InfoSeg na Universidade de Évora

Joaquim Godinho
Direção de Serviços de Informática
UNIVERSIDADE DE ÉVORA

ENCONTROS SAMA 2020

26 ABRIL 14h30-17h15 LISBOA

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Antecedentes

- **Normas abertas** : Com a publicação do Dec. Lei nº 36/2011 e a resolução do Conselho de Ministros 91/2012 foi estabelecida em Portugal a necessidade de adoção de normas abertas para a informação em suporte digital na Administração Pública. Através de Despacho reitoral 87/2014, de 18 de Agosto, a A Universidade de Évora, numa decisão pioneira entre as universidades portuguesas, passou a adotar o conjunto de normas abertas definidas por lei em toda a documentação oficial;
- **Rede Comum do Conhecimento**:
  - ✓ **Portal do Estudante da Universidade de Évora**, A iniciativa, contemplada na Operação 8002 do SAMA (Sistema de Apoios à Modernização Administrativa), surgiu da necessidade sentida em consolidar num único local, informação útil destinada inicialmente a candidatos ao ensino superior dos 1º, 2º e 3º ciclo
  - ✓ O **Sistema Interno de Promoção e Garantia da Qualidade da Universidade de Évora** (SIPGQ-UE) foi certificado em 2014 por um período de seis anos pelo Conselho de Administração da A3ES, Agência de Avaliação e Acreditação do Ensino Superior; essa certificação foi renovada em 2022 por um novo período de seis anos.
  - ✓ Considerada pela RCC como um caso de sucesso, a aplicação de **Gestão Documental** da Universidade de Évora (GesDoc) foi apresentada pelos Serviços de Informática da Universidade de Évora em Maio de 2014 na 1ª Jornada da Rede Comum de Conhecimento (RCC), promovida pela Agência para a Modernização Administrativa (AMA).
- Novo modelo de **Gestão de Serviços de Tecnologias de Informação**, baseado na conceção e desenvolvimento de práticas de gestão de serviços de TI alinhadas com normas e boas práticas internacionais como a ISO 20000 e o ITIL.

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

AVISO Nº 01/SAMA2020/2015

(Sistema de Apoio à Modernização e Capacitação da Administração Pública)

Operação temática 5: Segurança da informação e sistemas de gestão de informação

O contexto atual do sistema de informação na Administração Pública caracteriza-se por: *Grande complexidade e abrangência do sistema de informação; Constante inovação tecnológica; Crescente dependência das atividades de prestação de serviços da disponibilidade e integridade da informação, assim como da necessidade de racionalização de custos e de responder a requisitos legais e dos stakeholders sobre confidencialidade da informação.*

No âmbito do preconizado pela medida 1 da Resolução de Conselho de Ministros n.º 12/2012, de 7 de fevereiro, [illegible] e implementar um modelo de governação das TIC através de implementação de subprojectos [illegible] (que podem ser desenvolvidos separada ou conjuntamente):

- **Subprojecto A - Gestão do Risco e da Segurança da Informação**: É crítico avaliar e melhorar os processos de gestão do risco e da segurança da informação, de forma articulada através das redes de organizações ministeriais e em alinhamento com as estratégias em execução. O presente subprojecto tem como objetivo o reforço de competências, práticas e ferramentas de gestão do risco e da segurança da informação nas organizações ministeriais em alinhamento com os referenciais de boas práticas nestes domínios.

- ✓ **ISO 27001** — **Atividade 1 – Avaliação das Práticas de Segurança da Informação**
- **Atividade 2 – Gestão do Risco e da Segurança da Informação**
- ✓ **ISO 20000** — **Atividade 3 – Gestão dos Serviços de Informação – ISO 20000**

- **Subprojecto B - Gestão dos Serviços de Informação**: O presente subprojecto tem como objetivo o reforço de competências, práticas e ferramentas de gestão dos serviços de TIC em alinhamento com os referenciais de boas práticas nestes domínios.

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA · COMPETE 2020 · PORTUGAL 2020 · UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Objetivos

- Melhorar as práticas de segurança da informação da UE
- Melhorar a consciencialização dos utilizadores da UE para as ameaças de segurança da informação

Sensibilizar os utilizadores da UE para as ameaças de segurança da informação a que estão expostos

Identificar as vulnerabilidades dos sistemas da UE

Gerir o risco a que a UE está exposta e **preparar a sua resposta** caso o risco se concretize

Auditar a UE e perceber o seu **estado de maturidade** relativamente à segurança da informação

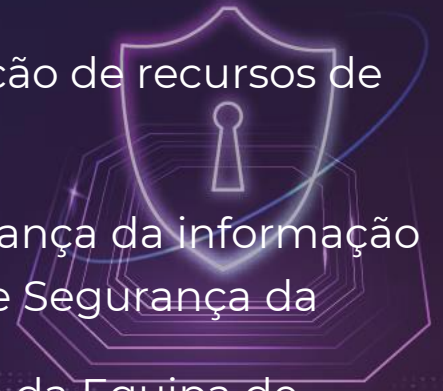
ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Atividades

- Avaliação (assessment) às práticas de (gestão) segurança da informação nas unidades orgânicas e direções de serviço da Universidade de Évora, usando como modelo de referência as normas internacionais ISO/IEC 27001 e ISO/IEC 27002
- Questionários de avaliação de comportamentos dos colaboradores da utilização de recursos de informação
- Testes de intrusão dos sistemas de informação e redes de comunicações
- Workshops interativos, presenciais e online : ações de sensibilização de segurança da informação
- Reforço de competências na área de Auditoria Interna com foco na Gestão de Segurança da Informação
- Reforço das competências técnicas da Equipa de Segurança da Informação e da Equipa de Auditoria Interna
- Implementação do (processo) Sistema de Gestão de Segurança da Informação com base nos requisitos e orientações das normas internacionais ISO/IEC 27001 e ISO/IEC 27002, utilizando também boas práticas internacionais como ITIL e COBIT.
- Definição da estrutura de Funções, Autoridades, Responsabilidades e Competências de Gestão de Segurança da Informação.
- Auditoria interna para verificar a eficácia da implementação do Sistema de Gestão; realizar o tratamento das constatações da auditoria, permitindo assim a concretização dos mecanismos de melhoria contínua do Sistema de Gestão segurança da informação



ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Resultados

- Colaboradores conscientes, que sabem como reagir perante situações que coloquem em causa a Segurança da Informação da Universidade de Évora
- Sistemas Informáticos mais seguros, com menos vulnerabilidades que podem ser exploradas por atacantes
- Universidade consciente dos riscos e preparada para reagir às ameaças, de forma mais organizada, rápida, eficaz e eficiente

A segurança deve ser uma preocupação de todos

- **Individual e coletivamente**

...e será certamente um problema para todos

- **Pessoal e institucionalmente**

...se não forem adotadas as medidas corretas no tempo adequado!

AMA MODERNIZAÇÃO ADMINISTRATIVA · PORTUGAL 2020 · Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Inquérito

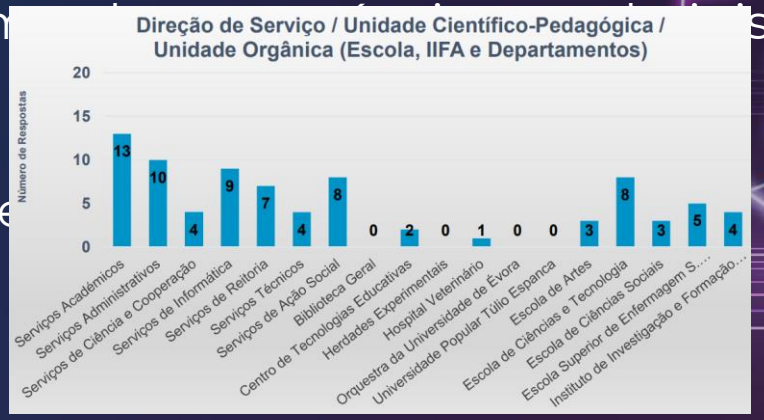
Avaliação do estado de maturidade dos colaboradores face às boas práticas de segurança da informação

Âmbito:

- "Utilizadores-chave" em áreas relevantes, nom[illegible]strativas
- Responsáveis por Unidades e Órgãos

Pontos fracos a melhorar:

- Cuidados na utilização de equipamento móve[illegible]
- Gestão de passwords
- "*clean desk clear screen*"
- Destruição de informação em suporte papel



De um modo geral pode-se concluir que existe uma razoável consciencialização dos colaboradores da Universidade de Évora relativamente à segurança da informação

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA · COMPETE 2020 · PORTUGAL 2020 · UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Workshop (presencial e on-line)

- Reconhecer os conceitos gerais de segurança da informação;
- Reconhecer os principais ataques de engenharia social;
- Reconhecer boas práticas de segurança da informação na gestão de informação, clean desk e clear screen;
- Conhecer algumas ameaças e boas práticas de segurança da informação relativas à utilização da internet;
- Conhecer as boas práticas a considerar com vista à segurança do seu equipamento móvel;
- Conhecer os requisitos de uma password forte/segura;
- Reconhecer boas práticas comportamentais a ter na presença de visitantes nas instalações da organização;
- Reconhecer um incidente de segurança da informação e saber como reagir perante essa situação;
- Reconhecer boas práticas de segurança da informação e aplicá-las no seu dia-a-dia.

Âmbito:

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Testes de intrusão

Realização de testes de intrusão à infraestrutura da Universidade de Évora, simulando as ações de um agente malicioso com o objetivo de conseguir acessos a sistemas e/ou informação sensível

Âmbito:

- Infraestruturas : redes, servidores e equipamentos terminais
- Sistemas e serviços : SIIUE, GESDOC, SIAG, MOODLE, DSPACE, WWW,...

Principais vulnerabilidades detetadas

- Vulnerabilidades da rede wifi a ataques conhecidos de negação de serviço e roubo de credenciais
- Vulnerabilidades no software exposto à Internet bem como versões de software desatualizado
- Falhas de configuração e vulnerabilidades nos mecanismos de cifra
- Impressoras com página de administração públicas
- Login vulnerável a *password-guessing*
- Clickjacking e falhas no tratamento de exceções
- Contas de mail comprometidas

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Auditoria

Realização de Auditoria Interna tendo como referência a ISO/IEC 27001 para verificar a eficácia da implementação do SGSI e avaliar a robustez de todo o sistema

Âmbito:

Serviços Académicos
- Processos específicos das unidades auditadas;
- Criação e classificação de informação – cuidados na criação, armazenamento e eliminação da informação;
- Cuidados de segurança no uso de dispositivos móveis, na utilização de equipamentos;
- Controlo de acessos físicos e lógicos – como são realizados os acessos às instalações de trabalho e aos sistemas de informação;
- Backups - práticas de realização de backups dos sistemas de informação e testes dos mesmos;
- Gestão de passwords – cuidados com a criação e alteração das passwords;
- Backups – cuidados com a realização de backups de informação que consta nos computadores de trabalho;
- Resolução de Incidentes – práticas de detecção e resolução de incidentes;
- Reporte de incidentes – que canais e a quem reportam problemas

Serviços Técnicos
- Segurança física - incêndios, intrusão, ...
- Controlo de acessos;...

Serviços Informática
- Gestão infraestrutura informática – regras de instalação e atualização de software;
- controlo contra *malware*, acessos e controlos na rede interna e externa;
- *Compliance* – como garantem a conformidade legal/regulamentar;
- Controlo de acessos lógicos e perfis de utilizadores

Divisão de Recursos Humanos
- Gestão de recursos – inventário de recursos (*HW e SW*) ;
- Contratação, mudança de funções, saída,...
- Segurança física

Serviços Académicos, Físicos e Financeiros
- Gestão de fornecedores e de contratos;

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Sistema de Gestão de Segurança de Informação

- Identificação do Âmbito de Proteção (a informação que se pretende proteger);
- Estabelecimento da Orgânica de Segurança de Informação, definição de Funções e Responsabilidades (onde estão identificados também Autoridades e Competências) e respetiva metodologia de funcionamento

Serviços Académicos

Planeamento da Gestão de Risco:

- Elaboração de Política e Metodologia de Gestão de Risco
- Estabelecimento do Processo de Gestão de Risco
- Elaboração de Análise de Tratamento de Risco

Serviços Informática

Planeamento da Gestão de Continuidade de Negócio

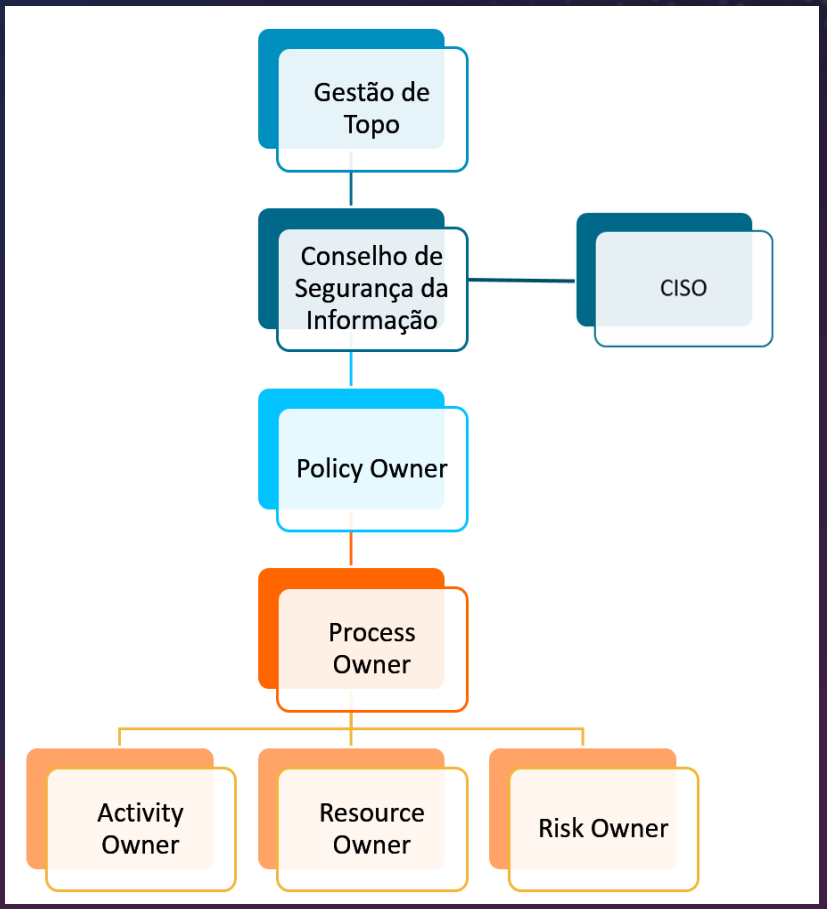
- Elaboração de Política de Gestão de Continuidade de Negócio
- Estabelecimento do Processo de Gestão de Continuidade de Negócio e procedimentos, no âmbito da Continuidade de Negócio e Disaster Recovery;
- Identificação de RPO's (Recovery Point Objective), RTO's (Recovery Time Objective)
- Definição do Plano de Continuidade de Negócio e Plano de Disaster Recovery com identificação de cenários de risco, potenciais incidentes críticos para o sistema, e ensaios de resposta aos cenários

InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

Sistema de Gestão de Segurança de Informação

- A implementação do SGSI seguiu os requisitos especificados na **norma ISO/IEC 27001:2013**. Esta norma, reconhecida internacionalmente, apresenta os requisitos de segurança para um Sistema de Gestão da Segurança da Informação de acordo com a estrutura organizacional, políticas, atividades de planeamento, responsabilidades, práticas, procedimentos, processos e recursos
- Implementou-se um sistema de gestão, baseado numa **abordagem de risco**, para estabelecer, implementar, operacionalizar, monitorizar, rever, manter e melhorar a segurança da informação



InfoSeg na Universidade de Évora

ENCONTROS SAMA 2020

SEGURANÇA DA INFORMAÇÃO DICAS

Acesso a rede Wi-Fi | Utilize adequadamente este recurso

Instale o certificado digital quando configurar o acesso Wi-Fi à rede eduroam. Garanta a segurança nas comunicações. Mais informação disponível em http://wifi.uevora.pt/
Evite aceder a *websites* que não sejam HTTPS - Verifique sempre que o *website* que está a aceder tem o cadeado verde e a ligação é cifrada (https://)
Evite transações de elevado risco em redes *wireless* públicas - Não aceda à sua conta bancária *online* ou aos serviços da universidade que contenham informação sensível. Em alternativa, utilize para esse efeito a rede do seu dispositivo móvel e mantenha-o sempre atualizado.
Não confie no nome da rede *wireless*, pode ser falsa - Garanta que está a usar uma rede fidedigna no local certo (por exemplo, só poderá conectar-se à rede *wireless* de sua casa se estiver em casa).

Apps | São seguras?

Utilize o seu dispositivo móvel como se fosse o seu computador - Com os mesmos cuidados: mantenha sempre o sistema operativo, *browser*, antivírus, *firewall* e *apps* atualizados!
Não instale *apps* fora das *app stores* oficiais - Utilize sempre fontes oficiais.
Não instale *apps* que não utiliza - Especialmente quando necessitam de permissões para aceder ao microfone, câmara, localização ou ficheiros do seu dispositivo.
Reduza este tipo de permissões ao mínimo!

***Phishing* | Não seja apanhado!**

Verifique se o email é fidedigno - Se o remetente corresponde ao nome que aparece, se não existem erros ortográficos que chamem à atenção e tente validar o remetente através de outros meios de comunicação, por exemplo por telefone.
Atenção aos emails fraudulentos! - Evite abrir emails e anexos de remetentes desconhecidos e verifique os *links* antes de clicar, passando o rato por cima (*mouse over*).
Apague o email de imediato!
Não envie dados sensíveis (palavras-passe, moradas, dados bancários, dados pessoais) por email. - Mesmo que não tenham acesso ao seu dispositivo, poderão conseguir intercetar a informação.

Gestão de Palavras-Passe | Mantenha-as seguras!

Utilize *passphrases* ao invés de palavras-passe, por exemplo: "sozinhos vamos mais rapido juntos vamos mais longe", ou se existir um limite de caracteres, por exemplo "eu nasci em evora no ano de 1559" = eN@EnAd59
Utilize gestores de palavras-passe - que guardem as suas palavras-passe em modo cifrado, para que não necessite de as memorizar. Dê preferência a gestores que funcionem localmente em detrimento de Serviços que guardam as palavra-passe na *Cloud*.
Altere a palavra-passe através do SIIUE - utilize este sistema para alterar a palavra-passe que utiliza no acesso aos serviços/sistemas da Universidade de Évora.
Não reutilize as suas palavras-passe, nem utilize a mesma palavra-passe em contexto pessoal e profissional - se o serviço que utiliza no âmbito pessoal for comprometido, não irá colocar em causa os serviços utilizados no âmbito profissional.

Clean Desk / Clear Screen* | *what you see is what you get!

Mantenha a sua informação segura - Bloqueie o equipamento na sua ausência. Configure sempre dispositivos de bloqueio automático no seu computador, portátil e *smartphone* (*password*, PIN, padrão, etc).
Não deixe documentos em cima da mesa - Principalmente se contiverem informação sensível/pessoal. Guarde a documentação num local seguro.

Antivírus e Atualização do sistema operativo e browser Proteja-se do *malware*!

Garanta que tem o antivírus instalado e configure as atualizações automáticas para o seu antivírus, sistema operativo e *browser*. Assim, estará protegido contra vulnerabilidades conhecidas.

UNIVERSIDADE DE ÉVORA

7.1 BILIÕES DE IDENTIDADES FORAM EXPOSTAS DEVIDO A FALHAS DE SEGURANÇA, NOS ÚLTIMOS 8 ANOS. NÃO VAMOS AUMENTAR ESSE NÚMERO!
SIGA AS BOAS PRÁTICAS...

Gestão de Palavras-Passe
Mantenha-as seguras!

As palavras-passe são utilizadas como forma de autenticação e proteção. São elas que separam os atacantes da sua informação sensível.

DICAS

Utilize passphrases ao invés de palavras-passe, por exemplo: "sozinhos vamos mais rapido juntos vamos mais longe", ou se existir um limite de caracteres, por exemplo "eu nasci em evora no ano de 1559" = eN@EnAd59

Utilize gestores de palavras-passe - que guardem as suas palavras-passe em modo cifrado, para que não necessite de as memorizar.

Utilize duplo factor de autenticação - sempre que possível, se o atacante tiver acesso à palavra-passe, não consegue aceder à sua informação.

Altere a palavra-passe através do SIIUE - utilize este sistema para alterar a palavra-passe que utiliza no acesso aos serviços/sistemas da Universidade de Évora.

Não reutilize as suas palavras-passe, nem utilize a mesma palavra-passe em contexto pessoal e profissional - se o serviço que utiliza no âmbito pessoal for comprometido, não irá colocar em causa os serviços utilizados no profissional.

Apps
São seguras?

Milhões de downloads são feitos diariamente para dispositivos móveis. Não descarregue apps de fontes desconhecidas. E mesmo as apps existentes em app stores oficiais podem não ser 100% seguras!

DICAS

Utilize o seu dispositivo móvel como se fosse o seu computador - Com os mesmos cuidados: mantenha sempre o sistema operativo, browser, antivírus, firewall e apps atualizados!

Não instale apps fora das app stores oficiais - Utilize sempre fontes oficiais.

Não instale apps que não utiliza - Especialmente quando necessitam de permissões para aceder ao microfone, câmara, localização ou ficheiros do seu dispositivo.
Reduza este tipo de permissões ao mínimo!

Antivírus e Atualização
do sistema operativo e browser
Proteja-se do malware!

Frequentemente são identificadas vulnerabilidades no sistema operativo e/ou browser que utiliza, colocando em causa a segurança de informação. Atualize o sistema operativo, browser ou antivírus para não estar vulnerável a fraquezas conhecidas pelos atacantes.

DICAS

Garanta que tem o antivírus instalado e configure as atualizações automáticas para o seu antivírus, sistema operativo e browser. Assim, estará protegido contra vulnerabilidades conhecidas.

Phishing
Não seja apanhado!

Os ataques de phishing são um dos métodos mais eficazes e utilizados para se infiltrarem na sua rede e dispositivos. **77% dos ataques de engenharia social são feitos recorrendo a phishing!**

DICAS

Verifique se o email é fidedigno - Se o remetente corresponde ao nome que aparece, se não existem erros ortográficos que chamem à atenção e tente validar o remetente através de outros meios de comunicação, por exemplo por telefone.

Atenção aos emails fraudulentos! - Evite abrir anexos de remetentes desconhecidos e verifique os links antes de clicar, passando o rato por cima (mouse over).

Não abra emails enviados por remetentes desconhecidos ou com assuntos suspeitos. Apague o email de imediato!

Não envie dados sensíveis (palavras-passe, moradas, dados bancários, dados pessoais) por email. - Mesmo que não tenham acesso ao seu dispositivo, poderão conseguir interceptar a informação.

Cofinanciado por:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Acesso a rede Wi Fi
Utilize adequadamente este recurso!

Todos os dias se conecta a múltiplas redes Wi-Fi para ter acesso à internet. Mas a informação que transmite pode ser capturada por atacantes e os seus dispositivos móveis podem ser infetados por malware.

DICAS

Utilize VPN quando possível para proteger os dados transmitidos na rede - Os seus dados são cifrados enquanto utiliza uma rede wireless insegura.

Instale o certificado digital quando configurar o acesso Wi Fi à rede eduroam. Garanta a segurança nas comunicações. Mais informação disponível em http://wifi.uevora.pt/

Não aceda a websites que não sejam HTTPS - Verifique sempre que o website que está a aceder tem o cadeado verde e a ligação é cifrada (https://)

Evite transações de elevado risco em redes wireless públicas - Não aceda à sua conta bancária online ou aos serviços da universidade que contenham informação sensível. Em alternativa, utilize para esse efeito a rede do seu dispositivo móvel e mantenha-o sempre atualizado.

Não confie no nome da rede wireless, pode ser falsa - Garanta que está a usar uma rede fidedigna no local certo (por exemplo, só poderá conectar-se à rede wireless de sua casa se estiver em casa).

Clean Desk / Clear Screen
what you see is what you get!

Todos os dias manuseamos informação em papel que depositamos em cima da mesa. Trabalhamos informação digital nos dispositivos e saímos de perto deles sem os bloquear. Para o atacante se houver informação visível pode tornar-se apetecível!

DICAS

Mantenha a sua informação segura - Bloqueie o equipamento na sua ausência. Configure sempre dispositivos de bloqueio automático no seu computador, portátil e smartphone (password, PIN, padrão, etc)

Não deixe documentos em cima da mesa - Principalmente se contiverem informação sensível/pessoal. Guarde a documentação num local seguro.

Veja mais informação em **http://www.si.uevora.pt**, nos Serviços Disponibilizados

InfoSeg na Universidade de Évora
… e depois?

ENCONTROS SAMA 2020

Conselho de Segurança da Informação e Proteção de Dados Pessoais *Despacho 23/2018*

Regulamento do Conselho de Segurança da Informação e Proteção de Dados Pessoais *Despacho 4551/2018 (DR 2.ª série, N.º 89 de 9 de maio de 2018)*

Encarregado de Proteção de Dados *Despacho 60/2018*

Rede Nacional CSIRT

Adesão à Rede Nacional de CSIRTs, *28/6/2019*

Teletrabalho e Ensino a distância

Responsável de Segurança do Ciberespaço *Despacho 5/2022*

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Instituições aderentes

metaredTIC Pt

Universidade do Algarve

Universidade da Madeira

Instituto Politécnico de Bragança

Instituto Politécnico de Santarém

Instituto Politécnico de Portalegre

Escola Superior de Saúde de Santa Maria

Universidade Nova de Lisboa - Reitoria

Universidade dos Açores

UA - Universidade de Aveiro

ISLA - Instituto Politécnico de Gestão e Tecnologia

Instituto Politécnico de Viana do Castelo

Escola Superior de Saúde Norte da Cruz Vermelha Portuguesa

Escola Superior de Educação de Paula Frassinetti

Instituto Politécnico de Setúbal

ISEC Lisboa - Instituto Superior de Educação e Ciência

UP - Universidade do Porto

Instituto Politécnico de Tomar

Universidade Autónoma de Lisboa

Instituto Universitário de Lisboa ISCTE-IUL

Escola Superior de Enfermagem de Coimbra

Instituto Politécnico de Leiria

Universidade de Lisboa - IST

IPAM - Instituto Português de Administração de Marketing

Instituto Politécnico do Porto

Universidade de Trás-os-Montes e Alto Douro

Universidade Lusíada

Universidade Europeia

Maiêutica - Cooperativa de Ensino Superior

Instituto Superior de Administração e Gestão - ISAG

Instituto Politécnico de Beja

Instituto Politécnico de Viseu

Instituto Politécnico de Coimbra

Academia da Força Aérea

Universidade Nova de Lisboa - Nova SBE

Universidade de Évora

Universidade de Coimbra

Escola Superior de Enfermagem de Lisboa

ESAP - Escola Superior Artística do Porto (CESAP - Cooperativa de Ensino Superior Artístico do Porto, C. R. L.)

Universidade Nova de Lisboa - Nova IMS

Escola Superior de Enfermagem São Francisco das Misericórdias

Autónoma Academy

Universidade de Lisboa

Universidade Católica Portuguesa

Entidades parceiras

Fundação para a Ciência e Tecnologia

Agência para a Modernização Administrativa

Centro Nacional de Cibersegurança

Portugal Digital

International Data Corporation

Direção-Geral do Ensino Superior

KIT DE SENSIBILIZAÇÃO PARA A CIBERSEGURANÇA

ENCONTROS SAMA 2020

O que inclui?

Manual de implantação

O **manual** é o guia de aplicação do kit e contém informações sobre os materiais, além de um calendário para a sua distribuição dentro de uma universidade.

Ataques direcionados

A consciencialização começa com um ou dois exercícios que permitirão avaliar o nível de sensibilização da comunidade universitária para a segurança, ao mesmo tempo que despertam o interesse em aprender mais, Estes exercícios consistem em ataques-surpresa.

Estão incluídos dois ataques direcionados para lançar, um por correio eletrónico e outro através de uma pen USB. Podem lançar-se ambos no início, ou um no início e outro no final da sensibilização. O manual explica em pormenor como lançar estes ataques.

Pósteres e trípticos

Depois de lançar um ataque direcionado, colocaremos em lugares de passagem frequente dois tipos de materiais: pósteres e trípticos.

O kit inclui pósteres em dois tamanhos (A3 e A2). Estes elementos essencialmente gráficos visam sensibilizar os membros da comunidade, para que estes se sintam uma parte ativa da segurança da nossa universidade.

Além dos pósteres, foram criados para este kit vários trípticos que também podemos disponibilizar à comunidade universitária. Os trípticos combinam gráficos e textos para transmitir aspetos importantes de segurança relacionados com as ações de formação.

Ações de formação

Uma vez despertado o interesse, propõe-se a realização de um processo formativo que combina a distribuição de materiais para leitura e visualização com a organização opcional de diálogos. Esta fase é composta por sete blocos temáticos ou pacotes: a informação, fraudes por correio eletrónico, as palavras-passe, o posto de trabalho, o teletrabalho, dispositivos móveis e redes sociais.

#ProtegeOTeuCampus
Edição 2022-23

ENCONTROS SAMA 2020

II Ciclo de Webinars

Módulo (NAU)	Data	Webinar
Para que nos serve a Proteção de Dados?	Out/2022	Webinar: 27/10/2022 -14H30 Url de acceso à gravação do webinar: https://youtu.be/vT09lsHRDJ8 Documentação: Para que nos serve a Proteção de dados? - Júlio Fernandes
A minha informação está segura? Dicas para proteção da informação.	Nov/2022	Webina: 28/11/2022 - 14H30 Url de acceso à gravação do webinar: https://youtu.be/kk1ódioFFN4 Documentação: A minha informação está segura? Dicas para proteção da informação

- + A informação
- + O correio eletrónico
- + As palavras-passe
- + O posto de trabalho
- + Os dispositivos móveis
- + O teletrabalho
- + As redes sociais

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

InfoSeg na Universidade de Évora

UNIVERSIDADE DE ÉVORA

ENCONTROS SAMA 2020

Obrigado!

jjg@uevora.pt

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional