Política Geral de Segurança da Informação

REVISÕES

Histórico de Revisões			
Revisão	**Data**	**Alterações**	**Responsável**
01	25/09/2019	Versão Inicial	Samuel Silvério
02	01/10/2020	Revisão da política geral	Samuel Silvério
03	06/01/2021	Adição de requisitos (Item 6 - Uso de dispositivos moveis, item 7 - Acesso à internet 8 - Uso de E-mail); Modificação do Item 6 para Item 9 – Controles e aplicações	Samuel Silvério
04	08/09/2021	Adicionado item Pessoas e cargo – papéis e responsabilidades	Kauã Morateli
05	08/01/2022	Adicionado item DPO – papéis e responsabilidades	Kauã Morateli
06	10/01/2023	Revisão da Política sem Alteração	Samuel Silvério

APROVAÇÕES

Revisado por		
Nome	**Função**	**Data**
Samuel Silvério	Superintendente de Tec. da Informação	10/01/2023

Aprovado por		
Nome	**Função**	**Data**
Marcos Stati	COO – Chief Operating Officer	10/01/2023

Sumário

1. Introdução 4

2. Propósito 4

3. Escopo 4

4. Papéis e Responsabilidades 5

4.1. Comitê Gestor de Segurança da Informação – CGSI 5

4.2. Gerência de Segurança da Informação 5

4.3. Gestores da Informação 6

4.4. Usuários da Informação 6

4.5. DPO 6

5. Diretrizes 7

6. Uso de dispositivos Móveis 7

6.1. Notebook 8

6.2. Uso de notebook particular em redes Winover 8

6.3. Celular 8

7. Acesso a internet 9

8. Uso de E-mail 9

9. Controles e aplicações 10

9.1. Segurança nas comunicações 11

9.1.1. Propriedade das informações e software 11

9.1.2. Classificação da informação 11

Uso Público 12

Uso Interno 12

Uso Confidencial 12

10. Sanções e Punições 12

11. Casos omissos 12

12. Glossário 13

13. Revisões 14

14. Gestão da Política 14

1. Introdução

A WINOVER CONTACT CENTER atua com Padrão World Class atendendo aos principais segmentos de mercado, com estrutura e capacidade para absorver qualquer tipo, tamanho e/ou complexidade de operações/carteiras, superando as entregas de resultados e reforçando sua posição de referência no mercado. Persuadir, Conquistar e Convencer, mais que um Contact Center, a WINOVER é especialista em Recuperação de Crédito e SAC.

Todas as estratégias adotadas pela WINOVER, sejam comerciais, tecnológicas ou de qualquer outra natureza, circulam entre diversas áreas por diferentes meios de transportes, armazenamento e comunicação, para que possam ser estruturadas, discutidas e colocadas em prática.

Para alcançar a excelência e os objetivos com sucesso, a WINOVER depende fundamentalmente dessas informações, disponíveis em seus sistemas ou em material físico. É por isso que a WINOVER trata tais dados como "bem" valioso.

Nesse sentido a WINOVER determina a sua Política Geral de Segurança da Informação, como complemento do sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas e com o objetivo de assegurar níveis adequados de proteção as informações.

2. Propósito

A Política de Segurança da Informação é uma declaração formal da WINOVER, acerca de seu comprometimento com a proteção das informações e dados pessoais de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários e prestadores de serviços.

A política tem por propósito estabelecer diretrizes e normas de segurança da informação que conceda aos colaboradores e parceiros da WINOVER os cuidados e aplicações de seus processos de proteção de dados e aderência aos controles a segurança da informação e privacidade de dados pessoais garantidas por lei.

A política tem por seus objetivos:

Garantir a confidencialidade dos dados em posse da WINOVER, preservar a integridade de seu conteúdo que possam causar constrangimento, prejuízo de imagem corporativa, direitos intelectuais e/ou riscos financeiros a WINOVER, Clientes e parceiros, e garantir sua disponibilidade quanto aos acessos a esses dados.

3. Escopo

Essa política se aplica a todos os funcionários, diretores, executivos, acionistas, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam à serviço e disponibilizam de ativos corporativos, sendo esses tangíveis ou não da WINOVER, suas Unidades, subsidiárias e/ou coligadas.

4. Papéis e Responsabilidades

Pessoas e cargos:

Comitê Gestor de Segurança da Informação / Membros do conselho:
Simone Paula, Vanusa Santos, Paulo Silva, Marcos Stati;
Gerência / Gestor de Segurança: Samuel Silvério, Analista de Segurança da Informação;
DPO: Samuel Silvério.

4.1. Comitê Gestor de Segurança da Informação – CGSI

Conta com a participação de colaboradores com um nível mínimo hierárquico de liderança, nomeados para participar do CGSI pelo período de um ano.

É composto por no mínimo um representante da Alta Gestão e das áreas de Tecnologia da Informação, Facilities, Recursos Humanos, Operações (representado pelo COO) e Financeiro.

O CGSI se reúne formalmente pelo menos uma vez ao ano.

Reuniões adicionais podem ser feitas se necessário, em casos de incidentes graves ou assuntos relacionados à segurança da informação e gestão de privacidade da dados pessoais que são relevantes para a WINOVER.

É de responsabilidade do CGSI:

- Elaborar novas políticas e normas relacionadas à Segurança da Informação e revisar as já existentes;
- Garantir a disponibilidade dos recursos necessários relacionados à Segurança da Informação e, que as atividades de segurança da informação sejam executadas em conformidade com este documento;
- Promover a divulgação e treinamento deste documento e tomar as medidas necessárias para extinguir qualquer cultura de segurança da informação não aderentes a política de segurança de informação da WINOVER.

4.2. Gerência de Segurança da Informação

É responsabilidade da Gerência de Segurança da Informação:

- Conduzir a gestão e a operação da segurança da informação, tendo este documento como base;
- Garantir o apoio ao CGSI;
- Elaborar e propor ao CSGI as normas necessárias para o cumprimento deste documento,
- Identificar e avaliar ameaças à segurança da informação, propor e, se aprovado, implantar medidas para redução dos riscos;
- Realizar as ações cabíveis para o cumprimento dos termos da política;
- Garantir o tratamento adequado quanto a gestão dos incidentes de segurança da informação.

4.3. Gestores da Informação

O Gestor da Informação é uma atribuição designada ao(s) responsável(eis) dentro de uma ou mais áreas da empresa, ao qual será designado pelas seguintes responsabilidades:

- Gerenciar as informações sob a sua responsabilidade, durante todo o seu ciclo de vida, incluindo a criação, manuseio, transporte e descarte conforme as normas estabelecidas pela WINOVER;
- Identificar e classificar as informações sob a sua responsabilidade conforme normas, critérios e procedimentos adotados;
- Autorizar, revogar e revisar o acesso à informação e sistemas sob sua responsabilidade;
- Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário.

4.4. Usuários da Informação

É responsabilidade dos Usuários da Informação:

- Ler e cumprir os termos da Política Geral de Segurança da Informação, e as demais normas e procedimentos de segurança aplicáveis;
- Ler e cumprir o "Termo de Confidencialidade e Sigilo" e responsabilidades atribuídas.
- Encaminhar quaisquer dúvidas ou esclarecimentos sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao CGSI;
- Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política, ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da WINOVER;
- Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item Sanções e Punições.

4.5. DPO

É de responsabilidade do DPO:

- Treinar e orientar os funcionários da empresa sobre os requisitos de conformidade com LGPD;
- Realizar avaliações e auditorias regulares para garantir a conformidade com LGPD;
- Servir como ponto de contato entre a empresa e a autoridade supervisora;
- Manter registros das atividades de processamento de dados realizados pela organização;
- Responder ou informar os titulares de dados pessoais sobre como seus dados estão sendo usados e quais medidas de proteção implementadas pela organização;

- Assegurar que os pedidos de acesso ou apagamentos de dados feito por titulares de dados pessoais, sejam atendidos ou respondidos, conforme necessário;

5. Diretrizes

A WINOVER é comprometida com a legislação em vigor aplicável, bem como do Estatuto da Companhia e do Código de Ética e Conduta. E para a condução de suas atividades empresariais é necessário o estabelecimento de uma Política de Segurança da Informação estruturada e clara que possibilite aderência a essas conformidades.

A finalidade da gestão de Segurança da Informação da WINOVER é afirmar o caráter geral e abrangente de todos os pontos relacionados à Segurança da informação, fornecendo suporte as operações críticas do negócio, minimizando riscos identificados e seus eventuais impactos para WINOVER, bem como a especificação de procedimentos e controle necessários para proteger as informações.

A Diretoria e o Comitê Gestor de Segurança da Informação afirmam o compromisso com a gestão da Segurança da Informação, sendo assim, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

É política da Winover Contact Center:

- Criar, estabelecer e seguir as políticas, normas e procedimentos de segurança da informação, garantindo que as condições básicas de confidencialidade, integridade e disponibilidade da informação da WINOVER sejam alcançadas através da adoção de controles contra ameaças vindas de fontes externas e/ou internas;

- Educar e conscientizar empregados e, onde pertinente, terceiros contratados e clientes, sobre as práticas de Segurança da Informação adotadas pela WINOVER;

- Disponibilizar as políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas;

- Respeitar os requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

- Agir em incidentes de segurança da informação, garantindo que sejam registrados, classificados, investigados, corrigidos, documentados e se necessário, informado as autoridades apropriadas;

- Garantir a continuidade do negócio pela criação, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

- Aprimorar de maneira contínua a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

6. Uso de dispositivos Móveis

6.1. Notebook

Cada estação de trabalho possui uma identificação, “Mac Address”, os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado, na estação de trabalho, será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação, tenha certeza de que a ela está bloqueada para acessos.

A Winover poderá, a qualquer momento, realizar auditoria no notebook, fornecidos para atividades de seus colaboradores, consultores, ou/e representantes externos.

Não utilize nenhum tipo de software sem autorização e homologação da área de infraestrutura de TI.

Não é permitido gravar nas estações de trabalho da empresa Winover, MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria ou não homologado pela área de segurança da Informação.

Todos os dados relativos à Winover devem ser mantidos no servidor, onde existe sistema de backup diário.

6.2. Uso de notebook particular em redes Winover

Em caso necessário, é pautada em aspectos técnicos ou tecnológicos, será autorizada a utilização de uso de notebooks pessoais no ambiente da rede Winover.

Para tal, faz-se indispensável a aprovação formal, por escrito, dos membros da diretoria, devidamente assistido pela área de suporte em caso de exercer suas atividades internas com o equipamento descrito.

Serão, portanto, de responsabilidade do Suporte as configurações relativas aos dispositivos de rede e de domínio de rede da Winover, bem como, a instalação de software para garantir e assistir a segurança da empresa.

A Winover poderá, a qualquer momento, solicitar a realização de auditoria no notebook pessoal.

Restrições:

a) Não podem ser executados nos notebooks, aplicativos de característica maliciosa, que possam comprometer o funcionamento da rede, bem como a captura de informações confidenciais, como, por exemplo: senhas de usuários, programas, softwares, documentos etc.

b) Fica proibida a apropriação de arquivos que não seja de uso pessoal do proprietário do notebook.

6.3. Celular

A Winover disponibiliza o aparelho de celular e/ou chip corporativos a colaboradores autorizados. Esses colaboradores devem atentar-se as diretrizes de segurança:

- Os celulares devem conter senha de acesso.
- O acesso ao e-mail se dá através de utilização do aplicativo Microsoft 365 ou Microsoft Outlook (controle através de conta de e-mail).
- Se atentar aos avisos e as normas de utilização de celular nas áreas da empresa;

NOTA: Para colaboradores que utilizam o celular pessoal é liberado o uso do chip corporativo, devendo os mesmos atender às diretrizes de segurança.

7. Acesso a internet

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos colaboradores da Winover, não é permitido o seu uso para fins recreativos durante o horário de trabalho. Estes acessos poderão ser efetuados durante o horário de almoço, desde que dentro das regras de uso definidas nesta política ou pelo Diretor responsável da área.

Colaboradores com acesso à Internet não poderão efetuar upload / download de qualquer software licenciado para à Winover ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Haverá geração de relatórios dos sites acessados pelos usuários, sob demanda.

Somente navegação de sites homologados serão permitidas. Casos específicos que exijam outros tipos de serviços, como download de arquivos, deverão ser solicitados diretamente à equipe de suporte com autorização do responsável da área mediante a chamado e aprovação.

É proibida a divulgação de informações confidenciais da Winover em grupos de discussão, listas, bate-papo e afins, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou previstos em lei.

É expressamente proibido o uso de software de comunicação instantânea, não homologados/ autorizados pela Diretoria da área.

O acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas, com conteúdo racista são bloqueados e as tentativas de acesso serão monitoradas.

Não será permitida a utilização de serviços de streaming, tais como Rádios On-Line, Usina de Som e afins.

8. Uso de E-mail

O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens.

Nossos servidores de e-mail encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são importantes. Para isto algumas regras devem ser obedecidas:

- É proibido o envio de grande quantidade de mensagens de e-mail (spam) e evitem arquivos anexos muito grandes, não sendo permitidos arquivos maiores que 20MB, isso inclui qualquer tipo de mala direta ou e-mail em lote, como por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.

- É proibido o acessar o e- mail por meio de Webmail ou softwares não homologados pela Winover para o e-mail corporativo, podendo ser liberado somente por via de chamado com aprovação da diretoria previamente documentada.

- É proibido o envio de e-mail mal-intencionado, tais como “e-mail bomb” ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso.

- Evitar o uso de Linguagem Coloquial em respostas aos e-mails comerciais, como abreviações de palavras e uso de gírias.

- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis. Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos.

- Desconfie de qualquer e-mail com assuntos estranhos ou desconhecidos e de instituições bancárias ou órgãos públicos que solicitem atualização cadastral ou troca de senha e no caso de recebimento consultem o Suporte TI antes de abrir ou clicar em algum item do e-mail.

- Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza de que solicitou este e-mail.

- É obrigatória a utilização de assinatura nos e-mails, seguindo padrão estabelecido pela Winover.

- É proibido o envio de materiais de natureza pornográfica e racista por meio de e-mail da empresa;

- É proibido o envio de e-mails que sejam prejudiciais à capacidade técnica da rede;

- É proibido forjar qualquer informação do cabeçalho do remetente.

9. Controles e aplicações

9.1. Segurança nas comunicações

Neste item são definidas como serão tratadas as informações institucionais, forma de uso, possibilidade ou não de disponibilização ao ambiente externo ou a terceiros. Assim, sempre que houver a necessidade de utilização de informações de conteúdo institucional, é necessário atentar-se para as determinações abaixo descritas:

9.1.1. Propriedade das informações e software

Os dados e informações criados nos Recursos Computacionais da WINOVER são de sua propriedade e devem ser utilizados pelos Colaboradores, Prestadores de Serviços, Consultores e Coligadas, **exclusivamente**, no exercício de suas atividades junto à empresa.

Reiteramos a soberania da WINOVER para gestão das informações das nossas subsidiárias e/ou coligadas para prestação de contas e controle de acesso imparcialmente conforme parágrafo descrito acima.

Os softwares adquiridos no mercado ou desenvolvidos internamente pertencem exclusivamente a WINOVER, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas, elaboradas e/ou desenvolvidas pelos Colaboradores, durante a vigência da relação de emprego ou contrato, ou quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações tecnológicas e segredos comerciais, pertencentes a WINOVER, sendo vedada a cópia ou disponibilização através de qualquer meio (eletrônico ou físico) para ambiente externo a WINOVER.

Toda estrutura mantida pela WINOVER, composta pela rede, telefonia, correio eletrônico, internet e outros meios de comunicação, são instrumentos de trabalho de sua propriedade que, disponibiliza aos associados a fim de tornar suas tarefas mais eficientes. Da mesma forma, todos os documentos, estejam eles em forma impressa ou eletrônica, ou que circulem por estes meios, também são de propriedade da WINOVER e todos os associados devem aceitar os esforços para protegê-los do uso indevido.

É proibido o uso destes documentos fora da WINOVER cujo objetivo não seja atender, exclusivamente, aos interesses da instituição, e, ainda assim, sua retirada ou envio somente poderá ser efetuado com autorização do CGSI e do responsável pela TI. Sua retirada ou envio com qualquer outra finalidade constitui violação a esta política. A sua transmissão via correio eletrônico, fax, email ou outro meio, deverá ser feita com o máximo de atenção e seguindo as regras de segurança e confidencialidade constantes nesta Política e no Código de Ética.

Os documentos alterados fora da WINOVER devem ter seus arquivos, manuais ou na rede, atualizados imediatamente. Lembramos que todas as ações realizadas nos computadores corporativos têm os logs (registro de eventos) registrados, podendo ser a qualquer tempo auditados e monitorados, com o objetivo de garantir a aplicação desta Política.

9.1.2. Classificação da informação

As informações que transitam pela WINOVER são, para fins desta Política, classificadas em padrões distintos, a saber:

Uso Público

Informação aquelas destinadas a disseminação fora da WINOVER. Possuem caráter informativo geral e são direcionadas a colaboradores, clientes e investidores. Exemplos: material de marketing, apresentações internas, redes sociais, podendo esses compartilhar livremente desde que seja mantido a sua integridade

Uso Interno

Informação de uso exclusivo para os colaboradores da WINOVER. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a WINOVER ou seus clientes e associados estão sujeitos a aplicação das sanções e punições conforme essa política. Essas informações não podem se tornar pública e só poderão ser compartilhadas mediante autorização.

Uso Confidencial

Também se destinam a uso interno da WINOVER. Entretanto, diferem das informações de natureza interna à medida que sua extensão em uma eventual divulgação, poderia afetar significativamente os negócios da WINOVER, seus clientes, investidores e associados. Exemplos: registros de funcionários, planos salariais, informações sobre clientes, sejam elas genéricas ou específicas, classificação de crédito, saldos de contas correntes. Sua divulgação é proibida, salvo se solicitada por órgão fiscalizador competente (BACEN, CVM e Receita Federal, por exemplo), situação na qual deverá ser prestada por uma das seguintes pessoas: Contador, Controller, Auditor Interno, Advogado ou um dos sócios.

10. Sanções e Punições

As violações desta política, normas e procedimentos de segurança, serão passíveis de penalidade e a aplicação de sanções e punições serão analisadas pelo CGSI e alinhadas com o corpo jurídico da Winover.

No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a WINOVER, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

11. Casos omissos

Os casos omissos serão avaliados pelo CGSI para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Sendo obrigação do usuário da informação da WINOVER adotar, sempre que possível, outras medidas de segurança além das aqui previstas.

12. Glossário

Informação: Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (baseados em troca de mensagens) ou transacionais (realizadas operações que envolvam, por exemplo, a transferência de valores monetários). A informação pode estar presente em inúmeros elementos desse processo, chamados: ativos, os quais são alvos de proteção da segurança da informação

Ativo: Todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada, os equipamentos que ela é manuseada, transportada e descartada.

Riscos: Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente impactos de negócio.

Impacto: Abrangência dos danos causados por incidente de segurança sobre um ou mais processos de negócio.

Incidente: Fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

Ameaças: São agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização.

Vulnerabilidade: São fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de

segurança da informação: confidencialidade, integridade e disponibilidade.

Confidencialidade: Informação não divulgada para partes não autorizadas.

Integridade: Informação completa e exata.

Disponibilidade: Informação acessível e utilizável pelas partes autorizadas.

Comitê Gestor De Segurança Da Informação: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da WINOVER, que tem por finalidade tratar questões ligadas à Segurança da Informação.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Usuário da informação: Empregados com vínculo empregatício de qualquer área da WINOVER ou terceiros alocados na prestação de serviços, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da WINOVER para o desempenho de suas atividades profissionais.

13. Revisões

Esta política é revisada com periodicidade anual ou conforme o entendimento do CGSI.

14. Gestão da Política

A Gestão da Segurança da Informação é responsável por manter e revisar esta política.

Aprovada pela Diretoria da Winover Contact Center Ltda.

A presente política foi revisada e aprovada no dia 10/01/2023.

Essa política passa a vigorar com as atualizações conforme data de aprovação da revisão e assinatura dos responsáveis pelo SGSI da WINOVER.

Mogi das Cruzes - SP, 10 de Janeiro de 2023

Samuel Santo Silvério
Superintendente de TI

Marco Stati
COO – Chief Operating Officer