ORDEM
DOS ENGENHEIROS
REGIÃO SUL

Ordem dos Engenheiros (OE)

Região Sul (RS)

Regulamento e Boas Práticas de Segurança de Sistemas de Informação

Aprovado na Reunião do Conselho Diretivo da Região Sul
de 11 de maio de 2023

1 INTRODUÇÃO

Este documento privilegia a integração de mecanismos de deteção de riscos em tecnologias de informação da Ordem dos Engenheiros, bem como a segurança operacional. Mitigando os riscos sob a forma de ameaças, torna-se necessário definir um conjunto de normas e políticas de segurança de sistemas de informação que promovam a prevenção ativa, limitando a ocorrência de erros, omissões, perdas, e divulgação indevida de informação.

A integração de melhores práticas, visa o uso dos recursos e conteúdos disponibilizados com medidas de segurança relevantes ao correto manuseio de ferramentas e gestão de equipamentos em sistemas de informação.

A evolução constante das tecnologias impõe a necessidade de atualização periódica destas políticas e normas para assegurar a sua relevância e adequação às necessidades.

Esta política aplica-se a todos os utilizadores que têm acesso a qualquer sistema informático ou computador da OE, incluindo aqueles que acedam remotamente aos recursos computacionais ou de rede da OE.

2 REQUISITOS DE SEGURANÇA

O processo de desenvolvimento de normas de segurança sistemas de informação vê a informação e tecnologia de sistemas de informação como um todo. Esta abordagem pode ser aplicada quer a ambientes de rede complexos quer a ambientes de computadores isolados.

2.1 Propriedade, uso e devolução de equipamentos

Todos os equipamentos disponibilizados pela OE, são obrigatoriamente devolvidos (2 dias úteis) quando requeridos, para atualização, auditoria ou recondicionamento.

2.2 Informação Confidencial (membros) e RGPD

Toda a Informação de associados (membros engenheiros) ou de colaboradores deve ser considerada CONFIDENCIAL e tratada com a máxima segurança, devendo sempre ser assegurados os requisitos legais em vigor (RGPD, ISO9001, ISO27001, outros referenciais).

2.3 Discos. Encriptados (BitLocker)

Todos os discos de portáteis da OE-RS, em utilização por colaboradores ou membros eleitos, bem como discos ou PEN's para transporte temporário de informação sensível, devem estar encriptados com BitLocker. Solicitar apoio técnico nos serviços para implementar esta medida de segurança.

2.4 Autenticação e gestão de passwords

Todas as passwords devem ter uma complexidade mínima (mínimo de 10 caracteres, alfanuméricos, números, maiúsculas).

As passwords devem ser renovadas a cada seis meses;

A utilização de login e password é obrigatória para acesso a informação e serviços de informação da OE-RS.

Quando o utilizador se ausentar temporariamente do computador deverá bloquear /terminar a sessão (Logout), de modo a evitar acessos não autorizados.

2.5 Partilha de logins /passwords

As passwords e logins de acesso a serviços internos e/ou externos da OE-RS, são pessoais e intransmissíveis.

2.6 Utilização de VPN

Para situações de trabalho remoto, os colaboradores podem solicitar acesso via VPN e fundamentar o seu pedido, sendo avaliado pelos serviços de IT.

3 GESTÃO DE RECURSOS

O processo que envolve a gestão de recursos do sistema, visa o tratamento de toda a informação, acessos /permissões, monitorização e cópias de segurança.

3.1 Controlo de Acesso

Os sistemas são parametrizados para garantir que o utilizador só tem acesso à informação e recursos do sistema que são estritamente necessários para a execução das suas funções.

São proibidas todas as formas de tentativa de acesso a sistemas ou espaços de armazenamento, para os quais não tenha sido dada autorização.

3.2 Monitorização

Os sistemas guardam registos de eventos considerados relevantes previamente selecionados (como sejam Logins – Logouts, acessos a ficheiros, etc.) e armazenam um rasto de auditoria num ficheiro de sistema protegido de forma a providenciar um meio de monitorização.

3.3 Cópias de Segurança (Backups)

Implementou-se uma política de backups com periodicidade de realização de backups e período de retenção das cópias. São efetuadas cópias dos ficheiros residentes nos discos dos servidores. As cópias de segurança nos equipamentos manuseados por cada utilizador, é da responsabilidade do utilizador a que está atribuído esse equipamento, com exceção às pastas de serviço partilhadas (conteúdo partilhado e gerido num servidor de ficheiros).

3.4 Segurança Física

Todo o equipamento informático disponibilizado pela Ordem dos Engenheiros, é alterado ou atualizado pelos Serviços de Sistemas de Informação. Não são permitidas, quaisquer práticas de atualização, sem conhecimento e autorização prévia dos Serviços de Informática. (p.e. a atualizações de processador, memória ou placas de circuitos, adicionar ou remover periféricos, alterar conectividade entre equipamentos).

4 POLÍTICAS DE UTILIZAÇÃO

4.1 Antivírus (AV)

A instalação e utilização de antivírus atualizado é obrigatória em todos os postos de trabalho da OE-RS.

O software recebido do exterior pode introduzir vírus informáticos na rede interna da OE. Estes vírus podem também ser transportados, de e para os sistemas da OE dos utilizadores através de dispositivos de armazenamento externo, mails, acessos a sites infetados.

4.2 Conteúdos proibidos

Não é permitido produzir ou reproduzir conteúdo com características ofensivas, difamatórias ou suscetíveis de violar a privacidade ou outros direitos de terceiros.

4.3 Acesso à Internet (WEB)

No quotidiano, a Internet contem informações úteis. Contudo, a tecnologia inerente à usabilidade da Internet, não é isenta de ameaças. A OE está empenhada em fornecer aos seus colaboradores, os mecanismos seguros e adequados no acesso à Internet.

O uso como meio pessoal, não deverá interferir, envolver solicitações ou estar associado a qualquer atividade lucrativa externa que, venha a comprometer, criar atritos, ou situações de embaraço para a OE. Como qualquer outro equipamento de escritório, os abusos de uso pessoal da Internet e violações das políticas e orientações da OE, estão sujeitos a ações disciplinares.

4.3.1 Downloads

É expressamente proibida a visita de sites ou a divulgação de conteúdos ofensivos da moral e dos bons costumes, designadamente os seguintes:

- Conteúdo impróprio, obsceno, pornográfico ou pedófilo;
- Conteúdo discriminatório, ofensivo ou perturbador em relação a determinada raça, sexo, religião, nacionalidade, naturalidade, deficiência ou traços físicos ou orientação política ou sexual, idade;
- Conteúdo que desrespeite quaisquer direitos de autor ou direitos conexos, marcas, segredos comerciais ou outros direitos de propriedade intelectual;
- Conteúdo difamatório ou passível de violar os direitos de terceiros;

4.4 Correio Eletrónico (Email)

O correio eletrónico é um meio rápido e fácil de comunicação com utilizadores, quer da OE, quer de entidades externas. Contudo, existem regras que devem ser cumpridas.

O uso pessoal, deverá ser efetuado com moderação e razoabilidade, e deverá assentar nos princípios da adequação, da proporcionalidade, da mútua colaboração e confiança.

4.4.1 Autenticação da conta de Email

A utilização do correio eletrónico está sujeita aos requisitos mínimos de identificação e autenticação estabelecidos em **2.4**.

4.4.2 Retenção do Correio Eletrónico

Os Serviços de Informática da OE estabeleceram e mantêm um processo sistemático de gravação, retenção de mensagens de correio eletrónico e respetivos registos históricos.

As mensagens armazenadas podem ser removidas periodicamente, apagadas acidentalmente pelos utilizadores, ou perdidas se ocorrerem problemas com os sistemas de informação.

Os sistemas de correio eletrónico não devem ser usados como arquivo de informação.

4.4.3 Subscrição de listas de correspondência; reenvio para cadeias de solidariedade

Os funcionários da OE podem subscrever listas de correspondência se tal for relevante para a execução da sua função. Os Serviços de Informática pode restringir a subscrição de listas de correspondência que gerem volume excessivo de mensagens de correio eletrónico.

É proibido o envio de mensagens para cadeias de solidariedade, boas causas, concursos, advertências de vírus, e de outra natureza.

5 EQUIPAMENTO INFORMÁTICO E SOFTWARE

5.1 Inventário físico

Os Serviços de Informática são responsáveis pelo registo e atualização de todo o software. instalando as atualizações consoante venham a ser disponibilizadas.

5.2 Instalação de Software (SW) terceiro nos equipamentos da OE-RS

A instalação de software aprovado deve ser assegurada pelos serviços da OE-RS.

Não é permitida a instalação de SW desconhecido ou não aprovado pela OE-RS, constituindo uma violação das regras de segurança de informação instituídas.

5.3 Licenciamento de software

É essencial que a utilização deste software seja controlada de forma adequada para proteger os utilizadores e a OE em particular.

É da inteira responsabilidade dos Serviços de Informática garantir o cumprimento das condições de licenciamento. Caso isto não aconteça e se forem encontradas cópias ilegais de software, ou for feito uso não autorizado deste, a OE ficará exposta a possíveis processos judiciais e os colaboradores envolvidos a ações disciplinares.

5.4 Auditoria de Software

Todos os computadores da O.E serão auditados regularmente, conforme condições dos acordos assinados com as empresas produtoras de software, de modo a manter o reconhecimento de cumprimento das normas, perante as entidades que zelam pelos Direitos de Autor.

6 INCIDENTES DE SEGURANÇA

Um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação.

6.1 O que fazer?

Em caso de suspeita ou observação /evidência de um incidente de segurança (vírus, perda de informação, comportamento suspeito), é obrigatória a comunicação imediata para o telefone 933 071 279 e para o email tecnologia@sul.oep.pt, desligando de imediato o(s) equipamento(s) afetado(s)