ERSE
ENTIDADE REGULADORA
DOS SERVIÇOS ENERGÉTICOS

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

novembro 2019

Título: Política Geral de Segurança da Informação
Edição: ERSE
Entidade Reguladora dos Serviços Energéticos
novembro 2019

Índice

CONTROLO DE VERSÕES E HISTÓRICO DO DOCUMENTO

Controlo de versões

Título	Política Geral de Segurança da Informação		
Autor	Direção de Administração Geral		
Versão	2.0	**Data Versão**	25-11-2019
Revisto/Validado por	Ana Peralta	**Data Revisão/Validação**	25-11-2019
Aprovado por	Conselho de Administração	**Data Aprovação**	09-12-2019
		Nº Total Páginas	16

Histórico do Documento

Versão	Data	Elaborado/Verificado/Aprovado	Descrição das alterações efetuadas
1.0	31-10-2017	Direção de Administração Geral	Documento base
2.0	25-11-2019	Ana Peralta / Elvira Carlota	Alteração do capítulo "Conceitos", para "Termos e Definições". Inclusão de um capítulo de Introdução, incluindo os anteriores de Objetivo e Âmbito e Audiência, de forma a uniformizar com as restantes políticas Alteração da nomenclatura definida para as Políticas Setoriais, e inclusão de duas novas políticas

Lista de Distribuição

UO	Responsável
Toda a ERSE	N/A

TERMOS E DEFINIÇÕES

Nesta política considera-se a definição dos seguintes conceitos:

- *Informação* – qualquer recurso resultante do processamento, manipulação e organização de dados ou outros elementos que represente conhecimento.

- *Formato de Informação* – A informação poderá existir de forma estruturada (em estruturas de dados) ou não estruturada (texto, conhecimento, voz) em formato eletrónico (documento eletrónico, aplicação, *datamart*, site) ou físico (impressa ou manuscrita, transmitida por correio ou meios vocais).

- *Ciclo de Vida da Informação* - Momentos relevantes da existência da informação desde a sua criação, à sua transmissão, manutenção e destruição.

- *Ativo de Informação* - Toda a informação e quaisquer outros dispositivos que processam, transmitem ou armazenam informação com valor para a ERSE, nomeadamente aplicações de negócio e outro tipo de software, redes de dados, servidores e computadores pessoais, pessoas, instalações.

- *Colaboradores* - Todos aqueles que colaboram com a ERSE enquanto profissionais, formadores, consultores, trabalhadores, trabalhadores temporários ou outros.

- *Segurança da Informação* – Mecanismos de proteção da informação em todos os seus formatos e em todas as fases do seu ciclo de vida, no sentido de preservar o valor que possui para o indivíduo ou para a ERSE.

- *Incidentes de Segurança de Informação* – Toda e qualquer ocorrência que compromete os princípios de segurança da informação com prejuízo financeiro, reputacional ou operacional para a ERSE.

- *Sistema de Gestão de Segurança da Informação* - Processo permanente de avaliação de riscos, implementação de controlos, monitorização e melhoria contínua relacionada com a proteção dos ativos de informação.

1 INTRODUÇÃO

1.1 OBJETIVOS E ÂMBITO

A informação assume um papel crítico no desenvolvimento e sustentabilidade das atividades da ERSE, pelo que incidentes de segurança da informação poderão ter impactos relevantes a nível reputacional, operacional, financeiro ou outros.

A crescente exposição a ameaças, internas ou externas, exige uma regulamentação clara das matérias de Segurança de Informação e o empenho de todos na sua aplicação.

A Política Geral de Segurança da Informação, descrita neste documento, tem como principal missão estabelecer as diretrizes globais de Segurança de Informação (SdI) para a ERSE e assim:

- Contribuir para a manutenção da confiança dos colaboradores, parceiros, consumidores e entidades dos setores na capacidade da ERSE em proteger a informação sob a sua responsabilidade;
- Assegurar que os ativos de informação estão protegidos de processos de utilização, divulgação, alteração ou destruição não autorizados, de forma consistente com a sua importância e sensibilidade;
- Garantir uma capacidade de resposta eficaz a eventuais incidentes de segurança da informação, minimizando o respetivo impacto financeiro, reputacional e operacional;
- Respeitar as obrigações legais e regulamentares respeitantes à atividade da ERSE face a questões de Segurança da Informação.

1.2 AUDIÊNCIA

Em conformidade com as melhores práticas internacionais e com a legislação e regulamentação em vigor, a Política Geral de Segurança da Informação estabelece (i) os grandes princípios orientadores, (ii) a estruturação da Política de Segurança da Informação pelos vários domínios de atuação, (iii) a responsabilidade por esta função na ERSE, e é aplicável:

- À estrutura orgânica da ERSE;
- A todos os colaboradores da ERSE e entidades externas com acesso aos ativos de informação da ERSE;
- A todos os ativos de informação que se encontrem sob a jurisdição ou responsabilidade da ERSE, independentemente do formato que a informação possa adotar e fase do seu ciclo de vida.

2 ESTRUTURA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação na ERSE é suportada por uma estrutura Normativa devidamente hierarquizada:

- Política Geral de Segurança da Informação,
    - Políticas Sectoriais de Segurança da Informação
        - Normas, Procedimentos e Configurações de Segurança da Informação

A Política Geral de Segurança da Informação, definida no presente documento, estabelece os princípios globais através dos quais os ativos de informação devem ser protegidos, as grandes orientações a seguir e as responsabilidades pela sua aplicação.

As Políticas Sectoriais de Segurança da Informação (nível 2) formalizam as decisões de gestão, definições e regras para proteção dos ativos de informação nos diversos domínios relevantes da segurança da informação em conformidade com os requisitos de negócio e com a legislação e regulamentação relevantes. Estas políticas determinam o nível de segurança mínimo a ser obtido e estabelecem os critérios de avaliação dos resultados.

O 3º nível pretende operacionalizar as políticas sectoriais em Normas, Procedimentos e configurações específicas de Segurança da Informação em função dos diversos processos e tecnologias da Organização de forma a garantir o nível adequado de segurança da informação.

A Política Geral de SdI, as Políticas Sectoriais e os Procedimentos de SdI são desenvolvidos pela Direção de Administração Geral (DAG).

3 REGRAS ESPECÍFICAS ERSE

PRINCÍPIOS GERAIS

O Sistema de Gestão de Segurança da Informação da ERSE assenta num conjunto de princípios fundamentais a todos os domínios da Segurança da Informação:

1. Confidencialidade – Garantia da proteção contra o acesso não autorizado à informação.

2. Integridade – Garantia da correção e completude da informação e dos seus métodos de utilização, processamento e transporte.

3. Disponibilidade – Garantia do acesso à informação de pessoas ou processos autorizados, de acordo com os requisitos identificados pela ERSE.

4. Autenticidade - Garantia da identidade das pessoas ou processos que acedem ou emitem informação.

5. Não repudiação – Garantia de que o interveniente em qualquer troca de informação não será capaz de negar a sua participação no processo.

6. Privacidade – Garantia da utilização da informação pessoal de cada indivíduo com quem a ERSE se relaciona (entidades do sector, colaboradores, consumidores e prestadores de serviços) exclusivamente para os fins acordados ou permitidos pela lei.

Os princípios fundamentais da Segurança da Informação, acima mencionados, são completados por princípios transversais que contribuem para o Sistema de Gestão da Segurança da Informação adequado e que são:

1. Acesso Condicionado ao Desempenho - Acesso individual exclusivo aos ativos de informação necessários ao desempenho das funções;

2. Não dependência do Secretismo – Garantia que a implementação de mecanismos e controlos de segurança não dependem apenas do seu conhecimento por um grupo restrito de indivíduos;

3. Segurança em profundidade - Existência de controlos parcialmente sobrepostos nos vários níveis dos processos e nas várias camadas dos ativos de informação;

4. Segregação de funções - Separação real e permanente entre a autorização e a execução de cada processo, no âmbito da segurança de informação, por forma a garantir que ninguém, individualmente, tem controlo exclusivo sobre um ativo de informação ou processo associado;

5. Proporcionalidade - A aplicação dos princípios gerais de segurança da informação é proporcional ao risco do ativo de informação;

6. Homogeneidade - A gestão da segurança da informação deve adotar métodos e padrões globais, no universo da ERSE;

7. Resiliência - A conceção do Sistema de Gestão de Segurança da Informação deve garantir a robustez de todos os elementos envolvidos, pessoas processos e tecnologia.

8. Manutenção da confiança - O nível de proteção deve ser consistente em todas as componentes dos ativos de Informação.

4 POLÍTICAS SECTORIAIS DE SEGURANÇA DA INFORMAÇÃO

De acordo com as melhores práticas internacionais, os temas inerentes à Gestão da Segurança da Informação organizam-se em grandes domínios cujas políticas sectoriais sumariamente se descrevem:

A política de Gestão de Risco de Segurança da Informação descreve os requisitos e o modelo para a avaliação dos riscos de segurança da informação e a definição de planos de tratamento de risco adequados.

A política de Gestão de Ativos de Informação estabelece uma estrutura para a classificação de segurança de todos ativos de informação. Define, igualmente, o conjunto de controlos para garantir a disponibilidade, integridade, confidencialidade e, se necessário, a não repudiação da informação em função do seu nível de classificação.

A política de Gestão de Entidades Externas descreve os requisitos para a proteção da informação da ERSE quando esta é acedida, manuseada ou preservada por entidades ou pessoas externas à ERSE ou quando existe a partilha ou transferência de controlo de processos de negócio ou da gestão de sistemas de informação, que implicam um determinado grau de troca de informação, coordenação e confiança entre a ERSE e a entidade terceira.

A política de Gestão de Acessos define os requisitos de segurança a ser cumpridos na identificação, autenticação, autorização e registo do acesso dos utilizadores aos sistemas de informação em todas as fases do ciclo de vida do utilizador.

A política de Passwords estabelece as regras sobre a definição de passwords de utilizador, para o acesso a sistemas de informação.

A política de Utilização Aceitável dos Sistemas de Informação e Comunicação define as regras para uma utilização adequada dos sistemas de informação e serviços corporativos da ERSE postos à disposição de cada colaborador ou prestador de serviços, para suporte aos processos de negócio nomeadamente, aplicações, posto de trabalho, equipamentos, internet, correio eletrónico, correio físico, telefone.

A política de Segurança Física aborda as questões relacionadas com a segurança dos colaboradores, prestadores de serviços e todos os indivíduos que se relacionem com a ERSE incluindo, mas não limitado a, ações e procedimentos a desencadear sempre que alguém entra, muda de funções ou sai do universo ERSE.

A política de Gestão de Operações de Sistemas de Informação e de Comunicações define as regras de segurança para a exploração dos sistemas de informação e transmissão de informação da ERSE, incluindo os canais de comunicação estabelecidos com redes externas.

A política de Aquisição, Manutenção e Desenvolvimento dos Sistemas de Informação define os requisitos de segurança e controlos a ter nos processos de desenvolvimento, aquisição, manutenção evolutiva e corretiva de sistemas de informação.

A política de Backups, define os mecanismos a implementar para garantir a salvaguarda e recuperação de informação da ERSE, face a uma contingência.

A política de Gestão de Incidentes de Segurança define as categorias de incidentes de segurança da informação e estabelece as regras base para a gestão das ocorrências.

Sempre que necessário, cada política sectorial, traduzir-se-á em Normas ou outros documentos internos que espelharão regras específicas, procedimentos ou configurações, sendo a respetiva elaboração sujeita a critérios de exequibilidade, impacto na Organização, minimização de riscos e de avaliação de necessidades.

5 RESPONSABILIDADES NA SEGURANÇA DE INFORMAÇÃO

Compete ao Conselho de Administração da ERSE aprovar a Política Geral de Segurança de Informação e respetivas Políticas Sectoriais, bem como, patrocinar o Plano Global da Segurança de Informação, nomeadamente através da afetação dos meios humanos e financeiros necessários à implementação das iniciativas.

A DAG assume as responsabilidades de:

- Revisão e controlo da execução do Plano Global de Segurança da Informação;
- Manutenção e controlo da implementação das Políticas Gerais e Sectoriais de Segurança da Informação na ERSE e coordenação da sua operacionalização em Normas, Procedimentos e Configurações de Segurança;
- Produção e acompanhamento dos indicadores internos e externos de Segurança da Informação;
- Apoio às Unidades Orgânicas na avaliação do risco de Segurança da Informação, definição dos requisitos e preparação dos respetivos planos de mitigação;
- Gestão da atribuição de acessos a utilizadores internos ou externos;
- Promoção da consciencialização e sensibilização sobre a segurança da informação;
- Definição de uma arquitetura e respetiva utilização segundo os padrões de segurança de informação.

Na ERSE, cada Unidade Orgânica é responsável pelo respeito e aplicação das políticas de segurança da informação, no âmbito das suas funções, e pela:

- Execução e aplicação das normas, procedimentos e configurações relevantes;
- Definição de quais os perfis acesso a atribuir aos respetivos colaboradores;
- Classificação da sua informação.

A DAG será responsável pela (i) identificação, divulgação da legislação em matéria de Segurança da Informação, (ii) supervisão do ponto de vista legal de todos os contratos realizados com as entidades em matérias de segurança da Informação, (iii) registo das bases de dados junto das entidades, nacionais ou estrangeiras, que se afigurem competentes;

A área de Compliance, caso venha a existir, será responsável pela (i) divulgação e apoio à implementação da regulamentação em matéria de Segurança da Informação, (ii) gestão do ambiente de controlo interno associado à Segurança da Informação e (iii) garantia da conformidade das Políticas de Segurança da Informação com as normas legais relevantes.

Cada indivíduo é responsável pelas suas ações na medida em que estas estejam relacionadas com a proteção dos ativos de informação a que acede ou manuseie.

6 REVISÕES À POLÍTICA GERAL DE SEGURANÇA DE INFORMAÇÃO

A Política Geral de Segurança da Informação da ERSE é revista anualmente, ou sempre que ocorram alterações significativas na (i) Legislação e Regulamentação aplicável, (ii) Estratégias de alto nível ou de Sistemas de Informação e (iii) Alteração de níveis de risco, percecionados.

Todas as alterações à presente Política serão aprovadas pelo Conselho de Administração da ERSE e deverão ser publicadas e divulgadas a todos os colaboradores.

7 CONFORMIDADE

O cumprimento das Políticas de Segurança da Informação da ERSE é obrigatório.

Cada colaborador, interno ou externo, é individualmente responsável pelo conhecimento, compreensão e cumprimento das suas obrigações na correta utilização e proteção da informação da ERSE. As violações às políticas de segurança poderão originar processos disciplinares, bem como ações de natureza cível ou penal.

As exceções à presente política deverão ser previamente justificadas através de um processo formal de aceitação de risco. Todas as exceções às políticas de segurança da informação devem ser previamente autorizadas e formalmente registadas e monitorizadas.

Quaisquer dúvidas sobre o âmbito ou a aplicação da presente política, devem ser dirigidas ao Conselho de Administração da ERSE.

Serão implementadas medidas de carácter geral para monitorizar comunicações internas ou externas e/ou padrões de utilização e manuseamento da informação ou dos sistemas, sempre cumprindo estritamente a lei da proteção da privacidade individual.

Rua Dom Cristóvão da Gama, 1 – 3.º
1400- 113 Lisboa

Telefone: 213 033 200