



Pilares da Segurança da Informação para o âmbito do Sistema de Gestão da Segurança da Informação:

CONFIDENCIALIDADE

Propriedade dos dados que indica em que medida estes não se tornaram acessíveis ou foram divulgados a pessoas, processos ou entidades não autorizados.

INTEGRIDADE

Propriedade dos dados cuja exatidão e coerência são preservadas independentemente das modificações efetuadas.

DISPONIBILIDADE

Propriedade dos dados ou dos recursos serem acessíveis e utilizáveis após solicitação de uma entidade autorizada.

Em caso de dúvida ou deteção de alguma situação anómala ou suspeita utilize os seguintes contactos:

Telefone: 269860780

gsi@apsinesalgarve.pt

suporte.informatico@apsinesalgarve.pt

BOAS PRÁTICAS PARA A SEGURANÇA DA INFORMAÇÃO

I



APS

Administração
dos Portos de Sines
e do Algarve S.A.

A Segurança da Informação é da responsabilidade de todos. Com pequenos gestos é possível contribuir para um espaço de trabalho mais seguro, agradável e eficiente.



NAS SALAS DE REUNIÕES

Ao de abandonar a sala, assegure-se que apagou toda a informação dos meios informáticos existentes, assim como não deixou nada em cima da mesa.



NO POSTO DE TRABALHO

Para proteger a informação, comece por manter o seu espaço de trabalho limpo e em ordem.

Após a impressão de documentos, recolha-os de imediato. Não deixe documentação nos equipamentos de impressão.

Se for necessário imprimir documentos com informação sensível, recorra à impressão com recurso à utilização de código de proteção.

Utilize os equipamentos de destruição de documentos e media para eliminar documentos não necessários.



UTILIZAÇÃO DE MEIOS INFORMÁTICOS

Escolha palavras-chave de qualidade, complexas de adivinhar mas fáceis de memorizar, utilizando de forma intercalada maiúsculas, minúsculas, números e símbolos. Veja as recomendações disponíveis na Instrução Operativa IO001.

Bloqueie o computador ao ausentar-se do posto de trabalho. No final do dia desligue o computador. Nas situações de transição de turno encerre a sessão para que o novo utilizar necessite de se identificar.

Seja prudente ao navegar na internet, evitando sítios suspeitos e comprovando a fiabilidade de todos os ficheiros descarregados antes de o ativar ou executar.

Tome as devidas precauções para prevenir o spam e o phishing nos correios eletrónicos.

Não utilize dispositivos ou abra ficheiros executáveis de origem desconhecida ou duvidosa.

Não transporte programas ou jogos de e para a organização.

Guarde os documentos e informação de trabalho em repositórios centralizados para garantir a disponibilidade, integridade e confidencialidade.

Respeite a política de classificação e manuseamento da informação e na rede informática só ligue equipamentos ou media pertencentes à APS.

Em caso de suspeita de vírus ou falha de Segurança da Informação desligue o computador e fale com o suporte informático.