UNIVERSIDADE DE ÉVORA

Jornadas Computação Científica 2019

PORTUGAL INCoDe.2030

Levantamentos, avaliações e resultados
na Universidade de Évora

Joaquim Godinho

Direcção de Serviços de Informática

Patrocinadores **Platina**

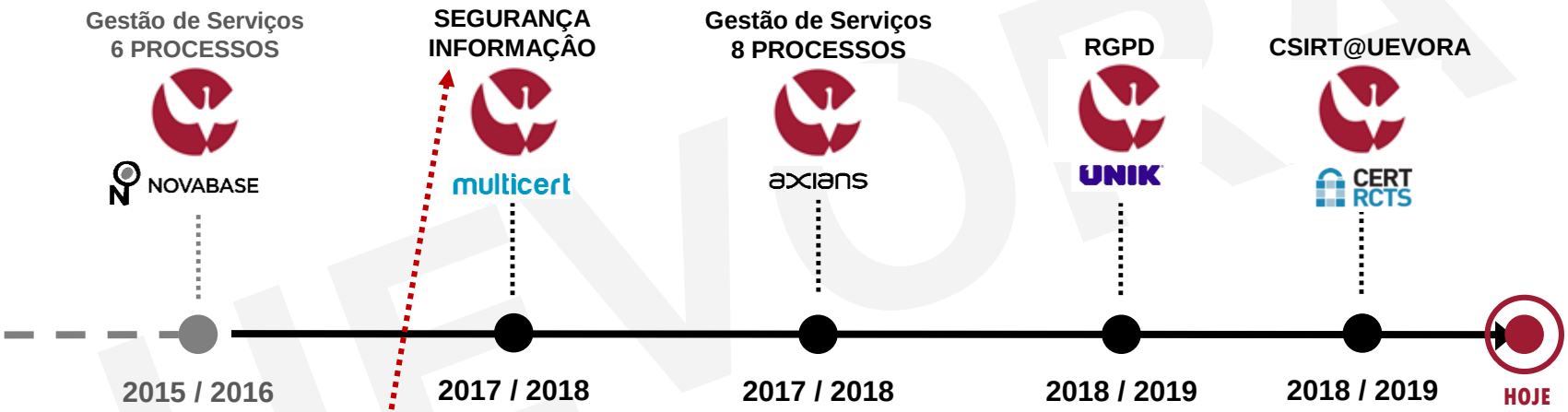
Patrocinadores **Ouro**

Patrocinadores **Prata**

Apoios

Organização

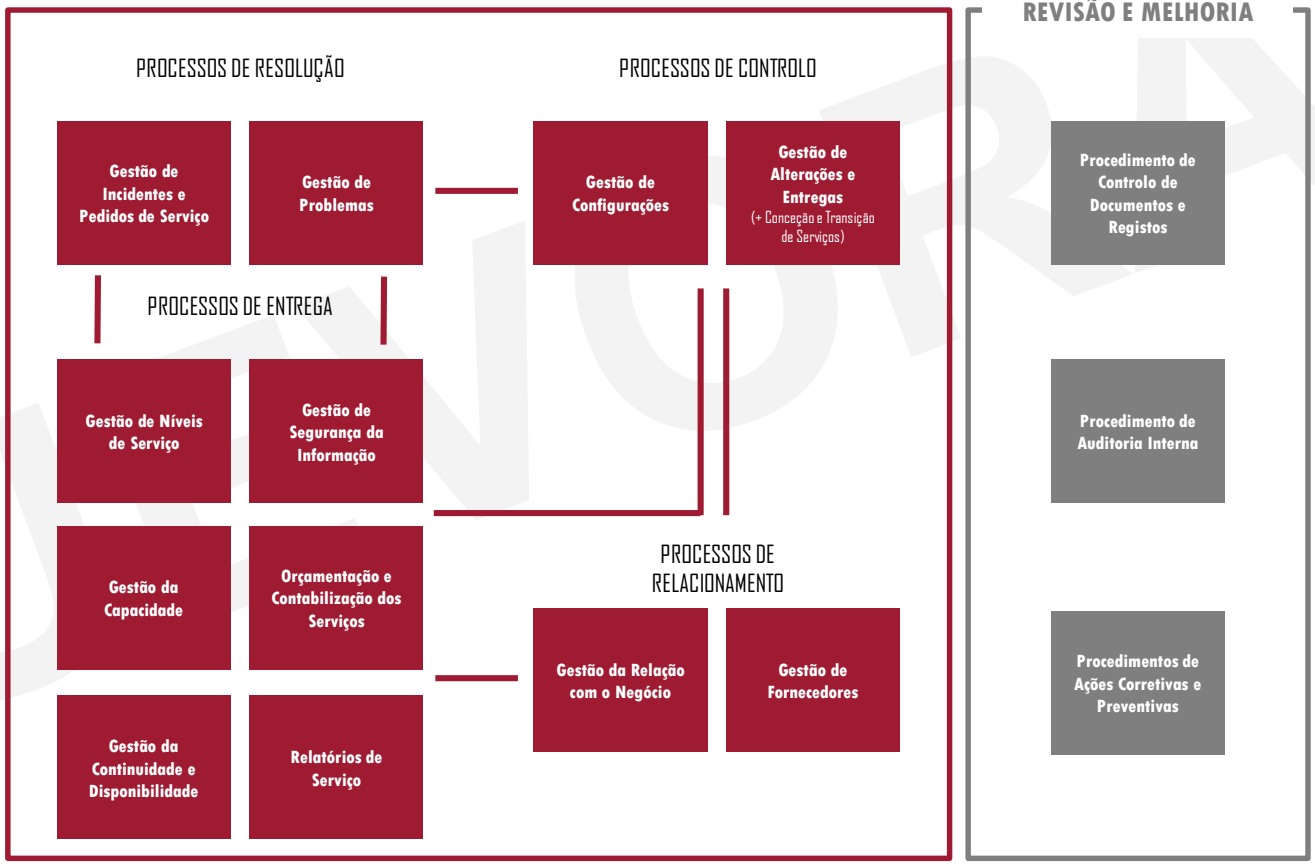
A História…



- Gestão de Pedidos de Serviço
- Gestão de Incidentes
- Gestão de Configurações
- Gestão de Alterações
- Gestão da Capacidade
- Gestão da Segurança da Informação

Gestão de Serviços TI (2015…2018)

- ITIL/ITSM
- ISO2000



Visão Geral do Sistema de Gestão de Serviços TI

CLIENTES

CANAIS

DSI

CATÁLOGO DE SERVIÇOS

SOLUÇÃO DE GESTÃO DE SERVIÇOS

OTRS

SERVICE DESK

PEDIDO DE SERVIÇO

INCIDENTE

Gestão de Pedidos de Serviço

Gestão de Incidentes

MODELO DE GESTÃO DE SERVIÇOS

Processo de Gestão de Incidentes e Pedidos de Serviço

Restaurar o serviço e executar pedidos de serviço, dentro dos níveis de serviço acordados.

Incidentes / Incidentes Graves

Registar e caraterizar	Escalar	Investigar e diagnosticar	Aplicar solução	Comunicar e fechar

Pedidos de Serviço

Analisar	Escalar	Executar	Comunicar e fechar

O QUE EU VOU CONSEGUIR COM ESTE PROCESSO ?

1. Controlo sobre todo o ciclo de vida dos incidentes e pedidos de serviço reportados (desde o seu registo ao seu fecho).
2. Incidentes e pedidos de serviço registados, classificados, priorizados, analisados, resolvidos e fechados.
3. Informação rápida sobre o estado e o progresso de resolução dos incidentes e pedidos de serviço reportados.
4. Visibilidade sobre os incidentes e pedidos de serviço não resolvidos de acordo com os níveis de acordo de serviço (SLA) definidos.
5. Partilha de informação relevante para a correção e resolução de incidentes e pedidos de serviço entre as equipas de trabalho.
6. Maior eficiência e produtividade na correção e resolução de incidentes e pedidos de serviço entre as equipas de trabalho.

Gestores de incidentes são os "super-heróis" do ITIL e o seu lema é "resolver depressa !"

INCIDENTE

- Os incidentes são interrupções de um serviço, uma redução na qualidade desse serviço ou uma falha de um componente.
- São eventos inesperados e não planeados que devem ser tratados com a maior brevidade possível e são, juntamente com os pedidos de serviço a principal responsabilidade de um *ServiceDesk*.
- Um incidente (ou mais) pode originar o registo de um problema.
- Os incidentes precisam ser registados na aplicação do *ServiceDesk* para que possam ser monitorizados e rastreados.

PROBLEMA

- Os problemas são o PORQUÊ / a causa raiz de um ou mais incidentes.
- Corrigir um problema geralmente requer testes para descobrir qual é a causa que lhe está subjacente e deste modo encontrar uma solução permanente.

Gestores de problemas são os "investigadores do CSI" que investigam as causas, colocam as questões adequadas, identificam o que aconteceu, porquê e como resolver de forma definitiva.

Processo de Segurança da Informação

Gerir a segurança da informação ao nível acordado, dentro de todas as atividades de gestão de serviços

Segurança da Informação

Avaliar o risco	Documentar os controlos *	Aprovar os controlos *	Implementar os controlos *	Avaliar a eficácia dos controlos *

* **Controlos:** Meios de gerir o risco, que inclui políticas, procedimentos, linhas de orientação, práticas ou estruturas organizacionais. O risco pode ser de natureza administrativa, tecnológica, de gestão ou legal.

Âmbito:
Serviços de Informática

Politica de Segurança da Informação
+ Segurança Física e Ambiental
+ Segurança das Comunicações
+ Segurança das Operações

Gestão de Risco

Conselho/Equipa de Segurança da Informação

Relatório de Avaliação do Risco de Segurança da Informação

O QUE EU VOU CONSEGUIR COM ESTE PROCESSO ?

1. Abordagem sistemática para uma gestão de riscos de segurança da informação mais eficaz e eficiente.
2. Aumento da fiabilidade e segurança da informação (no seus vários formatos) e dos sistemas, em termos de confidencialidade, integridade e disponibilidade.
3. Criação de uma cultura de segurança da informação, com o entendimento dos riscos e adoção de controlos como parte das práticas diárias de trabalho da organização.
4. Redução dos custos e alocação de recursos, com a implementação de controlos apropriados e suficientes.

Open-source Ticket Request System (OTRS)

Solução de gestão de serviços

- ***ServiceDesk***
- **Gestão de Incidentes e Pedidos de Serviço**
- **Gestão de Alterações**
- **CMDB (integrada com o Sistema de Informação da Universidade)**

… Incidentes de Segurança

… MAIOR TRANSPARÊNCIA

O OTRS permite a customização do catálogo de serviços, de acordo com as necessidades de serviços e infraestrutura da Organização.

… FÁCIL INTEGRAÇÃO

O OTRS permite a integração com outras soluções como o NAGIOS e OCS.

… RESPOSTAS RÁPIDAS

A automatização de processos e a integração de ferramentas de gestão de conhecimento permitem resultados rápidos e de alta qualidade.

… SUPORTE AOS UTILIZADORES

O OTRS permite aos utilizadores categorizarem e descreverem os incidentes e os pedidos de serviço, de forma fácil, rápida e segura.

… SIMPLIFICAÇÃO DA GESTÃO DE TICKETS

O OTRS permite a criação de filas de trabalho que recebem de forma automática a informação necessária para efetuarem a sua gestão de tarefas e prioridades.

… ESTATÍSTICAS E RELATÓRIOS

O OTRS permite a recolha de estatísticas e relatórios dinâmicos que vão suportar e facilitar a tomada de decisões.

Fonte: OTRS - https://otrs.com/otrs-solutions/it-service-managemer

Segurança da Informação (2017/18)

- Avaliação de *awareness* em Segurança da Informação
  - Realização de inquérito dirigido a todos os colaboradores da Universidade
- Sensibilização para a Segurança da Informação
  - Realização de workshop dirigido a responsáveis e "utilizadores-chave"
- Realização de Testes de Intrusão
  - Infraestruturas e serviços
- Divulgação e sensibilização a toda a organização
  - Comprometimento da gestão

Âmbito:

Universidade, Serviços de Informática e Serviços Académicos

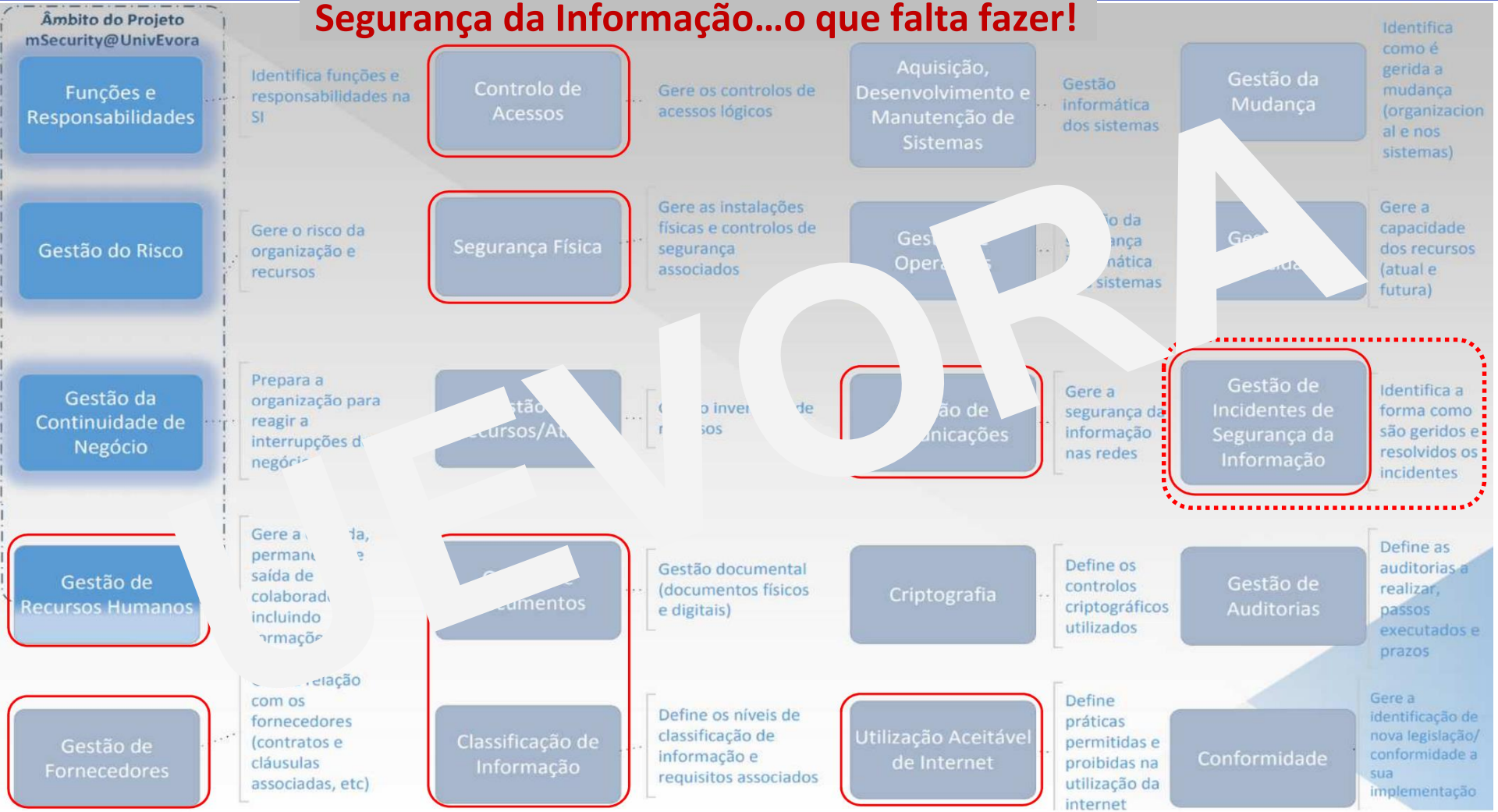
Sensibilizar os utilizadores da UE para as ameaças de segurança da informação a que estão expostos

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

Segurança da Informação…o que falta fazer!



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 DE SEGURANÇA DE INFORMAÇ

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. Dê preferência a gestores que funcione localmente em detrimento de Serviços que guardam as palavra-passe na Cloud.

Altere a palavra-passe através do SIIUE - utilize este sistema avra-passe que utiliza no acesso aos serviços/sistemas da Universid

Não reutilize as suas palavras-passe, nc palavra-passe em contexto pessoal e profissional - se o iliza no âmbito pessoal for comprometido, não irá colocar em os serviços no âmbito profissional.

Ap
Sã ras?

Milhõ loads são feitos diari para o móveis. Não desca apps de esconhecidas. E mesi apps exi app stores oficiais p não ser 1 s!

DICAS

Utilize o seu se fosse o seu computador - Com os mesmos cuidados istema 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 c us instal nfigure as atualizações automáticas para o irus, siste ivo e browser. Assim, estará protegido contra vulne es conhec

hing*
eja apan !

phishing s
me ficazes e
para n na s
dispos. dos
de enge. l s
recorrend

*São emails fra te com remetentes forjados ou com assuntos suspeitos, que procuram at iça para obter dados sensíveis ou fazê-lo visitar sites maliciosos.

DICAS

erifique 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 interceptar a informação.

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

Ace i Fi
mente

ecurso
Todos os dias se c múltiplas edes Wi-Fi para ter à internet. as a informação mite pode capturada s e os seus positiv n ser infetados

certificado digita onfigurar o acesso Wi Fi à rede eduroam. Garanta a nas comunicações. Mais informação disponível em http://wifi.uevora.pt/

Ev er a websites que não sejam HTTPS - Verifique sempre que o website que der 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.

Regulamento Geral de Proteção de Dados (2018/19)

Tipo	Data ▲	Assunto
Ordem de serviço	2018-03-15	Regulamento do Conselho de Segurança da Informação e **Proteção** de Dados Pessoais da Universidade de Évora
Despacho	2018-05-09	Regulamento do Conselho de Segurança da Informação e **Proteção** de Dados Pessoais
Despacho	2018-05-24	Nomeação do Encarregado de **Proteção** de Dados da Universidade de Évora
Despacho	2018-06-06	Composição do Conselho de Segurança da Informação e **Proteção** de Dados Pessoais

Artigo 3º

Composição

1- O CSIPDP é composto pelos seguintes membros:
   a) Presidente, cargo exercido pelo Reitor, ou titular com competências delegadas;
   b) Encarregado da Proteção de Dados (EPD);
   c) Responsável pela Segurança de Informação (RSI);
   d) Um representante de cada Unidade Orgânica;
   e) O Administrador da Universidade de Évora.
2- Os membros referidos nas alíneas b) a c) são designados pelo Reitor.

Adenda : f) Director dos Serviços de Ação Social

Artigo 5º

Encarregado da Proteção de Dados

1- O encarregado da proteção de dados tem as competências e funções definidas para o "Encarregado da Proteção de Dados" (*Data Protection Officer*), no âmbito do Regulamento Geral de Proteção de Dados.

Artigo 6º

Responsável pela Segurança de informação

1- O Responsável pela Segurança de Informação (*Chief Information Security Officer*) é a pessoa responsável pela coordenação e implementação da Gestão de Segurança da Informação na Universidade.

3- O Responsável pela Segurança de Informação reporta ao Reitor para garantir a disponibilidade dos recursos necessários, para a operacionalização e melhoria contínua da Gestão de Segurança da Informação.

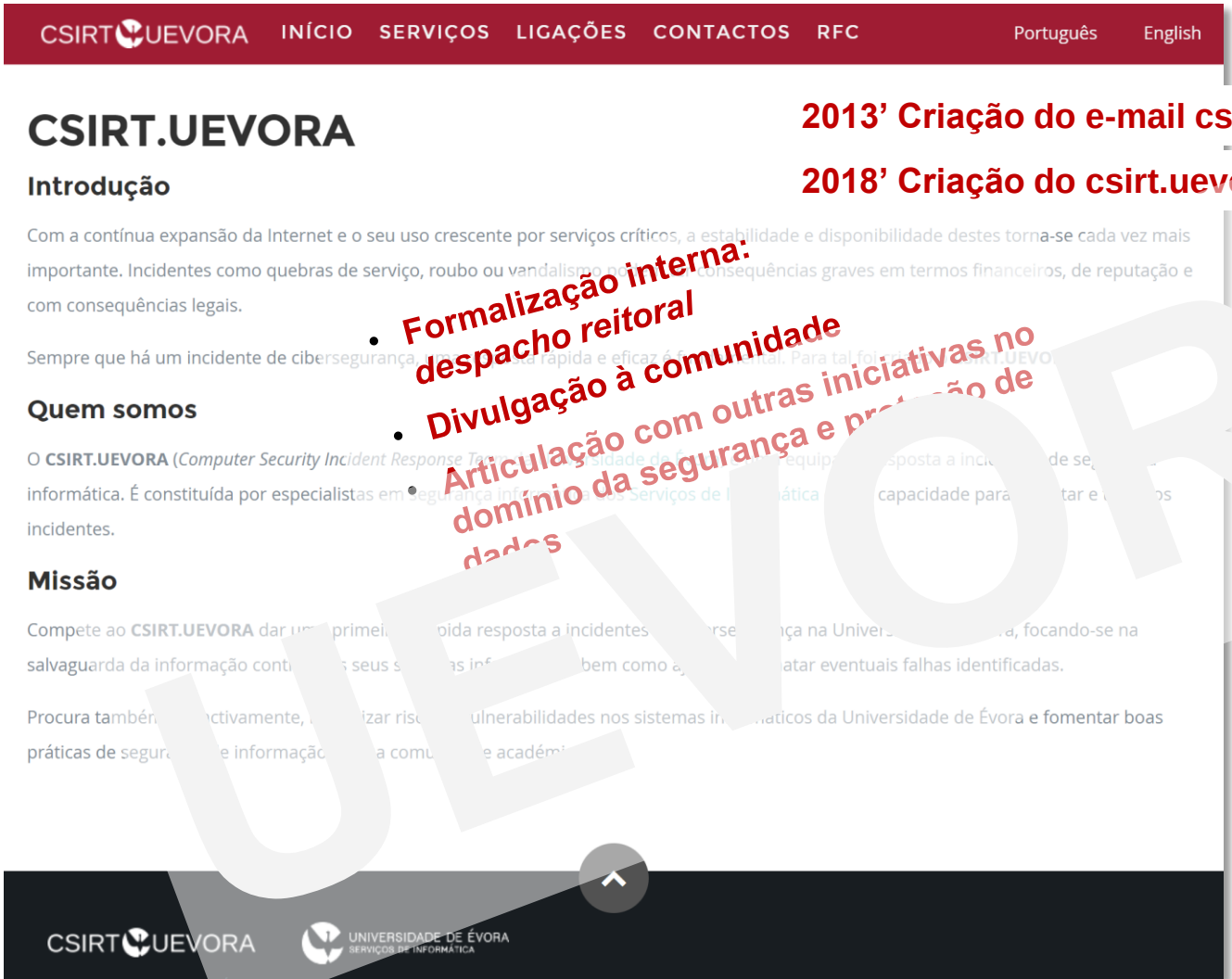
Regulamento Geral de Proteção de Dados (2018/19)

- Ambiente académico, dinâmico e pouco regulado
- Autonomia na…
  capacidade de decisão e … de implementação
  (UE = Data controller + Data processor)
- “Cultura organizacional fragmentada”
- Muuuitoooos dados pessoais: alunos, colaboradores, fornecedores, parceiros…

- Adotar uma abordagem incremental e modular
  - por áreas: académica, científica, administrativa…
  - por unidades: Escolas, Serviços,…
  - por domínios: legal, procedimental e técnico
- Assegurar apoio externo especializado
- Adquirir e reforçar competências internas : formação + sensibilização
- Promover uma “cultura” adequada : bom senso e ética + compromisso

Regulamento Geral de Proteção de Dados (2018/19)

- Avaliação de conformidade com o RGPD;
- Identificação dos dados pessoais e dados pessoais sensíveis, categorias e formas de tratamento;
- Elaboração de um Plano de Implementação do RGPD;
- Sensibilização dos “stakeholders”, dos responsáveis e dos utilizadores em geral relativamente ao RGPD



2013' Criação do e-mail csirt@uevora.pt

2018' Criação do csirt.uevora; adesão à RAC

- **Formalização interna: despacho reitoral**
- **Divulgação à comunidade**
- **Articulação com outras iniciativas no domínio da segurança e protecção de dados**

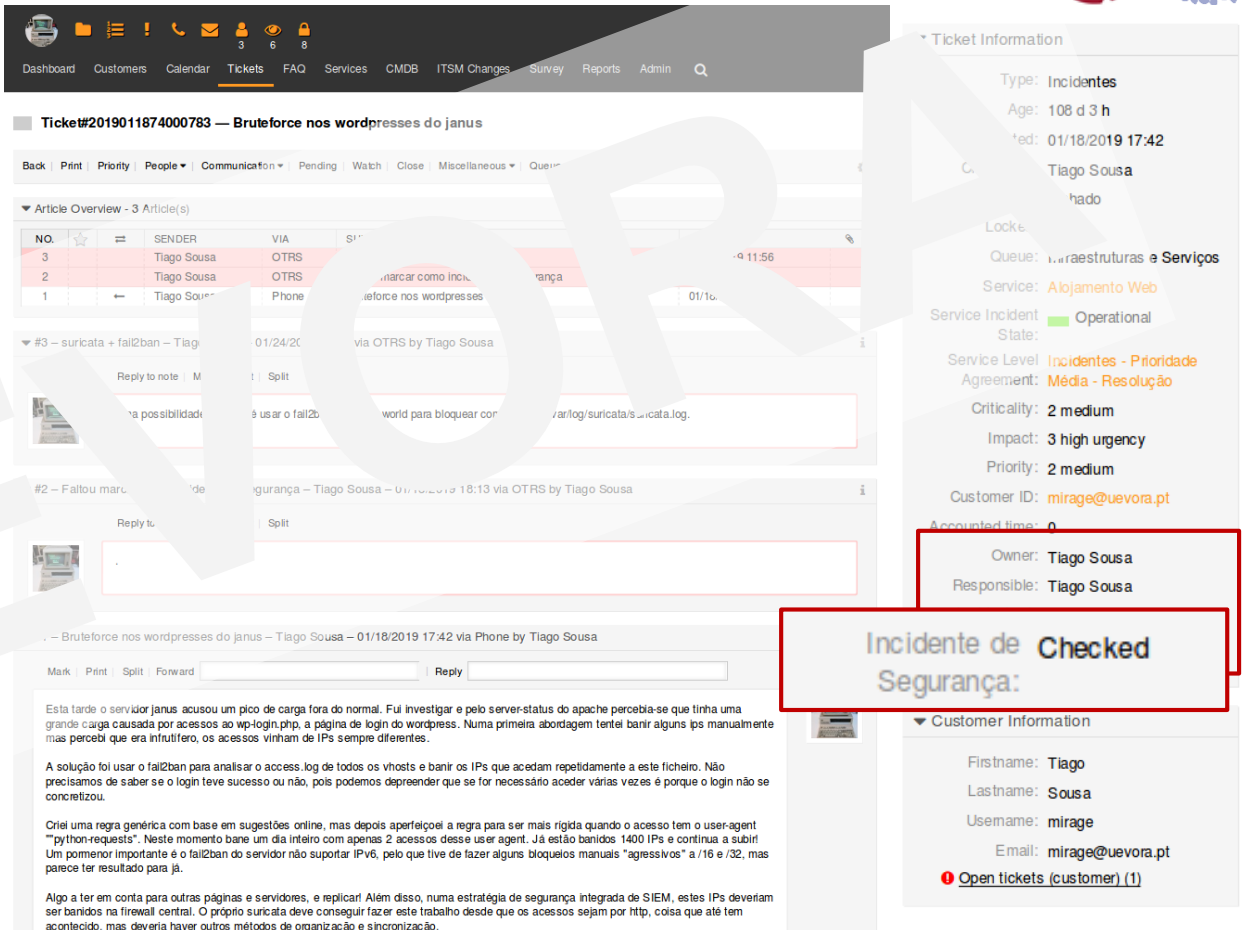
- 97 [illegible] registados desde 20[illegible] (Se[illegible]ontar com vic[illegible]yright)
- 7 e[illegible] 2019 (ate Abril)
  - [illegible]ginas comprometidas
  - Contas comprometidas
  - Serviços inseguros, Spamming, Brute force...
- Nem todos foram registados…
- Alertas RCTS-CERT

Incidente de Segurança

Registo CSIRT@UEVORA:
> OTRS “Checked”

Atribuição de responsável

Registo de resolução

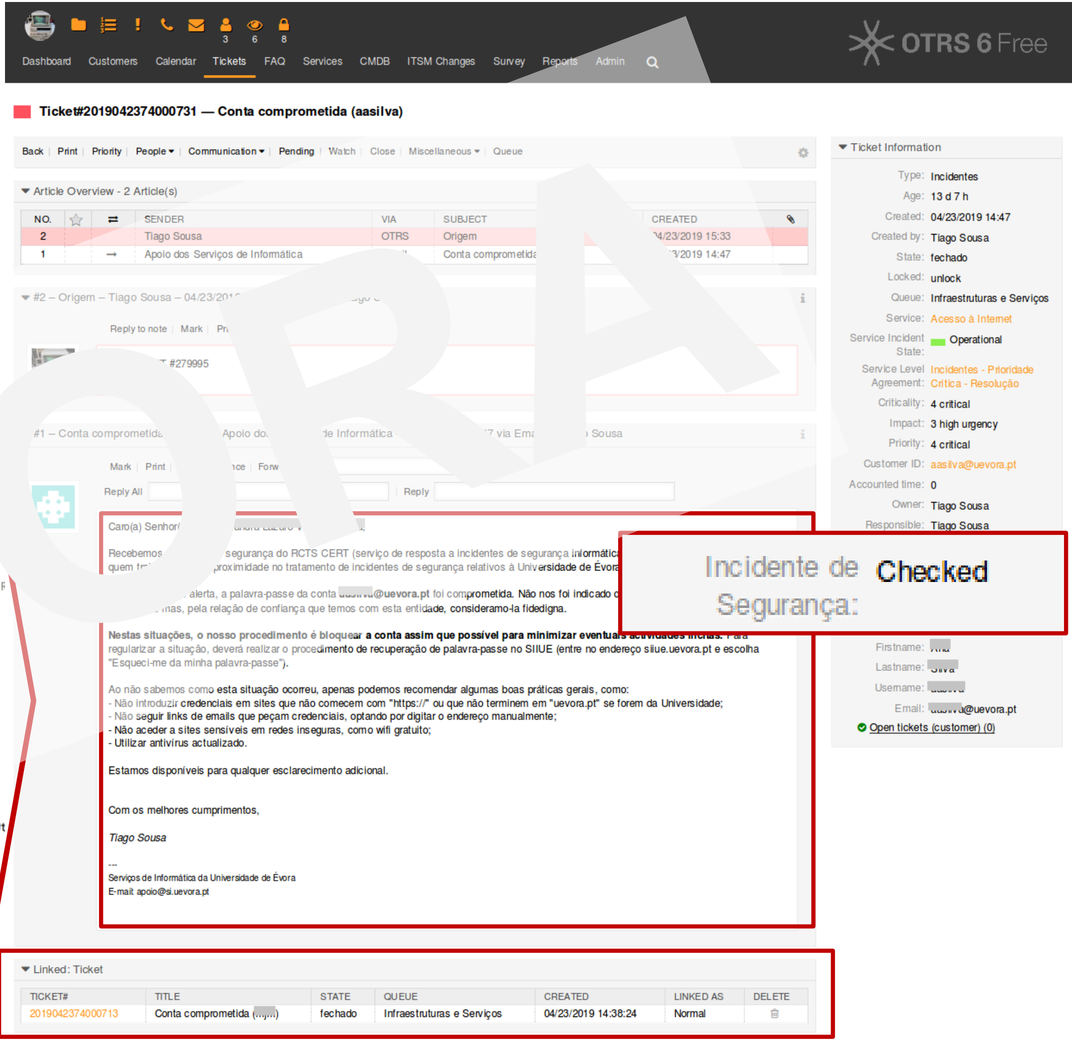


Incidente de Segurança

Alerta RCTS-CERT – Registo automático

x2 incidentes

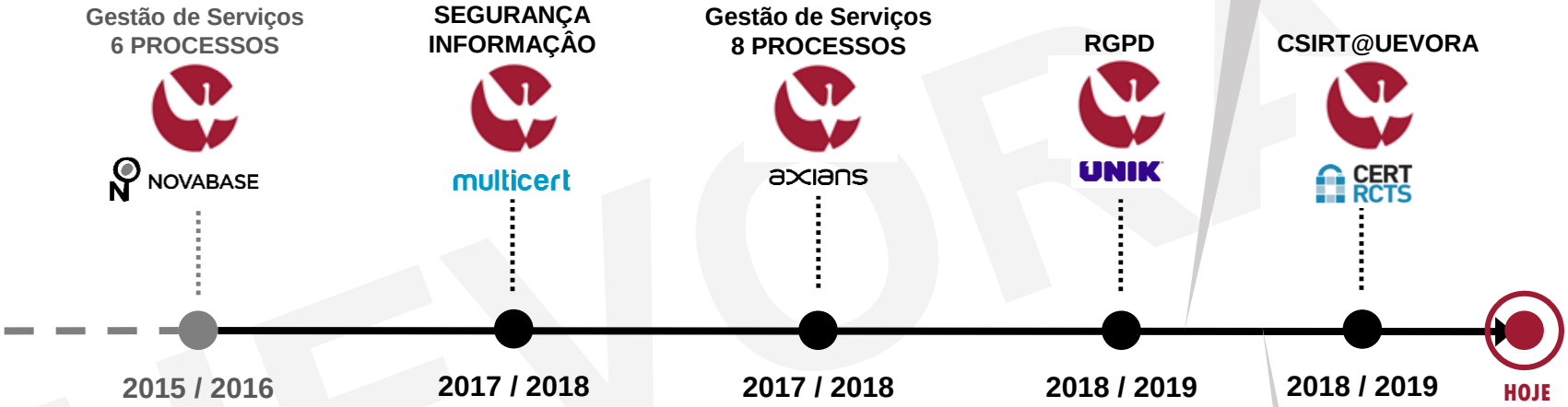
Notificação aos utilizadores



Moral da história…

O que correu bem

- Fases de “formação e sensibilização” e “apoio à implementação” cruciais para o desenvolvimento do projeto
- Evolução notória do nível de maturidade
- Demonstração das competências e capacidade da equipa



- **Colaboração “inter-pares” e Competências Internas**
  vs
- **Apoio Externo**
- **Mudança de mentalidade/cultura em toda a “organização”**
- **Disponibilidade de recursos (financeiros, humanos, materiais)**

O que podia ter corrido melhor

- Comunicação e gestão das expetativas da equipa ao longo do projeto
- “Sponsorship” da gestão de topo
- Mobilização da “comunidade”

UNIVERSIDADE DE ÉVORA

Jornadas Computação Científica 2019

PORTUGAL INCoDe.2030

Obrigado

jjg@uevora.pt

Patrocinadores **Platina**

Patrocinadores **Ouro**

Patrocinadores **Prata**

Apoios

Organização