POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
POLÍTICA

Sumário

1. Objetivo 3
2. Abrangência 3
3. Missão 3
4. Definições e Siglas 3
5. Segregação de Atividades e Funções 4
5.1 Conscientização e treinamento são fundamentais para a segurança 4
6. Senhas 4
7. Atribuições e Responsabilidades na Gestão de SI 5
7.1 Colaboradores 5
7.2 Diretorias e Gerências 5
7.3 Área de Controles Internos 5
8. Diretrizes de Segurança da Informação 6
9. Propriedade Intelectual 6
9.1 Ferramentas externas 6
10. Engenharia Social 7
11. Classificação da Informação 7
12. Boas Práticas de Comunicação Verbal Dentro e Fora da Singular 8
13. Requisitos de Segurança do Ambiente Físico 8
13.1 Nuvem 9
14. Requisitos de Segurança do Ambiente Lógico 9
14.1 Diretrizes Gerais 9
14.2 Diretrizes Específicas sobre Ativos de Informação 9
14.2.1 Sistemas 9
14.2.2 Máquinas – Estação de Trabalho 10
14.2.3 Política de Trabalho Remoto 10
14.2.4 Boas Práticas de Segurança para seu Notebook 11
14.2.5 Política de Mesa Limpa e Tela Limpa 11
14.2.6 Utilização de equipamentos particulares/terceiros dentro da empresa 13

14.2.7 Boas práticas de segurança para Impressões 13
14.2.8 Instalação de Softwares 13
14.2.9 Diretrizes quanto à utilização da Rede Corporativa 14
14.2.10 Diretrizes quanto ao uso de Mídias Removíveis e da porta USB 14
14.2.11 Diretrizes quanto ao uso da Internet 15
14.2.12 Recomendações sobre o uso do Correio Eletrônico (E-Mail) 16
14.2.13 Antivírus 16
14.2.14 Uso de Softwares de Mensageria 17
14.2.15 Controle de Acesso Lógico (Baseado em Senhas) 17
14.2.16 Uso de Inteligência Artificial 18
15. Legislações, regulamentos e acordos 18
16. Violações e Sanções 18
17. Vigência e Validade 18
18. Revisão do Documento 19
19. Histórico de Alterações 20

1. Objetivo

A Política de Segurança da Informação é uma declaração formal da SINGULAR, razão social ATOM TECNOLOGIA EM INFORMACAO LTDA, acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, representantes, administradores e demais descritos neste instrumento.

2. Abrangência

Todos os colaboradores e prestadores de serviços que estejam a serviço e utilizem ativos corporativos da SINGULAR.

3. Missão

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da SINGULAR.

4. Definições e Siglas

- **TI:** Tecnologia da Informação.
- **SaaS –** Software como serviço.
- **IaaS –** Infraestrutura como serviço.
- **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.
- **Backup:** É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
- **Mídias Removíveis:** Dispositivos que permitem a leitura e gravação de dados, tais como: CD, DVD, Disquete, Pen Drive, cartão de memória, entre outros.
- **USB:** É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

- **Softwares de Mensageria:** São programas que permitem aos usuários se comunicarem remotamente (à distância) através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

- **Firewall:** É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

- **Modem 3G:** É um dispositivo sem fio, com saída USB, para conexão em outro dispositivo, tais como Tablets (com suporte 3G), notebooks, netbooks, desktops etc., objetivando conexão com a internet. O modem 3G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, smartphones e notebooks) compatíveis com a tecnologia 3G.

5. Segregação de Atividades e Funções

No quadro de pessoal e de prestadores de serviços há a segregação de atividades e funções de forma que uma mesma pessoa não assuma simultaneamente responsabilidades das quais decorram interesses conflitantes, ainda que de forma meramente esporádica ou eventual. A delegação de atribuições deve ser formal, com responsabilidades claramente delimitadas mediante definição de poderes, limites e alçadas, inclusive em relação a serviços de terceiros.

5.1 Conscientização e treinamento são fundamentais para a segurança

A SINGULAR possui procedimentos que visam conscientizar os colaboradores e terceiros da necessidade da segurança das informações e aspectos previstos na Política de Segurança da Informação e Política de Processamento de serviço em nuvem. Os empregados são devidamente capacitados quanto à correta e eficiente utilização dos recursos, de acordo com as normas em vigor. A Gestão de Segurança da Informação da SINGULAR é realizada por colaboradores da Entidade, devidamente capacitados para a função.

6. Senhas

Senhas de caráter sigiloso, pessoal e intransferível são fornecidas aos colaboradores para acesso à rede corporativa, sistemas internos e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas deverão ser transmitidas a pessoas que não sejam colaboradores, sendo eles responsáveis pela manutenção de cada senha com suas características.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa ou nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras passíveis de engenharia social.

7. Atribuições e Responsabilidades na Gestão de SI

7.1 Colaboradores

Cabe a todos os colaboradores cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela SINGULAR; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a SINGULAR quanto ao descumprimento ou violação desta política ou qualquer fragilidade de segurança da informação identificada, pelo e-mail seguranca.informacao@singular.tec.br ou, então, pela plataforma Singular Studio (app.opensingular.com), abrindo um incidente de segurança da informação, se for o caso.

7.2 Diretorias e Gerências

Cabe às Diretorias e Gerências cumprirem e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação através dos procedimentos de incidentes de segurança.

7.3 Área de Controles Internos

Cabe a área propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

8. Diretrizes de Segurança da Informação

Conforme definição da norma NBR ISO/IEC 27002:2022, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

- **Confidencialidade**, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;
- **Integridade**, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **Disponibilidade**, a Política de Segurança da Informação deve ser divulgada a todos os colaboradores e demais descritos neste instrumento, e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para assegurar os itens descritos acima, 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 Política de Segurança da Informação da SINGULAR é aprovada e revisada anualmente pela Diretoria Executiva.

A Diretriz sobre Política de serviço em nuvem está descrita na Política de Processamento de Serviço em Nuvem GSI-003-POL.

9. Propriedade Intelectual

É de propriedade da SINGULAR todos os “designs”, criações, processos ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício ou por terceiros com a ATOM TECNOLOGIA EM INFORMACAO LTDA.

9.1 Ferramentas externas

É vedado o uso de ferramentas de criação de conteúdo ou documentação (como Canva ou Documentos Google, por exemplo) que não sejam de contratação direta da Singular.

Colaboradores devem procurar alternativas nas ferramentas oferecidas pelo pacote do Microsoft 365 contratado pela Singular.

Fica autorizado o uso do Canva excepcionalmente para produção de peças de divulgação interna ou para mídias sociais pelo Marketing ou pela área de Pessoas e Cultura.

10. Engenharia Social

Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

A Engenharia Social manifesta-se de diversas formas, e pode-se dividi-la em dois grupos. No entanto, o grande ponto em que engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízos à empresa:

Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois o engenheiro social nem sempre é alguém desconhecido.

Indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter as informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a se fazer é ignorar a oferta tentadora e apagar o e-mail imediatamente.

11. Classificação da Informação

É de responsabilidade dos Gestores de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

- **Público:** todo o conteúdo de todos os documentos de um determinado processo pode ser visualizado por qualquer pessoa, dentro e fora da organização.
- **Interno:** o acesso ao conteúdo desses documentos é aberto a toda organização, porém não devem ser divulgados ou informados externamente.
- **Sigiloso:** o acesso aos documentos e ao processo é exclusivo às pessoas a quem for atribuída permissão específica.

Para a realização da classificação devem ser considerados quatro aspectos importantes, conforme definido abaixo:

- **Integridade:** informação atualizada, completa e mantida por pessoal autorizado.
- **Disponibilidade:** disponibilidade constante e sempre que necessário para pessoal autorizado.
- **Valor:** a informação deve ter um valor agregado para a instituição.
- **Confidencialidade:** acesso exclusivo por pessoa autorizada.

Observações: Para maiores informações consultar Política de Classificação da Informação.

12. Boas Práticas de Comunicação Verbal Dentro e Fora da Singular

- Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho. Em locais públicos ou próximos a visitantes, seja ao telefone, com algum colega ou mesmo fornecedor.
- Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximo a pessoas desconhecidas.
- Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento às pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

13. Requisitos de Segurança do Ambiente Físico

13.1 Edifício Comercial

O perímetro físico da SINGULAR compreende o edifício comercial em que está estabelecida, em Brasília.

- A entrada é realizada através de identificação biométrica e são mantidos os devidos registros de colaboradores e visitantes.
- O acesso ao edifício de colaboradores demitidos é revogado pelas áreas de Controle Internos e Administrativa.
- A entrada em áreas, partes dedicadas ou dependências da SINGULAR por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros ou até mesmo colaboradores, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre será acompanhada de pessoas autorizadas.

- Áreas de acesso restrito devem ser respeitadas. Não se deve executar tentativas de acesso a elas ou utilizar máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores e prestadores de serviço.

13.2 Nuvem

As máquinas (servidores) que armazenam sistemas da SINGULAR estão em áreas protegidas, mantidas pelo provedor de nuvem.

- Os data centers da AWS seguem os controles de acordo com o link abaixo: https://aws.amazon.com/pt/compliance/data-center/controls

13.3 Mudanças Climáticas

A Singular entende que os impactos causados pelas mudanças climáticas não afetam de forma significativa o escopo do seu sistema de gestão de segurança da informação.

14. Requisitos de Segurança do Ambiente Lógico

14.1 Diretrizes Gerais

Todo acesso às informações e aos ambientes lógicos são controlados, de forma a garantir acesso apenas às pessoas autorizadas. As permissões são revistas periodicamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

14.2 Diretrizes Específicas sobre Ativos de Informação

14.2.1 Sistemas

Os sistemas possuem controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

As cópias de segurança (Backup) são testadas e atualizadas para fins de recuperação em caso de desastres.

Não são executados programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

Não são executados programas, instalado equipamentos, armazenado arquivos ou promovida ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

Não é permitido enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha considerada “robusta”.

14.2.2 Máquinas – Estação de Trabalho

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidas contra danos ou perdas, bem como o acesso, uso ou exposição indevida.

As estações de trabalho possuem códigos internos, os quais permitem a identificação na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do colaborador ou prestadores de serviço.

Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da SINGULAR só devem ser utilizadas em equipamentos com controles adequados.

Os usuários de TI devem utilizar apenas softwares e/ou plataformas online autorizados pela área de Infraestrutura TI, nos equipamentos da SINGULAR.

A área de Infraestrutura de TI estabelece os aspectos de controle, distribuição e instalação de softwares utilizados.

14.2.3 Política de Trabalho Remoto

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela organização, notificar imediatamente o seu gestor, o RH e Departamento de TI e procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência.

Os colaboradores que fizerem uso de ativos móveis se responsabilizarão pela segurança e uso adequado das informações nele contidas, conforme termo de responsabilidade de uso de ativos.

O trabalho remoto realizado com acesso aos ativos da SINGULAR somente é permitido por meio do acesso via VPN – Virtual Private Network, desbloqueio explícito de endereço de internet (IP) ou por equipamento homologado e autorizado pela SINGULAR, configurados com recursos de criptografia e softwares de segurança atualizados, monitorados e com senha forte de acesso.

A concessão do acesso via VPN será de exclusivo critério da organização e diante de solicitação, feita pelo Gestor, ao departamento de TI, que optará por qual rede o usuário terá permissão de acesso. A referida concessão será feita de forma individual, sendo os usuários responsáveis por seus acessos via VPN, bem como, por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os usuários deverão adotar medidas de cautela, para que terceiros não tenham acesso à sua conexão de VPN.

14.2.4 Boas Práticas de Segurança para seu Notebook

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

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 ou despacho junto à bagagem.

Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

Evite utilizar o notebook em locais públicos.

Em hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento.

Avalie se em pequenas viagens é realmente necessário levar o notebook.

14.2.5 Política de Mesa Limpa e Tela Limpa

Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário do expediente;

Informações sensíveis ou críticas para o negócio da organização devem ser trancadas em local separado e seguro (um armário ou cofre à prova de fogo);

Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;

Não anotar informações sensíveis em quadros brancos;

Não guardar pastas com documentos sensíveis em prateleira de fácil acesso;

Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas fragmentadoras (há uma máquina no DP);

Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;

Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;

Devolver, o quanto antes possível, todos os documentos obtidos por empréstimos de outros departamentos, quando eles não são mais necessários;

Computadores pessoais e terminais de computador e impressoras não devem ser deixados “logados”, caso o usuário responsável não esteja presente;

Nos computadores, acionar um protetor de tela que solicite uma senha para liberação toda vez que o usuário se ausentar;

Guardar agendas e cadernos de anotações numa gaveta trancada;

Manter os pertences pessoais em gavetas ou armários destinados para esse fim;

Nunca escrever senhas em lembretes e nem tentar escondê-las no local de trabalho;

Não deixar mídias, como CDs ou disquetes, nos drives;

Mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores;

Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários e desligar o computador;

Manter as gavetas e armários fechados e trancados e não deixar as chaves na fechadura;

Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados;

Trancar o local de trabalho ao deixá-lo, não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente;

Não salvar senhas em post-it digitais;

Não deixar arquivos confidenciais na área de trabalho do computador;

Todos os computadores ou servidores devem ser desligados após a utilização ou em caso de não operação por mais de quinze minutos;

As informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, devem ser guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;

Computadores e terminais devem ser mantidos desligados ou protegidos com mecanismo de travamento de tela e teclado controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegidos por tela de bloqueio, senhas ou outros controles, quando não usados;

É proibido o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, scanners ou máquinas fotográficas digitais);

14.2.6 Utilização de equipamentos particulares/terceiros dentro da empresa

Notebooks particulares para serem usados dentro da rede da empresa abrangida neste documento precisam ser avaliados pelo pessoal responsável de TI.

Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.

É responsabilidade de a área contratante encaminhar os terceiros sob sua responsabilidade para esta verificação.

14.2.7 Boas práticas de segurança para Impressões

A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado. Isto é, documentos esquecidos nas impressoras, com demora em retirada ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da empresa.

14.2.8 Instalação de Softwares

Os usuários da SINGULAR não devem instalar softwares não autorizadas em seus computadores. Caso haja a necessidade de um software específico para desempenhar determinada atividade, o usuário deve solicitá-lo através do formulário de *Solicitação de Inclusão de Novo Software*, disponível na intranet da SINGULAR. Após feita a solicitação,

será avaliada pelo CTO, que, caso aprove, definirá os critérios e perfis de acesso. Do CTO, a solicitação é enviada à área de Controles Internos, que realiza a revisão e informa a área de Suporte Técnico sobre a ativação do novo software. Caso seja aprovada a utilização, o colaborador é notificado para que abra um chamado ao suporte técnico de TI para que esses realizem a instalação.

A SINGULAR respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na SINGULAR.

A Infraestrutura de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

14.2.9 Diretrizes quanto à utilização da Rede Corporativa

Material sexualmente explícito ou qualquer outro conteúdo que fira a legislação em vigor não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

Somente os colaboradores que estão devidamente autorizados a falar em nome da SINGULAR para os meios de comunicação podem escrever em sites de Bate-Papo, Redes Sociais ou Grupos de Discussão (fóruns e newsgroups). Em caso de dúvidas, procure seu gestor.

Todos os arquivos devem ser gravados na rede (Geral), pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. É importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos etc.) nos drivers de rede (Geral), pois ocupam espaço comum limitado do departamento.

14.2.10 Diretrizes quanto ao uso de Mídias Removíveis e da porta USB

O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 3G e os pen drives merecem atenção. Tal vulnerabilidade não pode ser contida com firewalls ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios colaboradores da empresa.

Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da supervisão do departamento do solicitante. Para notebooks de supervisores e cargos acima esta liberação é efetuada por padrão.

Dentro da empresa dê preferência à utilização da rede evitando a utilização de modem 3G conectado à porta USB do computador ou redes Wifi particulares providos por celulares, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o colaborador abre a porta para acesso sem qualquer controle.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos, podendo danificar e corromper dados.

É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

14.2.11 Diretrizes quanto ao uso da Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à SINGULAR.

O acesso às páginas e websites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprios e de relacionamentos.

Sites considerados impróprios serão automaticamente bloqueados. Caso o colaborador não concorde com o bloqueio, deve procurar pela área de Segurança e explicar sua necessidade.

O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

14.2.12 Recomendações sobre o uso do Correio Eletrônico (E-Mail)

É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da SINGULAR.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Não utilizar o e-mail da empresa para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais etc.

Utilizar o e-mail para comunicações oficiais internas, as quais não necessitam obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pelo supervisor da área.

14.2.13 Antivírus

Antivírus dos servidores e estações são atualizados automaticamente.

A varredura por vírus é feita semanalmente nas estações e nos servidores.

14.2.14 Uso de Softwares de Mensageria

O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

Sistemas de mensageria possuem histórico de riscos associados à malwares (vírus, worms etc.), de forma que deve ser utilizado com zelo e cuidado.

O uso de sistemas de mensageria em redes de relacionamento pessoais é proibido no ambiente corporativo, por conta da natural assincronia das mensagens instantâneas oriundas de terceiros sem finalidades laborais, o que usualmente torna-se contraproducente.

O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que a ele estiverem conectados ou que estiverem em rede.

Exemplos de softwares de Mensageria: Skype, Hangouts, WhatsApp etc.

14.2.15 Controle de Acesso Lógico (Baseado em Senhas)

Todo usuário deve 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 da sua senha pessoal.

Recomenda-se senhas de qualidade para assegurar a confidencialidade das informações que tenha autorização de acessar para executar as atividades organizacionais.

Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

Não armazenar senhas nos navegadores (Mozilla, Chrome, Internet Explorer etc.), pois são facilmente visualizadas e comprometem a segurança das informações.

A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada pelo usuário de TI no primeiro acesso.

A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.

Sobre acessos, consultar a Política de Controle de Acessos Lógicos.

14.2.16 Uso de Inteligência Artificial

O uso de inteligência artificial para otimização do trabalho é incentivado na SINGULAR, entretanto, devem ser observadas recomendações.

Por questões de controle interno, é aconselhado o uso do chat agregador de múltiplas IAs da SINGULAR, o chatai.opensingular.com.

Apesar dos termos de privacidade das IAs disponíveis no chatai.opensingular.com garantirem o não compartilhamento de dados com terceiros (openai.com/consumer-privacy, policies.google.com/privacy), não se deve compartilhar informações sensíveis da SINGULAR ou dos clientes da SINGULAR.

15. Legislações, regulamentos e acordos

A SINGULAR identifica as legislações e regulamentações no sistema AMMRISK, controlado pela área de controles internos. Quando há modificações relevantes ao negócio, a área de controles internos envia a comunicação por e-mail para as áreas pertinentes.

A conformidade com as normas, legislações e regulamentações são verificadas nas análises críticas da Alta Direção, que ocorrem trimestralmente.

16. Violações e Sanções

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

O colaborador, prestador de serviço e demais descritos neste instrumento infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

17. Vigência e Validade

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

18. Revisão do Documento

Este documento deve ser revisado anualmente ou quando alguma alteração se fizer necessária.

19. Histórico de Alterações

Versão	Data	Natureza das alterações	Elaboração	Aprovação
01	08/03/2023	Elaboração da versão inicial	Fernando Turatti	Daniel Bordin
02	10/05/2023	Alteração sobre instalação de softwares	Gustavo Vieira	Daniel Bordin
03	05/03/2024	Revisão anual	Gustavo Vieira	Fernando Turatti
04	05/03/2025	Revisão anual / Incremento ao item 14.2.11	Gustavo Vieira	Daniel Bordin
05	18/06/2025	Adição ao item 9	Gustavo Vieira	Daniel Bordin
06	15/08/2025	Adição ao item 7.1 (Singular Studio para abertura de incidentes)	Gustavo Vieira	Vinicius Nunes
07	26/08/2025	Alteração item 13 (melhorar definição para o perímetro físico da Singular)	Gustavo Vieira	Vinicius Nunes
08	04/09/2025	Adição item 14.2.16, sobre inteligência artificial	Gustavo Vieira	Vinicius Nunes
09	16/10/2025	Adição ao item 13 (adequação mudanças climáticas)	Gustavo Vieira	Vinicius Nunes
10	09/02/2026	Atualização itens 9.1, 13.1	Gustavo Vieira	Vinicius Nunes

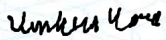
21 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 17 de March de 2026, 17:03:35

GSI-001-POL Política de Segurança da Informação pdf

Código do documento 2eaa4309-cb73-4735-9c9b-8a3200001aa4

Assinaturas

Vinicius Uriel Cardoso Nunes
vinicius.nunes@singular.tec.br
Assinou



Eventos do documento

16 Mar 2026, 14:21:44
Documento 2eaa4309-cb73-4735-9c9b-8a3200001aa4 **criado** por GUSTAVO VIEIRA DO CARMO (6807ae33-c9d8-4618-919c-1d2e1ca76e36). Email:gustavo.vieira@singular.tec.br. - DATE_ATOM: 2026-03-16T14:21:44-03:00

16 Mar 2026, 14:24:47
Assinaturas **iniciadas** por GUSTAVO VIEIRA DO CARMO (6807ae33-c9d8-4618-919c-1d2e1ca76e36). Email: gustavo.vieira@singular.tec.br. - DATE_ATOM: 2026-03-16T14:24:47-03:00

17 Mar 2026, 15:54:55
VINICIUS URIEL CARDOSO NUNES **Assinou** (df29295d-8543-4abb-a549-177939f063e0) - Email: vinicius.nunes@singular.tec.br - IP: 187.32.205.209 (187-032-205-209.static.ctbctelecom.com.br porta: 31792) - Geolocalização: -15.755632267532874 -47.89302947726295 - Documento de identificação informado: 021.427.131-57 - DATE_ATOM: 2026-03-17T15:54:55-03:00

Hash do documento original
(SHA256):82c5b9c76faae147c8a368039b7854e3dca777513b42e2469b75433bdf86899a
(SHA512):bee53ab621bc4782227b7698638d4e6d3e1be5b3a3ba6fedc9ffa24b011c3343b1e0a85b3bddbf9950fa0ab4409619c3a942a8822105c632aa22ce4b3905e8c7

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign
Integridade certificada no padrão ICP-BRASIL
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.