronic)-Mail - Correio Eletrônico;

ESTAÇÃO DE TRABALHO: computador (Desktop ou notebook) e seus periféricos que o Usuário utiliza para exercer suas atividades profissionais;

INCIDENTE DE SEGURANÇA: um ou mais eventos indesejados ou inesperados, que tenham uma probabilidade de acarretar riscos ou danos a direitos dos titulares, comprometendo as operações do negócio e/ou ameaçando a Segurança da Informação e/ou permitindo acesso indevido ou ilícito sem o consentimento do titular de dados;

INTEGRIDADE: propriedade de salvaguarda da exatidão e completeza da informação mantendo todas as características originais estabelecidas pelo proprietário da mesma; princípio que tem como objetivo garantir que apenas pessoas, entidades e processos autorizados possam alterar o conteúdo das informações corporativas;

INTELIGÊNCIA ARTIFICIAL (IA): conceito abrangente relacionado à capacidade de um sistema informatizado em reproduzir competências semelhantes à inteligência humana tais como raciocínio, aprendizagem, planeamento e a criação de novos conteúdos.

INTELIGÊNCIA ARTIFICIAL GENERATIVA (IAG): parte da IA relacionada à criação de novos conteúdos tais como texto, imagens, áudios, dados sintéticos a partir de dados pré-existentes. Exemplos são ChatGPT, Bard, Copilot e DALL-E.

INTERNET: sistema global de rede de computadores interligados através de um conjunto padrão de protocolos;

LGPD: Lei 13.709/18 – Lei Geral de Proteção de **Dados pessoais**;

LOG: termo técnico para descrever o registro das transações que ocorrem quando um software é utilizado;

***ONEDRIVE*:** serviço de armazenamento na nuvem da Microsoft;

MFA (MÚLTIPLO FATOR DE AUTENTICAÇÃO): sistema de validação adicional ao processo de autenticação tradicional (usuário + senha) com o objetivo de aumentar a segurança de acesso.

PHISHING: técnica utilizada por criminosos que tem por objetivo "pescar" informações relevantes dos usuários através de mensagens ou sites falsos. Exemplos de informações coletadas indevidamente são, senhas, dados pessoais, contas bancárias e número de cartões de crédito***;***

PST: arquivo de dados do Outlook que contém mensagens e outros itens do Outlook de uma determinada conta, o qual é salvo no computador;

RECURSOS DA REDE CORPORATIVA: consistem em todas as Pastas Corporativas, serviços, sistemas e equipamentos de Tecnologia da Informação da LOGUM;

SEGURANÇA DA INFORMAÇÃO: está diretamente relacionada com a **proteção** de um conjunto de informações de ativos de informação, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da **segurança da informação**: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

***SOFTWARE*:** é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de *softwares*;

***SOFTWARES* HOMOLOGADOS:** softwares habilitados para funcionamento no Ambiente de Automação e TI da LOGUM, testados e aprovados previamente pela Gerência de Tecnologia;

***SOFTWARES* LICENCIADOS:** softwares para os quais tenham sido adquiridas Licenças de Uso fornecidas pelos seus respectivos fabricantes;

***SPAM*:** mensagem não solicitada, normalmente indesejada, enviada para um grande número de pessoas;

TA: Tecnologia da Automação;

TIC: Tecnologia da Informação e Comunicação;

***USB*:** é um tipo de conexão em computadores que permite a comunicação entre computadores e mídias removíveis de armazenamento de dados ou periféricos (teclado, mouse, etc.);

USUÁRIO: qualquer colaborador da LOGUM (funcionário, estagiário, terceiro, temporário, contratado ou subcontratado) que utiliza algum serviço de informação disponibilizado pela LOGUM na execução de suas funções;

***VPN* (*VIRTUAL PRIVATE NETWORK* OU REDE VIRTUAL PRIVADA):** meio de comunicação seguro através da internet para acesso remoto aos sistemas LOGUM.

3. Abrangência

Esta **Política** se aplica:

i. aos funcionários e estagiários da Logum

ii. a todos os **terceiros**, sejam eles pessoas físicas ou jurídicas, que atuam para ou em nome da Logum e que utilizam ativos de Informação da LOGUM, tais como computadores, *e-mail*, rede corporativa, Sistemas (SAP, Mastersaf etc.), links de dados e repositório de dados;
iii. aos **titulares de dados pessoais**, cujos dados são tratados pela Logum.

A adesão a esta **Política** é obrigatória a todos os destinatários acima indicados na medida em que se relacionam com a Logum.

4. Diretrizes da Segurança da Informação

A **informação** é um ativo de propriedade da Logum que tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. Esta **Política** estabelece as diretrizes para a proteção da informação a diversos tipos de ameaça a fim de garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios.

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir o acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, confidencialidade e disponibilidade dos bens.

A Segurança da Informação é aqui caracterizada por:

i. **Autenticidade:** garante a identidade de quem está enviando a informação, ou seja, propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mudanças ao longo de um processo;
ii. **Confidencialidade:** é a garantia de que a informação é acessível somente às pessoas com acesso autorizado;
iii. **Integridade:** é a salvaguarda da exatidão e integralidade da informação e dos métodos de processamento;
iv. **Disponibilidade:** garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação (Logum).

Para assegurar esses quatro itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de **COMPORTAMENTO SEGURO** e **CONSISTENTE** com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

A interpretação da presente **Política**, bem como dos documentos correlatos, deverá ser feita de forma restritiva. Sendo assim, caso alguma atividade não esteja abarcada pelos documentos mencionados, esta deverá ser submetida a um processo de validação formal por parte do Gestor do colaborador ou terceiro, antes de sua execução.

Todas as informações geradas, acessadas, manuseadas, armazenadas ou descartadas durante a atividade dos usuários, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade, responsabilidade e de direito de uso exclusivo da Logum, sendo utilizados para fins profissionais exceto os casos explicitados nesta Política.

Toda e qualquer utilização de obras intelectuais, softwares, desenhos industriais, marcas, identidades visuais e/ou quaisquer outros sinais distintivos atuais ou futuros da Logum são de propriedade intelectual da Logum.

Todos os Recursos de TIC de propriedade e/ou sob responsabilidade da Logum devem ser usados para fins profissionais, exceto para os casos explicitados nesta política, e utilizados de forma lícita, ética e moral, seguindo as regras da Logum.

A Logum realizará o controle de acessos aos seus ambientes, ativos e informações, devendo os usuários respeitarem as regras impostas e vinculadas a cada acesso fornecido.

A contratação de colaboradores e terceiros que envolvam o compartilhamento de informações de propriedade e/ou sob responsabilidade da Logum deverá ser acompanhada de termos de confidencialidade e cláusulas contratuais relativas à segurança da informação.

A Logum adota um mecanismo e processo de salvaguarda (*backup*) completa de seus sistemas com fins de conformidade com requisitos legais, operacionais e de lógica de negócio. No caso de falhas ou incidentes de segurança da informação, será realizada a recuperação das informações através destes *backups*.

A Logum realiza o monitoramento de seus ambientes – físicos e virtuais – para que a eficácia dos controles seja garantida e a proteção do patrimônio assegurada.

A Logum possui um canal de comunicação de incidentes, cuja divulgação é realizada junto a seus colaboradores para o reporte de incidentes de segurança da informação, através do *e-mail* tecnologia@logum.com.br.

A Logum respeita os regulamentos e leis relativos à proteção da privacidade e **dados pessoais** do Brasil, assim como demais normas relacionadas, adotando uma postura de conformidade com as boas práticas e medidas de segurança em privacidade e proteção de **dados pessoais**.

A Logum adotará um programa de revisão/manutenção desta **Política** e suas normas complementares sempre que necessário. Todas as alterações serão devidamente comunicadas aos colaboradores e terceiros abarcados por esta **Política**;

Todas as dúvidas relacionadas a esta **Política** deverão ser encaminhadas à Área de Tecnologia da Informação, através do *e-mail* tecnologia@logum.com.br

4.1 Engenharia Social

Engenharia social é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a fornecer dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Além disso, tais criminosos podem tentar explorar a falta de conhecimento do usuário.

As grandes fragilidades onde os criminosos virtuais se baseiam são na falta de **conscientização do usuário em relação à Segurança da Informação** e na exploração da confiança de pessoas para obtenção de informações sigilosas e importantes.

A engenharia social se manifesta de diversas formas, mas podemos dividir em dois grandes grupos:

i. **Diretos:** caracterizados pelo contato direto entre o criminoso virtual e a vítima, através de telefonemas e até mesmo pessoalmente, tendo em vista que o engenheiro social nem sempre é alguém desconhecido;

ii. **Indiretos:** caracterizados pela utilização de *softwares* ou ferramentas de invasão, como por exemplo, vírus, Cavalo de Tróia, ou através de sites ou *e-mails* falsos, mensagens falsas através de whatsapp, para assim obter informações desejadas.

Atenção especial para o ***phishing*** que pode se manifestar de diversas formas. Algumas bastantes simples com conversas falsas em *softwares* de mensagens instantâneas e *e-mails* com *links* suspeitos. Fora isso, existem páginas inteiras na internet construídas para imitar sites de compras, bancos e outras instituições.
Todas estas maneiras, no entanto, convergem para o mesmo ponto: roubar informações confidenciais de pessoas ou empresas.
O melhor a fazer é ignorar e deletar o *e-mail* ou mensagem imediatamente, porém, em caso de dúvidas favor acionar a equipe do *Help Desk*.

5. Segurança do Ambiente Físico

5.1 Todos os equipamentos de TI da Logum (servidores, *notebooks*, etc) são inventariados e identificados como patrimônio da empresa de forma única e individual, salvo itens de baixo valor, tais como mouse, teclado, *nobreak*, e etc., e sua utilização é restrita aos usuários autorizados;

5.2 A entrada nas áreas de armazenamento de ativos (*Data Center*) tem acesso devidamente controlado e monitorado. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviços, e até mesmo funcionários sem acesso liberado) será acompanhada de ou autorizada por pessoas autorizadas;

5.3 Os ativos que ofereçam risco à Segurança da Informação podem ser temporariamente desativados pela Gerência de Tecnologia;

5.3 Os ativos de TI são disponibilizados aos usuários, de acordo com os cargos ocupados, para que possam desempenhar suas funções, mediante assinatura do "Termo de Adesão à Política de Segurança da Informação" – Anexo I e Contrato de Comodato – Anexo II;

5.4 Para disponibilização de ativos à terceiros há necessidade de aprovação da área da Logum atendida, mediante análise da real necessidade para o desempenho da atividade;

5.4 Os dispositivos móveis, tais como *notebooks e celulares*, serão disponibilizados aos usuários que necessitem de mobilidade ou que sejam elegíveis à Política de Trabalho Híbrido – *Home Office* e Presencial;

5.5 A utilização de qualquer ativo, de propriedade da Logum, poderá ser suspensa ou monitorada quando houver qualquer indício de utilização ou compartilhamento inapropriado, ou ainda vazamento de informações que estiverem sob a responsabilidade do usuário;

5.6 Os ativos de propriedade da Logum devem ser devolvidos pelo usuário em caso de desligamento ou sempre que solicitado pela Gerência de Tecnologia;

5.7 Os ativos sob a responsabilidade dos usuários não podem ser compartilhados com terceiros (incluindo familiares);

5.8 Quando aplicável, os ativos descontinuados devem ter seus dados apagados, sobrescritos ou até mesmo os respectivos discos de memória (HD) serem removidos pela equipe do *Help Desk*;

5.9 O uso dentro das instalações da empresa, de quaisquer equipamentos de gravação, fotografia, som ou outro tipo de equipamento similar, somente poderá ser realizado a partir da autorização do gestor responsável pelo terminal ou escritório.

6. Segurança do Ambiente Lógico

6.1 Sistemas / *Softwares*

6.1.1 As estações de trabalho, incluindo *notebooks*, devem conter exclusivamente *softwares* licenciados e homologados. O padrão de configuração dessas estações é definido pela Gerência de Tecnologia e não pode ser modificado sem autorização da mesma;

6.1.3 Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários autorizados ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

6.1.4 Não é permita a execução de programas que tenham como finalidade a decodificação de senhas, monitoramento ou exploração não autorizada da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total dos arquivos ou a indisponibilidade de serviços;

6.1.5 Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa;

6.1.6 Não enviar ou compartilhar informações confidenciais, independente do meio (e-mail, OneDrive, etc), quando não autorizado**;**

6.1.7 As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada regularmente, por amostragem, e mantida atualizada;

6.1.8 O acesso aos sistemas é permitido somente após a autenticação do usuário;

6.1.9 As credenciais de acesso são de uso pessoal, nominativas, intransferíveis e de responsabilidade exclusiva dos usuários;

6.1.10 É proibida qualquer tentativa de acesso não autorizado aos sistemas;

6.1.11 As licenças para utilização dos sistemas são concedidas pela empresa aos usuários que necessitem dos recursos para desempenho das suas funções. A utilização poderá ser monitorada, e a licença suspensa, a qualquer momento, por decisão da Gerência de Tecnologia;

6.1.13 Qualquer *software* que, por necessidade do trabalho tiver que ser instalado, deverá ser avaliado pela Gerência de Tecnologia, para que o mesmo possa ser homologado e só assim serem disponibilizados aos usuários da área solicitante;

6.1.14 A empresa reconhece os direitos autorais dos *softwares* que usa e reconhece que deve pagar o justo valor por eles, coibindo e monitorando o eventual uso indevido de programas não licenciados. É terminantemente proibido o uso de *softwares* ilegais (sem licenciamento) na Logum;

6.1.15 A Gerência de Tecnologia poderá valer-se deste instrumento para desinstalar, sem prévio aviso, todo e qualquer *software* sem licença de uso, em atendimento à Lei 9.609/98 (Lei do *Software);*

6.1.16 No caso de uso de ferramentas de IA (Inteligência Artificial) ou IAG (Inteligência Artificial Generativa), informações confidenciais não devem ser utilizadas, exceto se autorizado pelo Diretor da área;

6.17 Cadastros em sistemas de IAG, tais como ChatGPT e BARD, para uso corporativo e particular devem ser realizados, respectivamente, através de e-mail corporativo e particular. Ou seja, não é permitido o uso de IAG para uso particular utilizando contas corporativas, bem como não é permitido acessar IAG para fins de trabalho utilizando contas particulares.

6.2 Estações de trabalho

6.2.1 As estações de trabalho possuem códigos internos, os quais permitem que elas sejam identificadas. Desta forma, tudo o que for executado na estação de trabalho é de responsabilidade do usuário;

6.2.2 No caso de uma estação de trabalho ser realocada para outro usuário, esta será formatada e todos os dados serão apagados;

6.2.3 As estações de trabalho, por padrão, possuem bloqueio a todo Dispositivo de Armazenamento Móvel, tais como HD externo e pen drive. A liberação destes dispositivos, quando justificável, deve ser solicitada formalmente pelo gestor da área informando o período e o motivo, o qual será analisado pelo gestor de Tecnologia. Vale salientar que, caso a liberação seja autorizada, o usuário é responsável pelos danos causados por possíveis vírus ou outras ameaças que tais dispositivos possam conter;

6.2.4 A Gerência de Tecnologia não realiza cópias de segurança das informações armazenadas localmente nas estações de trabalho. As cópias de segurança (*backup´*s) são realizadas somente nas informações armazenadas nos Servidores Corporativos (diretórios de rede Público, Corporate, etc.). Desta forma, é de responsabilidade do usuário manter os arquivos de trabalho armazenados corretamente nos Servidores Corporativos;

6.2.5 O acesso a estação de trabalho deverá ser encerrado no final do expediente, quando o usuário deverá desconectar o seu acesso à *VPN* e desligar o equipamento;

6.2.6 Antes de se afastar da estação de trabalho, o usuário deverá obrigatoriamente, bloquear a estação de trabalho;

6.2.7 Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízos à Logum, só devem ser utilizadas em equipamentos com controles adequados;

6.2.8 Apenas o pessoal autorizado pela Gerência de Tecnologia pode instalar softwares nas estações de trabalho dos usuários e devem utilizar apenas softwares licenciados pela Logum. Em caso de dúvidas, favor consultar a área de TI através dos canais de suporte (Help Desk);

6.2.9 A Gerência de Tecnologia deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados;

6.2.10 - Arquivos pessoais podem ser salvos na estação de trabalho ou OneDrive Corporativo, mas em hipótese nenhuma podem ser salvos nos servidores corporativos.

6.3 Equipamentos Particulares ou de Terceiros na empresa

6.3.1 *Notebooks* particulares ou de terceiros para serem utilizados na rede corporativa precisam, obrigatoriamente, ser avaliados e aprovados pela Gerência de Tecnologia.

6.3.2 É de responsabilidade da área contratante de prestadores de serviços, incluir no contrato entre as partes cláusula declarando a responsabilidade da empresa terceira sobre todo e qualquer software instalado nos equipamentos dos mesmos. Sugere-se a reavaliação semestral dos equipamentos.

6.3.3 É de responsabilidade da área contratante encaminhar os equipamentos de terceiros sob sua responsabilidade para o *Help Desk* para que sejam verificadas as atualizações de antivírus, existências de vírus e a instalação de certificado para acesso à rede corporativa.

6.4 Dispositivos de Armazenamento Móvel

6.4.1 O uso de dispositivos de armazenamento móveis, por padrão, não é permitido na empresa. Exceções deverão ser solicitadas formalmente pelo gestor da área informando o período e o motivo, o qual será analisado pelo gestor de Tecnologia. Vale salientar que, caso a liberação seja autorizada, o usuário é responsável pelos danos causados por possíveis vírus ou outras ameaças que tais dispositivos possam conter;

6.4.2 Informações devem ser transmitidas usando as ferramentas corporativas disponíveis (*e-mail,* diretório Temporário, *Onedrive*) que mantém a segurança requerida;

6.4.4 No caso de comprovação de utilização de dispositivos móveis sem autorização, o usuário será responsabilizado no caso de perda/vazamento de informação ou no caso de entrada de vírus ou *softwares* maliciosos na rede corporativa.

6.5 Ferramentas de Comunicação

6.5.1 Recomenda-se a utilização do *Microsoft Teams* como ferramenta de comunicação, devendo ser utilizado prioritariamente para atividades de negócios, podendo ser monitorado e utilizado para fins de auditoria. A solicitação e aprovação de todos os participantes precisa estar gravada como evidência no início da gravação.

6.6 Sistemas de CFTV e Controle de Acesso

6.6.1 Os terminais possuem monitoramento de câmeras por CFTV e as imagens são gravadas e armazenadas;

6.6.2 O monitoramento contínuo por CFTV é realizado em nas áreas externas e em algumas áreas internas.

7. Gerenciamento de Senhas e Autenticação

Todo usuário deverá ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo de sua senha pessoal, não podendo em hipótese alguma repassar a mesma para outros usuários.

7.1 A senha do usuário deverá conter no mínimo 08 (oito) caracteres, devendo conter letras, números e caracteres especiais e não se deve repetir as cinco últimas senhas;

7.2 A senha deve ser alterada, no mínimo, a cada quatro meses.

7.2.1 Exemplos de composição de senhas que devem ser evitadas:

- Nome e sobrenome, especialmente os contidos no Login do Usuário;
- Números de documentos, matrículas funcionais, senhas bancárias ou de cartão de crédito, telefones, placas de carro ou datas que possam ser relacionadas ao usuário ou familiares;
- Palavras encontradas em dicionários;
- Palavras sugeridas a partir de objetos ou locais que possam ser vistos da mesa do Usuário;
- Palavras invertidas.

7.3 A senha não deve ser anotada em nenhum local - papéis, cadernos, post-its (ou similares) ou em qualquer material que as senhas possam ficar visíveis;

7.4 Não incluir senhas em processos automáticos de acesso ao sistema, mesmo que disponíveis;

7.5 Não armazene senhas de acesso em equipamento pessoal;

7.6 Não utilize senhas de acesso à rede da Logum para fins pessoais;

7.7 O usuário deve se certificar de que não está sendo observado ao digitar a sua senha;

7.8 A criação/envio de senhas pela equipe de TI (inicial ou não) deve ser realizada de forma segura. A senha inicial deve ser trocada pelo usuário em seu primeiro acesso;

7.9 A solicitação de recuperação ou desbloqueio de senha deverá ser solicitada pelo próprio usuário ao Suporte de TI (Help Desk). Ao receber uma nova senha, é responsabilidade do usuário alterar a senha temporária por uma definitiva na primeira utilização;

7.10 O Usuário que não efetuar acesso à rede corporativa em um período igual ou superior a 60 (sessenta) dias terá sua conta bloqueada;

7.11 Caso o usuário tenha 7 (sete) tentativas de acesso malsucedidas e consecutivas, sua conta será bloqueada por 30 minutos;

7.12 O uso de acesso via *VPN* deverá ser restrito a usuários que necessitem de acesso à rede corporativa estando fora das localidades físicas de trabalho e para os usuários elegíveis à Política de Trabalho Híbrido – Home Office e Presencial.

8. Correio Eletrônico (*e-mail*)

O correio eletrônico é de propriedade da LOGUM e seu uso é permitido para as atividades profissionais dos usuários. O uso particular do correio eletrônico é aceito desde que não prejudique o desenvolvimento das atividades profissionais.

8.1 O endereço de *e-mail* disponibilizado ao usuário é de uso pessoal e intransferível, portanto, é terminantemente proibido modificar ou substituir a identidade do remetente ou destinatário de uma mensagem do correio eletrônico.

8.2 É vedado o uso de sistemas de *webmail* terceiros (*Gmail, Hotmail, Yahoo*, etc.) para fins profissionais. O uso do correio eletrônico para envio e recebimento de *e-mail* deverá ocorrer exclusivamente através do correio eletrônico da Logum, com extensão @logum.com.br.

8.3 Os *PST´s* das bases de *e-mails* não devem ser salvos nas estações de trabalho e nos servidores corporativos pelos usuários.

8.4 É proibido:

a) enviar ou arquivar no servidor de *e-mail* mensagens contendo assuntos que provoquem perturbação ou assédio a outras pessoas ou que comprometam a imagem do negócio da Logum perante seus clientes, fornecedores, clientes e comunidade em geral; temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;

b) cadastrar a conta de *e-mail* da Logum em qualquer tipo de site para fins particulares;

c) efetuar configuração de *e-mails* pessoais nas estações de trabalho. Caso seja necessário o acesso aos *e-mails* pessoais através da estação de trabalho, este deve ser realizado através de *webmail;*

d) executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou com características suspeitas. Em caso de dúvidas consulte o *Help Desk*;

e) executar ou abrir *links*/endereços de *e-mails* suspeitos, como por exemplo bancos solicitando alguma informação pessoal. Verifique sempre se o *e-mail* ou endereço do *link* são realmente de fontes conhecidas. Em caso de dúvidas consulte o *Help Desk*;

f) utilizar o *e-mail* corporativo para envio de grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando *e-mails* do tipo corrente, materiais preconceituosos ou discriminatórios e os do tipo de boatos virtuais. Em caso de dúvidas consulte o *Help Desk*;

g) criar regra para redirecionar o e-mail para qualquer outra conta, ainda que seja corporativa, sem aprovação da Diretoria. Tal criação de regra é monitorada por TI.

8.6 Anexos que contenham as extensões a seguir serão automaticamente bloqueados: .ace, .ani, .app, .docm, .exe, .jar, .reg, .scr, .vbe, .vbs, .bat, .cmd.

8.7 A disponibilização do correio eletrônico pode ser suspensa a qualquer momento por decisão do gestor da área do usuário ou da Gerência de Tecnologia.

8.8 As concessões e revogações de acesso ao serviço de correio eletrônico devem ser autorizadas pelo gestor da área do usuário e encaminhadas à Gerência de Tecnologia.

8.9 A utilização do correio eletrônico pode ser monitorada para fins de Segurança da Informação e nos processos de auditoria.

8.10 O monitoramento para fins disciplinares somente poderá ocorrer com a autorização do Comitê de Ética.

8.11 Os usuários devem evitar o envio de grandes volumes de anexos por *e-mail* (tamanho acima de 30 MB). Nestes casos, para o tráfego de grandes volumes de arquivos, deve-se utilizar uma das alternativas a seguir:

- via diretório "Temporário" (transferência entre usuários com acesso à rede corporativa);
- através do *Onedrive*.

8.12 Não é permitida a alteração da assinatura de *e-mail* por parte dos usuários. Tais assinaturas somente são alteradas através de solicitação formal da Gerência de Recursos Humanos.

8.13 As assinaturas dos *e-mails* de funcionários e estagiários seguirão o padrão abaixo, onde os dados de "Nome" e "Cargo" serão informados pela Gerência de Recursos Humanos. No caso dos estagiários, a nomenclatura do "Cargo" será "ESTAGIÁRIO". Números de telefone fixo e celular (quando aplicável) serão informados, respectivamente, pelas áreas de TI e Administrativa:

lōgum

Nome
Cargo
Logum Logística S.A.
t. + 55 21 2517-xxxx
c. + 55 21 xxxxx-xxxx
www.logum.com.br

8.14 As assinaturas dos *e-mails* dos terceirizados que prestam serviços nas instalações da empresa seguirão o padrão abaixo, onde os dados de "Nome", "Cargo" e "Empresa" serão informados pelo gestor do contrato. Números de telefone fixo serão informados pela área de TI:

lōgum

Nome
Cargo + Nome da empresa terceirizada
A serviço da Logum Logística S.A.
t. + 5521 2517-52xx
www.logum.com.br

8.15 Os *e-mail*s deverão ser classificados conforme sua criticidade e avaliação dos remetentes (usuários), seguindo as classificações abaixo. Vale observar que ao se criar um *e-mail*, por padrão estes serão classificados como nível de permissão "Pública

Nível de Permissão	Classificação	Restrições

Criptografar Somente	Confidencial	Somente o(s) destinatário(s) poderá(ão) ler a mensagem. A criptografia não poderá ser retirada pelo(s) destinatário(s)
	Restrita	
	Uso Interno	
Não encaminhar	Confidencial	Somente os destinatários podem ler a mensagem, mas não podem encaminhar, imprimir ou copiar o conteúdo. Quem aplicou a restrição tem total acesso à mensagem e a todas as respostas.
	Restrita	
	Uso Interno	
Altamente Confidencial	Confidencial	Somente os destinatários com endereços da Logum podem ler, editar mensagens anteriores e responder a todos. Quem aplicou a restrição poderá revogar qualquer permissão aos destinatários.
	Restrita	
Confidencial	Confidencial	Somente os destinatários com endereços da Logum podem ter total acesso às funcionalidades da mensagem. Quem aplicou a restrição poderá revogar qualquer permissão aos destinatários.
	Restrita	
Pública	Sem restrições	É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma, tipo de *e-mail* mais comumente utilizado.

8.16. Em caso de necessidade de acesso ao *backup* da base de e-mails (*PST*), o gestor responsável da área deve solicitar formalmente ao Comitê de Ética explicando o motivo pelo qual há necessidade de tal acesso. Após aprovação do Comitê de Ética e preenchimento/assinatura do "Termo de Responsabilidade" (Anexo III), o *PST* será criado e disponibilizado para o gestor ou algum usuário designado por este.

8.17. Os backups de e-mails de ex-funcionários são armazenados pela Logum por tempo indeterminado.

8.18 - E-mails com mais de 2 anos são movidos automaticamente para a caixa de e-mail "Arquivo morto online" do próprio usuário.

9. Acesso à Rede Corporativa

9.1 O acesso aos recursos da Rede Corporativa é realizado por meio do processo de Autenticação, utilizando as Credenciais de Acesso;

9.2 A licença para a utilização da Rede Corporativa é uma concessão da empresa aos usuários que necessitam deste recurso para desempenhar suas funções. A utilização poderá ser monitorada e a licença suspensa a qualquer momento por decisão do gestor da área do usuário ou da Gerência de Tecnologia;

9.3 Pasta Corporativa chamada "Temporário" tem o propósito de área de transferência e colaboração de arquivos temporários. Portanto, seu conteúdo é automaticamente excluído mensalmente, sem prévia comunicação;

9.4 É proibida a gravação de arquivos de uso pessoal nos diretórios corporativos "CORPORATE", "PUBLICO" e "TEMPORARIO". Tal gravação, se realmente necessária, deve ser realizada na respectiva estação de trabalho;

9.5 Caso seja necessária a criação de uma nova pasta (diretório) na Rede Corporativa (CORPORATE ou PUBLICO), o Gestor responsável deve encaminhar um *e-mail* à Gerência de Tecnologia contendo as seguintes informações:

- Nome da nova Pasta Corporativa;
- Usuários que terão acesso à mesma;
- Tipo de acesso, por exemplo, somente leitura, leitura e edição, etc.

9.6 Os funcionários elegíveis à Política de Trabalho Híbrido – *Home Office* e Presencial automaticamente terão acesso remoto à rede corporativa (via *VPN*). Os funcionários não elegíveis precisam de autorização dos gestores para que tenham o acesso. Tais acessos remotos podem ser monitorados e bloqueados pela Gerência de Tecnologia ou por solicitação do respectivo gestor.

9.7 - A utilização de VPNs da Logum requer o uso de duplo fator de autenticação;

9.8 Diretores, Gerentes e Coordenadores têm acesso livre à *VPN*. Demais funcionários terão a *VPN* liberada de segunda à sexta-feira, das 08 às 20 horas. Exceções deverão ser aprovadas e controladas pelos gestores da área e Recursos Humanos;

9.9 É proibido o armazenamento de arquivos considerados improdutivos nos servidores da empresa, tais como, "Corporate", "Público" e "Temporário". São considerados arquivos improdutivos: filmes, fotos, músicas - excetuando-se os casos em que estes estejam diretamente relacionados às atividades do usuário, materiais contendo assuntos que provoquem perturbação ou assédio a outras pessoas ou que comprometam a imagem do negócio da Logum perante seus clientes, fornecedores, clientes e comunidade em geral; temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético. A Gerência de Tecnologia poderá remover tais arquivos sem anuência do usuário;

9.10 Arquivos organizacionais devem ser salvos, preferencialmente, no “Corporate” ou “Público”, pois, arquivos gravados no computador (local) não possuem cópia de segurança (*backup*). É importante reforçar que não é de responsabilidade de TI a recuperação de arquivos que não respeitem as diretrizes desta **Política.**

9.11 Arquivos pessoais podem ser salvos no *Onedrive*. Em caso de dúvidas, favor procurar o *Help Desk.*

10. Acesso à Internet

A internet é um recurso corporativo disponibilizado nos escritórios e terminais habitados da Logum, ou através dos celulares corporativos, aos usuários para o desenvolvimento das atividades profissionais, enriquecimento intelectual ou como ferramenta de busca de informações, ou seja, tudo que possa vir a contribuir para o desenvolvimento das atividades relacionadas à empresa.

10.1 O acesso é monitorado;

10.2 A não ser quando indicado de forma diferente pelo gestor da área, todos os usuários terão acesso à Internet.

10.3 O acesso à Internet para fins particulares é permitido desde que sejam respeitados os dispositivos legais e normativos vigentes, notadamente os estabelecidos nesta **Política**. Tal uso não deve interferir no desempenho do próprio profissional ou de qualquer outro usuário, prejudicar o desempenho dos recursos disponíveis ou comprometer a imagem do negócio.

10.4 Os sites identificados como não seguros são automaticamente bloqueados. Ainda assim é responsabilidade do usuário não acessar tais sites, dentre eles:

- Redes Sociais (exceto *Linkedin*);
- *Blogs*, Sites de Chats e Páginas Pessoais;
- *Streaming* (exceto *Spotify; Youtube*);
- Conteúdo Adulto/Sexual Explicito;
- Jogos;
- Associações Criminosas, Preconceituosas, Extremistas, Armas, etc.;
- Drogas e Álcool;
- Pirataria.

10.5 Caso algum usuário tenha necessidade de acessar algum site bloqueado pelo sistema, o gestor da área deverá formalizar tal solicitação, com justificativas, por *e-mail* à Gerência de Tecnologia.

10.6 É proibida a utilização de recursos que visem mascarar e/ou ocultar o tráfego de dados pela rede Logum, tais como serviços de *Proxy* ou de *VPN´s* não autorizadas. A identificação da utilização deste tipo de recurso é passível de suspensão do direito do usuário de acessar a Internet nos ambientes corporativos**.**

11. Retenção de Dados

O gerenciamento do ciclo de vida das informações da empresa é vital para o bom desenvolvimento dos negócios. Da criação até o descarte, as etapas do ciclo de vida das informações exigem planejamento e processos para garantir a continuidade do negócio e evitar a perda do conhecimento técnico.

Os detalhes sobre a retenção e descarte de **dados pessoais** podem ser consultados na Política de Privacidade e Proteção de **Dados pessoais**.

12. Gestão de Incidentes

Implementamos medidas técnicas e organizacionais para proteger contra roubo, uso indevido e acesso, divulgação, alteração e destruição não autorizados. Essas medidas incluem questões físicas, administrativas e eletrônicas (digitais) de segurança de acordo com a sensibilidade, quantidade, distribuição e formato das informações coletadas.

No entanto, sempre há um certo nível de risco envolvido quando as informações são coletadas, processadas e armazenadas, e, não é possível garantir a totalidade da segurança das informações.

Em caso de incidente as etapas listadas abaixo deverão ser seguidas.

12.1 Notificação interna – se qualquer incidente for identificado, seja por monitoramento automático, seja ativamente pelos usuários ou por uma pessoa externa, o primeiro passo é registrar esse incidente através de um dos canais de comunicação constantes no item 18 (abaixo).

12.1.1 Usuário – é responsável por registrar o incidente através dos canais citados no item 18 (abaixo) ou pedir ajuda ao *Help Desk*;

12.1.2 Detecção Automática através de softwares e sistemas específicos;

12.2 Para qualquer registro relacionado a incidentes envolvendo "**dados pessoais",** o usuário que identificou o incidente deverá comunicá-lo imediatamente ao seu gestor e/ou Comitê LGPD, os quais seguirão procedimento PR-000.000-COR-NS2-LOG-002 para tratar e comunicar tal fato aos titulares de dados pessoais envolvidos e a ANPD.

12.3 A análise da criticidade será realizada pelo Comitê de LGPD com base em critérios específicos.

12.4 Notificação Externa – será realizada notificação em até 72 horas (setenta e duas) horas, diretamente na plataforma eletrônica SEI (Sistema Eletrônico de Informações) da Presidência da República (PR), em caso de vazamento de informações, conforme orientações da ANPD (Agência Nacional de Proteção de Dados). Os titulares de **dados pessoais** serão igualmente comunicados quanto ao problema, sendo o prazo contado a partir do momento de constatação do incidente.

12.5 Atualizações periódicas sobre o tratamento do incidente serão realizadas interna e externamente;

12.6 Testes regulares serão realizados periodicamente para avaliar a eficiência relacionada aos requisitos de segurança e privacidade de **dados pessoais**.

12.7 A Logum classifica seus Incidentes de segurança da informação conforme a seguir:

Impacto	**Significativo**	• Severidade 1
	Médio	• Severidade 2
	Baixo	• Severidade 3

12.8 A classificação de impacto deve ser definida da seguinte maneira:

Guia de classificação de impacto				
Classificação	**Sistema**	**Informação**	**Recuperabilidade**	**Marca**
Significativo	Os sistemas ou serviços com impacto significativo nos negócios estão inoperantes, comprometidos ou severamente degradados	Afeta dados confidenciais, sensíveis ou de alto risco que podem ter implicações significativas ao titular, considerações regulatórias significativas ou impacto significativo nas organizações ou indivíduos afetados.	A recuperação do incidente é imprevisível e extremamente complexa.	Alto impacto ou ameaça negativa grave à Logum, marca ou reputação mais ampla.
Médio	Os sistemas ou serviços com impacto médio nos negócios ou no cliente estão inoperantes, comprometidos ou severamente degradados.	Afeta dados confidenciais que podem ter implicações no cliente e risco médio a baixo de danos às organizações ou indivíduos afetados.	A recuperação do incidente pode ser imprevisível e complexa.	Médio risco de impacto na marca ou imagem para Logum, clientes e parceiros

Baixo	Os sistemas ou serviços com impacto médio a baixo nos negócios estão inoperantes, comprometidos ou degradados.	Somente informações públicas são afetadas e não têm implicações no cliente.	A recuperação do incidente não é complexa, mas pode exigir coordenação com diferentes áreas da Logum.	Baixo risco de impacto na marca ou imagem para Logum, clientes e parceiros

12.9 Tipos de Incidentes:

Tipo de Incidente	Descrição	Exemplo
Acesso não autorizado	Um indivíduo obtém acesso lógico ou físico sem permissão a uma rede, sistema, aplicativo, dados ou outro recurso da Logum.	Ator desconhecido faz login na conta de um usuário remotamente.
Denial of Service (DoS) – Negação de Serviço	Um ataque que impede ou prejudica com êxito a funcionalidade normal autorizada de redes, sistemas ou aplicativos, esgotando os recursos. Essa atividade inclui ser a vítima ou participar do DoS	O site Logum é prejudicado por solicitações de conexões falsas de endereços IP maliciosos.
Phishing	Mensagens personalizadas, com informações bem convincentes, como nome, sobrenome e outros dados, que levam o usuário a acreditar que está recebendo um *e-mail* legítimo de alguém familiar.	O usuário recebe uma mensagem dizendo que seus dados precisam ser atualizados, pois a conta bancária pode ser desativada

Engenharia Social	Método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.	Abordagem via telefone para obter acesso não autorizado, seja se passando por um funcionário da empresa, fornecedor ou terceiros.
Malware/Código Malicioso	É qualquer parte de um software que tenha sido codificada com o objetivo de danificar dispositivos, roubar dados e causar danos às pessoas. Vírus, cavalos de Tróia, spywares e ransomwares estão entre os diferentes tipos de malwares.	Arquivos são infectados por ransomware, criptografando todo conteúdo do disco, sendo possível acessá-los mediante a pagamento.
Uso indevido/Mal uso dos sistemas	Uma pessoa viola a política de uso aceitável.	Sistema possui softwares não autorizados.
Scan/Probe/ Tentativa de Acesso	Qualquer atividade que procure acessar ou identificar um computador, portas abertas, protocolos, serviços ou outras ações para exploração posterior. Essa atividade nem sempre resulta em comprometimento ou negação do serviço.	O firewall externo da Logum está sendo "scaneado" por um IP externo suspeito para identificar portas abertas.
Roubo e perda de notebook e celular corporativo	Equipamentos que são dedicados aos profissionais da Logum que são roubados ou perdidos no período em que estão sob a guarda do profissional.	Roubo de notebook e/ou celular corporativo em qualquer situação.
Violação de políticas	Reúne um conjunto de diretrizes e boas práticas para o uso seguro das informações.	Uso de softwares não permitidos
Vulnerabilidade técnica	Fraqueza que pode permitir a um atacante explorar um sistema e acessar informações não autorizadas.	Ausência de patches de segurança do sistema operacional

Outros/Investigações	Incidentes não confirmados que são potencialmente atividades maliciosas ou anômalas consideradas pela entidade que relata para solicitar uma revisão adicional.	Suspeita de aumento de tráfego originado por um servidor.

13. Gestão de Mudança

13.1 A Gestão de mudanças da área de Automação é tratada conforme procedimento de SMS – PCR-SMS-003 – Gestão de Mudanças;

13.2 Mudanças relacionadas ao SAP são acompanhadas através do *software* SOLMAN.

14. Proteção de Dados e Auditoria

14.1 Sistemas de TI e comunicação possuem registros de log que são gerados automaticamente. Esses logs são armazenados nas estações de trabalho e na rede, permitindo a detecção de erros, controle de acesso e atividades de usuários;

14.2 Todos os dados e informações são protegidos por mais de uma camada de proteção;

14.3 Todos os notebooks e desktops possuem criptografia de disco rígido (Bitlocker) habilitada a fim de impedir o acesso das informações salvas nestes dispositivos por pessoas não autorizadas.

15. Papéis e Responsabilidades

15.1 – Todos os usuários (funcionários, estagiários, prestadores de serviços)

a) cumprir fielmente a **Política de Segurança da Informação**, bem como políticas e normas correlatas, como Política de Privacidade e Proteção de **Dados pessoais**, Propriedade Intelectual, Compliance, etc;
b) buscar orientação de gestores em caso de dúvidas relacionadas à Segurança da Informação;
c) comunicar imediatamente eventuais casos de violação de Segurança da Informação, através da Gerência de Tecnologia, Comitê da LGPD ou Canal de Denúncias;
d) proteger as informações contra acessos, modificações, destruição, divulgações não autorizadas;
e) responder pelo adequado uso dos ativos de TI que estiverem sob sua responsabilidade, de acordo com as diretrizes desta **Política** e regras de patrimônio e *compliance*;
f) manter os arquivos de trabalho armazenados nos Servidores Corporativos (diretórios de rede);
g) não salvar arquivos particulares nos servidores corporativos;

h) relatar ao gestor imediato e à Gerência de Tecnologia sempre que identificar ou ocorrer dano, furto, roubo ou perda de um ativo de TI. Em caso de furto ou roubo será necessário apresentar o Registro de Ocorrência no órgão competente conforme previsto no Contrato de Comodato;
i) responder pelas atividades que ocorram na sua conta de usuário;
j) manter sigilo quanto a senha de acesso aos recursos da rede corporativa;
k) bloquear a estação de trabalho sempre que se afastar do equipamento, mesmo que esteja trabalhando em *Home Office*;
l) desligar a estação de trabalho diariamente ao final do expediente;
m) impedir o uso dos ativos de TI por outras pessoas, exceto em caso de reparo por pessoas autorizadas por TI;
n) responder pelo uso adequado dos serviços e recursos disponibilizados com: Correio Eletrônico, sistemas, internet, etc.;
o) não armazenar dados corporativos em equipamento pessoal;
p) não deixar documentos impressos na impressora e/ou copiadora, nem tampouco sobre as estações de trabalho
q) configurar o bloqueio do celular corporativo através de PIN, biometria ou senha.

15.2 – Gestores

a) cumprir e fazer cumprir fielmente esta **Política de Segurança da Informação**, bem como políticas e normas correlatas, como Política de Privacidade e Proteção de **Dados pessoais**, Propriedade Intelectual, Compliance, etc;
b) assegurar que os membros de suas equipes tenham acesso e conhecimento desta **Política;**
c) comunicar imediatamente eventuais casos de violação de Segurança da Informação, através da Gerência de Tecnologia, Comitê da LGPD ou Canal de Denúncias;
d) solicitar ou revogar solicitação junto à Gerência de Tecnologia quanto a disponibilização dos ativos de TI, acessos de rede corporativa, sistemas e internet necessários para o desempenho das funções dos usuários sob sua gestão;
e) comunicar à Gerência de Tecnologia sempre que for necessário transferir a responsabilidade de um ativo de TI para um outro usuário;
f) informar imediatamente à Gerência de Tecnologia sobre os casos de inclusão, exclusão ou alteração de terceiros sob sua gestão;
g) comunicar à Gerência de Tecnologia a ocorrência de direitos de acesso desnecessários dos usuários sob sua gestão;
h) rever de forma periódica (não superior a 06 meses), o perfil de acesso em todos os sistemas (SAP, SGT, Portal de Agendamento, etc.) dos usuários sob sua gestão;

15.3 – Gerência de Tecnologia

a) atualizar esta Política, sempre que necessário;
b) administrar os ativos de TI de forma a garantir a conformidade desta **Política;**
c) elaborar o contrato de comodato para entrega dos *notebooks*;
d) garantir a ativação e desativação das contas, senhas e acessos de usuários por solicitação da Gerência de Recursos Humanos e/ou gestores;
e) avaliar e tratar qualquer exceção relativa à esta **Política;**
f) comunicar imediatamente à Diretoria Executiva sobre qualquer incidente relativo à Segurança da Informação.

15.4 – Gerência de Recursos Humanos

a) comunicar à Gerência de Tecnologia todos os casos de admissão, desligamentos, afastamentos e férias para que a área possa providenciar os acessos ou bloqueios necessários;

b) comunicar à Gerência de Tecnologia as alterações de cargo, telefone, filial, etc., para os devidos ajustes de assinatura de *e-mail* e atualização de cadastro do *outlook*;

15.5 – Comitê de continuidade operacional, segurança patrimonial e da informação

a) propor alterações na Política de Segurança da Informação;
b) analisar casos que envolvam segurança da informação e que não estejam contemplados na Política;
c) Promover melhoria contínua da segurança da informação;
d) Investigar possíveis violações desta política.

15.6 – Diretoria

a) Patrocinar para que a Política seja cumprida em todos os níveis;
b) Fornecer os recursos necessários para cumprimento da Política

16. Violação da Política de Segurança da Informação

16.1 Toda e qualquer violação às diretrizes contempladas nesta **Política** devem ser informadas à Gerência de Tecnologia.

16.2 Toda violação deverá ser investigada para determinação das medidas necessárias, visando a correção de falhas ou reestruturação do sistema.

Nota: Em caso de dúvidas quanto aos procedimentos e responsabilidades descritos nesta **Política**, o usuário ou gestor deverá entrar em contato com a Gerência de Tecnologia.

17. Boas Práticas

17.1 Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega de trabalho, ou mesmo fornecedor/cliente;

17.2 Não é permitida a divulgação de nomes e tratativas de assuntos confidenciais;

17.3 Quando em deslocamentos de carro, coloque o *notebook* no porta-malas ou em local não visível;

17.4 Ao movimentar-se com o *notebook*, se possível, não utilize malas convencionais para *notebook* e sim mochilas ou malas discretas. Não coloque o *notebook* em carrinhos de aeroportos e nem despache junto com a bagagem;

17.5 Em locais públicos mantenha sempre o *notebook* à vista, não se distanciando do equipamento;

17.6 Avalie se em pequenas viagens realmente é necessário levar o *notebook*;

17.7 Não conecte o equipamento em redes *Wi-fi* desconhecidas, essas redes podem conter mecanismos para captura de dados do seu dispositivo;

17.8 Documentos enviados para impressão devem ser retirados imediatamente das impressoras;

17.9 Documentos confidenciais não devem ficar expostos com fácil acesso, como por exemplo, sobre mesas.

18. Controles implementados

Além de todas as proteções existentes com o objetivo de mitigar riscos de ataques cibernéticos, tais como Datacenter redundante para caso de *Disaster Recovery*, VPN e pacote Office com duplo fator de autenticação, criptografia de todos os discos rígidos dos notebooks, sistema de análise de vulnerabilidades, sistema backup para os principais servidores de automação, política de senha "forte", a Logum possui alguns controles para avaliar a eficácia de seus sistemas:

a) Ativação periódica dos servidores backup de automação (anual);
b) Revisão periódica do perfil de acesso dos principais sistemas (SAP, SGT e Portal de Agendamento (semestral);
c) Simulação periódica de incidentes envolvendo dados pessoais (semestral);
d) Campanha de e-mail phishing (semestral);
e) Treinamento da Política de Segurança da Informação (anual);
f) Revisão periódica dos perfis de acesso aos diretórios do Corporate (semestral);
g) Avaliação contínua das vulnerabilidades identificadas pelo software específico e tratamento sob demanda;
h) Monitoramento contínuo dos principais recursos (CPU, memória e disco) dos principais equipamentos de TI e Telecom.

19. Canais de Comunicação

Para esclarecimentos de dúvidas quanto a Política de Segurança da Informação ou para comunicação de eventuais incidentes de segurança, os canais de comunicação abaixo podem ser acionados individual ou coletivamente:

Gerência de Tecnologia
e-mail: tecnologia@logum.com.br

Encarregado/DPO:
Nome: José Ricardo Pinheiro
e-mail: dpo@logum.com.br

Comitê da LGPD
e-mail: comitelgpd@logum.com.br

Canal de Denúncias:
Atendimento telefônico: 0800 721 14 39
Site: https://ethicspeakup.com.br/logum/

Para esclarecimentos de dúvidas relacionadas a utilização de ferramentas, acessos, etc., favor acionar o Help Desk através do *e-mail*: helpdesk@logum.com.br.

Anexo I - Termo de Recebimento e Adesão às Políticas da Logum Logística S.A.

Eu, [**NOME COMPLETO**], [qualificação], inscrito(a) no CPF sob nº [completar], na qualidade de [escolher entre: funcionário, estagiário], declaro que recebi cópia, li, entendi e aceito os termos contidos nos documentos abaixo:

- Código de Ética e Conduta;
- Política de Segurança da Informação;
- Política de Privacidade e Proteção de Dados Pessoais.

Declaro ainda que:

- concordo em cumprir todas as diretrizes contidas nas referidas políticas, bem como as normas e procedimentos nelas citadas;
- estou ciente e concordo que as referidas políticas, e este Termo de Recebimento e Adesão, fazem parte dos documentos que compõem a relação contratual firmada com a Logum;
- tenho ciência que quaisquer descumprimentos às regras nelas contidas, por ação ou omissão, podem dar causa a ações disciplinares, incluindo a rescisão do respectivo contrato;
- me responsabilizo por adotar as medidas de segurança estabelecidas nas Políticas de Segurança da Informação e de Privacidade e Proteção de Dados Pessoais;
- estou ciente que devo comunicar imediatamente qualquer incidente de segurança da informação à Gerência de Tecnologia para adoção das medidas técnicas cabíveis, bem como qualquer violação às regras estabelecidas nas demais políticas aos Canais de Comunicação pertinentes, citados em cada uma das políticas.

Local e data

_____

Nome por extenso
CPF:

Anexo II – Contrato de Comodato

COMODANTE: LOGUM LOGÍSTICA S.A., com Sede na Avenida Presidente Wilson, nº 231, Sala 902, Centro – CEP: 20.030-021 – Rio de Janeiro/RJ, inscrita no CNPJ/MF sob o nº 09.584.935/0001-37, neste ato representada por seu procurador Sr(a). (nome), (nacionalidade), (Estado Civil), (Cargo), portador da carteira de identidade nº xxxxx (órgão emissor), C.P.F. nº xxx.xxx.xxx-xx, com endereço comercial na sede da empresa, na forma do Estatuto Social da Logum;

COMODATÁRIO: (nome completo do usuário), nacionalidade, Estado Civil, Cargo, portador da Carteira de Identidade nº XXXXXXXXXXXXX, C.P.F. sob o nº xxx.xxx.xxx-xx, e, com endereço comercial na Avenida Presidente Wilson, nº 231, Sala 902, Centro – CEP: 20.030-021 – Rio de Janeiro/RJ.

As Partes acima identificadas têm, entre si, justo e acertado o presente Contrato de Comodato de Equipamentos de TI, doravante denominado simplesmente CONTRATO, que se regerá pelas cláusulas seguintes e pelas condições descritas no presente.

Cláusula 1ª. O presente contrato tem como OBJETO, a transferência, pela COMODANTE ao COMODATÁRIO, dos direitos de uso e gozo dos Equipamentos descritos a seguir, por prazo indeterminado:

- (descrição dos equipamentos, com marca, modelo, número série, cor, etc)
-

Cláusula 2ª. Os Equipamentos, objeto deste CONTRATO, serão utilizados, prioritariamente, no desempenho das funções profissionais do COMODATÁRIO.

Cláusula 3ª. O COMODATÁRIO está obrigado a comunicar imediatamente à COMODANTE eventuais defeitos encontrados nos Equipamentos e disponibilizá-los para conserto, bem como a apresentar Registro de Ocorrência na hipótese de furto ou roubo do Equipamento.

Cláusula 4ª. O COMODATÁRIO se obriga, ainda, que no caso de quebra, dano integral ou parcial, decorrente de mau uso, que impeça ou limite a utilização dos Equipamentos, roubo ou furto (sem apresentação do Registro de Ocorrência), perda etc., a reembolsar
o valor equivalente ao Equipamento, conforme Nota Fiscal do produto, em até 30 (trinta) dias, podendo, inclusive, ser utilizado o desconto em folha.

Cláusula 5ª. O COMODATÁRIO declara que recebe o equipamento em perfeito estado de conservação e funcionamento e se compromete de outro lado, a não só conservá-lo e guardá-lo, como igualmente a vigiá-lo, como **FIEL DEPOSITÁRIO** do mesmo, como ora nomeado.

Cláusula 6ª. O COMODATÁRIO deverá devolver o equipamento à COMODANTE sempre que for solicitado, a qualquer tempo e independente do término ou da rescisão do contrato de trabalho e no idêntico estado em que foi entregue.

Por estarem assim justos e contratados, firmam o presente instrumento, em duas vias de igual teor, juntamente com 2 (duas) testemunhas.

Local, data.

_____	_____
COMODANTE	COMODATÁRIO

Testemunhas:

_____	_____
Nome:	Nome:
CPF:	CPF:

Anexo III – Termo de Responsabilidade para Acesso de e-mails de Terceiros

Eu, [**NOME COMPLETO**], [qualificação], inscrito(a) no CPF sob nº [completar], na qualidade de usuário, declaro estar ciente e comprometido em observar e cumprir todas as diretrizes, normas e procedimentos da LOGUM no decorrer do acesso e uso da base de *e-mails* do ex-usuário xxxx (*e-mail*: xxxx@logum.com.br), cujo conteúdo fica disponível para meu conhecimento e que eventualmente possa conter dados pessoais do ex-usuário ou de terceiros.

Estou ciente ainda de que:

- qualquer ativo (inclusive os de Tecnologia da Informação) que acesse, armazene, transforme ou transporte informações que se definam como **dado pessoal**, identificando ou tornando uma pessoa física identificável, deverá ser condizente com os interesses da LOGUM e na forma por esta autorizada.

- a Política de Segurança da Informação prevê o monitoramento dos *e-mails* corporativos, e se me deparar com **dados pessoais** de terceiros ao utilizar o *e-mail* corporativo, tal uso e monitoramento deve atender aos objetivos determinados pela empresa, e ser impessoal e sem discriminação observando as normas impostas pela LGPD – Lei 13.709/18 – Lei Geral de Proteção de Dados Pessoais.

- qualquer pesquisa que seja feita em *e-mails* corporativos deverá ser procedida exclusivamente para a finalidade determinada pela LOGUM e que, caso me depare com **dados pessoais**, incluindo **dados pessoais sensíveis**, não vou salvar, utilizar, acessar, reproduzir, transmitir, ou proceder com qualquer outro tipo de tratamento desses **dados pessoais** em discordância das regras para proteção dos mesmos.

- qualquer infração ao exato e pontual cumprimento de quaisquer das condições descritas neste Termo e nos documentos relacionados, por minha ação ou omissão, constituirá infração e poderá caracterizar condição para encerramento justificado do meu contrato de trabalho ou de prestação de serviços. Reconheço que este Termo passa a integrar respectivamente meu contrato de trabalho ou prestação de serviço.

Sendo assim, me responsabilizo por adotar as medidas de segurança estabelecidas nas Políticas internas, incluindo a Política de Segurança da Informação e a Política de Privacidade e Proteção de Dados, buscando proteger **dados pessoais** de quaisquer Titulares eventualmente identificados em *e-mails* corporativos, devendo comunicar imediatamente à Gerência de Tecnologia qualquer incidente de segurança que possa acarretar risco ou dano relevante, conforme prevê a LGPD.

Local e data

_____

Nome por extenso
CPF: