AUTORIDADE NACIONAL DE SEGURANÇA RODOVIÁRIA

POLÍTICA DE SEGURANÇA
DA INFORMAÇÃO

HOMOLÓGO

Assinado por: **RUI PAULO SOARES RIBEIRO**
Num. de Identificação: 06218240
Data: 2023.12.31 10:07:46+00'00'
Certificado por: **Diário da República Eletrónico**
Atributos certificados: **Presidente - Autoridade Nacional de Segurança Rodoviária**

DEZEMBRO.2023

AUTORIDADE NACIONAL SEGURANÇA RODOVIÁRIA

FICHA TÉCNICA

PLANO DE SEGURANÇA DA INFORMAÇÃO

AUTORIA

Autoridade Nacional de Segurança Rodoviária

Avenida de Casal de Cabanas, n.º 1

2734-507 Barcarena

mail@ansr.pt

www.ansr.pt

CONCEÇÃO TÉCNICA

Divisão de Apoio ao Desenvolvimento Organizacional

Núcleo de Informática

DATA DE EDIÇÃO

Dezembro 2023

Índice

LISTAGEM DE SIGLAS

ANSR	Autoridade Nacional de Segurança Rodoviária
SI	Sistema de Informação
RNSI	Rede Nacional de Segurança Interna
QNRCS	Quadro Nacional de Referência para a Cibersegurança
CNCS	Centro Nacional de Cibersegurança
DADO	Divisão de Apoio e Desenvolvimento Organizacional
NIF	Núcleo de Informática
COSI	Centro Operacional de Segurança Informática
VPN	Virtual Private Network
RCS	Responsável de Cibersegurança

INTRODUÇÃO

A Autoridade Nacional de Segurança Rodoviária, doravante designada por ANSR, é um serviço da Administração Pública Central do Estado que tem por missão o planeamento e coordenação da segurança rodoviária, bem como a aplicação do direito contraordenacional rodoviário.

A Cibersegurança é a prática de proteger as redes e os sistemas de informação no ciberespaço, doravante designado por SI, através de medidas de prevenção, monitorização, deteção, análise e correção, garantindo a confidencialidade, integridade e disponibilidade da informação e dos sistemas.

A ANSR, apesar de ter os seus sistemas de informação na dependência direta da Rede Nacional de Segurança Interna, doravante designada por RNSI, está empenhada em garantir que os seus ativos, procedimentos e sistemas estão em conformidade com o disposto na Lei n.º 46/2018, de 13 de agosto, e no Decreto-Lei n.º 65/2021, de 30 de julho, que a regulamenta.

A presente política foi escrita com base nas diretrizes do *Quadro Nacional de Referência para a Cibersegurança (QNRCS), Centro Nacional de Cibersegurança (CNCS)*, que dá cumprimento à Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 23 de maio.

ÂMBITO

A presente Política de Segurança da Informação visa estabelecer um quadro de Cibersegurança que, por um lado, sistematize um conjunto de medidas e orientações destinadas a prevenir incidentes de segurança informática e, por outro, reduza o risco associado a ciberameaças, designadamente, no tocante à salvaguarda da informação e dos sistemas de informação (SI) da ANSR.

O âmbito de aplicação desta Política compreende os colaboradores, estagiários, prestadores de serviços e outros parceiros da ANSR e aplica-se a todos os seus ativos tecnológicos (em operação ou inativos), bem como a todas as áreas de funcionamento da ANSR cuja atuação tenha impacto na Cibersegurança.

OBJETIVOS

A presente Política de Segurança da Informação tem como objetivos:

- Cumprir com as obrigações legais e regulamentares aplicáveis à ANSR, nomeadamente, em matéria de Cibersegurança;
- Assegurar a disponibilidade, integridade e confidencialidade dos seus ativos;
- Identificar as vulnerabilidades e ameaças de segurança a que os seus Sistemas de Informação estão expostos;
- Habilitar a organização com ferramentas que possibilitem a gestão do risco de forma sistematizada;
- Garantir a existência de mecanismos de acesso e proteção, que forneçam a segurança da informação e dos SI;

- Garantir a deteção de incidentes que coloquem em causa o correto funcionamento dos SI e estabelecer procedimentos que garantam a continuidade do negócio, bem como a recuperação de processos e serviços;
- Estabelecer um conjunto de linhas orientadoras que protejam os colaboradores da ANSR no ciberespaço;
- Promover a melhoria continua dos SI, incluindo a Cibersegurança no desenho e implementação dos seus sistemas.

RESPONSABILIDADES

O Presidente da ANSR é responsável por manter a presente política de Cibersegurança atualizada e assegurar a sua execução, garantido os meios técnicos e financeiros para cumprir com os objetivos propostos.

A Divisão de Apoio e Desenvolvimento Organizacional, doravante designada por DADO, no âmbito das atribuições que lhe estão cometidas, pode propor ao Presidente da ANSR alterações à presente política, bem como a todos os documentos e estratégias implementadas no âmbito da Cibersegurança.

É dever da DADO, através do Núcleo de Informática, doravante designado por NIF, informar a RNSI, na plataforma de *ticketing* (SMAX) disponibilizada por aquela entidade, sempre que se verifique um incidente de segurança, disponibilizando-se para fornecer toda e qualquer informação solicitada pelo Centro Operacional de Segurança Informática (COSI) da RNSI, bem como para prestar todo o apoio necessário à mitigação do incidente.

Constitui-se ainda, responsabilidade da DADO:

- Propor a nomeação de um ponto de contacto permanente com o CNCS;
- Propor a nomeação de um responsável pela Cibersegurança (RCS).

É competência do Presidente da ANSR a aprovação dos mesmos.

A ANSR deve comunicar ao CNCS, no prazo de 20 dias úteis, o ponto de contacto permanente e o responsável pela Cibersegurança (RCS).

No âmbito das suas funções, o RCS nomeado deverá:

- Assegurar a implementação de boas práticas de segurança que mantenham a integridade, confidencialidade e disponibilidade da informação e sistemas da ANSR;
- Promover ações de formação e sensibilização em Cibersegurança;
- Desenvolver políticas e procedimentos de segurança da informação e Cibersegurança;
- Desenvolver um Plano de Segurança;
- Participar na gestão de incidentes;
- Garantir a execução da gestão do risco;
- Avaliar o desempenho de todos os procedimentos de segurança da informação e Cibersegurança implementados e propor medidas de melhoria dos mesmos;
- Desenvolver um relatório anual, nos termos definidos no artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho.

O ponto de contacto permanente deverá assegurar os fluxos de informação a nível operacional e técnicos, previstos no artigo 4.º do Decreto-Lei n.º 65/2021, de 30 de julho com o CNCS.

RECOMENDAÇÕES DE SEGURANÇA

Todos os colaboradores da ANSR são responsáveis pela proteção dos ativos da organização, devendo, no âmbito das suas funções, conhecer as suas responsabilidades na mitigação de riscos de segurança, zelando pela integridade, confidencialidade e disponibilidade da informação e sistemas da ANSR.

Responsabilidades de Cibersegurança

- Os colaboradores são responsáveis pela proteção e uso adequado dos equipamentos informáticos que lhe são atribuídos pela ANSR, devendo estes ser utilizados exclusivamente para fins profissionais;
- Todas as senhas utilizadas devem ter um mínimo de 12 caracteres, incluindo uma combinação de letras maiúsculas, minúsculas, números e símbolos. É imperativo que cada senha seja única e não reutilizada em diversas contas ou serviços. A política exige a alteração das senhas a cada 90 dias, sem repetir as últimas cinco utilizadas. A partilha de senhas é proibida, assim como a sua anotação em locais inseguros. Recomenda-se vivamente a utilização da autenticação vários fatores (no mínimo dois), sempre que disponível, para reforçar a segurança. Em caso de suspeita de comprometimento de uma senha, o utilizador deve proceder à sua imediata alteração e reportar o incidente à equipa de segurança da informação.
- É obrigatório o uso de VPN no acesso aos SI fora das instalações da ANSR;
- Aquando do exercício das suas funções em teletrabalho, é expressamente proibido aos trabalhadores da ANSR o uso de redes WI-FI públicas (redes WI-FI de cafés, centros comerciais e outros lugares que representem um elevado risco de Cibersegurança);
- Em caso de receção de e-mail fraudulento o colaborador não deve abrir qualquer ficheiro anexo ao mesmo, deverá, no entanto, enviar o e-mail fraudulento como anexo para o endereço de correio eletrónico suporteTI@ansr.pt;
- As falhas no funcionamento dos SI ou suspeita de vírus/*malware* devem ser comunicadas ao NIF, através da sua plataforma de *ticketing*;
- É expressamente proibido o acesso a sites da Internet ou o download de ficheiros que possam colocar em causa a integridade da infraestrutura tecnológica, devendo, em caso de dúvida, contactar-se a equipa de suporte do NIF para aferir a existência de risco de segurança.

Responsabilidades de Segurança da Informação

- É fornecido um correio eletrónico a cada colaborador, que deverá ser utilizado apenas para fins profissionais, sendo o trabalhador responsável pelo conteúdo das comunicações/mensagens realizadas;
- O uso de correio eletrónico destina-se apenas a fins profissionais, sendo o seu uso para fins pessoais permitido, na medida do estritamente necessário;
- É proibida a partilha de correio eletrónico que contenha *malware* e a disseminação de spam ou outros atos fraudulentos (por exemplo, *Phishing*);
- Não seguir ligações (*links*) de e-mails suspeitos;
- É recomendado o bloqueio do computador sempre que o trabalhador se afaste do seu posto de trabalho;
- É recomendado aos colaboradores seguirem uma política de “Clean Desk”, guardando de forma segura documentos, pen-drives, discos externos e outros acessórios amovíveis da ANSR, sempre que se ausentem dos seus postos de trabalho, evitando acessos não autorizados;
- O uso de impressoras e digitalizadoras da ANSR destinar-se apenas para fins profissionais, qualquer documento que seja impresso deve ser retirado da impressora de forma imediata, evitando leituras não autorizadas dos mesmos;
- Todos os colaboradores, fornecedores e prestadores de serviço da ANSR que, em virtude das suas funções, tenham acesso a dados pessoais ou a qualquer informação obtida durante o exercício das suas funções, estão a obrigados a manter o sigilo sobre os mesmos, protegendo a sua confidencialidade, salvo obrigação legal.

PROTEÇÃO DE DADOS PESSOAIS

No âmbito de todas as atividades de tratamento de dados pessoais realizadas pela ANSR no cumprimento das suas atribuições devem ser observados os princípios, regras e práticas estabelecidos no Regulamento Interno de Proteção de Dados Pessoais da ANSR em vigor à data do tratamento.

OBJETIVOS DE SEGURANÇA

1 - Identificar

1.1 – Gestão de Ativos

A ANSR reconhece a importância dos seus ativos (i.e. dados, colaboradores, equipamentos, sistemas, plataformas, aplicações e instalações), mantendo-os, por isso, devidamente identificados, inventariados e protegidos de acordo com o seu valor e criticidade. Sempre que se justifique, para equipamentos, sistemas, plataformas e aplicações, deve ser nomeado um responsável pelo ativo.

Cada ativo deve ser inventariado com base nas regras definidas no artigo 4.º do Regulamento n.º 183/2022.

O inventário de ativos deve ser assinado pelo responsável pela Cibersegurança e enviado anualmente para CNCS através do endereço eletrónico sri@cncs.pt, juntamente com o relatório anual.

1.2 – Classificação de Informação

A classificação de informação é um processo focado em garantir o nível adequado de proteção de dados, assim sendo, deve ser assegurada a correta classificação de toda a informação, de acordo com o seu valor, criticidade, sensibilidade e requisitos legais, com base nos seguintes níveis de classificação:

- Confidencial (nível mais elevado de confidencialidade);
- Restrito (nível médio de confidencialidade);
- Uso Interno (nível mais baixo de confidencialidade);
- Público (informação disponível para todos).

1.3 – Gestão de Fornecedores

No âmbito dos contratos celebrados com a ANSR, é obrigação dos prestadores de serviço, fornecedores e outras entidades externas seguir as orientações da presente política.

Todos os contratos celebrados com fornecedores e/ou prestadores de serviço que impliquem, durante o seu desenvolvimento, o acesso a informação e/ou sistemas da ANSR, devem incluir cláusulas de confidencialidade que abranjam os seus colaboradores e garantam a não divulgação de qualquer informação relativa à organização.

É responsabilidade dos fornecedores reportar todo e qualquer incidente de Cibersegurança à ANSR.

1.4 – Gestão do Risco

Deve ser assegurada a execução de uma estratégia de gestão do risco, que seja seguida de forma transversal por toda a organização e, não menos importante, garanta a gestão sistemática de todo o ciclo de vida dos riscos.

A gestão do risco deve considerar os seguintes aspetos:

- Identificação e documentação de vulnerabilidades que coloquem em causa os seus ativos;

- Análise das ameaças e vulnerabilidades, estabelecendo critérios para avaliar a probabilidade e o impacto das mesmas e assim calcular o nível de risco associado e definir a resposta mais adequada ao nível aferido;
- Tratamento dos riscos de acordo com a avaliação do nível de risco associado e o procedimento a seguir. Poderão ser seguidas quatro abordagens para minimização de danos, nomeadamente:
  - › Evitar o risco: reduzir a probabilidade de ocorrência do risco ou o seu impacto;
  - › Aceitar o risco: aceitação do risco deve ser sempre reconhecida pela ANSR;
  - › Mitigar o risco: implementação de medidas de controlo que limitem o impacto de ameaças ou vulnerabilidades;
  - › Transferir o risco: transferir para terceiros o impacto de uma ameaça.

2 - Proteger

2.1 – Controlo de Acessos

Todas as credenciais estão vinculadas à identidade dos colaboradores, estando implementados mecanismos de autenticação que permitem a manutenção da integridade e confidencialidade da informação.

De modo a reduzir, ao máximo, o risco de incidentes de segurança todas as credenciais atribuídas a colaboradores, fornecedores, prestadores de serviços e outras entidades externas devem ser emitidas, geridas, verificadas, revogadas e auditadas de acordo com o princípio de menor privilégio e segregação de funções.

A ANSR, nos termos legalmente exigidos, deve proceder à verificação das referências/antecedentes de novos colaboradores.

2.2 – Controlo de Acessos Remotos

Todos os acessos remotos à rede e sistemas da ANSR são cifrados e seguros, sendo efetuados através de aplicação disponibilizada pela RNSI, estando os mesmo devidamente documentados e controlados.

A atribuição e revogação de VPNs está sujeita a regras e restrições sendo sempre necessário uma autorização formal do responsável de unidade orgânica.

2.3 – Controlo Físico

A ANSR tem implementadas medidas de segurança física, as quais, se aplicam aos colaboradores e aos visitantes das instalações, destinadas a impedir o acesso não autorizado às instalações e garantir a proteção de todos os ativos de informação, instalações, postos de trabalho e colaboradores da organização, mantendo, ainda, o registo de entradas e saídas de pessoas externas.

Toda a informação confidencial, redes e sistemas de informação estão alojados em espaços protegidos por barreiras físicas e controlo de acessos baseado em cartões de identificação NFC. Apenas colaboradores devidamente autorizados podem aceder a estes espaços.

A ANSR segue todas as políticas e regulamentos contra desastres naturais, falhas de energia, incêndios e inundações, tendo implementado mecanismos que asseguram a proteção dos seus SI e colaboradores.

2.4 – Formação e Sensibilização

A ANSR deve promover a formação e sensibilização dos seus colaborados para a Cibersegurança, através do desenvolvimento de ações de formação que abordem diferentes temáticas da segurança digital e assim contribuir para a segurança dos trabalhadores e da organização durante o uso do ciberespaço.

2.5 – Controlo de Desenvolvimento de Aplicações

Todos os desenvolvimentos de novos aplicativos/aplicações, bem como todas as manutenções evolutivas dos seus sistemas, devem seguir as melhores práticas da indústria, devendo ser realizados testes em ambiente de qualidade antes da aceitação de qualquer solução em produção.

Deve ser assegurado o desenvolvimento e evolução dos SI de forma segura, nomeadamente, através do uso de sistema de controlo de versões.

Os ambientes de desenvolvimento, qualidade e produção devem estar separados de forma física e lógica, sendo os acessos a cada ambiente realizados de forma independente. Apenas a RNSI tem acesso aos ambientes de produção, estando garantida a confidencialidade, integridade e disponibilidade dos dados e SI.

2.6 – Segurança dos dados

Os sistemas de informação devem proteger a confidencialidade e integridade dos dados a cargo da ANSR, esta proteção deve aplicar-se em toda a linha, devendo garantir o transporte de informação de forma segura e de acordo com a sua classificação.

Devem ser definidos controlos de segurança que detetem e impeçam a fuga não autorizada de informação das suas instalações e sistemas.

Os procedimentos de eliminação de informações de forma segura devem ser aplicados com base na norma ISO/IEC 27001:2013.

3 - Detetar

No âmbito da sua atividade, a ANSR reconhece a importância da identificação, análise e tratamento de vulnerabilidades de segurança nos seus SI, e das possíveis consequências legais, financeiras e de reputação ,submetendo os SI a auditorias de segurança efetuadas pela RNSI.

Igualmente, todos os SI estão projetados tendo em consideração a segurança, produzindo *logs* de erros e de outros eventos relevantes que permitam, em caso de falha, repor o correto funcionamento do serviço. Sempre que possível, serão também implementadas plataformas de monitorização dos SI, que disponibilizem informações relevantes e ferramentas de alarmística que notifiquem as partes interessadas.

As auditorias efetuadas pela equipa do COSI da RNSI identificam, avaliam e documentam vulnerabilidades de segurança que coloquem em causa a confidencialidade, integridade e disponibilidade dos SI da ANSR, sendo estabelecidas propostas de resolução de vulnerabilidades identificadas.

Todas as vulnerabilidades encontradas são tratadas de acordo com o nível de severidade definido nos relatórios de análise realizados pela RNSI.

A ANSR encontra-se na dependência direta da RNSI, estando a monitorização da rede a cargo desta última.

4 – Responder

De forma a garantir a resiliência dos SI, a ANSR deve assegurar um conjunto de procedimentos de segurança que possibilitem a minimização de impactos e perdas durante incidentes e desastres, de modo a garantir a disponibilidade da informação e dos sistemas.

4.1 – Plano de Resposta e Recuperação de Incidentes

O plano de resposta e recuperação de incidentes deve implementar o procedimento de notificação de incidentes ao CNCS de acordo com os termos dos artigos 11.º e 16.º do Decreto-Lei n.º 65/2021, de 31 de julho de 2021 e sistematizar procedimentos de identificação, análise, categorização e tratamento de incidentes, para garantir uma correta alocação de recursos sempre que se verifique a necessidade de conter e mitigar incidentes. Neste plano deve ser estabelecido

4.2 – Plano de Continuidade de Negócio

Deve estar implementado um plano de continuidade de negócio que, perante qualquer incidente que afete a infraestrutura, a informação ou os SI, permita à ANSR continuar a operar dentro dos seus níveis *standard* de serviço, minimizando o impacto do incidente.

4.3 – Plano de Comunicação

Para uma resposta rápida e eficaz na deteção, contenção e resolução de incidentes, os procedimentos de comunicação de incidentes devem estar devidamente identificados, sendo transversais a toda a ANSR.

5 – Recuperar

5.1 – Melhoria Continua

Os planos de resposta/recuperação e o plano de continuação de negócio devem ser testados de forma periódica com o intuito de aferir a eficácia dos mecanismos de resposta e recuperação, identificar pontos de falha e projetar melhorias aos procedimentos já implementados. Estes planos devem ainda incorporar lições aprendidas após a sua execução garantido o rigor, aplicabilidade e resultados das atividades de recuperação.

Numa ótica de melhoria contínua, todos os procedimentos de segurança descritos serão periodicamente revistos, garantindo que continuam atualizados face a possíveis alterações legais ou regulamentares.

Deve ser executada, anualmente, uma auditoria aos procedimentos de segurança implementados na ANSR que verifique e garanta a conformidade dos mesmos em relação a esta política e com o disposto na Lei n.º 46/2018, de 13 de agosto, e no Decreto-Lei n.º 65/2021, de 30 de julho, que a regulamenta.

5.2 – Cópias de Segurança

A ANSR, em conjunto com a RNSI, realiza cópias de segurança das suas bases de dados de rede com vista a garantir a integridade, confidencialidade e disponibilidade dos dados. As cópias de segurança têm como objetivo garantir a segurança dos dados, a rápida recuperação dos mesmo se eventualmente forem perdidos e garantir o restauro das bases de dados se necessário.

INCUMPRIMENTO

Todos os colaboradores, estagiários, prestadores de serviços e outros parceiros da ANSR que, deliberadamente, violem esta política ficam sujeitos à aplicação de medidas disciplinares, sanções contratuais, cessação contratual e/ou à participação às autoridades policiais e judiciais das situações que indiciem a prática de crime.

APROVAÇÃO E REVISÃO

A Política de Segurança da Informação é aprovada pelo Presidente da ANSR e deve ser revista sempre que se verifique alguma alteração no âmbito da Cibersegurança, na organização interna da ANSR ou no enquadramento legal aplicável, bem como nas melhores práticas a observar.

VIGÊNCIA E VALIDADE

A presente Política entrará em vigor no dia seguinte à sua aprovação, devendo ser objeto de publicitação junto de todas as partes interessadas através da *Intranet* e da página da *Internet* da ANSR,