ESCOLA SUPERIOR DE ENFERMAGEM DE COIMBRA

VERSÃO	MOTIVO DA REVISÃO	ELABORADO POR	APROVADO POR	DATA APROVAÇÃO
0.1	Criação e redação preliminar	Serviço de Informática	N/A	N/A
1.0	Redação final	Serviço de Informática	Responsável de Segurança	07/06/2023

Elaboração	Verificação	Aprovação
Serviço de Informática	Responsável de Segurança Dulce Silva	Presidente:
Data: 31 . 05 . 2023	Data: 07 . 06 . 2023	Data: 12 . 6 . 23

Regulamento de Segurança do Sistema de Informação

Escola Superior de
Enfermagem de Coimbra

ÍNDICE

Preâmbulo

A informação é considerada pela **Escola Superior de Enfermagem de Coimbra**, como um ativo estratégico, fundamental e de considerável valor para a prossecução da sua missão.

Dando cumprimento aos compromissos assumidos em sede de Politica de Segurança da Informação, elaborada em linha com os avanços legislativos nacionais: Lei 46/2021 e Decreto-lei 65/2021, e europeus: Diretiva (EU) 2022/2555, a Escola Superior de Enfermagem de Coimbra redigiu o presente Regulamento de Segurança da Informação por forma a garantir a confidencialidade, integridade e disponibilidade da informação, incluindo dados pessoais, evitando que esta seja, de modo acidental ou ilícito, perdida, destruída, alterada indevidamente ou acedida por quem não autorizado. Para tal, com este documento estabelecem-se os direitos e deveres dos Órgão da Escola e utilizadores do Sistema de Informação da Escola em todas as suas componentes, digitais e físicas.

CAPÍTULO I - DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto do Regulamento

O presente Regulamento objetiva definir as regras e práticas para assegurar a garantia de confidencialidade, privacidade, integridade, disponibilidade da informação gerida pelo sistema de informação da Escola Superior de Enfermagem de Coimbra, doravante identificada como **ESEnfC**, com vista à prevenção de ocorrência e mitigação do impacto de eventuais incidentes que possam comprometer o regular funcionamento da Escola, a violação da privacidade de dados pessoais e a demonstração permanente de conformidade legal aplicável.

O disposto no presente Regulamento observa de forma estrita a conformidade com a legislação e normativos em vigor em matéria de proteção de dados pessoais, criminalidade informática e segurança de redes, sistemas de informação e Cibersegurança, respetivamente, Regulamento (UE) 679/2016 de 27 de abril, Regulamento Geral sobre a Proteção de Dados, RGPD, Lei 58/2019 de 8 de agosto, execução nacional do RGPD, Lei n.º 46/2018 de 13 de agosto – Regime Jurídico da Segurança do Ciberespaço, Decreto Lei 65/2021 de 30 de julho e Lei 109/2009 de 15 de Setembro – Lei do Cibercrime.

Artigo 2.º

Âmbito do Regulamento

1. O Regulamento de Segurança do Sistema de Informação aplica-se a todos as pessoas autorizadas a aceder e a tratar informação da **ESEnfC**, independentemente do seu formato, físico ou digital, tendo como objetivo orientar ou regular as suas ações no domínio da segurança dos sistemas de informação.
2. O presente Regulamento aplica-se a toda a informação mantida e tratada sob a responsabilidade da **ESEnfC**, independentemente do seu suporte de registo: eletrónico ou digital, físico (incluindo papel), audiovisual, verbal ou outro.

Artigo 3.º

Definições

Regulamento da Segurança do Sistema de Informação – Documento que orienta ou regula as práticas que as pessoas ou sistemas no domínio da segurança do sistema de informação devem executar nas suas ações diárias;

Sistema de Informação - Conjunto integrado de componentes para recolha, armazenamento e processamento de dados, automatizado ou não, que suportem o fornecimento de informações e conhecimento a uma organização;

Confidencialidade - propriedade de que a informação não é disponibilizada ou divulgada a indivíduos entidades ou processos não autorizados;

Integridade - propriedade da exatidão da informação e dos seus métodos de processamento;

Disponibilidade - propriedade de ser acessível e utilizável quando necessária por uma entidade ou pessoa formalmente autorizada;

Tratamento de incidentes - todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente.

Não repudio – garantia que todos os utilizadores quando na condição de emissores de informação ou quando partilham dados pessoais com destinatários autorizados, serão sempre identificados física e/ou digitalmente com valor probatório legal.

Segurança de Sistemas de Informação – enquadramento organizacional de cultura, políticas, processos, procedimentos e estruturas organizacionais e ambiente operacional utilizado para assegurar a confidencialidade, privacidade, integridade, e disponibilidade da informação essencial de uma organização.

Segurança das redes e dos sistemas de informação - capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles;

Sistema informático - qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

Dados informáticos - qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

Incidente - um evento com um efeito adverso na segurança das redes e dos sistemas de informação;

Informação e ativo essenciais – informação e recursos que têm um valor crítico para a Escola como suporte ao normal desenvolvimento das suas atividades.

Artigo 4.º

Pessoa autorizada

Considera-se pessoa autorizada para efeitos do presente documento, as/os funcionárias/os da **ESEnfC**, as/os contratada/o(s), incluído corpo docente, as/os colaboradora/e(s) em regime de prestação de serviços e outros agentes que utilizem recursos da **ESEnfC** ou pessoais para aceder, armazenar, fazer *backup* ou realocar qualquer informação da Escola.

CAPÍTULO II - GESTÃO DE ACESSOS

Artigo 5º

Acesso à informação

A **ESEnfC** restringe o acesso à informação através da aplicação de controlos lógicos e físicos que garantam que:

1. O acesso à informação está restrito a quem necessita de a conhecer para a prossecução das suas competências - Necessidade de Conhecer;
2. O acesso a espaços físicos que contenham dados, quer em formato físico quer em formato digital, apenas deve ser concedido caso seja necessário para o desempenho das funções atribuídas - Necessidade de Uso.

Artigo 6º

Responsabilidades gerais da ESEnfC

1. Definir e manter um processo formal de disponibilização de contas de acesso do sistema de informação para atribuir, alterar ou revogar os direitos de acesso para todos os tipos de pessoa autorizada em todos os sistemas e serviços.
2. Garantir que o acesso a componentes do sistema de informação, dispositivos, aplicações, sistemas ou similares, é feito mediante um processo de autenticação auditável, podendo recorrer ao uso de credenciais de acesso, como nome de utilizador e palavra-passe ou equivalente, atribuídas pelo Serviço de Informática, com base em proposta de superior hierárquico, consoante o caso, responsável de órgão, responsável de unidade cientifico-pedagógica, dirigente de unidade diferenciada ou responsável de serviço.
3. Promover a atribuição de direitos de acesso e privilégio às componentes do sistema de informação, mediante a definição de perfis com privilégios mínimos e diferenciados, seguindo o princípio da necessidade de conhecer e aceder à informação.
4. Definir, aprovar e comunicar uma **Política de Uso Aceitável** de recursos do Sistema de Informação da ESEnfC.
5. Aprovar e comunicar, perante as partes interessadas definidas em sede de Plano de Segurança, uma Política de Segurança da Informação e uma Política de Privacidade e Tratamento de Dados Pessoais.

Responsabilidades - dirigentes

1. A/O dirigente de cada unidade organizacional da estrutura descrita no artigo 18º da versão vigente dos Estatutos da **ESEnfC**, nomeadamente: Órgão de Governo; outros órgãos; unidades cientifico-pedagógicas, unidades diferenciadas; estruturas de apoio e serviços, que superintenda cada pessoa autorizada, é responsável por definir as necessidades de acesso às componentes do sistema de informação e correspondente perfil de permissões.
    a. O Serviço de Informática (SI) é responsável pela criação de contas de correio eletrónico para toda a instituição e pela criação de utilizadores dentro da própria unidade.
    b. O serviço de Recursos Humanos e os Serviços Académicos mantêm responsabilidades conjuntas na criação de utilizadores na intranet e nas aplicações de gestão escolar.
    c. Os dados de saúde (dados considerados sensíveis) dos utilizadores do serviço de saúde escolar estão alojados na *Cloud*, sendo a Unidade Diferenciada de Ação Social Saúde Escolar e Saúde no Trabalho (UDASSEST) responsável pela definição de perfis de acesso ao sistema de suporte a este serviço. A criação efetiva dos acessos é da responsabilidade do SI, bem como a migração dos dados dos utilizadores do sistema.
    d. O Gabinete de Relações Nacionais e Internacionais é responsável pela definição de perfis de acesso ao sistema de suporte às candidaturas *Erasmus* (*Erasmus Without Paper)*, cujos dados estão alojados fora da ESEnfC, sendo a criação efetiva dos utilizadores da responsabilidade do SI.
    e. O Serviço de Documentação e Informação (CDI), ao abrigo de um protocolo celebrado entre a ESEnfC e o Serviço Integrado das Bibliotecas da Universidade de Coimbra, utiliza o sistema informático de empréstimos bibliográficos de modo a incluir no SIIB/UC as bases de dados bibliográficos da Escola. O SI é responsável quer pela criação dos

utilizadores solicitados pelo CDI quer pelo envio periódico dos dados dos utilizadores, que ficam alojados fora da Escola, para migração na aplicação.

2. As unidades organizacionais acima indicadas são responsáveis pela gestão do ciclo de vida dos acessos digitais, incluindo revisão e cancelamento de contas de pessoa utilizadora.
3. Os serviços responsáveis pela criação de acessos ao sistema de informação, mantêm um registo atualizado de contas de acesso ativas, bem como um histórico de contas entretanto desativadas, sempre que tecnicamente possível.

Responsabilidades – Serviço de Informática

1. O SI designa um número suficiente de recursos aos quais são concedidos acessos privilegiados para suporte das operações de gestão e administração de rede.
2. O SI é responsável pela manutenção dos sistemas de suporte a procedimentos automatizados para criação de contas do corpo discente.
3. O SI identifica e apresenta ao Presidente, eventual necessidade de recurso a prestadores de serviços externos, assegurando que a execução dos serviços esteja devidamente regulada por clausulado contratual que salvaguarde os requisitos específicos de segurança da Escola bem como o cumprimento de legislação aplicável.
4. O SI é responsável pela gestão da atribuição de equipamentos informáticos de uso individual, incluindo a entrega, recolha, eliminação segura de dados e restantes procedimentos de manutenção.

Responsabilidades – Serviços Administrativos: Recursos Humanos

1. O serviço de Recursos Humanos, da unidade Serviços Administrativos, comunica ao SI processos de cessação, ou outra alteração, da relação laboral, a fim de que o SI possa executar as diligências necessárias para suspensão, cancelamento ou adequação dos acessos atribuídos, bem como à recolha de eventuais equipamentos e implementação de ações de manutenção, salvaguardando informações de carater confidencial.

Responsabilidades – Serviço de Saúde Escolar

1. O serviço de Saúde Escolar, comunica ao SI processos de cessação de utilização do sistema de saúde escolar, a fim de que o SI possa executar as diligências necessárias para inativação das contas de acessos atribuídas.

Responsabilidades – Gabinete de Relações Nacionais e Internacionais

1. O Gabinete de Relações Nacionais e Internacionais comunica ao SI processos de cessação da necessidade de utilização do sistema *Erasmus Without Paper*, a fim de que o SI possa executar as diligências necessárias para inativação das contas de acessos atribuídas.

Responsabilidades – Serviço de Documentação e Informação

1. O Serviço de Documentação e Informação comunica ao SI processos de cessação da necessidade de utilização do sistema, a fim de que o SI possa executar as diligências necessárias para inativação das contas de acessos atribuídas.

CAPÍTULO III - DIREITOS, DEVERES E RESTRIÇÕES

Artigo 7.º

Direitos da pessoa autorizada

1. A pessoa autorizada tem direito à liberdade e privacidade no âmbito do processamento informático dos seus dados pessoais e no âmbito do trabalho técnico da sua responsabilidade e autoria. A **ESEnfC** disponibiliza, sempre que possível, redes abertas para uso pessoal. O uso em segurança destas redes é da responsabilidade da pessoa utilizadora seguindo política de uso aceitável.
2. A pessoa autorizada tem, ainda, os seguintes direitos:
    a. Direito de informação: No momento da recolha de dados pessoais, ou, caso a recolha de dados não seja feita diretamente junto de si, logo que os mesmos sejam tratados, a pessoa autorizada tem o direito de receber informação sobre:
        i. Qual a finalidade do tratamento;
        ii. Quem é responsável pelo tratamento dos dados;
        iii. A quem podem ser comunicados os seus dados;
        iv. Quais as condições em que pode aceder e retificar os seus dados.
    b. Direito de oposição:
        i. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, se feito com base na prossecução do interesse público ou exercício de autoridade pública, ou feito no interesse legítimo da **ESEnfC**;
        ii. A **ESEnfC** cessa eventual tratamento de dados pessoais, caso não apresente razões imperiosas e legítimas para o mesmo sobre o qual prevaleçam interesses, direitos e liberdades da pessoa autorizada.

Artigo 8.º

Deveres da pessoa autorizada

1. A pessoa autorizada deve respeitar sempre a liberdade e a privacidade alheias.
2. As pessoas autorizadas são responsáveis pelo correio eletrónico originado a partir de contas de *email* para as quais têm autorização de uso.
3. As pessoas autorizadas devem respeitar as boas práticas para a escolha ou composição de palavras-passe resilientes a ataques ou tentativas de acesso indevido, nomeadamente:
    a. Não usar como palavras-passe, palavras do dicionário, datas, ou outras facilmente associáveis à pessoa autorizada;
    b. Manter as palavras-passe confidenciais, recorrendo ao uso de *software* dedicado ou arquivo em ficheiros cifrados com acesso restrito;
    c. Não manter as palavras-passe escritas em papéis ou locais visíveis;
    d. Mudar as senhas regularmente, seguindo as orientações do SI
    e. Não gravar senhas de forma automática em aplicações acessíveis a partir de computadores partilhados;

f. As senhas de determinado sistema informático não devem ser reutilizadas em sistemas de diferente âmbito, mesmo que em contexto de uso na Escola;

g. Excetuam-se da alínea anterior, as senhas de utilização múltipla usadas em mecanismos de *single sign on* (serviços de autenticação que conectam a pessoa autorizada em várias aplicações);

h. Não reutilizar *passwords* em uso em sistemas da **ESEnfC** em contextos de uso pessoal.

Artigo 9.º

Restrições relacionadas com os acessos de cada pessoa autorizada

1. A pessoa autorizada não pode ceder as suas credenciais de acesso nem pode usar as credenciais de terceiros.
2. A pessoa autorizada é a única responsável pelo uso indevido dos seus privilégios de acesso e deverá comunicar imediatamente ao SI, alguma suspeita de uso indevido através dos canais de helpdesk.
3. A pessoa autorizada não deve partilhar os seus privilégios de acesso com terceiros, caso tal ocorra é considerado o único responsável pelo uso dos mesmos.
4. A pessoa autorizada não deve tentar executar acessos não autorizados.

Artigo 10.º

Restrições relativas à pessoa autorizada

1. A pessoa autorizada não pode interferir com dados, programas ou sistemas, nem intercetar informação de outra pessoa autorizada ou da **ESEnfC**.
2. A pessoa autorizada deve abster-se de atitudes que possam causar prejuízos morais ou materiais às restantes pessoas autorizadas e ao sistema de informação da **ESEnfC.**
3. A pessoa autorizada não pode, em circunstância alguma, proceder à ligação de novos equipamentos à rede informática sem prévio conhecimento e autorização do SI.
4. A pessoa autorizada não deve usar recursos informáticos para fins não relacionados com a missão dos serviços da Escola.
5. A pessoa autorizada não pode instalar aplicações, *software* ou similar, nem alterar a configuração das aplicações ou sistemas instalados, sem autorização prévia do SI.
6. A pessoa autorizada não pode realocar dispositivos ou equipamentos informáticos, sem autorização do SI.

SECÇÃO I - DO CORREIO ELETRÓNICO (E-MAIL)

Artigo 11.º

Responsabilidades

1. O Serviço de Informática é responsável pela gestão da infraestrutura de correio eletrónico, incluindo a implementação dos processos de criação e gestão de acessos a caixas de correio eletrónico.

2. O SI, conjuntamente com outras unidades organizacionais/encarregado/a de proteção de dados/responsável de segurança, deve promover ações de sensibilização para um uso seguro do sistema de correio eletrónico institucional.
3. Dever-se-á privilegiar o uso de contas de correio eletrónico que recorram a listas de distribuição na comunicação institucional com terceiros.

Artigo 12.º

Condicionantes à utilização do correio eletrónico (e-mail)

1. O uso do sistema de correio eletrónico institucional deve seguir os princípios gerais condizentes com o Código de Conduta da **ESEnfC**.

2. São interditos na utilização de correio eletrónico os seguintes procedimentos:
    a. Falsificar mensagens de correio eletrónico;
    b. Usar o endereço de *email* institucional para registo em redes sociais ou plataformas e sítios web similares não diretamente relacionados com o desempenho de funções profissionais e institucionais;
    c. Usar o sistema de *email* da **ESEnfC** para criar ou distribuir mensagens disruptivas ou ofensivas, incluindo comentários ofensivos sobre raça, sexo, deficiências, orientação sexual, pornografia, crenças e práticas religiosas, crenças políticas ou origem nacional;
    d. Reencaminhar mensagens de acesso restrito, que contenham informações confidenciais, para destinatários não expressamente autorizados a aceder à informação.

Artigo 13.º

Acesso ao serviço de correio eletrónico (e-mail)

1. O acesso à componente de administração das caixas de correio eletrónico dos serviços, está reservado, em exclusivo, ao SI, ou a prestadores de serviços a operar sob responsabilidade do SI. A administração deste serviço restringe-se à criação, suspensão, eliminação e gestão de atributos gerais do serviço de correio eletrónico.
2. O disposto no preceito anterior não poderá pôr em causa qualquer disposição legal sobre direitos, liberdades e garantias da pessoa autorizada.

SECÇÃO II - DA COMUNICAÇÃO E TRANSFERÊNCIA DE INFORMAÇÃO

Artigo 14.º

Transferência e partilha de informação

1. A preservação da confidencialidade das informações institucionais e da privacidade de todos que com a **ESEnfC** colaboram são princípios fundamentais devendo para isso as pessoas autorizadas:
    a. Manter reserva sobre informação considerada confidencial acedida no decurso do desempenho da atividade profissional ao serviço da **ESEnfC**;

b. Manter reserva sobre eventual informação considerada do foro privado da qual se obtém conhecimento autorizado no decurso do desempenho da atividade profissional ao serviço da **ESEnfC**;

c. Não abordar informações de carácter institucional ou profissional em locais públicos ou privados sem garantia de reserva de privacidade;

d. Não enviar dados da **ESEnfC** em suporte digital para serviços em *cloud* pública, ou plataformas de uso similar, acedidas através de contas de acesso suportadas por credenciais de acesso – correio eletrónico – não institucionais.

SECÇÃO III - DO USO DE REPOSITÓRIOS

Artigo 15.º

Responsabilidades

1. A **ESEnfC** deve promover a implementação de repositórios digitais centralizados, que permitam o controlo de acessos com base na definição de permissões por pessoa autorizada, devendo existir repositórios partilhados por unidade organizacional e, sempre que se justifique, repositórios de acesso individual.
2. O SI é responsável pela criação e gestão de infraestrutura de suporte aos repositórios digitais.
3. Cada unidade organizacional referida no artigo 6º é responsável pela adequada atribuição de acessos aos repositórios digitais.
4. O SI é responsável pela definição, manutenção e monitorização de procedimentos de cópia de *backup* apropriados que salvaguardem os ativos selecionados da infraestrutura digital de forma a garantir a integridade e disponibilidade.

Artigo 16.º

Uso de repositórios digitais

1. A pessoa autorizada deve usar os repositórios digitais (diretorias) centralizados atribuídos a cada unidade organizacional. Apenas sobre os mesmos é garantida a aplicação do procedimento de *backup* em vigor.
2. Os repositórios de acesso individual não devem ser usados para arquivo de dados não respeitantes às atividades da **ESEnfC** por forma a promover o uso eficiente dos recursos de processamento de informação e para salvaguardar a privacidade da pessoa utilizadora.

SECÇÃO IV – DO ESPAÇO DE TRABALHO E DOCUMENTOS EM FORMATO FÍSICO

Artigo 17.º

Condicionantes quanto ao espaço de trabalho

1. A pessoa autorizada deve seguir os princípios da mesa limpa e do ecrã limpo.
2. Os espaços de trabalho devem ser organizados por forma prevenir a ocorrência de violações de segurança que impliquem perdas, acessos ou alterações não autorizados de informação em formato físico e em formato digital.

3. Os documentos em formato físico que são transportados para fora dos espaços físicos da **ESEnfC**, quando autorizados, devem estar protegidos contra acesso indevido.
4. As impressões devem ser recolhidas da impressora tão rápido quando possível, e, caso se imprima documentos confidenciais, deve-se acompanhar, presencialmente, a saídas das folhas e garantir que foram todas recolhidas da impressora, devendo ser privilegiado o uso de código de ativação de impressão, quando tecnicamente possível.
5. A destruição de documentos em suporte físico, incluindo cartões de identificação em fim de vida, deve ser feita com recurso a meios adequados que impossibilitem a reconstituição dos documentos, tais como trituradoras adequadas.

Artigo 18.º

Restrições relativas à pessoa autorizada

1. A pessoa autorizada não pode fazer registo fotográfico, vídeo ou similar de documentos em formato físico ou outro suporte de dados, quando não autorizado, ou quando tal registo não decorra, diretamente, de competências constantes dos Estatutos da Escola.

SECÇÃO V – TRABALHO REMOTO E TELETRABALHO

Artigo 19.º

Acesso remoto

1. O acesso, em modo remoto, a componentes do sistema de informação implementadas no centro de dados da Escola é feito em exclusivo através das soluções providas e geridas pelo Serviço de Informática.

Artigo 20.º

Teletrabalho

1. A execução de funções em formato teletrabalho requer autorização prévia do Presidente da Escola.
2. O SI disponibiliza ao trabalhador/a em teletrabalho, meios de suporte ao exercício de funções que apliquem os mesmos níveis de acesso que o trabalhador/a mantinha em trabalho presencial.
3. O SI realiza uma sessão prévia com o/a trabalhador/a para apresentação do funcionamento do sistema a usar bem como das regras de segurança a seguir.
4. O/A trabalhador/a em teletrabalho não deve manter quaisquer dados no equipamento em uso para acesso remoto.

SECÇÃO VI – DISPOSITIVOS MÓVEIS

Artigo 21.º

Uso de dispositivos móveis

Considera-se, para efeitos do presente Regulamento, como dispositivo móvel os seguintes dispositivos: computador portátil em uso em formato de mobilidade; tablet; smartphones e similares, propriedade

da **ESEnfC** ou não, que seja usado para acesso, processamento e armazenamento de informação detida pela Escola.

A pessoa utilizadora de dispositivos móveis que sejam usados para aceder a recursos da **ESEnfC**, deve garantir a implementação de boas práticas de segurança:

a. Uso obrigatório de Password, PIN ou equivalente, para autenticação e acesso a dispositivo;

b. Não deixar os equipamentos móveis em veículos automóveis sem vigilância;

c. Os dispositivos apenas devem ter as ligações Wifi e Bluetooth ativas, quando necessário;

d. Os dispositivos portáteis devem ter os dados encriptados sempre que seja tecnicamente possível.

No caso de perda ou roubo de um dispositivo móvel que contenha dados, ou que permita o acesso a dados da **ESEnfC,** é obrigatória a comunicação imediata Presidente da **ESEnfC** e ao SI.

CAPÍTULO IV – SEGURANÇA E MONITORIZAÇÃO

Artigo 22.º

Regime Jurídico da Segurança no Ciberespaço

1. A **ESEnfC** assegura a disponibilização de recursos adequados ao cumprimento das obrigações legais decorrentes do Regime Jurídico da Segurança no Ciberespaço.
2. A **ESEnfC** designa, junto do Centro Nacional de Cibersegurança, Autoridade Nacional de Cibersegurança, o/a Responsável de Segurança da Escola. Este assume a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.
3. A Presidência, os serviços administrativos (Recursos Humanos) e o Serviço de Informática devem, conjuntamente, definir e promover a implementação de ações de formação sobre temáticas atinentes à Cibersegurança e proteção de dados pessoais com vista à capacitação para a segurança da informação e promoção da privacidade.

Artigo 23.º

Deveres do Serviço de Informática

1. Cabe ao SI a obrigação de:
   a. Manter um inventário de todos os ativos digitais essenciais para a suporte da prestação dos serviços da **ESEnfC**;
   b. Colaborar com o/a Responsável de Segurança designado na elaboração e atualização do Plano de Segurança, adequando-o ao contexto da Escola e ao horizonte de ameaças avaliado, nos termos do prescrito no Regime Jurídico da Segurança do Ciberespaço;
   c. Executar as competências atribuídas em sede de Plano de Segurança da **ESEnfC**.
   d. Detetar, mitigar e notificar incidentes de segurança nos termos do quadro legal vigente, incluindo o Regime Jurídico da Segurança do Ciberespaço e o Regulamento Geral sobre a Proteção de Dados;
   e. Controlar o acesso físico ao centro de dados, salas técnicas e bastidores;

f. Aplicar e manter um processo de realização de cópias de segurança e verificar periodicamente a sua integridade, segundo Política de Backups vigente;

g. Verificar periodicamente os *logins,* acessos e registos de auditoria dos sistemas para controlar tentativas de violação e quebras de segurança;

h. Criar e preservar registos de incidentes de segurança e fazer a sua notificação às autoridades competentes, caso necessário, nos termos do Regime Jurídico da Segurança no Ciberespaço seguido procedimento de Gestão de Incidentes vigente;

i. Acompanhar as orientações técnicas e alertas de segurança emitidos pelo Centro Nacional de Cibersegurança e outras entidades competentes.

Artigo 24.º

Monitorização e criação de registos

1. **Monitorização do tráfego de rede**

   a. O SI é responsável pela promoção da segurança da infraestrutura institucional com recurso a ferramentas automatizadas de inspeção de tráfego e deteção de intrusões, com vista à deteção e bloqueio de tráfego potencialmente malicioso, assim com de tentativas de acesso não autorizadas.

   b. O SI deve promover o uso de sistemas de controlo de tráfego que privilegiem o bloqueio em detrimento da deteção por meio de inspeção de tráfego.

   c. O acesso aos dados resultantes de processos de monitorização só poderá ser concretizado com recurso a contas de acesso nominais ou de identificação unívoca.

   d. A rastreabilidade dos acessos deve, sempre que tecnicamente possível ser garantida por meio da parametrização dos sistemas para criação de *logs* de registo, incluindo, pelo menos, a informação sobre quem acedeu, data e hora, operações efetuadas. Os *logs* devem, sempre que possível, ser assinados digitalmente.

Artigo 25.º

Apoio técnico

Solicitações da pessoa autorizada ao Serviço de Informática

1. O SI atuará de forma autónoma, ou de forma articulada, com fornecedores externos, para ultrapassar quaisquer condições que se considerem anómalas na operação dos sistemas informáticos, respeitando os seguintes preceitos:

   a. A comunicação com o SI para efeitos de apoio - *helpdesk* - deverá ser feita, preferencialmente, por via eletrónica através de email, ou via telefone;

   b. Este procedimento dará origem a um registo eletrónico que servirá de suporte na resposta ao pedido e para controlo interno;

   c. Os pedidos de assistência serão, sempre que possível, realizados por acesso remoto, estando os recursos do SI autorizados a ligarem-se aos postos apenas no decurso da resolução de problema ou incidente reportado;

   d. Remete-se para pedido de suporte por contacto telefónico, situações urgentes sempre que se verifique que o serviço da pessoa autorizada se encontra paralisado por força de

problema no sistema informático, ou outro, que perturbe o normal funcionamento da globalidade de um serviço ou ainda quando esteja em causa a segurança do sistema informático.

Artigo 26.º

Dever de notificação de incidentes de segurança

1. As pessoas autorizadas do sistema de informação têm o dever de comunicar ao SI qualquer tentativa de acesso não autorizado ou qualquer outro uso indevido de recursos digitais por comunicação ao serviço de helpdesk.
2. As pessoas autorizadas do sistema de informação têm o dever de comunicar ao SI qualquer tentativa de acesso não autorizado ou qualquer outro uso indevido de recursos físicos do Sistema de Informação da **ESEnfC.**

Artigo 27.º

Incidentes e suas consequências

1. Os incidentes de segurança relacionados com o sistema de informação da **ESEnfC** deverão ser comunicados à/ao responsável pela segurança previsto no art.º 22.º, competindo-lhe diligenciar pela execução do procedimento de Gestão de Incidentes integrado no Plano de Segurança da Escola.

CAPÍTULO V - AUDITORIA E REGIME DISCIPLINAR

Artigo 28.º

Auditoria

1. O cumprimento deste regulamento, incluindo a atividade realizada pelas pessoas autorizadas nos equipamentos informáticos da Escola poderá, em qualquer altura, ser objeto de auditoria a realizar sob gestão do/a Responsável de Segurança designado/a, de forma a garantir o cumprimento das normas de utilização e de modo a assegurar a qualidade e o bom funcionamento da prestação dos serviços de tecnologias de informação e comunicação.
2. As auditorias são realizadas pelo SI ou por entidade externa detentora de competências adequadas sob execução de contrato de serviços.
3. A informação constante do relatório da auditoria é considerada confidencial, pelo que não pode ser utilizada para outros fins sem o prévio conhecimento e a autorização do Presidente da **ESEnfC**.

Artigo 29.º

Regime disciplinar

O não cumprimento das normas do presente regulamento pode determinar a abertura dos competentes procedimentos disciplinares, nos termos da lei, sem prejuízo da responsabilidade criminal que vier a ser apurada nessa sede.

CAPÍTULO VI - DISPOSIÇÕES FINAIS

Artigo 30.º

Procedimento, comunicação e localização do Regulamento

O presente regulamento interno é publicitado formalmente nos termos da Lei, sendo o mesmo diploma disponibilizado na *intranet* e distribuído, via *email*, para todos os recursos incluídos no âmbito deste Regulamento.

Artigo 31.º

Aprovação do Regulamento

O presente Regulamento foi aprovado pelo Presidente da Escola, no seguimento de proposta do Serviço de Informática.

Artigo 32.º

Revisão do presente regulamento

O presente regulamento poderá ser objeto de alteração por iniciativa de Órgão competente.

Artigo 33.º

Dúvidas e omissões

As dúvidas e omissões do presente regulamento serão resolvidas por recurso à interpretação da legislação habilitante, com base em critérios de equidade, mediante decisão da/o Presidente da Escola.

Artigo 34.º

Entrada em vigor

O presente documento entra em vigor após a deliberação de aprovação.