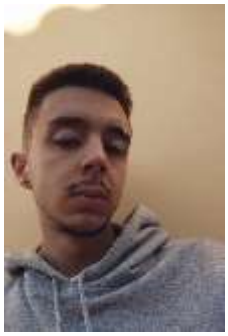
Universidade do Minho

MEI - Mestrado em Engenharia Informática

Engenharia de Segurança

1º ano / 2º semestre

Grupo 11 – Avaliação Prática 1

 pg47848 - Hugo Marques	 Pg46538 - José Florindo
 pg44420 - Nuno Mata	 a84288 - José Santos

20 de março de 2022

Conteúdo

1 - Introdução

A área da engenharia de segurança é extremamente vasta e abrange inúmeras áreas de outros campos da ciência. Nos dias que correm é quase impossível não estar perto de um dispositivo que necessite de um determinado tipo de proteção, seja um sensor biométrico, um smartphone, um router, entre outros. Se atentarmos a outros casos, apercebemo-nos que a engenharia de segurança é também aplicada em dispositivos médicos ou dispositivos bancários, sendo por isso uma área extremamente requisitada para conceber e assegurar a proteção dos mais diversos sistemas que podemos encontrar no nosso dia a dia.

O presente relatório surge no âmbito da Unidade Curricular de Engenharia de Segurança integrada no perfil de Criptografia e Segurança da Informação do curso de Mestrado em Engenharia Informática da Universidade do Minho.

Este é o primeiro de três projetos que ainda serão abordados na presente UC e propostos pelo professor. O objetivo do projeto passa pela análise de um tema (PA) e devido ao elevado número de grupos de trabalho na UC foram introduzidos diferentes temas para diferentes grupos. Ao nosso grupo (11), o professor propôs-nos o seguinte tema: *Operation Security*.

A ideia é estudar e analisar os requisitos evidenciados nos standards europeus *ETSI* [1] no âmbito das assinaturas digitais e serviços de confiança relacionados (em especial, no contexto do Regulamento *eIDAS)* [2] e relacioná-los com as normas e recomendações de melhores práticas de segurança efetuada por um standard da família *ISO/IEC 27000* [3].

2 - Contextualização

A ISO (International Organization for Standardization) é uma organização independente que desenvolve e promove normas, testes, padronizações e certificações de segurança da informação que facilitam e servem como base para a criação de um Sistema de Gestão de Segurança de Informação (SGSI), sendo aplicável a qualquer entidade. As certificações da família ISO 27000 foram desenvolvidas em parceria entre a **ISO** e a **IEC** (International Electrotechnical Commission), outra organização dedicada a standards. A ISO possui 2 principais normas:

- **ISO 27001** – padrão para sistema de gestão da segurança da informação (ISMS - *Information Security Management System*);
- **ISO 27002** – norma para tecnologia de informação, técnicas de segurança e guia de boas práticas para controlos de segurança da informação. Deve ser usada em conjunto com a ISO 27001. [4]

Enquanto isso, a Comissão Técnica (TC) *Electronic Signatures and Infrastructures* (ESI) lida com assinaturas digitais e serviços de confiança relacionados e publica standards europeus nesse âmbito. O TC ESI também cobre requisitos de política, segurança e técnicos para os *trust service providers* (TSP), como autoridades de certificação, autoridades de carimbo de data/hora, TSP fornecendo funções de validação ou criação de assinatura remota, provedores de entrega eletrónica registados e provedores de preservação de dados de longo prazo. O trabalho desta comissão passa também por apoiar o *Regulamento eIDAS*, bem como os requisitos gerais da comunidade internacional para proporcionar confiança nas transações eletrónicas.

3 - Segurança de operações: standards ISO27002

Tal como descrito na documentação *ISO 27002*, o objetivo deste tema da segurança de informações pretende garantir que as operações de processamento de informação são realizadas de forma correta e segura. Com vista em alcançar esse objetivo são apresentados uma série de standards, nesta documentação, que devem ser seguidos de forma a potenciar a implementação com sucesso de operações que lidam com o processamento de informações. São então diferenciados os 7 seguintes tópicos de interesse para os quais serão apresentadas as boas praticas a serem seguidas, de acordo com a *International Organization for Standardization* 27002(ISO):

3.1 - Procedimentos operacionais e responsabilidades

O primeiro tópico pretende garantir que o funcionamento das instalações onde o processamento de informação ocorre emprega operações corretas e seguras. Para atingir este objetivo são apresentados **guias de implementação** para cada um dos diferentes processos que devem ser considerados neste tópico.

3.1.1 - Documentação dos procedimentos operacionais

Neste ponto afirma-se que deve ser desenvolvida documentação relativa aos procedimentos e disponibilizada a todos os utilizadores que dela necessitarem. Sendo assim introduzido o guia de implementação relativo a este ponto, onde vão ser descritos quais procedimentos operacionais devem ser documentados de forma a especificar as instruções para o seu correto funcionamento, que incluem:

- Instalação e configuração de sistemas;
- Tratamento e processamento de informação, quer seja manual ou automaticamente;
- Funcionamento de backups;
- Procedimentos para o reinício e recuperação do sistema no evento de falha;
- Procedimentos de monitorização, etc.

3.1.2 - Gestão de mudanças

Ainda sobre este tópico são apresentadas algumas boas praticas a ter em consideração, de forma a haver controlo, caso ocorram mudanças na empresa, processos de negócio e instalações/sistemas de processamento de informações que possam afetar a segurança da informação. Afirmando-se que deve existir documentação de itens como:

- Identificação e registo de mudanças significativas;
- Planos e testes relativos a mudanças;
- Comunicação dos detalhes referentes às mudanças a todas as pessoas de interesse, etc.

O controlo inadequado de mudanças aos sistemas e instalações de processamento de informações são uma causa comum de falhas de sistema e segurança.

3.1.3 - Gestão de capacidade

Aqui a preocupação é principalmente relativa à performance do sistema. Por isso é aconselhado a monitorização dos recursos do sistema e a sua continua "afinação". É ainda referido que devem ser feitas projeções relativas aos requisitos futuros de capacidade para que o sistema possa garantir uma boa performance. De forma a atingir estes objetivos devem ser elicitados e identificados os requisitos de capacidade do sistema, tendo em consideração o quão critico é o sistema em causa. Fornecer capacidade suficiente pode ser alcançado através do seu aumento, mas também através da redução da demanda. Sendo expostos alguns exemplos de gestão de demanda de capacidade:

- Exclusão de dados obsoletos;
- Otimização de processos de *batch*;
- Otimização de queries à base de dados, etc.

3.1.4 - Separação dos ambientes de desenvolvimento, testes e operacionais

Neste ponto é referido que deve haver uma separação dos ambientes de desenvolvimento, testes e operacionais de forma a reduzir o risco de acessos e mudanças ao ambiente que não são autorizadas. Com esse objetivo deve ser identificado e implementado o nível de separação necessário, tendo em conta os seguintes itens:

- Regras para a transferência de software do estado de desenvolvimento para o estado operacional devem definidas e documentadas;
- Software de desenvolvimento e operacional deve ser executado em diferentes sistemas ou em diferentes processadores do computador, como também em diferentes domínios e diretorias;
- Mudanças a sistemas e aplicações operacionais devem ser testadas em ambientes de teste previamente a serem aplicadas ao sistema operacional, etc.

3.2 - Proteção contra *malware*

O objetivo deste tópico é a garantia de que a informação/ instalações de processamento de informação estão protegidas contra *malware*.

3.2.1 - Controlos contra *malware*

A documentação relativa a este ponto refere que devem ser implementados controlos de deteção, prevenção e recuperação em combinação com a atenção apropriada dos utilizadores de forma a proteger os sistemas contra *malware.* Esta proteção deve basear-se em software de reparação e deteção de *malware,* e também gestão de

controlos de acessos e mudanças no sistema, para isso são apresentadas as seguintes medidas:

- Estabelecimento de políticas que proíbem o uso de *software* não autorizado;
- Implementação de controlos para a deteção e impedimento de *software* não autorizado;
- Implementação de controlos para a deteção e impedimento de acesso a *websites* maliciosos (e.g. *blacklisting*);
- Instalação e atualização regular de *software* de deteção e reparação de *malware* para fazer o *scan* aos computadores como um controlo preventivo;
- Isolar ambientes onde *malware* possa ter impactos catastróficos, etc.

3.3 - Backup

As boas práticas apresentadas neste tópico resumem-se à proteção contra a perda de dados.

3.3.1 - Backup de informação

Cópias de backup da informação, software e imagens do sistema devem ser feitas e testadas regularmente de acordo com a política de backup estabelecida. Assim sendo, devem ser definidas as medidas de backup dentro de cada empresa, para que todas as informações e software essenciais sejam recuperados em caso de perda. No plano de backup deve considerar-se:

- Devem ser produzidos registos completos das cópias de *backup* e documentação dos procedimentos de recuperação;
- A extensão e frequência com que são realizados *backups;*
- Os *backups* devem ser guardados remotamente, de forma a não sofrerem danos caso ocorra um desastre no edifício principal;
- Em situações que o nível de confidencialidade é importante, os *backups* devem ser protegidos por métodos de criptografia, etc.

3.4 - *Logging* e monitorização

O registo de eventos e a produção de evidências é o objetivo deste tópico e para isso são descritas as boas práticas a serem seguidas na implementação dos diferentes passos inerentes a este ponto.

3.4.1 - *Logging* de eventos

Eventos, atividade do utilizador, erros, falhas e eventos relacionados com a segurança de informação devem ser guardados num *log* de eventos e analisados regularmente, o *log* de eventos deve incluir:

- IDs de utilizador;

- Atividades do sistema;
- Datas, horas e detalhes de eventos chave, e.g. *log-on* e l*og-off;*
- Mudanças ao sistema de configurações;
- Ficheiros acedidos e o tipo de acesso, etc;

O registo de eventos é a base para a monitorização automática, que é capaz de gerar relatórios de atividade e alertar automaticamente o sistema de segurança.

3.4.2 - Proteção da informação nos registos

As instalações que fazem os registos e a própria informação nos registos devem estar protegidas contra adulteração e acessos não autorizados. Para isso deve haver o controlo dos seguintes itens:

- Alterações ao tipo de mensagens que são guardadas;
- Ficheiros de *log* que sejam alterados ou apagados;
- Capacidade de armazenamento do ficheiro de *log* excedida, resultando em falhas no registo de eventos.

Os *logs* do sistema precisam ser protegidos, pois se os dados puderem ser modificados ou apagados, a sua existência pode criar uma falsa sensação de segurança.

3.4.3 - *Logs* de administrador e operador

Aqui tal como referido anteriormente defende-se que as atividades do administrador de sistema e do operador de sistema devem ser registadas e estes registos protegidos e regularmente revistos. Utilizadores com contas privilegiadas podem ter a capacidade de alterar os logs por isso é necessário os proteger e analisar constantemente.

3.5 - Controlo de *software* operacional

O objetivo do quinto tópico é a descrição de boas práticas para assegurar integridade dos sistemas operacionais.

3.5.1 - Instalação de *software* nos sistemas operacionais

Devem existir regras para controlar a instalação de *software* nos sistemas operacionais, no documento são dados os seguintes exemplos:

- a atualização do *software* operacional, aplicações e bibliotecas só deve ser realizada por administradores treinados e com autorização;
- os sistemas operacionais devem conter apenas código executável aprovado e não código em desenvolvimento ou compiladores;
- uma estratégia de reversão deve estar em vigor antes que alguma mudança seja implementada;

- deve ser mantido um registo de auditorias de todas as atualizações das bibliotecas e de programas operacionais, etc.

O *software* pode usar bibliotecas externas que devem ser monitorizados e controlados para evitar alterações não autorizadas, que podem introduzir falhas de segurança.

3.6 - Gestão de vulnerabilidades técnicas

O sexto tópico descreve como objetivo prevenir a exploração de vulnerabilidades técnicas. Por exemplo, não devem ser expostas ou de fácil acesso as tecnologias e *software* usados numa empresa, pois desta forma o processo de obtenção de informações para um potencial ataque torna-se mais demoroso. Algumas boas praticas para a gestão eficiente de vulnerabilidades técnicas são:

- dependendo da urgência com que uma vulnerabilidade técnica precisa ser tratada, a ação a tomar deve ser realizada de acordo com os controlos relacionados à gestão de mudanças ou seguindo procedimentos de resposta a incidentes de segurança da informação;
- Deve ser realizado e guardado um registo de todos os procedimentos realizados;
- Sistemas de alto risco devem ser sempre os primeiros a ser tratados;
- A empresa deve definir e estabelecer responsabilidades de gestão de vulnerabilidade, incluindo monitorização, avaliação de risco de vulnerabilidade, correção, rastreamento de ativos e quaisquer responsabilidades de coordenação necessárias, etc.

3.6.1 - Restrições de instalações de *software*

A implementação de regras que ditem qual o tipo de software pode, ou não, ser instalado pelos utilizadores devem ser criadas e implementadas. A instalação de software que não seja controlado pode introduzir vulnerabilidades que levam a vazamento de informações, perda de integridade ou outros incidentes de segurança da informação, ou a violação de direito de propriedade intelectual.

3.7 - Considerações a ter em auditorias a sistemas de informação

O objetivo deste tópico é minimizar o impacto que uma auditoria pode vir a ter num sistema de informação.

3.7.1 - Controlo de auditorias a sistemas de informação

O documento afirma que: auditorias e atividades envolvendo verificação de sistemas operacionais devem ser cuidadosamente planeados e acordados para minimizar interrupções nos processos de negócios. Por isso deve-se prestar atenção às seguintes recomendações.

- Os requisitos de auditoria para acesso a sistemas e dados devem ser acordados com os responsáveis apropriados;
- Os testes realizados em auditorias devem ser limitados ao acesso de "read only" ao software e aos dados;
- Testes em auditorias que possam afetar a disponibilidade do sistema devem ser executados fora do horário de funcionamento;
- Todos os acessos devem ser monitorizados e registado para produzir uma linha de referência, etc.

4 – Aplicação das normas nos requisitos ETSI

Após a recolha, análise e compreensão das principais normas de segurança de informação, dado o tema principal proposto, *Operation* Security, expostas no documento *ISO/IEC 27002*, versão 2013 [3], percebemos que o seu âmbito é vasto e começamos por recolher e analisar os requisitos apresentados no documento *ETSI* [1] e focamo-nos naqueles que eram possíveis de serem relacionados e aplicados às recomendações de melhores práticas efetuadas por um standard da família ISO, o ISO 270002, sendo este o objetivo principal do projeto.

A maior parte dos requisitos no documento *ETSI* [1], fazem referência a outras versões do documento, com alguns dos requisitos mais detalhados. Os requisitos recolhidos que acreditamos que pudessem ser aplicados às recomendações de segurança, no que diz respeito à segurança das operações, propostas pelo ISO, estão expostos a seguir.

Notação dos requisitos escolhidos:

- **OVR:** requisito geral (requisito aplicável a mais de 1 componente)
- **GEN:** Serviços de Geração de Certificados
- **REG**: Serviços de Registo
- **REV:** Serviços de Revogação
- **SDP:** Provisão de Dispositivo de Assunto

4.1. – Instalações, gestão e controlos operacionais

4.1.1 - Controlos Físicos

- **REQ-7.6-01:** O TSP (trust service provider) controla o acesso físico aos componentes do sistema do TSP cuja segurança é crítica para a prestação dos seus serviços de confiança e minimiza os riscos relacionados com a segurança física.
- **REQ-7.6-02**: O acesso físico aos componentes do sistema do TSP cuja segurança é fundamental para a prestação dos seus serviços de confiança será limitado a indivíduos autorizados. **Nota**: A criticidade é identificada através da avaliação de

risco, ou através de requisitos de segurança da aplicação, como exigindo uma proteção de segurança.

- **REQ-7.6-03:** Devem ser implementados controlos para evitar perdas, danos ou comprometimento de bens e interrupção das atividades comerciais.
- **REQ-7.6-04:** Devem ser implementados controlos para evitar o comprometimento ou roubo de informações e instalações de processamento de informações.
- **REQ-7.6-05:** As instalações relacionadas com a gestão da geração e revogação de certificados devem ser exploradas num ambiente que proteja fisicamente os serviços de compromissos através do acesso não autorizado a sistemas ou dados.
- **OVR-6.4.2-03:** Cada entrada na área fisicamente segura será sujeita a supervisão independente e a pessoa não autorizada será acompanhada por uma pessoa autorizada enquanto estiver na área segura.
- **OVR-6.4.2-04:** Todas as entradas e saídas devem ser registadas.
- **OVR-6.4.2-05:** A proteção física deve ser alcançada através da criação de perímetros de segurança claramente definidos (ou seja, barreiras físicas) em torno dos serviços de geração de certificados e de gestão de revogação.
- **OVR-6.4.2-06:** Todas as partes das instalações partilhadas com outras organizações devem estar fora do perímetro dos serviços de gestão da geração e revogação de certificados.
- **OVR-6.4.2-07:** Devem ser implementados controlos de segurança física e ambiental para proteger os recursos do sistema de alojamento das instalações, os próprios recursos do sistema, e as instalações utilizadas para apoiar o seu funcionamento.
- **OVR-6.4.2-08:** A política de segurança física e ambiental do TSP para sistemas relacionados com a geração de certificados e serviços de gestão de revogação deve abordar o controlo de acesso físico, proteção contra desastres naturais, fatores de segurança contra incêndios, falha dos serviços de apoio (por exemplo, energia, telecomunicações), colapso de estruturas, fugas de canalizações, proteção contra roubo, arrombamento e invasão, e recuperação de desastres.
- **OVR-6.4.2-09:** Devem ser implementados controlos para proteção contra equipamento, informação, meios de comunicação e software relacionados com os serviços do TSP que são retirados sem autorização.
- **OVR-6.4.2-10:** Outras funções relacionadas com as operações do TSP podem ser apoiadas dentro da mesma área segura, desde que o acesso seja limitado a pessoal autorizado.
- **OVR-6.4.2-11:** As chaves privadas **Root CA** devem ser mantidas e utilizadas fisicamente isoladas das operações normais, de modo que apenas o pessoal de confiança designado tenha acesso às chaves para utilização na assinatura de certificados CA (Certification Authority) subordinados.

4.1.2 - Controlos de Procedimento

- **REQ-7.4-04A:** O TSP deve administrar o acesso dos utilizadores aos operadores, administradores e auditores de sistemas aplicando o princípio dos "privilégios mínimos" ao configurar os privilégios de acesso.
- **REQ-7.4-05:** A administração deve incluir a gestão da conta de utilizador e a modificação ou remoção oportuna do acesso.
- **REQ-7.4-06:** O acesso à informação e às funções do sistema de aplicação deve restringido de acordo com a política de controlo de acesso.
- **REQ-7.4-07:** O sistema do TSP deve fornecer controlos de segurança informáticos suficientes para a separação de funções de confiança identificadas nas práticas do TSP, incluindo a separação das funções de administração da segurança e de funcionamento. Em particular, a utilização de programas utilitários do sistema deverá ser restringida e controlada.
- **REQ-7.4-08:** O pessoal do TSP deve estar identificado e autenticado antes de utilizar aplicações críticas relacionadas com o serviço.
- **REQ-7.4-09:** O pessoal do TSP deve ser responsável pelas suas atividades. **Exemplo**: Retendo registos de eventos.
- **GEN-6.4.3-02:** A emissão de certificados pela CA de raiz deve estar sob, pelo menos, duplo controlo por pessoal autorizado e de confiança, de tal forma que uma pessoa não possa assinar certificados subordinados por si só.

4.1.3 – Procedimentos de Registo de Auditoria

- **REQ-7.10-01:** O TSP deve registar e manter acessíveis durante um período adequado de tempo, incluindo após a cessação das atividades do TSP, todas as informações pertinentes relativas aos dados emitidos e recebidos pelo TSP, em particular, para efeitos de apresentação de provas em processos judiciais e para efeitos de assegurar a continuidade do serviço.
- **REQ-7.10-02:** A confidencialidade e integridade dos registos atuais e arquivados relativos ao funcionamento de serviços devem ser mantidos.
- **REQ-7.10-03:** Os registos relativos ao funcionamento dos serviços devem ser completa e confidencialmente arquivados de acordo com as práticas comerciais divulgadas
- **REQ-7.10-04:** Os registos relativos ao funcionamento dos serviços serão disponibilizados, se necessário, para efeitos de prova do correto funcionamento dos serviços, para efeitos de processo judicial.
- **REQ-7.10-05:** Deve ser registado o tempo exato de eventos significativos de sincronização ambiental, de gestão de chaves e sincronização do relógio.
- **REQ-7.10-06:** O tempo utilizado para registar os eventos conforme exigido no registo de auditoria deve ser sincronizado com UTC pelo menos uma vez por dia.

- **REQ-7.10-07:** Os registos relativos aos serviços devem ser mantidos por um período de tempo, conforme adequado para a prestação de provas jurídicas necessárias e conforme notificado nos termos e condições do TSP
- **REQ-7.10-08:** Os eventos devem ser registados de forma que não possam ser facilmente eliminados ou destruídos (exceto se forem transferidos de forma fiável para meios de longo prazo) no período de tempo que lhes é exigido.

  Exemplo: Isso pode ser conseguido, por exemplo, através da utilização de meios de escrita, de um registo de cada suporte amovível utilizado e da utilização de backup off-site ou através de armazenamento paralelo das informações em vários sites (por exemplo, 2 ou 3) independentes.
- **OVR-6.4.5-02:** Todos os eventos de segurança devem ser registados, incluindo alterações relacionadas com a política de segurança, arranque e encerramento do sistema, falhas no sistema e falhas no hardware, atividades de firewall e router e tentativas de acesso ao sistema PKI.
- **REG-6.4.5-03:** Todos os eventos relacionados com o registo, incluindo pedidos de nova chave de certificado ou renovação, devem ser registados.
- **REG-6.4.5-04:** Todas as informações de registo, incluindo as seguintes, devem ser registadas:
    - tipo de documento apresentado pelo requerente para apoiar o registo;
    - registo de dados de identificação únicos, números ou uma combinação dos mesmos (por exemplo, cartão de cidadão ou passaporte do requerente) de documentos de identificação, se aplicável;
    - localização de cópias de pedidos e documentos de identificação, incluindo o contrato de assinante
    - quaisquer escolhas específicas no contrato do assinante (eg. consentimento para a publicação do certificado;
    - identidade da entidade que aceita o pedido;
    - método utilizado para validar documentos de identificação, se houver;
    - nome da receção do TSP e/ou da autoridade de registo, se aplicável
- **REG-6.4.5-04A:** O TSP deve documentar a forma como a informação registada de acordo com o requisito anterior é acessível.
- **REG-6.4.5-05:** O TSP deve manter a privacidade das informações sobre o assunto.
- **GEN-6.4.5-06:** O TSP deve registar todos os eventos relacionados com o ciclo de vida das chaves CA.
- **GEN-6.4.5-07:** O TSP deve registar todos os eventos relacionados com o ciclo de vida dos certificados.
- **GEN-6.4.5-08:** O TSP deve registar todos os eventos relacionados com o ciclo de vida das chaves geridas pela autoridade de certificação, incluindo quaisquer chaves de assunto geradas pela CA.
- **REV-6.4.5-09:** O TSP deve registar todos os pedidos e relatórios relacionados com a revogação, bem como a ação resultante.

- **SDP-6.4.5-10:** O TSP deve registar todos os eventos relacionados com a preparação do dispositivo do sujeito.
- **OVR-6.4.5-11: O** TSP deve documentar com precisão o período de retenção das informações acima mencionadas nas suas declarações de práticas e indicar quais as informações que estão sujeitas a ser entregues através do seu plano de rescisão.

Para o registo de informações relativas a certificados qualificados da UE, aplicam-se os seguintes requisitos específicos:

- A informação deve ser mantida conforme necessário para cumprir os requisitos legais para além da cessação do TSP

Nota: O Regulamento (UE) n.º 910/2014 exige que um TSP qualificado "registe e mantenha acessível durante um período de tempo adequado, incluindo após a cessação das atividades do prestador de serviços confiáveis qualificado, toda a informação relevante relativa a dados emitidos e recebidos pelo prestador de serviços confiáveis qualificado, em particular, para efeitos de apresentação de provas em processos judiciais e para efeitos de assegurar a continuidade do serviço. Tal registo pode ser feito por via eletrónica". [2]

5 – Voto eletrônico online

As votações eletrónicas online trazem grandes preocupações a nível da segurança de informação. Os aspetos de validação e controlo de acesso e o de integridade de dados são discutivelmente uns dos mais importantes, mas existem outros como por exemplo a confidencialidade.

Neste capítulo serão indicadas quais as medidas e boas praticas que foram abordadas (tanto na documentação ISO 27000 como ETSI) sobre o nosso tema, de segurança de operações, que adequam num contexto de votação eletrónica.

5.1 – Medidas ISO

Proteção contra *malware*

Este tópico, abordado no subcapítulo 3.2, é muito relevante no contexto de votação eletrônica, já que o seu objetivo é a garantia de que as informações e sistemas de informação estão protegidos. As consequências de não haver esta garantia podem ser fatais naquilo que são as fundações de uma votação, pois abrem a porta a vulnerabilidades não só ao sistema como às informações e identidade dos utilizadores do sistema.

Documentação dos procedimentos operacionais

É também importante num sistema de votação online existirem medidas de procedimentos operacionais pela natureza crítica de um sistema deste tipo.

Gestão de mudanças

Devem ser registadas todas as mudanças pois os controlos inadequados de mudanças aos sistemas causam falhas de segurança e neste caso, sendo este um sistema tão critico, é obrigatório que não haja falhas de segurança.

***Logging* e monitorização**

Outro aspeto importante é o *logging* e monitorização do sistema, pois através do registo das informações é possível fazer uma monitorização automática e alertar automaticamente o sistema de segurança. Este aspeto pode ser particularmente útil caso haja uma alteração não solicitada aos dados do sistema, é de certa forma uma última linha de defesa para garantir que existe integridade dos dados.

Proteção da informação nos registos

Temos de garantir que a informação de log é protegida contra adulteração e acessos não autorizados, devendo também sempre cifrar as informações guardadas, para conseguirmos oferecer a garantia de que o sistema está a funcionar como previsto. Neste caso de adulteração de votos, conseguimos garantir que existe proteção.

Gestão de vulnerabilidades técnicas

Este tópico, referido no subcapítulo 3.6, tem relevância também neste contexto. Para um sistema critico como um de votação online é extremamente importante que não sejam divulgadas ou expostas informações referentes às tecnologias usadas no seu sistema. A consequência de não haver esta garantia pode traduzir-se em ataques direcionados às vulnerabilidades conhecidas das tecnologias usadas no sistema, o que aumenta a probabilidade de um ataque ser eficaz.

5.2 – Controlos Físicos

REQ-7.6-01 – É necessário um sistema de segurança para assegurar que a integridade do serviço não é comprometida.

REQ-7.6-02 – Apenas indivíduos autorizados têm acesso físico aos componentes do serviço.

REQ-7.6-03 – No caso de falha queremos ter um sistema que recupere o estado das votações.

REQ-7.6-04 – Devemos ter um controlo para evitar a adulteração dos votos.

OVR-6.4.2-03 – Qualquer entrada física na área por uma pessoa não autorizada, deve ser acompanhada por uma pessoa autorizada.

OVR-6.4.2-04 – Todas as entradas e saídas devem ser registadas, para no caso de haver uma falha de segurança ser possível identificar.

OVR-6.4.2-05 – A infraestrutura deve ser segura, contra pessoas não autorizadas a modificar o sistema e, portanto, deve haver barreiras físicas.

OVR-6.4.2-07 – Sendo isto um serviço de voto não queremos que haja falhas tanto no sistema como nas instalações utilizadas para apoiar o seu funcionamento.

OVR-6.4.2-08 – O sistema deve estar protegido contra incêndios, falhas naturais, etc. Como estamos a falar de um sistema de voto que pode decidir o rumo de um país, por exemplo, é importante que no caso de um incidente destes tenhamos medidas para retomar a integridade e a robustez do sistema.

5.3 – Controlos de Procedimento

REQ-7.4-04A – É importante o sistema ter privilégios de acesso porque nem toda a gente precisa de aceder às mesmas áreas.

REQ-7.4-06 – Como se trata de um sistema de votação eletrónica, a privacidade deve prevalecer acima de tudo, por isso deve haver um controlo de acesso às informações do sistema e de cada individuo respetivamente.

REQ-7.4-08 -- A assinatura ou chave móvel digital é essencial para identificar e autenticar uma determinada pessoa de modo a prestar o seu direito de voto.

GEN-6.4.3-02 -- É essencial haver um processo de confirmação de que um sistema de votação eletrónica está em conformidade com os requisitos e padrões prescritos. Isso poderá ser feito por medidas que vão desde teste e auditorias a certificações formais.

5.4 – Procedimentos de Registo de Auditoria

REQ-7.10-01 – Sendo este um processo de voto, tem de haver meios de usar como prova em processos judiciais, a veracidade dos votos.

REQ-7.10-02 – A confidencialidade e a integridade de um sistema de votação eletrónica online, obviamente tem de ser mantida.

REQ-7.10-04 – Caso seja necessário tem de haver uma maneira de disponibilizar os registos relativos ao funcionamento do serviço, para efeitos de prova.

REQ-7.10-05 – Sendo a segurança da solução um aspeto critico, deve ser registado exatamente o timestamp de eventos significativos de sistema.

REQ-7.10-07 – Os registos devem ser mantidos durante um período, conforme o necessário legalmente para a prestação de provas de que a votação decorreu sem adulteração de votos.

REQ-7.10-08 – Num Sistema de voto eletrónico não queremos de todo que os eventos possam ser eliminados. Queremos manter um rasto de tudo o que aconteceu na votação.

OVR-6.4.5-02 – Queremos assegurar que todos os eventos de segurança devem ser registados. Pois caso a votação tenha sido comprometida queremos ter informação sobre a mesma.

REG-6.4.5-04 – Queremos que o sistema tenha informação sobre todas as entidades que estejam registadas. Tais como documentos de identificação, etc. De forma a em caso de falha de segurança ser possível de saber a origem.

REG-6.4.5-05 – A privacidade do voto deve ser assegurada, não mostrando assim a identidade do eleitor.

6 - Referências

[1] - ETSI. (2021, 05). Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers . *ETSI EN 319 401 V2.3.1*, p. 23.

[2] - Europeia, J. O. (2014). REGULAMENTO (UE) N.o 910/2014 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE. *Jornal Oficial da União Europeia .*

[3] - ISO. (2013, 10). ISO/IEC 27002:2013. *Information technology — Security techniques — Code of practice for information security controls*, p. 80.

[4] - Wikipedia. (2021, 12 21). *ISO/IEC 27000-series*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_27000-series

[5] - ETSI. (2021, 11). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. *ETSI EN 319 411-2 V.2.4.1*, p. 31.