Política de Segurança da Informação

Destinatários:
Todos os colaboradores da Nors, prestadores de serviços, consultores, estagiários e terceiros

Data: 28/04/2026
Entrada em vigor: 28/04/2026
Emissão: Direção de Sistemas de Informação

Âmbito de aplicação:
Aplica-se a todos os colaboradores, prestadores de serviços, consultores, estagiários e terceiros que utilizem informação, equipamentos informáticos e recursos de rede da Nors, independentemente da sua localização ou natureza do vínculo contratual.

1. Visão geral

A presente Política de Segurança da Informação tem como objetivo proteger todas as empresas do Grupo Nors bem como os seus colaboradores e parceiros, contra ações ilegais ou prejudiciais praticadas por indivíduos, quer de forma deliberada quer não intencional.

Os sistemas associados à Internet, Intranet e Extranet, incluindo, entre outros, equipamentos informáticos, software, sistemas operativos, suportes de armazenamento e contas de rede que disponibilizam serviços como correio eletrónico, navegação na web e transferência de ficheiros, são propriedade da Nors. Estes sistemas devem ser utilizados exclusivamente para fins profissionais, no âmbito das atividades normais da empresa e de forma a servir os interesses da organização, dos seus clientes e parceiros.

A segurança da informação eficaz depende da participação ativa e do apoio de todos os colaboradores, prestadores de serviços e terceiros que tenham acesso a informações e/ou sistemas de informação da Nors. É responsabilidade de cada um ler, compreender e cumprir esta política, assegurando que as suas atividades são realizadas em conformidade com as regras aqui estabelecidas.

2. Propósito

A presente política tem como objetivo descrever a utilização aceitável e a proteção das informações dos ativos da empresa, para garantir a CIA (Confidencialidade, Integridade e Disponibilidade) da informação do Grupo Nors. Estas regras destinam-se a proteger os clientes, os colaboradores e a própria Nors. A utilização inadequada dos sistemas e da informação pode expor a empresa a diversos riscos, incluindo infeções por malware, compromissos de sistemas e serviços de rede, prejuízos financeiros e reputacionais, bem como riscos legais e de conformidade.

3. Âmbito

A presente política aplica-se à utilização de informação, equipamentos informáticos e recursos de rede utilizados pela Nors para a condução das suas atividades ou para interação com redes internas e sistemas empresariais, independentemente de serem propriedade ou estarem alugados pela Nors, por um colaborador ou por terceiros. Todos os colaboradores, prestadores de serviços, consultores, estagiários e outros trabalhadores da Nors e das suas subsidiárias devem agir com bom senso e responsabilidade na utilização adequada da informação, dos dispositivos eletrónicos e dos recursos de rede, em conformidade com as políticas e normas internas da Nors, bem como com a legislação e regulamentação aplicáveis.

4. Compromisso da Administração

A Administração da Nors assume a segurança da informação como um elemento essencial para a continuidade, resiliência, confiança e sustentabilidade das atividades da organização.

A presente Política de Segurança da Informação, bem como os objetivos de segurança da informação definidos no âmbito do Sistema de Gestão de Segurança da Informação (SGSI), encontram-se alinhados com a direção estratégica da Nors, com os objetivos de negócio, com as necessidades das partes interessadas e com os requisitos legais, regulamentares, contratuais, normativos e internos aplicáveis.

A Administração demonstra liderança e compromisso com o SGSI através da aprovação desta política, da definição de objetivos de segurança da informação, da disponibilização dos recursos necessários, da promoção da melhoria contínua e da integração dos requisitos de segurança da informação nos processos relevantes da organização.

A Administração compromete-se a assegurar que os recursos necessários para estabelecer, implementar, manter e melhorar continuamente o SGSI são disponibilizados de forma adequada, incluindo recursos humanos, tecnológicos, financeiros, organizacionais e de formação, tendo em consideração o contexto da organização, os riscos identificados e a criticidade da informação tratada pela Nors.

A Administração compromete-se ainda a comunicar, de forma adequada, a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do SGSI, promovendo uma cultura de segurança, responsabilidade e proteção da informação em toda a organização.

A Administração apoia os responsáveis das diferentes áreas organizacionais na demonstração de liderança em matéria de segurança da informação, assegurando que estes promovem o cumprimento das políticas, procedimentos, controlos e requisitos aplicáveis nas respetivas áreas de responsabilidade.

Os responsáveis de área devem assegurar que os requisitos de segurança da informação são compreendidos, aplicados e monitorizados no âmbito das atividades, processos, equipas e sistemas sob a sua responsabilidade.

5. Enquadramento do Sistema de Gestão de Segurança da Informação

A Nors estabelece, implementa, mantém e melhora continuamente um Sistema de Gestão de Segurança da Informação (SGSI), de acordo com os requisitos definidos pela organização e com as boas práticas aplicáveis em matéria de segurança da informação.

O SGSI tem como objetivo proteger a confidencialidade, integridade e disponibilidade da informação, reduzir riscos de segurança da informação, apoiar a continuidade das operações, reforçar a confiança das partes interessadas e assegurar o cumprimento dos requisitos legais, regulamentares, contratuais, normativos e internos aplicáveis.

A Nors compromete-se a integrar os requisitos do SGSI nos processos relevantes da organização, incluindo, mas não se limitando a:

a) gestão de acessos;
b) gestão de identidades e privilégios;
c) gestão de ativos;
d) gestão de alterações;
e) gestão de vulnerabilidades;
f) gestão de incidentes de segurança da informação;
h) continuidade de negócio e recuperação de desastre;

i) desenvolvimento seguro;
j) gestão de projetos tecnológicos;
k) onboarding, alteração de funções e offboarding de colaboradores;
l) formação e sensibilização em segurança da informação;
m) monitorização, logging e deteção de eventos de segurança;
n) gestão de risco de segurança da informação.

As áreas responsáveis devem assegurar que os requisitos de segurança da informação são considerados no planeamento, execução, monitorização, revisão e melhoria dos seus processos.

6. Princípios de Segurança da Informação

A segurança da informação na Nors assenta nos seguintes princípios:

- **Confidencialidade:** assegurar que a informação apenas é acedida, utilizada ou divulgada por pessoas, entidades, sistemas ou processos devidamente autorizados;
- **Integridade:** proteger a exatidão, completude, validade e fiabilidade da informação e dos respetivos métodos de processamento;
- **Disponibilidade:** assegurar que a informação, os sistemas e os serviços de suporte estão acessíveis quando necessários para a atividade da organização;
- **Necessidade de saber:** garantir que o acesso à informação é concedido apenas quando necessário para o desempenho das funções profissionais;
- **Menor privilégio:** assegurar que os acessos atribuídos são limitados ao mínimo necessário para a realização das atividades autorizadas;
- **Responsabilização:** garantir que colaboradores, prestadores de serviços, terceiros e responsáveis de processo compreendem e assumem as suas responsabilidades em matéria de segurança da informação;
- **Gestão baseada no risco:** definir, priorizar e rever controlos de segurança com base na avaliação dos riscos de segurança da informação;
- **Conformidade:** assegurar o cumprimento dos requisitos legais, regulamentares, contratuais, normativos e internos aplicáveis;
- **Melhoria contínua:** rever e melhorar continuamente o SGSI, os processos, os controlos e os objetivos de segurança da informação;
- **Proteção por defeito e desde a conceção:** considerar requisitos de segurança da informação desde as fases iniciais de processos, projetos, sistemas, alterações tecnológicas e relações com terceiros.

7. Objetivos de Segurança da Informação

A Nors estabelece objetivos de segurança da informação alinhados com esta política, com a direção estratégica da organização, com os resultados da avaliação de risco, com os requisitos aplicáveis e com as necessidades das partes interessadas.

Os objetivos de segurança da informação devem, sempre que praticável, ser mensuráveis, monitorizados, comunicados, revistos periodicamente e atualizados sempre que necessário.

Os objetivos de segurança da informação podem incluir, entre outros:

- a) proteger a confidencialidade, integridade e disponibilidade da informação;
- b) reduzir a probabilidade e o impacto de incidentes de segurança da informação;
- c) melhorar a capacidade de deteção, análise, resposta e recuperação perante incidentes;
- d) assegurar a gestão eficaz de identidades, acessos e privilégios;
- e) reduzir vulnerabilidades técnicas e promover a correção atempada de falhas de segurança;
- f) assegurar a continuidade e recuperação dos sistemas, serviços e processos críticos;
- g) reforçar a proteção contra ameaças como phishing, malware, ransomware, acessos indevidos e fuga de informação;
- h) promover a sensibilização, formação e consciencialização dos colaboradores em segurança da informação;
- i) assegurar o cumprimento dos requisitos legais, regulamentares, contratuais, normativos e internos aplicáveis;
- j) melhorar continuamente a eficácia do SGSI.

Os objetivos específicos de segurança da informação, incluindo métricas, metas, responsáveis, prazos, recursos necessários e métodos de avaliação, são mantidos como informação documentada no âmbito do SGSI.

8. Cumprimento de Requisitos Aplicáveis

A Nors compromete-se a cumprir os requisitos legais, regulamentares, contratuais, normativos e internos aplicáveis à segurança da informação.

Estes requisitos podem incluir, entre outros:

a) requisitos relacionados com proteção de dados pessoais;
b) requisitos de confidencialidade;
c) requisitos de continuidade de negócio;
d) obrigações contratuais assumidas perante clientes, fornecedores, parceiros e outras entidades externas;
e) requisitos de propriedade intelectual;
f) requisitos de auditoria interna e externa;
g) requisitos de segurança definidos por clientes ou entidades terceiras;
h) requisitos legais e regulamentares aplicáveis às geografias onde a Nors opera;
i) requisitos decorrentes de políticas, normas, instruções funcionais e procedimentos internos da organização.

Sempre que aplicável, devem ser considerados requisitos decorrentes do Regulamento Geral sobre a Proteção de Dados (RGPD), legislação nacional aplicável, obrigações setoriais, requisitos contratuais e boas práticas reconhecidas de segurança da informação.

Os requisitos aplicáveis devem ser identificados, mantidos, revistos e considerados na definição de políticas, controlos, objetivos, avaliação de riscos, planos de tratamento de risco e atividades de melhoria do SGSI.

9. Responsabilidades

A segurança da informação é uma responsabilidade partilhada por todos os colaboradores, prestadores de serviços, consultores, estagiários e terceiros que acedam à informação, sistemas, equipamentos ou recursos tecnológicos da Nors.

A **Administração** é responsável por:

a) aprovar esta Política de Segurança da Informação;
b) demonstrar liderança e compromisso com o SGSI;
c) assegurar o alinhamento da segurança da informação com a direção estratégica da organização;
d) assegurar a disponibilização dos recursos necessários para o SGSI;
e) promover a melhoria contínua da segurança da informação;
f) apoiar os responsáveis de área no cumprimento das suas responsabilidades em matéria de segurança da informação.

O **Departamento de Cybersecurity** é responsável por:

a) apoiar a definição, implementação e revisão de controlos de segurança da informação;
b) acompanhar riscos de segurança da informação;
c) monitorizar eventos e incidentes de segurança;
d) apoiar a resposta a incidentes de segurança da informação;
e) promover boas práticas de segurança;
f) apoiar ações de sensibilização e formação;
g) acompanhar vulnerabilidades, ameaças e oportunidades de melhoria.
h) coordenar a implementação, manutenção e melhoria das medidas técnicas e organizacionais de segurança da informação;
i) assegurar a articulação entre os requisitos do SGSI e os processos tecnológicos da organização;
j) apoiar a gestão de riscos tecnológicos e de segurança da informação;

k) assegurar a implementação de controlos técnicos adequados, em articulação com as equipas responsáveis.

Os **responsáveis de área** são responsáveis por:

a) garantir que os requisitos de segurança da informação são aplicados nos processos sob a sua responsabilidade;
b) assegurar que as suas equipas conhecem e cumprem esta política e os procedimentos aplicáveis;
c) colaborar na identificação, avaliação e tratamento de riscos de segurança da informação;
d) apoiar a implementação de ações corretivas e de melhoria;
e) comunicar necessidades, riscos, incidentes ou incumprimentos relacionados com segurança da informação.

Todos os **utilizadores** são responsáveis por:

a) cumprir esta política e as restantes políticas, normas, instruções funcionais e procedimentos aplicáveis;
b) proteger a informação a que tenham acesso;
c) utilizar os sistemas, equipamentos e recursos tecnológicos de forma adequada, autorizada e responsável;
d) reportar eventos, incidentes, vulnerabilidades, perdas, roubos, acessos indevidos ou situações suspeitas;
e) participar nas ações de formação e sensibilização aplicáveis;
f) respeitar os princípios de confidencialidade, integridade e disponibilidade da informação.

10. Relatórios de incidentes de segurança

Todos os utilizadores devem comunicar quaisquer eventos ou incidentes de segurança conhecidos ou suspeitos, incluindo violações das políticas internas e vulnerabilidades de segurança identificadas. Os incidentes devem ser reportados de imediato ou com a maior brevidade possível ao Departamento de Cybersecurity da Nors, através da abertura de um ticket "Reportar incidente de Segurança" no sistema de suporte ou através de contacto via email com o Departamento de Cybersecurity.

No momento da comunicação do incidente, o utilizador deve descrever claramente o evento ou observação, incluindo todos os detalhes relevantes que possam ajudar na análise e resposta ao incidente.

11. Denúncia de fraude anónima

O Regulamento de Comunicação de Infrações, tem como objetivo incentivar e permitir que colaboradores e outras partes interessadas reportem internamente questões graves, de forma a possibilitar a identificação, análise e correção de condutas ou ações inadequadas.

É responsabilidade de todos os colaboradores comunicar quaisquer violações ao Código de Ética da empresa ou suspeitas de incumprimento de leis e regulamentos aplicáveis às operações da Nors.

12. Política para dispositivos portáteis

Todos os dispositivos dos utilizadores finais (telemóveis, tablets, computadores portáteis, entre outros) devem cumprir a presente política. Os colaboradores devem ter especial cuidado ao abrir anexos de correio eletrónico provenientes de remetentes desconhecidos, uma vez que estes podem conter malware.

É estritamente proibido conceder acesso a qualquer outro indivíduo, quer de forma deliberada quer por negligência na proteção de um dispositivo.

Todos os dispositivos dos utilizadores finais, sejam pessoais (BYOD - Bring Your Own Device) ou propriedade da empresa, utilizados para aceder aos sistemas de informação da Nors devem cumprir as seguintes regras e requisitos:

- Os dispositivos devem possuir um protetor de ecrã protegido por palavra-passe ou mecanismo equivalente (por exemplo, autenticação biométrica), com bloqueio automático após um período de inatividade definido.
- Os dispositivos devem ser bloqueados sempre que forem deixados sem supervisão.
- Os utilizadores devem reportar imediatamente qualquer suspeita de utilização indevida, perda ou roubo de um dispositivo móvel ao Departamento de Cybersecurity da Nors, através da abertura de um ticket "Reportar incidente de Segurança" ou contacto via email para o Departamento de Cybersecurity.
- Informação confidencial não deve ser armazenada em dispositivos móveis ou em unidades USB, exceto quando estritamente necessário e devidamente autorizado.
- Após a cessação da relação laboral ou contratual, os utilizadores devem devolver todos os dispositivos propriedade da empresa.

13. Política de clean desk

Os utilizadores devem assegurar que não deixam informações ou documentos confidenciais expostos ou sem proteção nas suas secretárias ou áreas de trabalho. Devem igualmente assegurar que os ecrãs dos seus equipamentos se encontram bloqueados sempre que não estejam a ser utilizados ou quando se ausentarem do posto de trabalho.

14. Política de acesso e trabalho remoto

Trabalho remoto refere-se a qualquer situação em que colaboradores da organização desempenham as suas funções fora das instalações da empresa. Isto inclui teletrabalho, locais de trabalho flexíveis, ambientes de trabalho virtuais e atividades de manutenção remota.

Os computadores portáteis e outros recursos informáticos utilizados para aceder à rede da Nors devem respeitar as seguintes normas:

- As políticas da empresa devem ser cumpridas durante o trabalho remoto, incluindo as regras relativas a mesa limpa, impressão, eliminação de ativos e reporte de incidentes de segurança da informação, de forma a evitar o manuseamento incorreto ou a exposição acidental de informação confidencial.
- O acesso remoto aos recursos da Nors é obrigatório através da solução VPN corporativa (GlobalProtect), gerida centralmente pela Nors. Não é permitida a utilização de outros meios de acesso remoto não aprovados pela organização.
- Todos os equipamentos utilizados para aceder aos recursos da Nors devem estar sob gestão e controlo da Nors, incluindo a configuração, monitorização e aplicação de políticas de segurança.
- É obrigatória a utilização da solução de antivírus corporativa da Microsoft, gerida centralmente pela Nors, em todos os sistemas autorizados a aceder à rede e aos recursos.
- A autenticação multifator (MFA) é obrigatória para o acesso remoto e para o acesso a sistemas e aplicações corporativas, de acordo com as políticas de segurança definidas pela Nors.
- O acesso a aplicações e dados corporativos encontra-se sujeito a políticas de Conditional Access, definidas e geridas pela Nors, com o objetivo de restringir acessos com base em critérios de risco, conformidade do dispositivo, localização, tipo de autenticação e outros controlos de segurança aplicáveis.
- Não é permitido desativar, contornar ou alterar mecanismos de segurança geridos pela Nors, incluindo a VPN corporativa, o antivírus, o MFA, as configurações de segurança do equipamento e as políticas de Conditional Access.

15. Política de uso aceitável

As informações pertencentes à Nors e aos seus clientes, armazenadas em dispositivos eletrónicos e informáticos, quer sejam propriedade da empresa, alugados pela Nors, pertencentes a colaboradores ou a terceiros, são consideradas propriedade exclusiva da Nors para efeitos da presente política.

Os utilizadores de computadores portáteis ou outros dispositivos disponibilizados pela empresa devem utilizar os sistemas corporativos de partilha e armazenamento de ficheiros da Nors (SharePoint da Microsoft) para guardar documentos de trabalho. O armazenamento de documentos nesses sistemas constitui também uma forma de salvaguarda e cópia de segurança dos dados existentes nos equipamentos.

O acesso, utilização ou partilha de informação propriedade da Nors apenas é permitido quando devidamente autorizado e estritamente necessário para o desempenho das funções profissionais. Os colaboradores devem igualmente utilizar bom senso e responsabilidade no eventual uso pessoal dos equipamentos fornecidos pela empresa.

Para efeitos de segurança e manutenção da rede, colaboradores devidamente autorizados da Nors podem monitorizar equipamentos, sistemas e tráfego de rede a qualquer momento.

A Nors reserva-se ainda o direito de realizar auditorias periódicas às redes e sistemas, com o objetivo de verificar o cumprimento da presente política e das restantes políticas de segurança da informação.

15.1 Uso Inaceitável

De forma geral, as atividades descritas abaixo são proibidas. Os colaboradores podem ser excecionalmente dispensados destas restrições quando tal faça parte das suas responsabilidades profissionais legítimas, mediante aprovação prévia e devidamente documentada pela gestão. Em circunstância alguma um colaborador da Nors está autorizado a envolver-se em qualquer atividade ilegal ao abrigo das leis locais, nacionais ou internacionais enquanto utilizar recursos pertencentes à Nors.

ATIVIDADES ESTRITAMENTE PROIBIDAS

A lista seguinte não é exaustiva, mas apresenta exemplos de atividades consideradas utilização inaceitável.

- Violação de direitos de qualquer pessoa ou organização protegidos por direitos de autor, segredos comerciais, patentes ou outras formas de propriedade intelectual, incluindo a instalação ou distribuição de software pirateado ou de qualquer software que não esteja devidamente licenciado para utilização pela Nors.
- Cópia não autorizada de material protegido por direitos de autor, incluindo digitalização e distribuição de fotografias, música ou instalação de software sem licença válida.

- Acesso a dados, servidores ou contas para fins que não estejam relacionados com as atividades da Nors, mesmo que o utilizador possua permissões de acesso.

- Exportação de software, informação técnica, software de criptografia ou tecnologia em violação das leis e regulamentos internacionais ou regionais de controlo de exportação.
- Introdução de software malicioso na rede ou nos sistemas da empresa, incluindo vírus, worms, cavalos de Troia, phishing (via email) ou qualquer outro tipo de malware.
- Divulgação da palavra-passe da conta a terceiros ou permitir que outra pessoa utilize a conta do utilizador, incluindo terceiros no caso de trabalho a partir de casa.
- Utilização de recursos informáticos da Nors para aceder, obter ou transmitir material que viole leis relacionadas com assédio sexual ou ambiente de trabalho hostil.
- Realização de ofertas fraudulentas de produtos, bens ou serviços utilizando contas ou recursos da Nors.
- Realizar violações de segurança ou interferir com as comunicações de rede, incluindo acesso a dados para os quais o colaborador não é o destinatário autorizado.
- Realizar scans de portas ou avaliações de segurança sem notificação prévia e autorização da equipa responsável pela engenharia ou segurança da Nors.
- Contornar mecanismos de autenticação ou controlos de segurança de qualquer sistema, rede ou conta.
- Interferir com ou negar serviço a outros utilizadores ou sistemas, incluindo através de ataques de negação de serviço (DoS).
- Divulgar informações ou listas relativas a colaboradores, prestadores de serviços, parceiros ou clientes da Nors a entidades externas, sem autorização prévia da empresa.

15.2 E-mail e Atividades de Comunicação

Ao utilizar os recursos da empresa para aceder e utilizar a Internet, os utilizadores devem ter consciência de que representam a Nors e, como tal, devem agir de forma responsável e em conformidade com as políticas da empresa.

As seguintes atividades são estritamente proibidas, sem exceção:

- Envio de mensagens de correio eletrónico não solicitadas, incluindo o envio de spam, publicidade ou qualquer outro material promocional para pessoas que não tenham solicitado explicitamente essa informação.
- Qualquer forma de assédio através de e-mail, telefone ou mensagens de texto, seja através da linguagem utilizada, da frequência ou da dimensão das mensagens enviadas.
- Utilização não autorizada ou falsificação de informações no cabeçalho de mensagens de correio eletrónico.
- Solicitação ou redirecionamento de respostas para endereços de e-mail diferentes do endereço do autor da mensagem, com o objetivo de assediar terceiros ou obter respostas de forma indevida.
- Criação ou disseminação de correntes de e-mail, esquemas em pirâmide, esquemas de enriquecimento rápido ou qualquer outro tipo de esquema semelhante.
- Utilização de e-mails não solicitados originados nas redes da Nors ou através de serviços que atuem ou anunciem em nome da empresa.

15.3 Outras Políticas e Procedimentos Incorporados por Referência

A equipa é responsável por ler e cumprir todas as políticas relevantes às suas funções e responsabilidades.

Função	Propósito
Instrução Funcional - Gestão Acessos	Limitar o acesso a informações e sistemas de processamento de informações, redes e instalações.
Instrução Funcional — Plano de Continuidade de Negócios e Recuperação de Desastres (BCP & DRP)	Preparar a Nors para o caso de interrupções prolongadas de serviço causadas por fatores fora de controlo e restaurar os serviços da forma mais ampla possível num prazo mínimo.
Política de Criptografia	Garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, a autenticidade e/ou a integridade das informações.
Instrução Funcional - Plano de Resposta a Incidentes (IRP)	Política e procedimentos para incidentes de segurança da informação suspeitos ou confirmados.
Política de Acesso e Trabalho Remoto	Estabelecer requisitos de segurança para o trabalho remoto, assegurando que o acesso aos sistemas e dados da Nors é realizado de forma segura.
Política de Endpoint	Estabelecer medidas para prevenir, detetar e responder a malware, incluindo vírus, ransomware e outras ameaças.
Instrução Funcional - Logging	Definir os requisitos para geração, recolha, retenção e monitorização de logs, garantindo a deteção de incidentes e conformidade com requisitos de auditoria.
Política de Uso Aceitável (PUA)	Definir as regras e responsabilidades para a utilização adequada dos sistemas de informação, equipamentos e recursos tecnológicos da Nors.
Instrução Funcional - Gestão de Vulnerabilidades	Definir os processos para identificação, avaliação, priorização e remediação de vulnerabilidades em sistemas, aplicações e infraestruturas.
Instrução Funcional - Backup	Estabelecer os requisitos para a realização, retenção, proteção e teste de cópias de segurança da informação e sistemas críticos.
Instrução Funcional - Desenvolvimento Seguro	Definir os requisitos de segurança a integrar ao longo do ciclo de vida de desenvolvimento de software (SDLC).

16. Comunicação e Disponibilização da Política

A presente Política de Segurança da Informação deve ser comunicada a todos os colaboradores da Nors e, quando aplicável, a prestadores de serviços, consultores, estagiários e terceiros com acesso à informação, sistemas, equipamentos ou recursos tecnológicos da organização.

A comunicação da política pode ser realizada através de:

a) publicação em repositório documental interno;
b) publicação em intranet ou portal corporativo;
c) comunicação por email corporativo;
d) ações de formação e sensibilização;
e) sessões de onboarding;
f) comunicações internas da organização;
g) outros meios definidos pela Nors.

Sempre que aplicável, a Nors poderá manter evidência da comunicação, tomada de conhecimento, leitura ou aceitação desta política por parte dos destinatários.

A presente política, ou uma versão resumida adequada, pode ser disponibilizada a partes interessadas relevantes, incluindo clientes, fornecedores, parceiros, auditores, entidades reguladoras ou outras entidades autorizadas, sempre que apropriado e de acordo com os critérios definidos pela Nors.

A disponibilização externa da política deve respeitar os requisitos de confidencialidade, classificação da informação, proteção de dados e aprovação interna aplicáveis.

17. Revisão, Monitorização e Melhoria Contínua

A Nors compromete-se com a melhoria contínua do SGSI, assegurando que esta política, os processos, os controlos e os objetivos de segurança da informação são revistos e melhorados periodicamente.

A eficácia do SGSI deve ser acompanhada através de mecanismos adequados, incluindo, entre outros:

a) monitorização dos objetivos de segurança da informação;
b) acompanhamento de indicadores e métricas de segurança;
c) realização de avaliações de risco;
d) análise de incidentes de segurança da informação;
e) auditorias internas e externas;
f) revisão de controlos de segurança;
g) acompanhamento de planos de ação;
h) tratamento de não conformidades;
i) implementação de ações corretivas;
j) identificação e tratamento de oportunidades de melhoria;
k) revisão periódica pela gestão.

Esta política deve ser revista pelo menos anualmente ou sempre que ocorram alterações significativas, incluindo:

a) alterações no contexto interno ou externo da organização;
b) alterações relevantes nos riscos de segurança da informação;
c) alterações legais, regulamentares, contratuais ou normativas;
d) alterações na estrutura organizacional;
e) alterações em processos, sistemas, tecnologias ou fornecedores críticos;
f) ocorrência de incidentes relevantes;
g) resultados de auditorias;
h) alterações nos objetivos de segurança da informação;
i) identificação de oportunidades de melhoria.

Sempre que sejam identificados desvios, não conformidades, fragilidades ou oportunidades de melhoria, devem ser definidas, implementadas e acompanhadas ações corretivas ou de melhoria adequadas.

18. Violações e cumprimento da política

Qualquer violação desta política deve ser comunicada ao Gestor de Cibersegurança via email. As violações desta política podem resultar na perda imediata de privilégios de sistema e rede, além de ações disciplinares conforme os procedimentos internos da empresa, incluindo a possibilidade de demissão.

19. Histórico de versões

Versão	Data	Autor(a)	Aprovado por
1.0	28/04/2026	Nelson Rocha	Administração