* 1. VULNERABILIDADES E EXPOSIÇÕES COMUNS (CVE)

Este anexo contém as listas dos riscos de segurança e operacionais conhecidas. A alimentação destas listas é feita pelo AUDITOR antes mesmo de haver qualquer verificação de exposição do SISTEMA a cada risco.

As listas das vulnerabilidades conhecidas são transversais a todos os sistemas auditados pelo AUDITOR e funcionam com listas de verificação que se pretendem ser o mais completas e amplas possível.

Esta estratégia assenta na ideia de que muitos riscos de segurança e riscos operacionais são transversais a diferentes sistemas e organizações, e que a aprendizagem contínua do AUDITOR fruto da evolução individual dos sistemas pode ajudar no aumento iterativo da segurança de forma coletiva. Assim, e com base nesta estratégia, a cada auditoria de revisão é possível considerar e analisar uma maior quantidade de exposição a vulnerabilidades, fruto da experiência adquirida na revisão de outros sistemas.

* + 1. Infraestrutura

Nesta secção podem encontrar-se os formulários que apoiam o AUDITOR no levantamento de vulnerabilidades de infraestrutura.

* + - 1. Vulnerabilidades das barreiras de acesso à infraestrutura

Este anexo contém o formulário de suporte à verificação do funcionamento das barreiras de acesso à infraestrutura definidas no PSD do SISTEMA.

**VULNERABILIDADES DAS BARREIRAS DE ACESSO À INFRAESTRUTURA**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de funcionamento dos dispositivos envolvidos nas barreiras de acesso à infraestrutura. O funcionamento das barreiras de acesso ao nível dos SO é avaliado através dos modelos utilizados para verificar as vulnerabilidades de computadores e servidores.

A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar é fruto da aprendizagem contínua do AUDITOR nos diferentes sistemas que audita.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VBAI-V1.0A |

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O seu preenchimento facilita a identificação das vulnerabilidades a levantar e as medidas corretivas ou recomendações a propor. A coluna ITEM contém vulnerabilidades conhecidas que servem de guia à auditoria. A coluna REAÇÃO sugere a descrição da vulnerabilidade a registar, e medidas corretivas ou recomendações a sugerir.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| DESCRIÇÃO:  As barreiras de acesso à infraestrutura pela internet previstas no PSD estão total ou parcialmente inoperacionais (e.g. *firewall* desativada).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  As barreiras de acesso à infraestrutura pela internet estão total ou parcialmente inoperacionais. Se estas barreiras não estiverem em pleno funcionamento não existem impedimentos no acesso de estranhos ao SISTEMA, deixando-o vulnerável.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente no que diz respeito ao controlo de acesso à infraestrutura através da internet. |
| DESCRIÇÃO:  As barreiras de acesso à infraestrutura pela rede local não existem, ou estão previstas no PSD mas estão total ou parcialmente inoperacionais (e.g. a ligação de novos dispositivos à rede é admitida sem entraves por algum dos distribuidores (e.g. router do operador tem *switch* sem gestão de portas), etc.).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  O SISTEMA permite que qualquer equipamento possa ser ligado à rede local com ou sem fios. Esse equipamento pode por em causa a estabilidade do SISTEMA, por causa de más configurações ou pelo facto de conter *malware* e contaminar os outros dispositivos.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, instalando ou reativando as barreiras de acesso à infraestrutura a partir da rede local. |
| DESCRIÇÃO:  As palavras-chave de acesso à configuração dos dispositivos são as originais do dispositivo.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  A utilização de palavras-chave originais torna os dispositivos visados em vulnerabilidades do SISTEMA porque pode permitir o acesso silencioso por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à alteração de palavras-chave originais dos dispositivos. |
| DESCRIÇÃO:  As palavras-chave de acesso à configuração dos dispositivos são desconhecidas.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  As palavras-chave de acesso à configuração dos dispositivos são desconhecidas. A impossibilidade de acesso à configuração do dispositivo aumenta a probabilidade de acesso silencioso por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  No caso da impossibilidade de repor a palavra-chave de acesso à configuração do dispositivo, recomenda-se a implementando de barreiras adicionais de acesso ao SISTEMA com dispositivos cuja administração esteja totalmente sob o domínio da ORGANIZAÇÃO. |
| DESCRIÇÃO:  A versão de *firmware* atualmente instalada nos dispositivos não é a última estável disponibilizada pelos fabricantes.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem dispositivos com *firmware* que não têm instalada a última versão disponibilizada pelo fabricante. As atualizações de *firmware* podem impedir a invasão do sistema por estranhos porque resolvem vulnerabilidades descobertas.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente atualizando as *firmwares* desatualizados, prevendo a hipótese de resultar em inoperabilidade dos dispositivos. |
| DESCRIÇÃO:  Não existe nenhuma barreira adicional de acesso à rede pela internet, além dos dispositivos da operadora que fornece o serviço (e.g. *routers*).  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Como não existe nenhuma barreira adicional de acesso à rede local pela internet além dos equipamentos fornecidos pela operadora (e.g. routers), e como estes são acedidos por pessoal estranho à ORGANIZAÇÃO (e.g. correção de avarias do serviço), não é possível controlar e auditar tudo o que é feito no SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, implementando barreiras adicionais de acesso ao SISTEMA com dispositivos cuja administração esteja totalmente sob o domínio da ORGANIZAÇÃO. |
| DESCRIÇÃO:  Não existe nenhum dispositivo que funcione como primeiro nível de proteção contra *malware* ao nível da infraestrutura (e.g. *appliance* de segurança).  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Não existe nenhum dispositivo que funcione como primeiro nível de proteção de infraestrutura. Mesmo que os computadores do SISTEMA estejam protegidos com aplicações de segurança de SO, um primeiro nível de segurança de infraestrutura é sempre recomendável, até para promover que equipamentos sem SO também estejam protegidos (e.g. impressoras, NAS, etc.).  MEDIDA CORRETIVA:  Recomenda-se a implementação de um mecanismo adicional de proteção contra *malware* ao nível da infraestrutura com o objetivo de promover o aumento do nível de segurança do SISTEMA. |
| DESCRIÇÃO:  A subscrição da aplicação de proteção contra *malware* de infraestrutura caducou.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  A subscrição da aplicação de proteção contra *malware* de infraestrutura caducou. Se não estiver em funcionamento não protege o SISTEMA deixando-o vulnerável a ataques.  MEDIDA CORRETIVA:  Promover junto do RESPONSÁVEL PELO TRATAMENTO de dados que o serviço seja reposto o mais rapidamente possível alertando para os riscos e vulnerabilidades pelo facto de a aplicação estar caducada. |
| DESCRIÇÃO:  A aplicação de proteção contra *malware* de infraestrutura não se está a atualizar automaticamente.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  A aplicação de proteção contra *malware* de infraestrutura não está a atualizar-se automaticamente. Se não estiver em pleno funcionamento não protege o SISTEMA deixando-o vulnerável a ataques.  MEDIDA CORRETIVA:  Solicitar que o problema técnico seja resolvido o mais rapidamente possível. |
| DESCRIÇÃO:  A aplicação de proteção contra *malware* de infraestrutura não está totalmente ativa.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  A aplicação de proteção contra *malware* de infraestrutura não está totalmente ativa. Se não estiver em pleno funcionamento não protege o SISTEMA na totalidade, deixando-o vulnerável a ataques.  MEDIDA CORRETIVA:  Solicitar que o problema seja resolvido notificando o ADMINISTRADOR DE SISTEMA para ativação das proteções desligadas o mais rapidamente possível. |
| DESCRIÇÃO:  Existem acessos externos autorizados, que não possuem qualquer mecanismo de proteção de ligação.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem acessos externos autorizados, que não possuem qualquer mecanismo de proteção de ligação. Os acessos externos podem pôr em causa a privacidade, segurança, integridade e disponibilidade dos dados do SISTEMA (e.g. *man-in-.the-middle*).  MEDIDA CORRETIVA:  Recomenda-se a implementação imediata de mecanismos de proteção de ligações externas (e.g. VPN). |
| DESCRIÇÃO:  Os certificados digitais utilizados para validação de autenticidade ou encriptação de dados em comunicações da ORGANIZAÇÃO (e.g. ligação de sites da VPN, proteção da ligação para administração via http, etc.) estão caducados.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem certificados digitais utilizados na validação de autenticidade ou encriptação de dados em comunicações da ORGANIZAÇÃO que estão caducados. A comunicação sem certificados é insegura e deixa o SISTEMA vulnerável a ataques (e.g. *man-in-the-middle*).  MEDIDA CORRETIVA:  Promover a renovação dos certificados imediatamente, notificando o ADMINISTRADOR DE SISTEMA para a urgência deste processo. |
|  |  |
| DESCRIÇÃO:  Existem incoerências entre as exceções de acesso previstas no PSD, e as efetivamente aplicadas nos dispositivos de controlo de acesso à infraestrutura.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem incoerências entre as exceções de acesso previstas no PSD e as efetivamente aplicadas nos dispositivos de controlo de acesso à infraestrutura. A configuração abusiva de exceções pode facilitar o acesso não autorizado por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, solicitando ao ADMINISTRADOR DE SISTEMA que reconfigure as regras de exceção para apenas aquelas que estão previstas no PSD. Solicitar a alteração das palavras-chave dos dispositivos em causa. |
| DESCRIÇÃO:  Existe acesso à infraestrutura através de distribuidores de rede *wireless* sem autorização expressa e justificada em ata pelo RESPONSÁVEL PELO TRATAMENTO de dados.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existe acesso à infraestrutura através de distribuidores de rede *wireless* sem autorização expressa e justificada em ata pelo RESPONSÁVEL PELO TRATAMENTO de dados. Aceder à rede sem fios do SISTEMA é equivalente a utilizar a rede com cabo. O acesso ao SISTEMA não previsto no PSD e no Regulamento do SISTEMA facilita acessos não autorizados colocando os dados em risco.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, desativar imediatamente os acessos sem fios não autorizados e promover o debate do problema junto do RESPONSÁVEL PELO TRATAMENTO. |
| DESCRIÇÃO:  A chave de acesso aos dispositivos WiFi é a que vem de origem.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  A chave de acesso aos dispositivos WiFi é a que vem de origem. Manter a chave de acesso WiFi original dos dispositivos facilita o acesso por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, inativando o WiFi ou alterando a chave obedecendo às regras definidas. |
| DESCRIÇÃO:  A chave de acesso aos dispositivos WiFi não respeita a complexidade definida no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existe a possibilidade de as chaves de acesso WiFi poderem ser quebradas. Quanto mais complexas, mais difícil se torna a tarefa de as descobrir (quebrar). Como é utilizada uma chave de acesso WiFi fraca, esta pode ser descoberta e permitir o acesso não autorizado por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, alterando de imediato a chave de acesso WiFi respeitando a complexidade lá definida. |
| DESCRIÇÃO:  O tempo decorrido desde a última verificação de necessidade de utilizar distribuidores de rede *wireless* dentro do SISTEMA excede o previsto no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última verificação de necessidade de utilizar distribuidores de rede *wireless* excede o previsto no Regulamento do SISTEMA. A utilização de *wireless* na ORGANIZAÇÃO facilita o acesso à rede local por não ser necessário a ligação por cabo para aceder aos dados.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente revendo periodicamente a necessidade de se utilizar *wireless* dentro do SISTEMA. |
| DESCRIÇÃO:  É possível administrar os dispositivos a partir da rede pública ou através do meio sem fios.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem no SISTEMA dispositivos que podem ser configurados a partir da rede pública ou da rede sem fios, podendo esta funcionalidade ser utilizada como forma de facilitar o acesso ao SISTEMA através da reconfiguração irregular de dispositivos.  MEDIDA CORRETIVA:  Se possível, reconfigurar os dispositivos para que apenas possam ser reconfigurados a partir da rede privada e com ligação à rede por cabo. |
| DESCRIÇÃO:  O tempo decorrido desde a última alteração de palavras-chave dos dispositivos de infraestrutura excede o previsto no regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última alteração de palavras-chave de dispositivos de infraestrutura excede o prazo definido no Regulamento do SISTEMA. A troca periódica de palavras-chave dos dispositivos de infraestrutura previne casos de divulgação inadvertida e dificulta ataques do tipo tentativa-erro, força bruta, etc.  MEDIDA CORRETIVA:  Respeitar os prazos definidos no Regulamento do SISTEMA para troca das palavras-chave dos dispositivos de infraestrutura. |
| DESCRIÇÃO:  O tempo decorrido desde a última avaliação de atualidade das regras de exceção de acesso à infraestrutura pela internet e através dos distribuidores de rede sem fios excede o previsto pelo Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última avaliação de atualidade das regras de exceção de acesso à infraestrutura pela internet e através dos distribuidores de rede sem fios excede o previsto pelo Regulamento do SISTEMA. As regras de exceção de acesso à infraestrutura pela internet ou pelos distribuidores de rede sem fios devem ser revistos periodicamente com o objetivo de evitar a existência de regras em excesso e que possam facilitar o acesso não autorizado ao SISTEMA por estranhos.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA nomeadamente no que diz respeito aos prazos para revisão das regras de acesso à infraestrutura. |
| DESCRIÇÃO:  O tempo decorrido desde a última avaliação de atualidade das autorizações de acesso externo excede o previsto pelo regulamento.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última avaliação de atualidade das autorizações de acesso externo excede o previsto pelo regulamento. Os acessos externos representam vulnerabilidades mesmo que o risco tenha sido mitigado através da utilização de mecanismos adicionais de encriptação e autenticação. Assim, devem apenas existir enquanto são realmente necessários. A existência de acessos externos desnecessários mas previstos, põe em risco o SISTEMA porque facilita o acesso por estranhos.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA nomeadamente no que diz respeito aos prazos para revisão dos acessos externos autorizados. |
| DESCRIÇÃO:  O tempo decorrido desde a última alteração de chave de acesso dos dispositivos WiFi excede o previsto no regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última avaliação de atualidade das autorizações de acesso externo excede o previsto pelo regulamento. A alteração periódica das chaves de acesso WiFi resolvem problemas de divulgação desconhecida e de descoberta através de ferramentas de *hacking*. Se as chaves de acesso WiFi não forem alteradas periodicamente podem ser descobertas (quebradas) e utilizadas para acesso de estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, alterando de imediato a chave de acesso WiFi respeitando as regras lá definidas. |

* + 1. Computadores, servidores e equivalentes

Nesta secção encontram-se os formulários que apoiam na deteção de vulnerabilidades transversais aos computadores, servidores e equivalentes.

* + - 1. Vulnerabilidades transversais de computador, servidor ou equivalente

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades de um computador ou servidor.

**VULNERABILIDADES TRANSVERSAIS DE COMPUTADOR, SERVIDOR OU EQUIVALENTE**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades em computadores, servidores ou equivalentes do SISTEMA. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar é fruto da aprendizagem contínua do AUDITOR nos diferentes sistemas que audita.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VTCSE-V1.0A |

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria que são transversais a todos os SO. O seu preenchimento facilita a identificação das vulnerabilidades a levantar e as medidas corretivas ou recomendações a propor. A coluna ITEM contém vulnerabilidades conhecidas que servem de guia à auditoria. Na coluna IMPACTO deve ser respondido um dos seguintes três valores: i) SIM, se a vulnerabilidade estiver presente no SISTEMA; ii) NÂO, se a vulnerabilidade não estiver presente no SISTEMA; e iii) N/A se não aplicável. A coluna REAÇÃO apenas deve ser atendida se a coluna IMPACTO foi respondida com SIM.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| *HARDWARE* |  |
| DESCRIÇÃO:  A versão de *firmware* atualmente instalada (i.e. BIOS) não é a última estável disponibilizada pelo fabricante.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem computadores com versão de *firmware* desatualizada. Estas atualizações além de promoverem a estabilidade dos equipamentos, também contribuem para a proteção, estabilidade e bom funcionamento dos dispositivos e, consequentemente, do SISTEMA.  MEDIDA CORRETIVA:  Apesar da possibilidade de tornar o dispositivo inoperável, a atualização da *firmware* deve ser efetuada para proteger o dispositivo e o SISTEMA. |
| DESCRIÇÃO:  As baterias do dispositivo (e.g. BIOS) ou os mecanismos de refrigeração interna (e.g. dissipadores ou ventoinhas) não são substituídos há mais tempo do que o previsto no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem dispositivos cujos componentes consumíveis não são substituídos há mais tempo do que previsto no Regulamento de SISTEMA. A falha das baterias ou mecanismos de refrigeração pode fazer com que o UTILIZADOR se veja privado da utilização do dispositivo e pode mesmo causar outros problemas de resolução mais cara e complexa.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente agendando a substituição das baterias e mecanismos de refrigeração nos prazos previstos, de forma a não pôr em causa a disponibilidade e bom funcionamento do SISTEMA. |
| SO |  |
| DESCRIÇÃO:  O SO não se encontra na última versão disponibilizada pelo fabricante.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem dispositivos cujo SO não se encontra na última versão disponibilizada pelo fabricante. Um SO desatualizado torna o dispositivo vulnerável na medida em que não está a receber as correções para as vulnerabilidades entretanto já corrigidas pelo fabricante.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à manutenção das atualizações de segurança em dia. Promover que seja avaliado o impacto prévio de implementar as atualizações disponíveis e a utilização de serviços de atualização automática. |
| DESCRIÇÃO:  O SO não recebe atualizações porque o suporte foi descontinuado.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem dispositivos cujo SO não recebe atualizações porque o suporte foi descontinuado. As atualizações de segurança são vitais para que os dispositivos possam receber correções de vulnerabilidades já conhecidas. Utilizar um SO descontinuado pelo fabricante é um risco muito grande para o SISTEMA, porque significa que não são disponibilizadas correções para as vulnerabilidades conhecidas.  MEDIDA CORRETIVA:  Promover a substituição imediata do SO em causa. |
| DESCRIÇÃO:  As palavras-chave de acesso ao SO, do administrador ou utilizadores, foram alteradas há mais tempo do que o previsto no regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem palavras-chave de SO não alteradas há mais tempo do que o previsto no Regulamento de SISTEMA. A alteração periódica das palavras-chave é importante para prevenir divulgações desconhecidas ou descobertas através de ferramentas de *hacking*.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente no que diz respeito à periodicidade para alteração de palavras-chave. |
| DESCRIÇÃO:  O SO não bloqueia automaticamente o ecrã dentro do tempo previsto no Regulamento do SISTEMA ou o é possível existir desbloqueio sem as credenciais do utilizador.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem computadores que não bloqueiam de forma automática o ecrã no tempo previsto pelo Regulamento do SISTEMA. Se o ecrã não bloquear automaticamente e o UTILIZADOR se esquecer de o fazer, o SISTEMA fica acessível a qualquer pessoa que lhe possa aceder fisicamente.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito ao bloqueio automático de ecrã. Avaliar a necessidade de formação dos UTILIZADORES para que saibam a importância dos bloqueios de ecrã sempre que se ausentam da frente do computador. |
| DESCRIÇÃO:  A conta de convidado está ativada, pondo em causa o funcionamento da estratégia de barreiras de acesso à infraestrutura definidas no PSD do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE A REGISTAR:  Existem SO com a conta de convidado ativa. A conta de convidado permite a entrada não autenticada de UTILIZADORES através da rede, o que representa uma vulnerabilidade muito grave para o SISTEMA.  MEDIDAS CORRETIVAS OU RECOMEND. A SUGERIR:  Desativar imediatamente a conta de convidado do SO. |
| DESCRIÇÃO:  O sigilo das palavras-chave de administrador do SO foi comprometido ou estão a ser utilizadas de forma irregular ou não prevista no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem palavras-chave de administrador que foram comprometidas ou divulgadas. A conta de administrador permite instalar e desinstalar aplicações (incluindo as de proteção contra *malware*), e permite alterar permissões e partilhar informação de forma não prevista no PSD.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente no que diz respeito às palavras-chave e ao seu sigilo. Alterar imediatamente as palavras-chave comprometidas. Reavaliar as permissões e aplicações de segurança definidas nos dispositivos envolvidos. |
| DESCRIÇÃO:  O perfil da conta utilizada pelos UTILIZADORES do SO tem direitos ou permissões não previstas pelo Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem UTILIZADORES no SISTEMA com permissões de SO acima do necessário. Estes UTILIZADORES podem reconfigurar o SO ou as aplicações de segurança pondo em risco os dados e o SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, reajustando as permissões dos UTILIZADORES em causa. Reavaliar os itens do PSD relacionados com o dispositivo, e reavaliar o bom funcionamento e configurações das aplicações de segurança envolvidas na proteção do dispositivo. |
| DESCRIÇÃO:  O nome NetBios dos dispositivos torna o UTILIZADOR identificável.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem dispositivos cujo nome NetBios identifica o UTILIZADOR direta ou indiretamente. Sabendo quem trabalha com cada dispositivo, torna mais fácil um ataque direcionado.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, anonimizando o nome dos dispositivos com o objetivo de dificultar a sua procura em caso de invasão de SISTEMA. |
| DESCRIÇÃO:  O nome dos UTILIZADORES do SO torna o UTILIZADOR identificável.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem nomes de UTILIZADORES no SISTEMA que identificam a pessoa que trabalha nos dispositivos. A identidade do UTILIZADOR deve ser preservada de forma a garantir a sua privacidade.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, anonimizando imediatamente o nome dos UTILIZADORES do SO. |
| APS |  |
| DESCRIÇÃO:  As aplicações de proteção contra *malware* caducaram ou não existem.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem no SISTEMA dispositivos sem proteções contra *malware* ou com proteções caducadas. Um SO sem uma aplicação de segurança contra *malware* torna o dispositivo vulnerável e coloca o SISTEMA em risco.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de manter em dia as subscrições relacionadas com as aplicações de segurança. Devem também existir aplicações de proteção contra *malware* em todos os computadores. |
| DESCRIÇÃO:  As aplicações de proteção contra *malware* não estão totalmente operacionais.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem no SISTEMA aplicações de proteção contra *malware* que não estão totalmente operacionais. Um SO sem uma aplicação de segurança contra *malware* torna o dispositivo vulnerável e coloca o SISTEMA em risco.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de manter ativas e atualizadas as aplicações de segurança do SISTEMA. Rever as configurações das aplicações de proteção envolvidas. |
| DESCRIÇÃO:  As aplicações de proteção contra *malware* não estão totalmente atualizadas.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem no SISTEMA aplicações de proteção contra *malware* que não estão totalmente atualizadas. Um SO sem uma aplicação de segurança atualizada contra *malware* torna o dispositivo vulnerável e coloca o SISTEMA em risco.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de manter ativas e atualizadas as aplicações de segurança do SISTEMA. Rever as configurações das aplicações de proteção envolvidas. |
| DESCRIÇÃO:  As aplicações de proteção contra *malware* podem ser objeto de reconfiguração ou personalização pelo UTILIZADOR.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem no SISTEMA aplicações de proteção contra *malware* que podem ser reconfiguradas ou personalizadas pelo UTILIZADOR. Se for incorretamente reconfigurada pode deixar o dispositivo e o SISTEMA em risco.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente garantindo que apenas o ADMINISTRADOR DE SISTEMA possa fazer reconfigurações ao nível das aplicações de segurança. Rever as configurações das aplicações de proteção envolvidas. |
| DESCRIÇÃO:  A *firewall* do SO está inoperacional, pondo em causa o funcionamento da estratégia de barreiras de acesso à infraestrutura definidas no PSD do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem dispositivos com a *firewall* inoperacional. Se a *firewall* não estiver totalmente operacional, o SO está vulnerável a ataques desencadeados a partir da rede local (*wired* ou *wireless*). Além disso, as *firewall* do SO são complementares às de infraestrutura porque funcionam como barreiras de segunda linha.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente reativando de forma imediata as *firewall* envolvidas. Caso tenha sido desativada, frisar ao RESPONSÁVEL PELO TRATAMENTO de dados a importância da barreira, solicitando que avalie o motivo da desativação antes de a reativar, já que pode bloquear o funcionamento de recursos ou aplicações. |
| DESCRIÇÃO:  Existem incoerências entre as exceções de acesso previstas no PSD, e as efetivamente aplicadas na *firewall* do SO para o dispositivo.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem incoerências entre as regras de exceção de *firewall* de SO previstas no PSD com as que estão efetivamente aplicadas nos dispositivos. A existência de exceções desnecessárias facilitam o roubo de dados podendo também conduzir à indisponibilidade ou inoperabilidade do SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à manutenção de aplicações de segurança em funcionamento e as regras de exceção de *firewall* do SO estritamente necessárias. |
| DESCRIÇÃO:  O tempo decorrido desde a última avaliação de atualidade das regras de exceção na *firewall* do SO ou aplicação de segurança excede o previsto pelo regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem regras de exceção de *firewall* de SO não revistas há demasiado tempo. A existência de regras de exceção em excesso aumenta ao nível de vulnerabilidade do dispositivo e do SISTEMA. A avaliação regular das regras de exceção da *firewall* do SO ou da aplicação de segurança, permite diminuir a exposição ao risco desnecessário pelo SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito ao prazo para reavaliar as regras de exceção previstas de acesso ao SO. |
| DESCRIÇÃO:  Não existem ou não estão configuradas as aplicações de controlo de utilização de DEA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Não existem ou não estão configuradas as aplicações para controlo dos DEA. Se não estiverem a ser utilizadas aplicações para controlo os UTILIZADORES podem utilizar livremente DEA não autorizados. A utilização de DEA não autorizados, facilita a saída descontrolada de dados e a propagação de *malware* no SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de controlar a utilização de DEA. |
| DESCRIÇÃO:  As aplicações de controlo dos DEA não estão totalmente operacionais.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem aplicações de controlo de DEA que não estão totalmente operacionais. Se este controlo não estiver garantido, podem ser utilizados DEA não previstos no PSD. A utilização de DEA não autorizados, facilita a saída descontrolada de dados e a propagação de *malware* no SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de controlar a utilização de DEA. |
| DESCRIÇÃO:  As aplicações de controlo dos DEA podem ser reconfiguradas pelo utilizador.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem aplicações de controlo de DEA que podem ser reconfiguradas pelos UTILIZADORES. Se incorretamente reconfigurados ou personalizados, o controlo pode não ficar garantido. A utilização de DEA não autorizados, facilita a saída descontrolada de dados e a propagação de *malware* no SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à configuração exclusiva por parte do ADMINISTRADOR DE SISTEMA. |
| APS E UTILITÁRIOS |  |
| DESCRIÇÃO:  As aplicações de produtividade instaladas no SISTEMA não estão na última versão estável disponibilizada pelos fabricantes.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem aplicações de produtividade instaladas no SISTEMA que não estão na última versão disponibilizada pelo fabricante. A utilização de aplicações desatualizadas pode deixar o SISTEMA vulnerável a ataques.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente no que diz respeito à atualização das aplicações. |
| DESCRIÇÃO:  Pelo menos um dos componentes ou aplicações seguintes, não está na última versão disponibilizada pelo fabricante: Chrome, Firefox, Java, Acrobat reader e Flash player.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem utilitários ou *browsers* que não estão atualizados. Estes componentes são muitas vezes utilizados por *hackers* para invasão de sistemas. A sua não atualização deixa o SISTEMA vulnerável a ataques.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente no que diz respeito à atualização das aplicações. |
| OUTROS |  |
|  |  |
| DESCRIÇÃO:  Existem certificados digitais em vias de expirar, necessários ao funcionamento da ORGANIZAÇÃO, que podem condicionar ou inviabilizar o acesso ao SISTEMA (e.g. VPN, envio de e-mail, etc.).  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem certificados digitais em vias de expiração que podem influenciar o funcionamento do SISTEMA. Sem certificados válidos pode não ser possível aceder ao SISTEMA (e.g. através da VPN), utilizar corretamente o e-mail ou aceder a outros sistemas (e.g. *e-banking*).  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de manter as renovações de contratos e subscrições em dia. |
| DESCRIÇÃO:  Existem certificados digitais expirados necessários ao funcionamento da ORGANIZAÇÃO, que condicionam a utilização ou inviabilizam o acesso ao SISTEMA (e.g. VPN, envio de e-mail, etc.).  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem certificados digitais expirados necessários ao bom funcionamento do SISTEMA. Sem certificados válidos pode não ser possível aceder ao SISTEMA (e.g. através da VPN), utilizar corretamente o e-mail ou aceder a outros sistemas (e.g. *e-banking*).  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à necessidade de manter as renovações de contratos e subscrições em dia. |
| DESCRIÇÃO:  Existem certificados digitais ativos que não são necessários ao funcionamento da ORGANIZAÇÃO.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem certificados digitais ativos que não são necessários ao funcionamento da ORGANIZAÇÃO. Se utilizados de forma incorreta, podem identificar de forma legalmente aceite o seu dono. Em caso de invasão de SISTEMA podem ser utilizados de forma maliciosa.  MEDIDA CORRETIVA:  Promover a desinstalação imediata dos certificados em causa. |
| DESCRIÇÃO:  São usados mecanismos automáticos gravar palavras-chave de acesso a *sites* ou recursos nos dispositivos (cf. *browsers*, sistemas operativos, etc.).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  São utilizados mecanismos automáticos para guardar palavras-chave para facilitar o acesso a *sites* ou recursos nos dispositivos. No caso de invasão do computador, estas autenticações automáticas facilitam o acesso descontrolado à informação desses sites ou recursos.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à não gravação de palavras-chave para acesso facilitado a *sites*, recursos de rede ou recursos externos. |
| DESCRIÇÃO:  O computador é movido com regularidade para fora da esfera física da ORGANIZAÇÃO (e.g. CPP) e não tem ou não está operacional um mecanismo de encriptação de ficheiros (e.g. BitLocker) para inviabilizar o acesso à informação por estranhos.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem computadores que são movidos para fora da esfera física da ORGANIZAÇÃO (e.g. CPP) sem um mecanismo de encriptação de ficheiros em funcionamento que garanta a ilegibilidade do conteúdo. Sem um mecanismo de encriptação, em caso de roubo ou perda, os dados do dispositivo extraviado podem ser consultados por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, implementando medidas que impeçam o acesso à informação por estranhos. Não retirar da esfera da empresa os computadores visados até o problema estar resolvido. |
| DESCRIÇÃO:  Existem computadores portáteis (i.e. CPP) que não se encontram em nenhuma das localizações autorizadas.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem computadores portáteis (CPP) que não se encontram em nenhuma das localizações autorizadas. No caso de extravio ou furto, um CPP pode comprometer os dados da ORGANIZAÇÃO, podendo conduzir a incidentes de violação de dados e até acesso à infraestrutura por estranhos ao SISTEMA se assim estiver configurado.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, registar o IVD, avaliar a necessidade de notificação à AUTORIDADE DE CONTROLO, rever a necessidade de existir o CPP, e rever as necessidades de formação dos UTILIZADORES. |
| DESCRIÇÃO:  Existem servidores localizados em ambientes expostos a danos materiais.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem servidores localizados em ambientes expostos a danos materiais. É nos servidores onde estão armazenados os dados operacionais da ORGANIZAÇÃO, pelo que a sua avaria pode levar à inoperabilidade da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Recomendar a colocação do servidor numa sala devidamente arejada, com humidade controlada, e protegida a pessoas não autorizadas (e.g. prateleira alta e de preferência em armário inacessível). |
| DESCRIÇÃO:  Existem computadores ou servidores com instancias SQL instaladas e em execução desnecessariamente.  IMPACTO DE SUGESTÃO: Crítico | VULNERABILIDADE:  Existem computadores ou servidores com instancias SQL instaladas e em execução desnecessariamente. A oferta de serviços em excesso à rede expõe em demasia serviços que podem ser utilizados para invasão do SISTEMA.  MEDIDA CORRETIVA:  Recomendar a eliminação ou inativação imediata das instâncias desnecessárias. |

* + 1. SO
       1. Vulnerabilidades Windows Server 2016

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows Server 2016.

**VULNERABILIDADES DO WINDOWS SERVER 2016**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VW2016-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTODE DADOS e o ADMINISTRADOR DE SISTEMA (ou técnico).

Como as atualizações do Windows 2016 são cumulativas, as novas atualizações contemplam todas as que a precederam. Neste contexto, faz sentido atender essencialmente às atualizações de segurança lançadas após a data de lançamento da versão atual do SO (e.g. 1607).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| VERSÃO: 1607 (Windows 2016)  https://support.microsoft.com/en-us/help/4074590/windows-10-update-kb4074590 | |
| KB4074590  DATA:  DESCRIÇÃO:  Atualiza informação acerca de time zones que influenciar o funcionamento de certificados; atualiza a segurança dos *browsers* da Microsoft; contém atualizações de segurança diversas para o Microsoft Scripting Engine, Microsoft Edge, Internet Explorer, Microsoft Windows Search component, Windows Kernel, Windows Authentication, Device Guard, Common Log File System driver, e Windows storage and file systems.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem servidores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa os dados e a operabilidade da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Windows Server 2012 R2

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows Server 2012 R2.

**VULNERABILIDADES DO WINDOWS SERVER 2012 R2**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VW2012R2-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTODE DADOS e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os pacotes de atualização mensais (nomeadas como *“monthly rollup”* pela Microsoft) são cumulativas, i.e. as novas atualizações contemplam todas as que a precederam. Neste contexto, faz sentido atender essencialmente às atualizações de segurança lançadas após a data de lançamento do último pacote. (e.g. KB4074594).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| MONTHLY ROLLUP (2018-02): 4074594  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4074594 | |
| KB4074594  DATA:  DESCRIÇÃO:  Atualizações de segurança para: Internet Explorer, Windows Kernel, Common Log File System driver, Windows storage and file systems, Microsoft Windows Search component, e Windows SMB Server.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem servidores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa os dados e a operabilidade da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Windows Server 2012

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows Server 2012.

**VULNERABILIDADES DO WINDOWS SERVER 2012**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VW2012-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os pacotes de atualização mensais (nomeadas como *“monthly rollup”* pela Microsoft) são cumulativas, i.e. as novas atualizações contemplam todas as que a precederam. Neste contexto, faz sentido atender essencialmente às atualizações de segurança lançadas após a data de lançamento do último pacote. (e.g. KB4074594).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| MONTHLY ROLLUP (2018-02): 4074593  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4074593 | |
| KB4074593  DATA:  DESCRIÇÃO:  Atualizações de segurança para: Internet Explorer, Windows Kernel, Common Log File System driver, Windows storage and file systems, Microsoft Windows Search component, e Windows storage and file systems.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem servidores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa os dados e a operabilidade da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Windows Server 2008 R2

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows Server 2008 R2.

**VULNERABILIDADES DO WINDOWS 2008 R2**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VW2008R2-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

A partir do *Service Pack* 1 a Microsoft começou a lançar pacotes de atualização mensal. Estes pacotes, nomeados como *“monthly rollup”* pela Microsoft são cumulativos, i.e. um novo pacote contempla todas as atualizações de segurança lançadas após a data de lançamento do último pacote. (e.g. KB4074598).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| SERVICE PACK 1  https://support.microsoft.com/en-us/help/4074598/windows-7-update-kb4074598 | |
| KB4074598  DATA:  DESCRIÇÃO:  Atualizações de segurança para: Internet Explorer, Windows Kernel, Common Log File System driver, Windows storage and file systems, Microsoft Windows Search component, e Windows storage and file systems.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem servidores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa os dados e a operabilidade da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Windows 10

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows 10.

**VULNERABILIDADES DO WINDOWS 10**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VW10-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Como as atualizações do Windows 10 são cumulativas, as novas atualizações contemplam todas as que a precederam. Neste contexto, faz sentido atender essencialmente às atualizações de segurança lançadas após a data de lançamento da versão atual do SO (e.g. 1709).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| VERSÃO: 1709 (Windows 10)  https://support.microsoft.com/en-us/help/4074588/windows-10-update-kb4074588 | |
| KB4074588  DATA:  DESCRIÇÃO:  Atualiza informação acerca de *time* zones que influenciar o funcionamento de certificados; atualiza a segurança dos *browsers* da Microsoft; contém atualizações de segurança diversas para o Microsoft Scripting Engine, Microsoft Edge, Internet Explorer, Microsoft Windows Search component, Windows Kernel, Windows Authentication, Device Guard, Common Log File System driver, e Windows storage and file systems.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem computadores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa a integridade dos dados e o bom funcionamento dos dispositivos.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Windows 8.1

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows 8.1.

**VULNERABILIDADES DO WINDOWS 8.1**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VW81-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os pacotes de atualização mensais (nomeadas como *“monthly rollup”* pela Microsoft) são cumulativas, i.e. as novas atualizações contemplam todas as que a precederam. Neste contexto, faz sentido atender essencialmente às atualizações de segurança lançadas após a data de lançamento do último pacote. (e.g. KB4074594).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| MONTHLY ROLLUP (2018-02): 4074594  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4074594 | |
| KB4074594  DATA:  DESCRIÇÃO:  Atualizações de segurança para: Internet Explorer, Windows Kernel, Common Log File System driver, Windows storage and file systems, Microsoft Windows Search component, e Windows SMB Server.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem computadores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa a integridade dos dados e o bom funcionamento dos dispositivos.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Windows 8

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows 8.

**VULNERABILIDADES DO WINDOWS 8**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VW8-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| SO SEM SUPORTE  DATA: N/A  DESCRIÇÃO:  https://www.windowscentral.com/microsoft-ends-support-windows-8-asks-users-upgrade-windows-81-or-10  https://www.forbes.com/sites/gordonkelly/2016/01/12/microsoft-abandons-windows-8/#20143c1b2b64  https://www.microsoft.com/en-us/software-download/windows10?tduid=(ca5d0cfa36b60e2bc35fbdb30622eca9)(259740)(2542549)(UUwpUdUnU37077YYw)()  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem computadores para os quais já não existem atualizações de segurança deixando o SO vulnerável. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa a integridade dos dados e o bom funcionamento dos dispositivos.  MEDIDA CORRETIVA:  Promover a substituição do SO ou do dispositivo para que as atualizações de segurança fiquem garantidas. |

* + - 1. Vulnerabilidades Windows 7

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Windows 7.

**VULNERABILIDADES DO WINDOWS 7**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de SO. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VW7-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para o SO em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis ao SO em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

A partir do *Service Pack* 1 a Microsoft começou a lançar pacotes de atualização mensal. Estes pacotes, nomeados como *“monthly rollup”* pela Microsoft são cumulativos, i.e. um novo pacote contempla todas as atualizações de segurança lançadas após a data de lançamento do último pacote. (e.g. KB4074598).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| SERVICE PACK 1  htthttps://support.microsoft.com/en-us/help/4074598/windows-7-update-kb4074598 | |
| KB4074598  DATA:  DESCRIÇÃO:  Atualizações de segurança para: Internet Explorer, Windows Kernel, Common Log File System driver, Windows storage and file systems, Microsoft Windows Search component, e Windows storage and file systems.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem computadores com vulnerabilidades identificadas e não corrigidas. Um SO vulnerável pode ser objeto de ataque e invasão por estranhos ao SISTEMA pondo em causa a integridade dos dados e o bom funcionamento dos dispositivos.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança correspondente, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + 1. Microsoft Office
       1. Vulnerabilidades Office 2016

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO OFFICE 2016**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft Office. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VOFF16-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

A partir do *update* cumulativo de dezembro de 2014, todas as atualizações de produtos Office são incluídas num único pacote chamado pela Microsoft como “*Public Update* (PU)” (Link1). As atualizações podem ser feitas de forma automática utilizando o Link2 ou manualmente recorrendo ao Link1. Entre cada PU podem existir atualizações de segurança pontuais que são publicadas no Link3.

Link1: https://support.office.com/en-us/article/office-updates-a118ec61-f007-492f-bfa5-5a6f764d5471

Link2: https://support.office.com/en-us/article/install-office-updates-2ab296f3-7f03-43a2-8e50-46de917611c5

Link3: https://portal.msrc.microsoft.com/en-us

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/pt-pt/help/4077965/february-2018-updates-for-microsoft-office | |
| KB4077965  DATA: 13-02-2018  DESCRIÇÃO:  Atualizações de segurança diversas.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem dispositivos com a aplicação Microsoft Office desatualizada, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Office 2013

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO OFFICE 2013**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft Office. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VOFF13-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

A partir do *update* cumulativo de dezembro de 2014, todas as atualizações de produtos Office são incluídas num único pacote chamado pela Microsoft como “*Public Update* (PU)” (Link1). As atualizações podem ser feitas de forma automática utilizando o Link2 ou manualmente recorrendo ao Link1. Entre cada PU podem existir atualizações de segurança pontuais que são publicadas no Link3.

Link1: https://support.office.com/en-us/article/office-updates-a118ec61-f007-492f-bfa5-5a6f764d5471

Link2: https://support.office.com/en-us/article/install-office-updates-2ab296f3-7f03-43a2-8e50-46de917611c5

Link3: https://portal.msrc.microsoft.com/en-us

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/pt-pt/help/4077965/february-2018-updates-for-microsoft-office | |
| KB4077965  DATA: 13-02-2018  DESCRIÇÃO:  Atualizações de segurança diversas.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem dispositivos com a aplicação Microsoft Office desatualizada, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Office 2010

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO OFFICE 2010**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft Office. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VOFF10-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

A partir do *update* cumulativo de dezembro de 2014, todas as atualizações de produtos Office são incluídas num único pacote chamado pela Microsoft como “*Public Update* (PU)” (Link1). As atualizações podem ser feitas de forma automática utilizando o Link2 ou manualmente recorrendo ao Link1. Entre cada PU podem existir atualizações de segurança pontuais que são publicadas no Link3.

Link1: https://support.office.com/en-us/article/office-updates-a118ec61-f007-492f-bfa5-5a6f764d5471

Link2: https://support.office.com/en-us/article/install-office-updates-2ab296f3-7f03-43a2-8e50-46de917611c5

Link3: https://portal.msrc.microsoft.com/en-us

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/pt-pt/help/4077965/february-2018-updates-for-microsoft-office | |
| KB4077965  DATA: 13-02-2018  DESCRIÇÃO:  Atualizações de segurança diversas.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem dispositivos com a aplicação Microsoft Office desatualizada, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades Office 2007

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO OFFICE 2007**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft Office. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VOFF07-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

A partir do *update* cumulativo de dezembro de 2014, todas as atualizações de produtos Office são incluídas num único pacote chamado pela Microsoft como “*Public Update* (PU)” (Link1). As atualizações podem ser feitas de forma automática utilizando o Link2 ou manualmente recorrendo ao Link1. Entre cada PU podem existir atualizações de segurança pontuais que são publicadas no Link3.

Link1: https://support.office.com/en-us/article/office-updates-a118ec61-f007-492f-bfa5-5a6f764d5471

Link2: https://support.office.com/en-us/article/install-office-updates-2ab296f3-7f03-43a2-8e50-46de917611c5

Link3: https://portal.msrc.microsoft.com/en-us

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/pt-pt/help/4077965/february-2018-updates-for-microsoft-office | |
| KB4077965  DATA: 13-02-2018  DESCRIÇÃO:  Atualizações de segurança diversas.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem dispositivos com a aplicação Microsoft Office desatualizada, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança, garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + 1. Microsoft SQL Server
       1. Vulnerabilidades SQL Server 2017

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2017**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL17-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do Windows Update mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/pt-pt/help/4056498/cumulative-update-4-for-sql-server-2017 | |
| KB4056498  DATA: 20-02-2018  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem SBGD Microsoft SQL Server desatualizados, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para aceder aos dados ou invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança fazendo uma prévia avaliação de impacto, e garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades SQL Server 2016 SP1

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2016 SP1**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL16SP1-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do *Windows Update* mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/en-us/help/4057119/cumulative-update-7-for-sql-server-2016-sp1 | |
| KB4057119  DATA: 01-03-2018  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem SBGD Microsoft SQL Server desatualizados, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para aceder aos dados ou invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança fazendo uma prévia avaliação de impacto, e garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades SQL Server 2014 SP2

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2014 SP2**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL14SP2-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do *Windows Update* mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/en-us/help/4052725/cumulative-update-10-for-sql-server-2014-sp2 | |
| KB4052725  DATA: 16-01-2018  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem SBGD Microsoft SQL Server desatualizados, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para aceder aos dados ou invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança fazendo uma prévia avaliação de impacto, e garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades SQL Server 2012 SP4

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2012 SP4**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL12SP4-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do *Windows Update* mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/en-us/help/4057116/security-update-for-vulnerabilities-in-sql-server | |
| KB4057116  DATA: N/A  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem SBGD Microsoft SQL Server desatualizados, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para aceder aos dados ou invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança fazendo uma prévia avaliação de impacto, e garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades SQL Server 2008 R2 SP3

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2008 R2 SP3**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL08R2SP3-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do *Windows Update* mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/en-us/help/4057113/security-update-for-vulnerabilities-in-sql-server | |
| KB4057113  DATA: N/A  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem SBGD Microsoft SQL Server desatualizados, com vulnerabilidades de segurança identificadas que, não sendo corrigidas, podem ser exploradas por estranhos para aceder aos dados ou invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação das atualizações de segurança fazendo uma prévia avaliação de impacto, e garantindo a execução prévia de cópias de segurança e a tomada de medidas preventivas para o caso da atualização resultar na inoperabilidade do dispositivo. |

* + - 1. Vulnerabilidades SQL Server 2008 SP4

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2008 SP4**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL08SP4-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do *Windows Update* mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/en-us/help/4057114/security-update-for-vulnerabilities-in-sql-server | |
| KB4057114  DATA: N/A  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Crítico, um sistema com uma vulnerabilidade identificada e não corrigida pode ser objeto de ataque e invasão por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança, garantindo previamente a execução de cópias de segurança se necessário. |

* + - 1. Vulnerabilidades SQL Server 2005 SP4

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades do Microsoft Office 2016.

**VULNERABILIDADES DO SQL SERVER 2005 SP4**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades no Microsoft SQL Server. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar tem origem nos documentos de segurança publicados pelo fabricante (e.g. boletins de segurança da Microsoft (e.g. https://portal.msrc.microsoft.com/en-us), e noutros recursos disponíveis que identifiquem vulnerabilidades).

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VSQL05SP4-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas para a aplicação em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação de produtividade em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

Os produtos SQL são objeto periodicamente de *updates* cumulativos (CU). As atualizações podem ser feitas de forma manual. Cada novo CU contém todas as correções incluídas em CU’s anteriores. As CU podem ser disponibilizadas através do *Windows Update* mas com algum atraso temporal. As atualizações podem ser carregadas manualmente através do Link1.

Link1: https://technet.microsoft.com/en-us/library/ff803383.aspx

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| https://support.microsoft.com/en-us/help/2463332/list-of-the-issues-that-are-fixed-in-sql-server-2005-service-pack-4 | |
| KB2463332  DATA: N/A  DESCRIÇÃO:  Contém correções que podem colocar em perigo a segurança do SISTEMA.  PRODUTO SEM SUPORTE  https://support.microsoft.com/en-us/help/2463332/list-of-the-issues-that-are-fixed-in-sql-server-2005-service-pack-4  IMPACTO DE SUGESTÃO: Critico | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Crítico, um sistema com uma vulnerabilidade identificada e não corrigida pode ser objeto de ataque e invasão por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover a aplicação da atualização de segurança, garantindo previamente a execução de cópias de segurança se necessário. |

* + 1. Outros
       1. Vulnerabilidades noutras aplicações

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades de outras aplicações.

**VULNERABILIDADES DE OUTRAS APLICAÇÕES**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades de outras aplicações do SISTEMA. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VOA-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas de outras aplicações em auditoria. Apesar de todas representarem vulnerabilidades para o SISTEMA, podem existir itens na lista que são aplicáveis à aplicação em auditoria mas que não são implementadas por decisão ponderada e tripartida entre o AUDITOR, RESPONSÁVEL PELO TRATAMENTO de dados e o ADMINISTRADOR DE SISTEMA (ou técnico).

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O campo IMPLEMENTAR deve ser preenchido com base na decisão tripartida de implementar ou não cada atualização de segurança: i) Sim, se a decisão foi favorável; e ii) Não se a decisão foi não implementar. No campo FUNDAMENTAÇÃO deve ser inserido um texto curto a explicar a decisão tomada. A coluna REAÇÃO apenas deve ser atendida no caso de resposta afirmativa ao campo IMPLEMENTAR.

|  |  |
| --- | --- |
| ATUALIZAÇÕES DE SEGURANÇA | IMPLEMENTAÇÃO |
| MOZILLA THUNDERBIRD | |
| KB2463332  DATA: N/A  DESCRIÇÃO: | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  MEDIDA CORRETIVA: |
| APACHE OPENOFFICE | |
| KB2463332  DATA: N/A  DESCRIÇÃO: | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  MEDIDA CORRETIVA: |
| ERP PRIMAVERA | |
| KB2463332  DATA: N/A  DESCRIÇÃO:  Existem discrepâncias entre os perfis de UTILIZADOR definidos no PSD e os que efetivamente estão implementados na aplicação. | IMPLEMENTAR:  FUNDAMENTAÇÃO: |
| **REAÇÃO** |
| VULNERABILIDADE:  Existem discrepâncias entre os perfis de UTILIZADOR definidos no PSD e os que efetivamente estão implementados na aplicação. Podem existir UTILIZADORES com acesso a dados de forma não prevista pelo RESPONSÁVEL PELO TRATAMENTO.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente garantindo que cada UTILIZADOR apenas acede à informação necessária ao cumprimento da sua função na ORGANIZAÇÃO. |

* + - 1. Vulnerabilidades em recursos de rede

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades dos recursos de rede presentes no SISTEMA.

**VULNERABILIDADES EM RECURSOS DE REDE**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de conteúdo e permissões dos recursos de rede.

A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar é fruto da aprendizagem contínua do AUDITOR nos diferentes sistemas que audita.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VRR-V1.0A |

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O seu preenchimento facilita a identificação das vulnerabilidades a levantar e as medidas corretivas ou recomendações a propor. A coluna ITEM contém vulnerabilidades conhecidas que servem de guia à auditoria. A coluna REAÇÃO sugere a descrição da vulnerabilidade a registar, e medidas corretivas ou recomendações a sugerir.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| DESCRIÇÃO:  O SO disponibiliza recursos partilhados não previstos no PSD.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem recursos de rede no SISTEMA não previstos pelo RESPONSÁVEL PELO TRATAMENTO no Regulamento de SISTEMA nem no PSD. A disponibilização de recursos não previstos na rede promove a dispersão dos dados e a cópia de segurança parcial dos dados.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA nomeadamente no que diz respeito à utilização de apenas os recursos de rede autorizados pelo RESPONSÁVEL PELO TRATAMENTO. |
| DESCRIÇÃO:  Existem ficheiros em locais que não os recursos designados pelo RESPONSÁVEL PELO TRATAMENTO.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem ficheiros em localizações não previstas no PSD e no Regulamento de SISTEMA. Esses ficheiros contribuem para a desorganização da informação, podem por em risco o cumprimento de obrigações legais pela ORGANIZAÇÃO (e.g. direito ao acesso pelos TITULARES DOS DADOS) e também não estarão a ser objeto de cópia de segurança.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito aos recursos de rede autorizados. Rever as necessidades de formação dos UTILIZADORES. |
| DESCRIÇÃO:  Existem no SISTEMA ficheiros não são utilizados há mais tempo do que o previsto no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem ficheiros que não são utilizados há mais tempo do que o previsto no Regulamento do SISTEMA. A existência de ficheiros em excesso no SISTEMA aumenta o risco de perda de dados no caso de invasão e dificulta o cumprimento de obrigações legais (e.g. direito ao acesso ou apagamento dos TITUALRES).  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito ao tempo de manutenção de ficheiros. Rever as necessidades de formação dos UTILIZADORES. |
| DESCRIÇÃO:  O SGBD contém BD desnecessárias (e.g. bases de dados de teste do ERP) que dispersam a informação no SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem BD no SGBD desnecessárias ao funcionamento do SISTEMA e da ORGANIZAÇÃO. A existência de BD em excesso aumenta o risco de perda de dados no caso de uma invasão, e dificulta o cumprimento de obrigações legais (e.g. direito ao acesso ou apagamento dos TITULARES DOS DADOS).  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente na manutenção das BD efetivamente necessárias à operação da ORGANIZAÇÃO. |
| DESCRIÇÃO:  Estão a ser utilizados recursos externos de forma não prevista no Regulamento de SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Estão a ser utilizados recursos externos que não estão previstos no PSD nem no Regulamento de SISTEMA. A existência deste tipo de recursos pode facilitar de forma considerável a saída descontrolada de dados, e a propagação de *malware* dentro do SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, utilizando apenas os recursos externos e fins autorizados. |
| DESCRIÇÃO:  Existem UTILIZADORES com acesso a recursos de forma irregular, i.e. não prevista no PSD.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem UTILIZADORES com acesso a recursos de forma não prevista no PSD. O acesso não autorizado a informação, significa que os UTILIZADORES podem manipular dados de forma irregular, podendo comprometer o SISTEMA nomeadamente facilitando a saída não prevista de dados.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente reconfigurar as permissões de acesso a dados para que seja congruente com o definido no PSD. |
| DESCRIÇÃO:  Existe informação que não está a ser objeto de cópias de segurança como previsto no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existe informação que não está a ser objeto de cópias de segurança com a regularidade prevista no PSD. A inexistência de cópias de segurança pode conduzir à perda de informação e à indisponibilidade do SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à execução das tarefas relacionadas com as cópias de segurança com a periodicidade prevista no PSD. |

* + - 1. Vulnerabilidades em ferramentas de comunicação

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades que podem estar presentes em ferramentas de comunicação (e.g. email, IM).

**VULNERABILIDADES EM FERRAMENTAS DE COMUNICAÇÃO**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de vulnerabilidades em ferramentas de comunicação. As vulnerabilidades relacionadas diretamente com o cliente de e-mail (e.g. Microsoft Outlook) são tratadas nos modelos previstos de cada produto (e.g. Microsoft Office).

A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar é fruto da aprendizagem contínua do AUDITOR nos diferentes sistemas que audita.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VFC-V1.0A |

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O seu preenchimento facilita a identificação das vulnerabilidades a levantar e as medidas corretivas ou recomendações a propor. A coluna ITEM contém vulnerabilidades conhecidas que servem de guia à auditoria. A coluna REAÇÃO sugere a descrição da vulnerabilidade a registar, e medidas corretivas ou recomendações a sugerir.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| DESCRIÇÃO:  Existe uma grande probabilidade de puderem vir a ser transmitidos DADOS PESSOAIS por e-mail, e a ORGANIZAÇÃO não utiliza o e-mail com certificado digital.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  A ORGANIZAÇÃO pode transmitir ou a vir a transmitir DADOS PESSOAIS e não existem certificados digitais para assinar digitalmente, para garantir a autenticidade do remetente e não adulteração do conteúdo durante a transmissão.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, avaliando os custos de utilização de certificados digitais no e-mail. |
| DESCRIÇÃO:  Existem contas de e-mail que não utilizam encriptação nas comunicações para envio e receção de e-mail (e.g. SSL).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Algumas contas de e-mail não utilizam um sistema de encriptação no envio ou receção de e-mail facilitando a visualização do conteúdo por estranhos durante a transmissão.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente na prevenção da legibilidade de conteúdo durante a transmissão na internet. |
| DESCRIÇÃO:  Os e-mails são mantidos apenas no computador local (i.e. são apagados do servidor externo) e não existe nenhum mecanismo de cópia de segurança dos mesmos.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem contas de e-mail que apenas mantem dados no computador local e não existe nenhum mecanismo de cópia de segurança de e-mail associada. No caso de perda de dados por falha de *hardware* ou roubo (físico ou virtual), o UTILIZADOR pode ficar privado da informação.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente na manutenção dos e-mails no servidor ou na existência de cópias de segurança dessa informação. |
| DESCRIÇÃO:  São utilizadas ferramentas de comunicação não autorizadas pelo RESPONSÁVEL PELO TRATAMENTO no pelo Regulamento do SISTEMA (e.g. skype, Messenger, etc.).  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  São utilizadas ferramentas de comunicação não autorizadas pelo RESPONSÁVEL PELO TRATAMENTO. A utilização incorreta deste tipo de ferramentas pode facilitar a saída descontrolada de dados e pode ser utilizada para invadir o SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente analisando a necessidade e medidas de mitigação de risco associadas à utilização de ferramentas de *Instant Messaging* (IM). |
| DESCRIÇÃO:  Existem UTILIZADORES que usam contas de e-mail que não pertencem ao contexto da ORGANIZAÇÃO.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem UTILIZADORES que usam contas de e-mail que não pertencem ao contexto da ORGANIZAÇÃO (e.g. e-mails pessoais). A utilização deste tipo de contas facilita a saída irregular de dados. Se forem utilizadas contas que identifiquem o UTILIZADOR pessoalmente, a ORGANIZAÇÃO fica vedada de acesso a esse conteúdo.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, solicitando que não sejam utilizadas contas além das utilizadas oficialmente no contexto da ORGANIZAÇÃO. |

* + - 1. Vulnerabilidades em responsabilidades de UTILIZADOR

Este anexo contém o formulário de acompanhamento à verificação de vulnerabilidades das responsabilidades atribuídas aos UTILIZADORES.

**VULNERABILIDADES DE RESPONSABILIDADES DE UTILIZADOR**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de existência de vulnerabilidades relacionadas com as responsabilidades atribuídas aos UTILIZADORES. A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI- VRU-V1.0A |

O quadro seguinte apresenta as vulnerabilidades conhecidas relacionadas com as responsabilidades atribuídas aos UTILIZADORES.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| DESCRIÇÃO:  Existem registos de UTILIZADOR relacionados com a verificação dos dispositivos de redundância elétrica, que não estão a ser corretamente preenchidos conforme responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO (e.g. periodicidade definida no PSD).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem registos de UTILIZADOR relacionados com a verificação dos dispositivos de redundância elétrica, que não estão a ser corretamente preenchidos conforme as responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO. Se não forem corretamente verificados, uma falha na redundância elétrica pode conduzir à indisponibilidade do SISTEMA e perda de dados.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente lembrando a importância dos registos de verificação dos dispositivos elétricos, com o objetivo de permitir a atuação técnica de forma preventiva e não reativa. |
| DESCRIÇÃO:  Existem registos de UTILIZADOR relacionados com a verificação de cópias de segurança, que não estão a ser corretamente preenchidos conforme responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO (e.g. periodicidade definida no PSD).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem registos de UTILIZADOR relacionados com a verificação de cópias de segurança, que não estão a ser corretamente preenchidos conforme as responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO. Se não forem corretamente verificadas, perante uma falha pode não ser possível repor o SISTEMA em funcionamento.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente lembrando a importância dos registos de verificação de cópias de segurança, com objetivo de prever falhas de SISTEMA e a necessidade de reposição de dados. |
| DESCRIÇÃO:  Existem registos de UTILIZADOR relacionados com a validação de conteúdo das cópias de segurança, que não estão a ser corretamente preenchidos conforme responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO (e.g. periodicidade definida no PSD).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem registos de UTILIZADOR relacionados com a validação de conteúdo das cópias de segurança, que não estão a ser corretamente preenchidos conforme as responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO. A validação de conteúdo é importante para se avaliar a capacidade de reposição do SISTEMA em funcionamento.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente lembrando a importância da validação de conteúdo de cópias de segurança com o objetivo de avaliar a capacidade de reposição do SISTEMA. |
| DESCRIÇÃO:  Existem registos de UTILIZADOR relacionados com a verificação de redundância de discos que não estão a ser corretamente preenchidos conforme responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO (e.g. periodicidade definida no PSD).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem registos de UTILIZADOR relacionados com a verificação de redundância de discos, que não estão a ser corretamente preenchidos conforme as responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO. A redundância de discos é vital para manter o funcionamento do SISTEMA e da ORGANIZAÇÃO perante uma falha de *hardware*.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente lembrando a importância dos registos da redundância de discos, com objetivo de mitigar os riscos associados a falhas de *hardware*. |
| DESCRIÇÃO:  Existem registos de UTILIZADOR relacionados com a verificação de redundância de servidores que não estão a ser corretamente preenchidos conforme responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO (e.g. periodicidade definida no PSD).  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem registos de UTILIZADOR relacionados com a verificação de redundância de servidores, que não estão a ser corretamente preenchidos conforme as responsabilidades atribuídas pelo RESPONSÁVEL PELO TRATAMENTO. A redundância de servidores é vital para manter o funcionamento do SISTEMA e da ORGANIZAÇÃO perante uma falha de *hardware*.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente lembrando a importância dos registos da redundância de servidores, com objetivo de mitigar os riscos associados a falhas de *hardware*. |
| DESCRIÇÃO:  O conteúdo das cópias de segurança não demonstra que as responsabilidades atribuídas aos UTILIZADORES estão a ser corretamente cumpridas, conforme o definido no PSD.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  O conteúdo das cópias de segurança não demonstra que as responsabilidades atribuídas aos UTILIZADORES estão a ser corretamente cumpridas, conforme o definido no PSD. Perante uma falha de *hardware* pode não ser possível repor o SISTEMA em funcionamento.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente lembrando a importância das cópias de segurança com objetivo de mitigar os riscos associados a perdas de informação. |
| DESCRIÇÃO:  O tempo decorrido desde a última atribuição de responsabilidades aos UTILIZADORES excede o tempo limite definido no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última atribuição de responsabilidades aos UTILIZADORES excede o tempo limite definido no Regulamento do SISTEMA. Se não forem revistas periodicamente, pode fazer com que os UTILIZADORES caiam na rotina de preencher as folhas de registo sem a atenção devida, podendo conduzir a vulnerabilidades do SISTEMA em caso de falha.  MEDIDA CORRETIVA:  Promover a reatribuição de responsabilidades como previsto no Regulamento do SISTEMA, com o objetivo de vincar as responsabilidades atribuídas a cada UTILIZADOR. |

* + - 1. Vulnerabilidades de outros dispositivos

Este anexo contém o formulário de suporte à verificação de vulnerabilidades noutros dispositivos do SISTEMA.

**VULNERABILIDADES DE OUTROS DISPOSITIVOS**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de vulnerabilidades noutros dispositivos do SISTEMA.

A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar é fruto da aprendizagem contínua do AUDITOR nos diferentes sistemas que audita.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VBAI-V1.0A |

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O seu preenchimento facilita a identificação das vulnerabilidades a levantar e as medidas corretivas ou recomendações a propor. A coluna ITEM contém vulnerabilidades conhecidas que servem de guia à auditoria. A coluna REAÇÃO sugere a descrição da vulnerabilidade a registar, e medidas corretivas ou recomendações a sugerir.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| DESCRIÇÃO:  A revisão dos equipamentos de redundância elétrica não acontece há mais tempo do que o previsto no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  A revisão dos equipamentos de redundância elétrica não acontece há mais tempo do que o previsto no Regulamento do SISTEMA. Em caso de falha o SISTEMA fica vulnerável a alterações elétricas podendo estar em causa a perda de informação e a sua disponibilidade.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito ao prazo de revisão de dispositivos de redundância elétrica. |
| DESCRIÇÃO:  Existem DEA autorizados no PSD não se encontram em nenhuma das localizações autorizadas.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem DEA autorizados no PSD que não se encontram em nenhuma das localizações autorizadas. No caso de extravio ou furto, um DEA pode comprometer os dados da ORGANIZAÇÃO, podendo conduzir a incidentes de violação de dados.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, registar o IVD, avaliar a necessidade de notificação à AUTORIDADE DE CONTROLO, rever a necessidade do DEA, e rever as necessidades de formação dos UTILIZADORES. |
| DESCRIÇÃO:  São utilizados DEA não previstos no PSD nem autorizados pelo RESPONSÁVEL PELO TRATAMENTO no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  São utilizados DEA não previstos no PSD nem autorizados pelo RESPONSÁVEL PELO TRATAMENTO. A utilização irregular de DEA pode facilitar a saída descontrolada de dados ou a propagação de *malware* no SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente cumprindo as regras de utilização de DEA e utilizando apenas os que estiverem autorizados. |
| DESCRIÇÃO:  O tempo decorrido desde a última verificação da necessidade de existência de cada DEA excede o previsto no Regulamento do SISTEMA.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última verificação de necessidade de se utilizarem DEA excedeu o previsto no Regulamento de SISTEMA. A utilização incorreta de DEA pode facilitar a fuga de dados do SISTEMA pelo que, apenas devem existir os estritamente necessários.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente revendo periodicamente a necessidade de se utilizarem DEA no SISTEMA. |
| DESCRIÇÃO:  Existem DEA que saem da esfera física da ORGANIZAÇÃO cujo conteúdo pode ser consultado por estranhos ao SISTEMA no caso de furto ou extravio.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem DEA que saem da esfera física da ORGANIZAÇÃO cujo conteúdo pode ser consultado por estranhos ao SISTEMA no caso de furto ou extravio. O roubo ou extravio de um DEA é também o roubo ou extravio do seu conteúdo. A utilização de DEAs com informação legível (i.e. não encriptada) facilita a consulta dos dados por estranhos ao SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, nomeadamente no que diz respeito à saída de DEAs da esfera física da ORGANIZAÇÃO. |
| DESCRIÇÃO:  O tempo decorrido desde a última limpeza de destinos de cópias de segurança foi ultrapassado, pondo em risco o cumprimento do direito ao apagamento ou acesso pelos TITULARES DOS DADOS.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  O tempo decorrido desde a última limpeza integral das cópias de segurança excede o previsto no Regulamento do SISTEMA. A existência de dados em excesso dificulta a resposta ao direito de apagamento e acesso dos TITUALRES DOS DADOS por parte da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, solicitando ao ADMINISTRADOR DE SISTEMA que limpe os destinos das cópias de segurança periodicamente como previsto no regulamento. |
| DESCRIÇÃO:  Não existem cópias de segurança fora da esfera física da ORGANIZAÇÃO.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Não existem cópias de segurança deslocalizadas, i.e., fora da esfera física da ORGANIZAÇÃO. Se houver um incêndio ou assalto, o suporte para onde estão a ser feitas as cópias pode ficar danificado ou ser furtado, não sendo possível restaurar os dados no SISTEMA.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento de SISTEMA, promovendo cópias de segurança fora da esfera física da ORGANIZAÇÃO, mas cumprindo as questões de segurança previstas. |
| DESCRIÇÃO:  Existem interfaces não utilizados e configurados que podem ser ligados sem autorização do ADMINISTRADOR DE SISTEMA (e.g. impressoras e computadores com várias placas de rede).  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Existem interfaces possíveis não utilizados que podem ser conectados sem autorização e prévia configuração por parte do ADMINISTRADOR DO SISTEMA. A ligação de um dispositivo erradamente configurado pode por em risco a operabilidade do SISTEMA e pode facilitar a propagação de *malware* caso esteja infetado.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, nomeadamente no que diz respeito à admissão de novos dispositivos. Proteger as interfaces não utilizadas através de aplicações de segurança, parametrização do dispositivo ou através da colocação de selos inquebráveis. |

* + - 1. Vulnerabilidades operacionais

Este anexo contém o formulário de suporte à verificação de vulnerabilidades operacionais da ORGANIZAÇÃO.

**VULNERABILIDADES OPERACIONAIS**

Este documento é preenchido pelo AUDITOR como auxiliar à verificação de vulnerabilidades operacionais da ORGANIZAÇÃO.

A forma *checklist* deste modelo visa promover a eficiência da auditoria, diminuindo a hipótese de esquecimento. A lista de itens a verificar é fruto da aprendizagem contínua do AUDITOR nos diferentes sistemas que audita.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO: (vazio)  DATA: (vazio)  AUDITOR: (vazio) | **PRIMEIRO DIA:** (vazio)  **ÚLTIMO DIA:** (vazio)  **MOD:** DSPI-VO-V1.0A |

O quadro seguinte apresenta uma lista de itens a verificar a cada auditoria. O seu preenchimento facilita a identificação das vulnerabilidades a levantar e as medidas corretivas ou recomendações a propor. A coluna ITEM contém vulnerabilidades conhecidas que servem de guia à auditoria. A coluna REAÇÃO sugere a descrição da vulnerabilidade a registar, e medidas corretivas ou recomendações a sugerir.

|  |  |
| --- | --- |
| ITEM | REAÇÃO |
| DESCRIÇÃO:  Pelo menos um dos servidores em produção não está abrangido por um compromisso de garantia (e.g. extensão) ou contrato de suporte do fabricante.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem servidores em produção não abrangidos por garantia ou contrato de suporte do fabricante. Uma avaria pode condicionar ou inviabilizar o acesso às aplicações ou dados do servidor. Atendendo à importância do dispositivo na infraestrutura, a avaria pode conduzir à substituição repentina e mal ponderada.  MEDIDA CORRETIVA:  Promover que seja efetuado um contrato com o fabricante que assegure componentes eletrónicos em caso de avaria. Se impossível ou inviável, promover a substituição do dispositivo. |
| DESCRIÇÃO:  Existe pelo menos um dispositivo importante para a operacionalidade da ORGANIZAÇÃO, mas cujo *software* é incompatível com novos computadores.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem dispositivos na ORGANIZAÇÃO vitais para o seu funcionamento, cujo *software* é incompatível com computadores recentes. Em caso de falha de um desses dispositivos pode por em causa a operacionalidade da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover a atualização ou substituição dos dispositivos envolvidos. |
| DESCRIÇÃO:  A ORGANIZAÇÃO tem endereços de e-mail que identificam UTILIZADORES e que inviabilizam o acesso à informação aquando da saída destes da ORGANIZAÇÃO.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem endereços de e-mail que identificam UTILIZADORES e que inviabilizam o acesso à informação aquando da saída destes da ORGANIZAÇÃO. Em caso de saída do UTILIZADOR TITULAR DOS DADOS, não será possível aceder ao conteúdo do e-mail porque seria uma violação de DADOS PESSOAIS.  MEDIDA CORRETIVA:  Promover a anonimização de endereços de e-mail e o cumprimento de boas práticas respeitantes à não utilização do e-mail para fins que não o profissional. |
| DESCRIÇÃO:  Existem dispositivos que aparentam ter informação pessoal que pode conduzir à violação de DADOS PESSOAIS aquando da saída de UTILIZADORES.  IMPACTO DE SUGESTÃO: Severo | VULNERABILIDADE:  Existem dispositivos no SISTEMA com DADOS PESSOAIS de UTILIZADOR cujo acesso pela ORGANIZAÇÃO após a sua saída (e.g. cessação de contrato), pode significar violação de DADOS PESSOAIS.  MEDIDA CORRETIVA:  Promover o cumprimento do Regulamento do SISTEMA, mantendo apenas a informação atual e necessária para a operacionalidade da ORGANIZAÇÃO. |
| DESCRIÇÃO:  Não existe suporte protocolado com pelo menos um parceiro responsável pela gestão dos domínios.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Não existe suporte protocolado com pelo menos um parceiro responsável pela gestão dos domínios. O acesso não protocolado com o parceiro responsável pela gestão de domínios, pode originar problemas de acesso aos diversos serviços da ORGANIZAÇÃO que se baseiam nesses domínios (e.g. sites, e-mail, etc.).  MEDIDA CORRETIVA:  Promover que RESPONSÁVEL PELO TRATAMENTO consiga protocolar o serviço com o parceiro, ou promover a substituição do parceiro. |
| DESCRIÇÃO:  Não existe suporte protocolado com algum dos parceiros responsáveis pela administração ou alojamento dos *sites* da ORGANIZAÇÃO.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Não existe suporte protocolado com algum dos parceiros responsáveis pela administração ou alojamento dos *sites* da ORGANIZAÇÃO. O acesso não protocolado pode originar indisponibilidades descontroladas dos serviços e impactar negativamente a imagem da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover que RESPONSÁVEL PELO TRATAMENTO consiga protocolar o serviço com o parceiro, ou promover a substituição do parceiro. |
| DESCRIÇÃO:  Não existe suporte protocolado com o parceiro responsável pelas caixas de e-mail.  IMPACTO DE SUGESTÃO: Critico | VULNERABILIDADE:  Não existe suporte protocolado com o parceiro responsável pelas caixas de e-mail. O acesso não protocolado pode originar indisponibilidades descontroladas do serviço, perda de dados e impactar negativamente a imagem da ORGANIZAÇÃO.  MEDIDA CORRETIVA:  Promover que RESPONSÁVEL PELO TRATAMENTO consiga protocolar o serviço com o parceiro, ou promover a substituição do parceiro. |

* 1. RECOMENDAÇÕES COMUNS

Nesta secção consta a lista de recomendações comuns que podem ser sugeridas para implementação por parte da ORGANIZAÇÃO.

|  |
| --- |
| DESCRIÇÃO |
| Implementar uma camada adicional de proteção de *malware* através de uma *appliance* de segurança. |
| Adquirir uma aplicação de segurança para encriptar ficheiros. |
| Adquirir uma aplicação de segurança para controlo de DEAs. |
| Configurar todos os IPs da rede como estáticos. |