**DSPI**

**DOSSIER DE SEGURANÇA E PRIVACIDADE INFORMÁTICA**

(Gesminho-Assessoria de Negócios, Lda.)

CONTEÚDO CONFIDENCIAL

O conteúdo deste documento é confidencial e apenas pode ser consultado e editado pelas pessoas devidamente autorizadas na secção I -2.4 – Pessoas Autorizadas, e pelo:

1. RESPONSÁVEL PELO TRATAMENTO de dados definido pelo RGPD;
2. Encarregado de Proteção de Dados em funções ou equivalente (DPO); e
3. ADMINISTRADOR DE SISTEMA Informático.

Versão da estrutura: 1.0

*Este dossier não pode ser reproduzido nem a sua estrutura reutilizada a não ser com a autorização expressa e por escrito do seu autor i.e. (TIC – Tecnologia Informática e Computadores Lda.)*

1. ROSTO DO DOSSIER

Este módulo contém informação genérica do DOSSIER de Segurança e Privacidade Informática (DSPI). Recomenda-se a sua consulta porque contextualiza o leitor e promove um melhor entendimento das restantes secções.

* 1. DEFINIÇÕES, SIGLAS E ACRÓNIMOS

Neste DOSSIER são utilizados siglas e acrónimos. Além disso são também utilizados termos regulamentados pelo RGPD. Neste contexto faz sentido inclui-los neste documento para contextualizar e facilitar a leitura.

* + 1. Definições

|  |  |
| --- | --- |
| TERMO | SIGNIFICADO |
| AUTORIDADE DE CONTROLO | Autoridade nacional responsável por fiscalizar o cumprimento do RGPD em Portugal. |
| DADOS PESSOAIS | *“… informação relativa a uma* ***pessoa singular identificada*** *ou* ***identificável****... é identificável uma pessoa singular que possa ser identificada direta ou indiretamente em especial por referência a um identificado (e.g. nome, número de identificação, dados de localização (e.g. coordenadas GPS, endereços IP, etc.), identificadores por via eletrónica; um ou conjugação de vários elementos como características físicas, fisiológica, genética, metal, económica, cultural ou social)…”* (Art.º 4, Nº. 1) |
| RESPONSÁVEL PELO TRATAMENTO | *“… a pessoa singular ou coletiva, a autoridade pública, a agência ou organismo que, individualmente, ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação, podem ser previstos pelo direito da União ou de um Estado-Membro”*. (Art.º 4, N. 7) |
| SUBCONTRATANTE | *“… pessoa singular ou coletiva… que trate os dados pessoais por conta do responsável pelo tratamento destes”.* (Art.º 4 Nº. 8) |
| TITULAR DOS DADOS ou TITULARES DOS DADOS | Pessoas ou pessoa singular dona dos seus dados pessoais. |
| TRATAMENTO DE DADOS PESSOAIS | *“… uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição”.* (Art.º 4, Nº. 2) |

* + 1. Gerais

Este documento utiliza também outros termos e que são apresentados ou descritos na tabela abaixo.

|  |  |
| --- | --- |
| TERMO | SIGNIFICADO |
| AUDITOR | Auditor responsável por validar as práticas relacionadas com o âmbito definido neste documento. |
| DSPI | Dossier de Segurança e Privacidade Informática. |
| DOSSIER | Documentos organizados de forma sistemática com o objetivo de comprovar a preocupação da EMPRESA com as questões de segurança e privacidade regulamentada pelo RGPD. |
| DPO | *Data Protection Officer* (Encarregado de proteção de dados). |
| N/A | Não aplicável. |
| ORGANIZAÇÃO | Empresa ou conjunto de empresas (i.e. grupo de empresas) que partilham o mesmo SISTEMA total ou parcialmente (i.e. Firjó - Fios e Malhas, Lda.). |
| RGPD | Sigla pelo qual é conhecido o Regulamento Geral de Proteção de Dados EU 2016/679. |
| SISTEMA | Conjunto de dispositivos, infraestruturas, UTILIZADORES e parceiros, que constituem o sistema informático da ORGANIZAÇÃO. Consideram-se pertencentes ao SISTEMA os dispositivos ligados de forma permanente (e.g. impressora ligada por rede) ou não (e.g. disco externo ou *pendrive* ligada conectada por USB). |
| SPRINT | Tempo decorrido entre duas auditorias de revisão seguidas. |
| UTILIZADOR ou UTILIZADORES | Pessoa ou pessoas que utilizam o SISTEMA. |

* + 1. Tecnologia

A tabela seguinte indica o significado de termos relacionados com tecnologia.

|  |  |
| --- | --- |
| TERMO | SIGNIFICADO |
| AP | *AccessPoints* (dispositivo para difusão de sinal WiFi) |
| BD | Base de dados |
| BIOS | *Basic Input/Output System* |
| DEA | Dispositivos externos de armazenamento (*pendrives*, discos externos, cartões de memória, outro) |
| KIS | *Kaspersky Internet Security* |
| IM | *Instant Messaging* |
| IVD | Incidente de Violação de Dados |
| LAN | *Local Area Network* (rede) (cabo ou WIFI) |
| NAS | *Network Attached Storage* |
| PSD | Plano de Segurança de Disponibilidade |
| SGBD | Sistema de Gestão de Base de Dados |
| SI | Sistema Informático |
| SO | Sistema operativo de computador ou outro dispositivo (e.g. Windows, Linux, Android, etc.) |
| SSL | *Secure Sockets Layer* |
| UOE | Unidades óticas de escrita (e.g. unidades de CD, DVD, *blue-ray*, ou equivalente) |
| UPS | *Uninterruptible Power Supply* |
| USB | *Universal Serial Bus* |
| VM | *Virtual Machine* (máquina virtual) |
| WIFI | Meio de comunicação sem fios (sinal de rádio) |

* + 1. Prefixos

A tabela seguinte apresenta as siglas utilizadas para definir componentes do SISTEMA.

|  |  |
| --- | --- |
| TERMO | SIGNIFICADO |
| APP | Outra aplicação (não de segurança), identificado na Caracterização de SISTEMA (e.g. APP001). |
| APS | Aplicação de Segurança , identificada na Caracterização do SISTEMA (e.g. APS001). |
| AUT | Autorização de acesso externo , identificada no Plano de Segurança e Disponibilidade (e.g. AUT001). |
| BAK | Dispositivo de *backup* , identificado na infraestrutura do SISTEMA (e.g. BAK001). |
| CPF | Computador fixo , identificado na infraestrutura de SISTEMA (e.g. CPF001). |
| CPP | Computador portátil , identificado na arquitetura de SISTEMA (e.g. CPP001). |
| DEA | Dispositivo Externo de Armazenamento , identificado na infraestrutura de SISTEMA (e.g. DEA001). |
| DEP | Departamento pertencente a uma empresa da ORGANIZAÇÃO, identificada no Rosto do DOSSIER (e.g. DEP001). |
| DPR | Dispositivo de produção , máquina ou dispositivo de produção (i.e. utilizado na atividade operacional da ORGANIZAÇÃO) (e.g. máquina de bordar, equipamento de corte, etc.), identificado na infraestrutura de SISTEMA (e.g. DPR001). |
| DRD | Distribuidor de rede com fio *(wired)*, identificado na infraestrutura de SISTEMA (e.g. DRD001). |
| DRS | Distribuidor de rede sem fio *(wireless)*, identificado na infraestrutura de SISTEMA (e.g. DRS001). |
| EMP | Empresa pertencente à ORGANIZAÇÃO, identificada no Rosto do DOSSIER (EMP001). |
| ESS | Equipamento de Segmentação ou Segurança , identificado na infraestrutura de SISTEMA (e.g. ESS001). |
| IMP | Impressora , identificada na infraestrutura de SISTEMA (e.g. IMP001). |
| OUT | Outro equipamento , identificado na infraestrutura do SISTEMA (e.g. OUT001). |
| PAR | Parceiro identifica uma empresa ou pessoa a quem se pode recorrer para suporte técnico, identificado na Caracterização do SISTEMA (e.g. PAR001). |
| PLI | Proteção de ligação , identificado no PSD (e.g. PLI001). |
| REC | Recurso de rede , identificado na Caracterização do SISTEMA (e.g. REC001). |
| REE | Equipamento de redundância elétrica , identificado na infraestrutura do SISTEMA (e.g. REE001). |
| SEG | Segmento , identifica um segmento de rede do SISTEMA. |
| SRV | Servidor (e.g. dados, ficheiros, etc.) número , devidamente identificado na arquitetura de sistema (e.g. SRV001). |
| USR | UTILIZADOR do SISTEMA , identificado na Caracterização do SISTEMA (e.g. USR001). |
| V | Vulnerabilidade , identificado nas Vulnerabilidades e Medidas Corretivas (e.g. V000001). |

* 1. OBJETO

Este DOSSIERdescreve o sistema e demonstra a preocupação da ORGANIZAÇÃO para com a segurança e privacidade de dados do seu SI. As secções que o compõem descrevem a informação organizada de forma a facilitar a leitura. A informação é sistematizada em quadros para facilitar o preenchimento e a consulta.

O DOSSIERfoi criado de forma a reunir toda a documentação que comprova e demonstra o percurso focado em melhorar continuamente os aspetos de segurança e privacidade regulamentados. Pretende registar o cumprimento das regras e das boas práticas conducentes à conformidade com o RGPD.

* + 1. Contextualização

Este documento comprova a importância dos aspetos de segurança, privacidade, integridade e disponibilidade para a ORGANIZAÇÃO. Contém toda a documentação resultante dos processos de auditoria realizadas sobre o SISTEMA ao longo do tempo (atas, vulnerabilidades, cópias de segurança, etc.). O objetivo principal deste documento é demonstrar a percurso do SISTEMA da empresa rumo a conformidade com o RGPD e demais legislação (e.g. *software* fidedigno).

Este DOSSIERalém de orientar os auditores nos processos de auditoria e relato, também foi criado com o objetivo de facilitar a consulta das provas de que o SISTEMA se mantém protegido e atual, utilizando o bom senso e atendendo à disponibilidade financeira para o investimento da ORGANIZAÇÃO.

Apesar de ser impossível garantir em absoluto que um sistema não seja vítima de ataque ou roubo de dados, este documento regula e regista todos os aspetos de segurança com o objetivo de apoiar a manutenção do SISTEMA no melhor nível possível de segurança.

Em suma, pretende demonstrar a aplicação de regras que visem aumentar o nível de conformidade com o RGPD, agregando a documentação que permite demonstrar a preocupação da ORGANIZAÇÃO com as questões de privacidade, segurança, integridade e disponibilidade dos dados.

* + 1. Âmbito e não âmbito

Este DOSSIERdocumenta apenas os aspetos de privacidade e segurança relacionados com o SI da ORGANIZAÇÃO. São considerados todos os dispositivos identificados durante as auditorias, ligados ou integrados com o SI através de um qualquer meio digital (e.g. LAN, USB, etc.). Os dispositivos e periféricos assumidos como âmbito deste DOSSIER, são apenas os que constam da arquitetura de sistema especificada mais à frente neste documento.

Não são considerados no âmbito, os dispositivos que não têm ligação ou integração com o SI (e.g. relógio de ponto de cartões em papel; equipamentos de impressão utilizados apenas para cópia sem utilização de LAN, USB ou DEA camaras de vigilância não ligadas por qualquer meio ao SI; etc.). Estão excluídos todos os dispositivos e equipamentos não considerados na arquitetura de sistema.

* + 1. Organização

Este ponto descreve a estrutura organizacional do SISTEMA. Um sistema pode servir várias empresas. Assim sendo, atendendo à dificuldade de fazer representar o sistema individual de cada uma, representa-se apenas o SISTEMA como pertencente à ORGANIZAÇÃO que pode conter várias empresas.

A ORGANIZAÇÃO Gesminho-Assessoria de Negócios, Lda. é constituída pelas empresas enumeradas no quadro abaixo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | EMPRESA | DEPARTAMENTO | | LOCALIZAÇÃO |
| EMP001 | Gesminho-Assessoria de Negócios, Lda. |  |  | Av. Alcaides Faria 402, 4705-106 BARCELOS |
|  |  | DEP001 | Sede | Av. Alcaides Faria 402, 4705-106 BARCELOS |

* + 1. Encarregado de proteção de dados (DPO)

O Art.º 29 do RGPD diz que o *“responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:*

* *O tratamento for efetuado por uma autoridade… excetuando tribunais no exercício da sua função jurisdicional;*
* *As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou*
* *As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala…“* (Art.º 37 N. 1).

Tendo por base o RGPD, o RESPONSÁVEL PELO TRATAMENTO não considerou necessário nomear um DPO para a ORGANIZAÇÃO conforme registado na ata única de 2018-05-21 resultante do diagnóstico inicial por si assinada.

* + 1. Pessoal autorizado

Apenas as pessoas indicadas no quadro abaixo estão autorizadas a manusear este documento, no entanto podem existir restrições mediante as permissões atribuídas.

|  |  |  |
| --- | --- | --- |
| NOME | PERFIL | PERMISSÕES |
| José Rodrigues | RESPONSÁVEL PELO TRATAMENTO | Apenas consulta |
| Marta Martinho | Auditor externo | Edita e consulta |
| Célio Carvalho | Administrador do SISTEMA | Apenas consulta |

* + 1. Revisões de estrutura

Neste ponto constam as revisões efetuadas na estrutura deste DOSSIER(e.g. reconfiguração de secções).

|  |  |  |
| --- | --- | --- |
| REVISÃO | | DESCRIÇÃO |
| Versão:  Data:  Autor: | 1.0  2018-02-15  Célio Carvalho | Estrutura inicial. |

Ordenação do registo mais recente para o mais antigo

* + 1. Diagnóstico inicial

O diagnóstico inicial é essencial para o DOSSIERde segurança, tendo em conta que é efetuado um levantamento exaustivo para caracterização do SISTEMA, do qual resulta a primeira ata onde estão indicadas as vulnerabilidades iniciais a tratar e respetivas medidas corretivas, se conhecidas. É composto por várias tarefas que têm por objetivo estruturar o DSPI e suportar a execução de auditorias periódicas devidamente documentadas.

Trata-se de uma fase complexa porque envolve simultaneamente o conhecimento do SISTEMA (cf. suporte técnico, infraestrutura, aplicações existentes, recursos e utilizadores), deteção das vulnerabilidades iniciais, criação de registos para apoio no diagnóstico inicial, e criação de registos para facilitar as auditorias de revisão.

De entre as várias tarefas executadas no diagnóstico inicial, salientam-se: i) aplicação do regulamento do SISTEMA (no anexo VI -1); ii) criação de registos para facilitar o processo de levantamento de dispositivos e aplicações que será integrado no módulo II - CARACTERIZAÇÃO DO SISTEMA; iii) criação de registos para facilitar o processo das auditorias de revisão, com arquivo no V - REGISTOS; iv) identificação de dispositivos e aplicações com os respetivos IDs constantes neste DOSSIER; v) levantamento dos compromissos a atender que serão especificados e controlados através do CALENDÁRIO; vi) identificação das estratégias já existentes ao nível da segurança e disponibilidade do SISTEMA (a incluir como ponto inicial de partida no módulo III - PLANO DE SEGURANÇA E DISPONIBILIDADE); e vii) especificação das vulnerabilidades e medidas corretivas que inicialmente constarão no módulo IV - VULNERABILIDADES E AUDITORIAS.

* 1. CALENDÁRIO

Nesta secção pode ser consultado o cronograma que contém marcos importantes para o sistema.

* + 1. Compromissos

O quadro seguinte resume as renovações, revisões e auditorias a que o sistema está sujeito. A informação está orientada ao compromisso, indica qual a periodicidade a tratar assim como a data das últimas 3 iterações de cada compromisso.

Este quadro vai permitir detetar erro humano, facilitando o cruzamento de dados com os marcos definidos no calendário da subsecção 3.2.

São exemplos de compromissos: i) renovações de licenciamento; ii) renovações de contratos de assistência; iii) revisões a *hardware* (e.g. UPS); iii) atualizações de segurança manuais periódicas; etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| COMPROMISSO | PERIODICIDADE (N) | N-2 | N-1 | N |
| Substituir consumíveis do CPF001 | Cada 4 anos |  |  |  |
| Substituir consumíveis do CPF002 | Cada 4 anos |  |  |  |
| Substituir consumíveis do CPF003 | Cada 4 anos |  |  |  |
| Substituir consumíveis do CPP001 | Cada 4 anos |  |  |  |
| Substituir consumíveis do SVR001 | Cada 4 anos |  |  |  |
| Revisão da UPS SEG001 | Cada 3 anos |  |  | 2015-07-09 |
| Renovação de licença ERP Primavera | Cada 12 meses |  |  | 2017-12-25 |
| Renovação das licenças do antivírus | Cada 12 meses |  |  | 2018-04-17 |
| Mudar palavras-chave de utilizador | Cada 12 meses |  |  |  |
| Reavaliação dos DEA | Cada 12 meses |  |  | 2018-05-21 |
| Limpar destino de cópias de segurança para garantir a minimização de ficheiros | Cada 12 meses |  |  |  |
| Rever responsabilidades atribuídas aos utilizadores | Cada 12 meses |  |  | 2018-05-21 |
| Reavaliação de regras de exceção de acesso à infraestrutura | Cada 12 meses |  |  | 2018-05-21 |

*Shift* à esquerda de todas as datas aquando da inserção de nova data na coluna N

* + 1. Cronograma

O cronograma seguinte distribui no tempo os compromissos da subsecção 3.1. O quadro apresenta os marcos em função da proximidade temporal. A coluna dos componentes é preenchida com códigos que são apresentados no módulo II - CARACTERIZAÇÃO DO SISTEMA.

A inserção de um marco recorrente pressupõe o preenchimento em todos os períodos representados em que o marco irá acontecer.

|  |  |  |  |
| --- | --- | --- | --- |
| ANO | DESCRIÇÃO | COMPONENTES | ESTADO |
| 2022 | | | |
| Dezembro | Renovação de licença ERP Primavera | APP003 |  |
| Dezembro | Substituir consumíveis de dispositivo | CPP001 |  |
| Maio | Substituir consumíveis de dispositivo | CPF001 |  |
| Maio | Substituir consumíveis de dispositivo | CPF002 |  |
| Maio | Substituir consumíveis de dispositivo | CPF003 |  |
| Maio | Limpar dados de cópias de segurança | DEA001,  DEA002,  DEA003,  SVR001,  CPP001 |  |
| Maio | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001,  CPF002,  CPF003,  CPP001,  SVR001 |  |
| Dezembro | Renovação de antivírus | APS001 |  |
| 2021 | | | |
| Dezembro | Renovação de licença ERP Primavera | APP003 |  |
| Julho | Revisão da UPS SEG001 | REE001 |  |
| Maio | Limpar dados de cópias de segurança | DEA001,  DEA002,  DEA003,  SVR001,  CPP001 |  |
| Maio | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001,  CPF002,  CPF003,  CPP001,  SVR001 |  |
| Dezembro | Renovação de antivírus | APS001 |  |
| 2020 | | | |
| Dezembro | Renovação de licença ERP Primavera | APP003 |  |
| Dezembro | Substituir consumíveis de dispositivo | CPP001 |  |
| Maio | Limpar dados de cópias de segurança | DEA001,  DEA002,  DEA003,  SVR001,  CPP001 |  |
| Maio | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001,  CPF002,  CPF003,  CPP001,  SVR001 |  |
| Dezembro | Renovação de antivírus | APS001 |  |
| 2019 | | | |
| Dezembro | Renovação de licença ERP Primavera | APP003 |  |
| Maio | Limpar dados de cópias de segurança | DEA001,  DEA002,  DEA003,  SVR001,  CPP001 |  |
| Maio | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001,  CPF002,  CPF003,  CPP001,  SVR001 |  |
| Abril | Substituir consumíveis de dispositivo | SVR001 |  |
| Abril | Renovação de antivírus | APS001 |  |
| 2018 | | | |
| Dezembro | Renovação de licença ERP Primavera | APP003 |  |
| Dezembro | Substituir consumíveis de dispositivo | CPP001 |  |
| Julho | Revisão da UPS SEG001 | REE001 |  |
| Maio | Substituir consumíveis de dispositivo | CPF001 |  |
| Maio | Substituir consumíveis de dispositivo | CPF002 |  |
| Maio | Substituir consumíveis de dispositivo | CPF003 |  |
| Maio | Limpar dados de cópias de segurança | DEA001,  DEA002,  DEA003,  SVR001,  CPP001 |  |
| Maio | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001,  CPF002,  CPF003,  CPP001,  SVR001 |  |

Ordenação de registos: futuro >> presente >> passado >> inicio

1. CARACTERIZAÇÃO DO SISTEMA

Este módulo apresenta todos os componentes que constituem o SISTEMA da ORGANIZAÇÃO. São apresentados os dispositivos, aplicações, recursos de rede e UTILIZADORES que o compõem, e parceiros que apoiam a ORGANIZAÇÃO com o suporte técnico necessário para assegurar a integridade e disponibilidade dos dados.

* 1. SUPORTE TÉCNICO

Esta secção documenta a informação referente às formas de contacto de suporte técnico, sendo o ID único em todas as subsecções.

* + 1. Fabricantes

No quadro seguinte, podem ser consultados contactos dos fabricantes de tecnologia com alguma relação atual com o SISTEMA (i.e. garantias ou contratos ativos com fabricantes).

|  |  |  |
| --- | --- | --- |
| ID | NOME | ACESSO |
| PAR004 | HP | TELEFONE: 210608027  HORÁRIO: Expediente |

* + 1. Parceiros ativos

Os contactos de parceiros, protocolados ou não protocolados com a ORGANIZAÇÃO, podem ser consultados no quadro seguinte.

|  |  |  |
| --- | --- | --- |
| ID | NOME | ACESSO |
| PAR001 | TIC - Tecnologia, Informática e Computadores, Lda. | TELEFONE: 253823453  HORÁRIO: Expediente |
| PAR002 | NOS | TELEFONE: 16200  HORÁRIO: 24x7x365 |
| PAR003 | JUFIL-Júlio Santos & Filhos, Lda. | TELEFONE: 229698120  HORÁRIO: Expediente |

* + 1. Parceiros inativos

No quadro seguinte estão identificados todos os parceiros inativos (e.g. encerramento da atividade).

|  |  |  |  |
| --- | --- | --- | --- |
| ID | NOME | ACESSO | OBSERVAÇÕES |
| (vazio) | (vazio) | TELEFONE: (vazio)  HORÁRIO: (vazio) | (vazio) |

* 1. INFRAESTRUTURA

Esta secção apresenta a infraestrutura do sistema catalogando todos os equipamentos, periféricos e outros dispositivos que o compõem. No caso de existirem equipamentos multifunções ou combo (e.g. *router* com *wireless*), apenas será atribuído um ID na categoria mais significativa do componente no contexto da arquitetura.

O SISTEMA é utilizado pela ORGANIZAÇÃO como suporte à sua operacionalidade. Nele estão instalados programas que tratam dados pessoais, cuja disponibilidade e funcionamento são importantes para que a ORGANIZAÇÃO cumpra com o disposto no RGPD.

Caso a ORGANIZAÇÃO já tenha identificado os componentes do SISTEMA noutro procedimento (e.g. identificação bens ao nível do imobilizado na contabilidade), os códigos de cada um, podem ser identificados em cada descrição (e.g. descrição do dispositivo, aplicação, etc.).

Os licenciamentos dos dispositivos e aplicações desta secção encontram-se no anexo VI -2. As credenciais dos equipamentos encontram-se em envelope fechado no anexo VI -3.

* + 1. Arquitetura do SISTEMA

A arquitetura de sistema constitui um aspeto fundamental para o SISTEMA, uma vez que, a partir dos diagramas que a descrevem, é possível ter uma visão do SISTEMA como um todo. Neste ponto, além do diagrama de alto nível da arquitetura do SISTEMA, são organizados em quadros os componentes constituintes da mesma.

* + - 1. Diagrama

/Users/martamartinho/Downloads/Arquitetura-2.pdfNesta subsecção pode ser visualizada a arquitetura de alto nível do SISTEMA, onde são apresentados os diferentes segmentos e equipamentos de segmentação.

* + - 1. Equipamentos de segmentação ou segurança

Os equipamentos de segmentação ou segurança representados no diagrama encontram-se organizados no quadro seguinte, onde além da descrição do equipamento, regista-se a localização deste na ORGANIZAÇÃO e a data em que foi adquirido.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| ESS001 | MARCA/ MODELO: HiltronTechnologies  CVE-3036020N  (equipamento cedido e assistido pela NOS)  AQUISIÇÃO: N/A | 192.168.1.1 | EMP001.DEP001 |

* + - 1. Segmentos de rede

No quadro seguinte encontram-se identificados os segmentos de rede criados a partir dos equipamentos de segmentação e segurança descritos no ponto anterior.

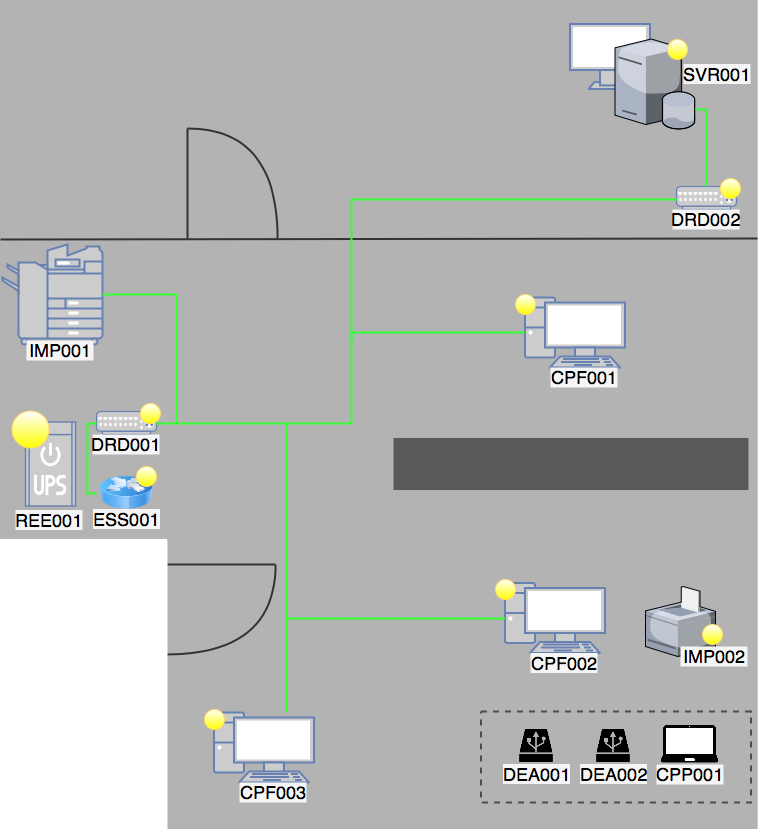
|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | EQUIPAMENTO DE SEGMENTAÇÃO |
| SEG001 | Sede da ORGANIZAÇÃO | ESS001 |

* + 1. Segmento 1

Este ponto descreve o segmento de rede identificado no quadro do ponto 5.1.3 com o ID SEG001 e tem como objetivo identificar todos os componentes que o constituem.

* + - 1. Diagrama

Na imagem seguinte pode ser consultada o diagrama deste segmento de rede. Os equipamentos estabilizados por cada dispositivo de redundância elétrica são identificáveis através dos círculos presentes no diagrama. Cada cor de círculo corresponde a um circuito estabilizado (e.g. os círculos amarelos são estabilizados pela REE marcada com o mesmo símbolo e cor).



* + - 1. Redundância elétrica

É essencial prevenir eventuais falhas de energia que comprometam a operacionalidade da ORGANIZAÇÃO, logo torna-se necessário controlar os componentes de redundância elétrica existentes. Pretende-se monitorizar estes recursos de redundância, com o objetivo de garantir a disponibilidade de dados, fazendo com que o SISTEMA seja mais tolerante a falhas.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| REE001 | MARCA/ MODELO:  APC Smart-UPS 2200  AQUISIÇÃO: Desconhecida | N/A | EMP001.DEP001 |

* + - 1. Servidores ou equivalentes

No quadro seguinte estão identificados os servidores físicos, virtuais ou equivalentes existentes no SISTEMA, mantendo informação acerca das suas características, da sua função e localização no SISTEMA.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | | LOCALIZAÇÃO |
| SVR001 | NOME NETBIOS: SERVIDOR  MARCA / MODELO: Dell OptiPlex 3020 MT  TIPO: Físico  PROCESSADOR: Intel Core i5-4590 CPU 3.30GHz  MEMÓRIA PRINCIPAL: 8 GB  MEMÓRIA SECUNDÁRIA: 240 GB (SSD); 500 GB (HDD)  FUNÇÃO: Servidor de ficheiros e de bases de dados  AQUISIÇÃO: 2016-04-18 | (dinâmico) | EMP001.DEP001 | |

* + - 1. Dispositivos de *backup*

No quadro seguinte são mantidas informações acerca dos dispositivos de cópias de segurança existentes no SISTEMA, como por exemplo NAS ou *tapes de backup*.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| (vazio) | NOME NETBIOS: (vazio)  MARCA / MODELO: (vazio)  FUNÇÃO: (vazio) | (vazio) | (vazio) |

* + - 1. Distribuidores de rede *wired*

Os distribuidores de rede com fios do SISTEMA encontram-se identificados do quadro seguinte.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| DRD001 | Conceptronic C100S8 Switch Fast Ethernet 8 portas 10/100 | N/A | EMP001.DEP001 |
| DRD002 | D-Link DGS-1008D 8 portas | N/A | EMP001.DEP001 |
| ESS001 | [ESS001] Inclui switch 4 portas | [ESS001] | [ESS001] |

* + - 1. Distribuidores de rede *wireless*

A informação relativa a equipamentos de rede sem fios existente no SISTEMA pode ser consultada no quadro seguinte.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| ESS001 | [ESS001] inclui *wireless* | [ESS001] | [ESS001] |

* + - 1. Computadores fixos

Nesta secção são apresentados os dados relativos aos computadores fixos no SISTEMA.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| CPF001 | NOME NETBIOS: MENA  MARCA / MODELO: Dell OptiPlex 390 (JPWD95J)  PROCESSADOR: Intel Core i3–2120 3.4 CPU 3.30GHz  MEMÓRIA PRINCIPAL: 4 GB  MEMÓRIA SECUNDÁRIA: 500 GB (HDD)  AQUISIÇÃO: 2012-04-19 | 192.168.1.101  (estático) | EMP001.DEP001 |
| CPF002 | NOME NETBIOS: JOSE  MARCA / MODELO: Dell OptiPlex 3010 (67H7ZZ1)  PROCESSADOR: Intel Core i3–3240 CPU 3.4GHz  MEMÓRIA PRINCIPAL: 4 GB  MEMÓRIA SECUNDÁRIA: 500 GB (HDD)  AQUISIÇÃO: 2013-12-31 | 192.168.1.103  (estático) | EMP001.DEP001 |
| CPF003 | NOME NETBIOS: PATRICIA  MARCA / MODELO: Dell OptiPlex 3110 (1MQDGZ1)  PROCESSADOR: Intel Core i3–3240 CPU 3.4GHz  MEMÓRIA PRINCIPAL: 4 GB  MEMÓRIA SECUNDÁRIA: 500 GB (HDD)  AQUISIÇÃO: 2013-12-31 | 192.168.1.102  (estático) | EMP001.DEP001 |

* + - 1. Computadores portáteis

O quadro seguinte regista a informação dos computadores portáteis que pertencem ao SISTEMA. Atendendo ao risco de extravio de informação, a localização destes dispositivos é essencial para a segurança dos dados. Assim, as localizações autorizadas destes dispositivos encontram-se definidas no PSD na secção 11.3.

|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP |
| CPP001 | NOME NETBIOS: DESKTOP-LQ34ROJ  MARCA / MODELO: Toshiba TECRA Z50-A-11R (C0368208E1E410K7)  PROCESSADOR: Intel Core i5–4200U CPU 1.6GHz  MEMÓRIA PRINCIPAL: 4 GB  MEMÓRIA SECUNDÁRIA: 240 GB (SSD)  AQUISIÇÃO: 2014-12-22 | (vazio) |

* + - 1. Impressoras, digitalizadores e multifunções

As impressoras, digitalizadores e multifunções existentes no SISTEMA, constam no quadro seguinte.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| IMP001 | DESCRIÇÃO: Impressora HP LaserJet M2727NF MFP  TECNOLOGIA DE IMPRESSÃO: Laser  TIPO: Multifunções  INTERFACES DISPONÍVEIS: LAN e USB  INTERFACE ATUAL: LAN  LEITOR DE USB OU CARTÕES: Não | 192.168.1.68  (estático) | EMP001.DEP001 |
| IMP002 | DESCRIÇÃO: HP OfficeJet Pro 8710  TECNOLOGIA DE IMPRESSÃO: Jato de tinta  TIPO: Multifunções  INTERFACES DISPONÍVEIS: LAN e USB  INTERFACE ATUAL: USB  LEITOR DE USB OU CARTÕES: USB | N/A | EMP001.DEP001 |

* + - 1. Dispositivos de produção

A informação relativa aos dispositivos usados na produção, tal como tipo de ligação ao SISTEMA, endereço IP (se aplicável) e localização, consta no quadro seguinte.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| (vazio) | DESCRIÇÃO: (vazio)  TIPO DE LIGAÇÃO AO SISTEMA: (vazio) | (vazio) | (vazio) |

* + - 1. Outros equipamentos

Os equipamentos que não se enquadram em nenhuma categoria dos pontos anteriores (e.g. relógios de ponto, camaras de vídeo) são registados no quadro seguinte.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ENDEREÇO IP | LOCALIZAÇÃO |
| (vazio) | (vazio) | (vazio) | (vazio) |

* + - 1. Dipositivos externos de armazenamento

São considerados dispositivos externos de armazenamento (DEA) todos aqueles cuja utilização normal permite transportar a informação para fora da esfera física do SISTEMA (e.g. *pendrives*, discos externos, cartões de memória, etc.). Atendendo ao risco de extravio de informação, a localização destes dispositivos é essencial para a segurança dos dados. Assim, as localizações autorizadas destes dispositivos encontram-se definidas no PSD na secção 11.3.

|  |  |  |
| --- | --- | --- |
| ID | TIPO | CONTEÚDO |
| DEA001 | Disco externo | Dispositivo utilizado para cópias de segurança onde consta informação operacional do ERP Primavera e dos restantes ficheiros da ORGANIZAÇÃO. |
| DEA002 | Disco externo | Dispositivo utilizado para cópias de segurança onde consta informação operacional do ERP Primavera e dos restantes ficheiros da ORGANIZAÇÃO. |

* + 1. Fora de uso

No quadro seguinte estão identificados os dispositivos inativados ou fora de uso. Embora atualmente já não pertençam ao SISTEMA, são mantidos nesta subsecção de forma a ser possível referenciar registos existentes.

|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | PARCEIRO |
| (vazio) | DESCRIÇÃO: (vazio)  MOTIVO DE INATIVIDADE: (vazio) | (vazio) |

* 1. APLICAÇÕES DE SEGURANÇA

As aplicações de segurança (APS) instaladas por dispositivo encontram-se especificadas no PSD. O ID de identificação das aplicações de segurança é único em toda a secção (e.g. infraestrutura, SO, etc.). Cada aplicação inclui uma lista com as proteções que oferece ao SISTEMA.

* + 1. Nível de infraestrutura

A informação relativa a aplicações de segurança ao nível de infraestrutura do SISTEMA é mantida no quadro seguinte.

|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | PROTEÇÕES |
| (vazio) | (vazio) | (vazio) |

* + 1. Nível de SO

No quadro seguinte consta a informação relativa a aplicações de segurança ao nível de SO.

|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | PROTEÇÕES |
| APS001 | Kaspersky Internet Security | Proteção antivírus e *firewall*. |

* + 1. Outros

As outras aplicações de segurança que não se enquadram nos quadros anteriores constam no seguinte (e.g. encriptadores de ficheiros).

|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | PROTEÇÕES |
| (vazio) | (vazio) | (vazio) |

* + 1. Fora de uso

As aplicações de segurança fora de uso no sistema devem ser mantidas no quadro seguinte de forma a ser possível referenciar os registos existentes.

|  |  |
| --- | --- |
| ID | DESCRIÇÃO |
| (vazio) | DESCRIÇÃO: (vazio)  MOTIVO DE INATIVIDADE: (vazio)  DATA: (vazio)  PARCEIRO: (vazio) |

* 1. OUTRAS APLICAÇÕES

Nesta secção são apresentadas todas as aplicações utilizadas no SISTEMA incluindo os SO. As licenças constituem o anexo VI -2 deste DOSSIER.

* + 1. Sistemas Operativos

As aplicações de produtividade do SISTEMA são mantidas no quadro seguinte.

|  |  |
| --- | --- |
| ID | DESCRIÇÃO |
| APP001 | Windows 10 Pro 64 bits |

* + 1. Aplicações de produtividade

As aplicações de produtividade do SISTEMA são mantidas no quadro seguinte.

|  |  |
| --- | --- |
| ID | DESCRIÇÃO |
| APP002 | Microsoft Office 2007 |
| APP004 | Microsoft SQL Server 2014 |
| APP005 | Microsoft Office 2013 |
| APP007 | Thunderbird |

* + 1. Aplicações operacionais

As aplicações operacionais (e.g. contabilidade, recursos humanos, gestão de produção, etc.) encontram-se identificadas no quadro seguinte.

|  |  |
| --- | --- |
| ID | DESCRIÇÃO |
| APP003 | ERP Primavera |
| APP006 | JUFIL |

* + 1. Aplicações por dispositivo

O quadro seguinte apresenta os SO e as aplicações de produtividade ou operacionais, instaladas por dispositivo.

|  |  |
| --- | --- |
| DISPOSITIVO | APLICAÇÕES |
| SVR001 | APP001, APP003, APP004 |
| CPF001 | APP001, APP002, APP003, APP006, APP007 |
| CPF002 | APP001, APP003, APP005, APP006 |
| CPF003 | APP001, APP003, APP005, APP006 |
| CPP001 | APP001, APP002 |

* + 1. Fora de uso

As aplicações fora de uso no SISTEMA devem ser mantidas no quadro seguinte de forma a ser possível referenciar os registos existentes.

|  |  |
| --- | --- |
| ID | DESCRIÇÃO |
| (vazio) | DESCRIÇÃO: (vazio)  MOTIVO: (vazio)  DATA: (vazio)  PARCEIRO: (vazio) |

* 1. RECURSOS DE REDE

Nesta secção incluem-se os recursos disponíveis na rede. O ID é único em toda a secção.

* + 1. Servidores de ficheiros e dados

O quadro seguinte apresenta os recursos de rede disponíveis no SISTEMA.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | TIPO | RECURSO PARTILHADO | CONTEÚDO |
|  | | (vazio) |  |
| REC001 | SBGD | PARTILHA / ORIGEM: SERVIDOR\Primavera  CREDENCIAIS: ANEXO VI -3 | Base de dados onde consta informação operacional do ERP Primavera (APP003, APP004). |
| REC002 | Pasta Patilhada | PARTILHA / ORIGEM: D:\Trabalho  CREDENCIAIS: ANEXO VI -3 | Ficheiros da ORGANIZAÇÃO |

* + 1. Recursos externos

Nesta secção constam os recursos externos que fazem parte do SISTEMA. Porque podem por em causa a privacidade e segurança dos dados, o quadro seguinte, além de os identificar individualmente também indica a justificação de utilização e a ata em que o RESPONSÁVEL PELO TRATAMENTO autoriza a sua utilização.

|  |  |  |
| --- | --- | --- |
| ID | SERVIÇO | DESCRIÇÃO DE CONTEÚDO |
| (vazio) | DESCRIÇÃO: (vazio)  CREDENCIAIS: (vazio) | (vazio) |

* + 1. Outros recursos

No quadro seguinte constam outros recursos de rede que não se enquadram nos pontos anteriores.

|  |  |  |
| --- | --- | --- |
| ID | TIPO | DESCRIÇÃO |
| [IMP002] | Impressora | Impressora HP cores IMP002 |

* + 1. Fora de uso

Os recursos de rede fora de uso no SISTEMA devem ser mantidas no quadro seguinte de forma a ser possível referenciar os registos existentes.

|  |  |  |
| --- | --- | --- |
| ID | DESCRIÇÃO | TIPO |
| (vazio) | DESCRIÇÃO: (vazio)  MOTIVO DE INATIVIDADE: (vazio) | (vazio) |

* 1. UTILIZADORES

Nesta secção encontra-se informação sobre os UTILIZADORES ativos e inativos do SISTEMA.

* + 1. Perfis de utilizador

Os perfis de UTILIZADOR do sistema encontram-se enumerados no quadro seguinte.

|  |  |
| --- | --- |
| PERFIL | PERMISSÕES |
| PER001 | PERFIL: Administrador  DESCRIÇÃO: acesso com permissões totais ao sistema operativo. |
| PER002 | PERFIL: Super administrador  DESCRIÇÃO: acesso com permissões totais a todo o SGBD. |
| PER003 | DESIGNAÇÃO: Super administrador  DESCRIÇÃO: acesso com permissões totais a qualquer base de dados do ERP. |
| PER004 | PERFIL: Utilizador  DESCRIÇÃO: acesso com permissões restritas ao sistema operativo. |

* + 1. Utilizadores ativos

Os UTILIZADORES ativos do SISTEMA encontram-se identificados no quadro seguinte, através do nome e tipo de permissão.

|  |  |
| --- | --- |
| ID | Nome |
| USR001 | José Monteiro |
| USR002 | Filomena Oliveira |
| USR003 | Patrícia Oliveira |
| [PAR001] | [PAR001] |

* + 1. Utilizadores inativos

Os UTILIZADORES inativos no SISTEMA devem ser mantidos no quadro seguinte de forma a ser possível referenciar os registos existentes.

|  |  |
| --- | --- |
| ID | Nome |
| (vazio) | (vazio) |

1. PLANO DE SEGURANÇA E DISPONIBILIDADE

Este módulo apresenta o Plano de Segurança e Disponibilidade (PSD) do SISTEMA, com o objetivo de promover a confidencialidade e disponibilidade dos dados. As secções que compõem este módulo pretendem demonstrar as medidas e dispositivos escolhidos pela ORGANIZAÇÃO para promover a segurança e disponibilidade dos dados e do SISTEMA.

O PSD é revisto periodicamente com o objetivo de acautelar novos dispositivos e aplicações de segurança ou disponibilidade existentes no mercado. Estas medidas podem ser sugeridas pelo AUDITOR ou pelo ADMINISTRADOR DE SISTEMA, fruto: i) da reavaliação dos riscos e da exposição a vulnerabilidades do SISTEMA; ii) da necessidade de melhorar continuamente o índice de proteção do SISTEMA com tecnologia atual; e iii) da maior disponibilidade de investimento da ORGANIZAÇÃO para investir em tecnologia relacionada com a segurança.

A edição do PSD é da responsabilidade do AUDITOR. Em cada auditoria de revisão o PSD deve ser revisto para avaliar a eficiência da proteção a novas ameaças. O AUDITOR deve promover que sejam sempre ponderados novos mecanismos de segurança, pesando sempre com bom senso o esforço de investimento de cada medida proposta e o impacto que pode representar na privacidade, segurança, integridade e disponibilidade dos dados e do SISTEMA.

É neste contexto que o controlo de versões de *software* e *firmware* instalados fazem parte integrante do PSD. Tendo por base o cruzamento das últimas versões estáveis de segurança disponibilizadas pelos fabricantes com as efetivamente implementadas no SISTEMA, o AUDITOR promove que o SISTEMA mantenha um baixo nível de exposição aos riscos, levantando vulnerabilidades quando as versões mais recentes não se encontrarem instaladas. Neste contexto, o PSD terá sempre as últimas versões estáveis de segurança disponibilizadas pelos respetivos fabricantes.

Alguns dos quadros apresentados nos itens seguintes solicitam um estado individual. Este estado pode ser utilizado pelo AUDITOR para definir: i) uma regra ainda não implementada; ii) uma regra em reavaliação; iii) uma regra de mitigação de risco; etc.

* 1. CONTROLO DE ACESSO À INFRAESTRUTURA
     1. Barreiras de acesso

As barreiras de acesso definidas no SISTEMA pretendem impedir o acesso ao SISTEMA por estranhos. As validações de barreiras de acesso são confirmadas a cada auditoria pelo AUDITOR.

* + - 1. Internet

No quadro seguinte constam os equipamentos que controlam o acesso (e.g. *routers*, *firewalls*, *appliances*, etc.), mantendo informação sobre a sua função e o domínio de administração (interno ou parceiro).

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | FUNÇÃO | QUEM ADMINISTRA |
| (vazio) | *Firewall* de administração interna exclusiva (ESS a implementar) | (vazio) |

* + - 1. Rede local

Neste ponto constam as barreiras de admissão à rede que devem ser configuradas nos dispositivos de distribuição de rede *wired* e *wireless* (e.g. *switchs* com gestão de portas, *accesspoints* com filtros *mac address*, etc.).

|  |  |
| --- | --- |
| DISPOSITIVO | DESCRIÇÃO |
| (vazio) | (vazio) |

* + - 1. Sistemas operativos (SO)

No quadro seguinte apresenta-se a informação relativa às barreiras de segurança cuja implementação deve ficar garantida nos SO, tais como *firewalls* por *software* (SO, KIS, etc.), conta de convidado inativa, acesso apenas com UTILIZADOR e palavra-chave a todos os recursos, etc.

|  |  |
| --- | --- |
| DISPOSITIVO / APLICAÇÃO | BARREIRAS |
| SVR001.APP001 |  |
|  | Conta de convidado inativada |
|  | Autenticação com nome de UTILIZADOR e palavra-chave |
| CPF001.APP001 |  |
|  | Conta de convidado inativada |
|  | Autenticação com nome de UTILIZADOR e palavra-chave |
| CPF002.APP001 |  |
|  | Conta de convidado inativada |
|  | Autenticação com nome de UTILIZADOR e palavra-chave |
| CPF003.APP001 |  |
|  | Conta de convidado inativada |
|  | Autenticação com nome de UTILIZADOR e palavra-chave |
| CPP001.APP001 |  |
|  | Conta de convidado inativada |
|  | Autenticação com nome de UTILIZADOR e palavra-chave |
| SVR001.APS001 |  |
|  | *Firewall* do Antivírus |
| CPF001.APS001 |  |
|  | *Firewall* do Antivírus |
| CPF002.APS001 |  |
|  | *Firewall* do Antivírus |
| CPF003.APS001 |  |
|  | *Firewall* do Antivírus |
| CPP001.APS001 |  |
|  | *Firewall* do Antivírus |

* + 1. Exceções de acesso

Esta secção contém as regras de exceção definidas nas barreiras de acesso. Apenas as regras abaixo estão previstas e autorizadas, devendo as restantes serem consideradas não conformidades se existirem. Esta validação é feita pelo AUDITOR a cada auditoria.

* + - 1. Internet

No quadro seguinte estão descritas as regras de acesso autorizadas por dispositivo.

|  |  |  |  |
| --- | --- | --- | --- |
| DISPOSITIVO | REGRA | DESCRIÇÃO | ESTADO |
| ESS001 |  |  |  |
|  | Rede pública (80) 🡪 ESS001 (80) | Suporte técnico remoto do parceiro | Ativo |

* + - 1. Rede local com fios

No quadro seguinte constam as regras de exceção definidas para acesso à rede local. Apenas são descritas regras de exceção se estiverem previstas barreiras de controlo de acesso ao meio com fios na rede local em 10.1.2.

|  |  |  |  |
| --- | --- | --- | --- |
| DISPOSITIVO | DISPOSITIVOS PERMITIDOS | ADMISSÃO | ESTADO |
| (vazio) |  |  |  |
|  | (vazio) | (vazio) | (vazio) |

* + - 1. Rede local sem fios

Regras de exceção para acesso à rede local sem fios podem ser consultadas no quadro seguinte (e.g. admissão por *mac address*). Apenas são descritas regras de exceção se estiverem previstas barreiras de controlo de acesso ao meio sem fios na rede local em 10.1.2.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | DISPOSITIVOS AUTORIZADOS | ESTADO |
| (vazio) |  |  |
|  | DISPOSITIVOS: (vazio)  ATA: (vazio)  JUSTIFICAÇÃO: (vazio) | (vazio) |

* + - 1. Sistemas operativos (SO)

As regras de exceção para acesso a computador fixos ou portáteis, servidores, ou outros equipamentos com SO, encontram-se descritas no quadro seguinte. Apenas as regras abaixo estão previstas e autorizadas. Todas as outras configuradas devem ser consideradas não conformidades. Na coluna REDES são enumeradas as redes em que as regras estão previstas.

|  |  |  |  |
| --- | --- | --- | --- |
| DISPOSITIVO | DESCRIÇÃO | REDES | ESTADO |
| SVR001 |  |  |  |
|  | PORTAS / DESCRIÇÃO: Partilha de Ficheiros do Windows | Local | Ativo |
|  | PORTAS / DESCRIÇÃO: Acesso ao SQL Server (Primavera) | Local | Ativo |

* + 1. Acessos externos

Nesta secção enumeram-se os acessos externos autorizados ao SISTEMA e mecanismos utilizados para minimizar o acesso não autorizado ao conteúdo transmitido através da rede pública.

* + - 1. Proteção de ligações

O quadro seguinte apresenta os mecanismos de proteção utilizados para proteger as ligações dos acessos externos autorizados, i.e. mitigação de risco no acesso inadvertido ao conteúdo transmitido na rede pública, e mecanismos de admissão de dispositivos remotos (e.g. certificado digital para admitir a ligação remota).

|  |  |
| --- | --- |
| ID | MECANISMOS DE PROTEÇÃO |
| (vazio) | (vazio) |

* + - 1. Acessos autorizados

No quadro seguinte consta informação sobre o tipo de acesso e quais os UTILIZADORES / dispositivos com autorização para acesso externo. Como os acessos externos podem por em causa a privacidade, segurança, integridade e disponibilidade dos dados e do SISTEMA, é identificada a autorização do RESPONSÁVEL DE TRATAMENTO e são enumeradas as medidas de proteção utilizadas em cada acesso autorizado.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | DISPOSITIVO | UTILIZADOR | TIPO | JUSTIFICAÇÃO | PROTEÇÕES |
|  | (vazio) | (vazio) |  |  |  |
| (vazio) |  |  | (vazio) | ATA:  (vazio)  JUSTIFICAÇÃO: (vazio) | (vazio) |

* 1. DISPOSITIVOS MÓVEIS

Esta secção apresenta as estratégias utilizadas para admissão de novos dispositivos de armazenamento externo (DEA). Apenas os DEA autorizados podem ser utilizados no SISTEMA. A validação das técnicas utilizadas para controlo dos DEA é feita pelo AUDITOR a cada auditoria.

* + 1. Mecanismos de controlo dos DEA

O quadro seguinte descreve como é feito o controlo da admissão de DEA (*pendrive*s, discos externos, etc.). É registada a utilização de aplicações de segurança que permitem bloquear o acesso não autorizado de DEA através de portas USB, leitores de cartões ou escritores de UOE.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | APLICAÇÃO DE SEGURANÇA | VERSÃO |
| DEA001 |  |  |
|  | Aplicação de segurança para cifrar a informação contida num dispositivo (APS a implementar) | (vazio) |
| DEA002 |  |  |
|  | Aplicação de segurança para cifrar a informação contida num dispositivo (APS a implementar) | (vazio) |
| CPP001 |  |  |
|  | Aplicação de segurança para cifrar a informação contida num dispositivo (APS a implementar) | (vazio) |

* + 1. Dispositivos/Utilizadores autorizados por DEA

No quadro seguinte estão registadas as autorizações de utilização de DEA por dispositivo/utilizador.

|  |  |  |  |
| --- | --- | --- | --- |
| DEA | DISPOSITIVOS/UTILIZADORES | JUSTIFICAÇÃO | ESTADO |
| DEA001 |  |  |  |
|  | CPF001/USR001 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Dispositivo utilizado para cópias de segurança onde consta informação operacional do ERP Primavera e dos restantes ficheiros da ORGANIZAÇÃO. | Ativo |
|  | SVR001/[PAR001] | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Em caso de perda ou destruição dos dados do servidor, o dispositivo pode ser utilizado pelo ADMINISTRADOR DO SISTEMA para reposição dos mesmos. |  |
| DEA002 |  |  |  |
|  | CPF003/USR003 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Dispositivo utilizado para cópias de segurança onde consta informação operacional do ERP Primavera e dos restantes ficheiros da ORGANIZAÇÃO. | Ativo |
|  | SVR001/[PAR001] | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Em caso de perda ou destruição dos dados do servidor, o dispositivo pode ser utilizado pelo ADMINISTRADOR DO SISTEMA para reposição dos mesmos. |  |

* + 1. Autorizações de mobilidade

No quadro seguinte estão registados os UTILIZADORES autorizados a movimentar dispositivos móveis (e.g. DEA, computadores portáteis, etc.), dentro e fora da ORGANIZAÇÃO (e.g. cópias de segurança deslocalizadas, passagem de ficheiro para máquina de produção, computador portátil do vendedor, etc.). No campo das localizações autorizadas devem ser inseridos os locais autorizados pelo RESPONSÁVEL PELO TRATAMENTO para cada dispositivo ou DEA (e.g. SRV001, domicilio do USR991, gabinete do USR992, viatura do USR993, etc.). Devem também ser mencionadas as medidas de proteção adicional no caso de transportarem DADOS PESSOAIS (e.g. dados encriptados através do APS991, o computador portátil não pode conter informação local além do catálogo de produtos, etc.).

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO / DEA | UTILIZADORES | JUSTIFICAÇÃO |
| DEA001 | USR002 |  |
|  |  | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Devem existir cópias de segurança deslocalizadas no SISTEMA  LOCALIZAÇÕES AUTORIZADAS: EMP001.DEP001; habitação do USR002  MEDIDAS DE PROTEÇÃO ADICIONAL: A informação contida no dispositivo encontra-se cifrada (APS a implementar) |
| DEA002 | USR003 |  |
|  |  | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Devem existir cópias de segurança deslocalizadas no SISTEMA  LOCALIZAÇÕES AUTORIZADAS: EMP001.DEP001; habitação do USR003  MEDIDAS DE PROTEÇÃO ADICIONAL: A informação contida no dispositivo encontra-se cifrada (APS a implementar) |
| CPP001 | USR001 |  |
|  |  | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Dispositivo usado para serviço externo prestado fora das instalações da ORGANIZAÇÃO.  LOCALIZAÇÕES AUTORIZADAS: EMP001.DEP001; habitação do USR001  MEDIDAS DE PROTEÇÃO ADICIONAL: A informação contida no dispositivo encontra-se cifrada (APS a implementar) |

* + 1. Dispositivos sujeitos a outras estratégias de bloqueio

O quadro seguinte apresenta outras estratégias de bloqueio permanente aplicadas em dispositivos onde não é possível ou exequível utilizar aplicações de segurança de bloqueio (e.g. cartões SD em impressoras).

|  |  |
| --- | --- |
| DISPOSITIVO | DESCRIÇÃO |
| IMP002 | Existência de selos inquebráveis nos orifícios de leitura de USB ou Cartões (a implementar) |

* 1. PERMISSÕES DOS UTILIZADORES

A validação de permissões dos UTILIZADORES é feita pelo AUDITOR em cada auditoria.

* + 1. Utilizadores autorizados por dispositivo

Nesta subsecção são enumerados os UTILIZADORES e respetivos perfis autorizados por dispositivo.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | UTILIZADOR | PERFIL |
| SVR001 |  |  |
|  | [PAR001] | APP001.PER001 |
| CPF001 |  |  |
|  | USR002 | APP001.PER004 |
|  | [PAR001] | APP001.PER001 |
| CPF002 |  |  |
|  | USR003 | APP001.PER004 |
|  | [PAR001] | APP001.PER001 |
| CPF003 |  |  |
|  | USR003 | APP001.PER004 |
|  | [PAR001] | APP001.PER001 |
| CPP001 |  |  |
|  | USR001 | APP001.PER004 |
|  | [PAR001] | APP001.PER001 |

* + 1. Utilizadores autorizados por aplicação

No quadro seguinte constam os perfis de acesso de cada UTILIZADOR a cada aplicação (e.g. faturação, contabilidade, gestão de produção, etc.). Apenas os UTILIZADORES mencionados têm autorização de acesso a cada aplicação mencionada.

|  |  |  |
| --- | --- | --- |
| APLICAÇÃO | UTILIZADOR | PERFIL |
| APP003 |  |  |
|  | USR001 | PER002 |
|  | [PAR001] | PER002 |
| APP004 |  |  |
|  | USR001 | PER003 |
|  | [PAR001] | PER003 |

* + 1. Utilizadores autorizados por recurso

O quadro seguinte mostra as permissões [RW,R] de cada UTILIZADOR por recurso.

|  |  |  |  |
| --- | --- | --- | --- |
| RECURSO | UTILIZADOR | AUTORIZAÇÃO | PERMISSÕES |
| REC001 |  |  |  |
|  | USR001 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que o UTILIZADOR possa desempenhar as suas funções na ORGANIZAÇÃO. | RW |
|  | USR002 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que o UTILIZADOR possa desempenhar as suas funções na ORGANIZAÇÃO. | RW |
|  | USR003 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que o UTILIZADOR possa desempenhar as suas funções na ORGANIZAÇÃO. | RW |
|  | [PAR001] | ATA: única de 2018-04-17  JUSTIFICAÇÃO: Necessário para que seja prestado o suporte técnico à ORGANIZAÇÃO. | RW |
| REC002 |  |  |  |
|  | USR002 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que o UTILIZADOR possa desempenhar as suas funções na ORGANIZAÇÃO. | RW |
|  | USR003 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que o UTILIZADOR possa desempenhar as suas funções na ORGANIZAÇÃO. | RW |
|  | USR001 | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que o UTILIZADOR possa desempenhar as suas funções na ORGANIZAÇÃO. | RW |
|  | [PAR001] | ATA: única de 2018-05-21  JUSTIFICAÇÃO: Necessário para que seja prestado o suporte técnico à ORGANIZAÇÃO. | RW |

* + 1. Utilizadores autorizados por recurso externo

O quadro seguinte mostra as permissões [RW,R] de cada UTILIZADOR por recurso externo.

|  |  |  |  |
| --- | --- | --- | --- |
| RECURSO | UTILIZADOR | AUTORIZAÇÃO | PERMISSÕES |
| (vazio) |  |  |  |
|  | (vazio) | ATA: (vazio)  JUSTIFICAÇÃO: (vazio)  CONHECE AS CREDENCIAIS [S/N]: (vazio) | (vazio) |

* 1. ILEGIBILIDADE DE DADOS E PROTEÇÕES DE MALWARE

Nesta secção identificam-se os dispositivos protegidos com mecanismos que impedem a legibilidade dos dados por estranhos, e enumeram-se também as proteções contra *malware* existentes no SISTEMA. Além disso identificam-se os dispositivos protegidos com mecanismos que impedem a legibilidade dos dados por estranhos ao SISTEMA.

* + 1. Mecanismos de ilegibilidade de dados por dispositivo

No quadro seguinte é possível consultar os mecanismos utilizados para prevenir o acesso irregular aos dados presentes nos dispositivos (e.g. DEA, computadores portáteis, etc.).

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | APLICAÇÃO | VERSÃO |
| DEA001 |  |  |
|  | Aplicação de segurança que assegure a confidencialidade dos dados através de cifragem da informação contida no dispositivo (APS a implementar) | A implementar |
| DEA002 |  |  |
|  | Aplicação de segurança que assegure a confidencialidade dos dados através de cifragem da informação contida no dispositivo (APS a implementar) | A implementar |
| CPP001 |  |  |
|  | Aplicação de segurança que assegure a confidencialidade dos dados através de cifragem da informação contida no dispositivo (APS a implementar) | A implementar |

* + 1. Proteções de *malware* de infraestrutura por dispositivo

O quadro seguinte apresenta os dispositivos de infraestrutura presentes na ORGANIZAÇÃO que contêm proteções contra *malware* (e.g. *appliances*).

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | APLICAÇÃO | VERSÃO |
| (vazio) |  |  |
|  | (vazio) | (vazio) |

* + 1. Proteções de *malware* de SO por dispositivo

O quadro seguinte apresenta as aplicações de segurança instaladas por dispositivo. Devem ser levantadas vulnerabilidades a todos dispositivos com SO que não estejam protegidas por este tipo de aplicação.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | APLICAÇÃO | VERSÃO |
| SVR001 |  |  |
|  | APS001 | 17.0.0.611 |
| CPF001 |  |  |
|  | APS001 | 17.0.0.611 |
| CPF002 |  |  |
|  | APS001 | 17.0.0.611 |
| CPF003 |  |  |
|  | APS001 | 17.0.0.611 |
| CPP001 |  |  |
|  | APS001 | 17.0.0.611 |

* 1. ATUALIZAÇÕES DE SEGURANÇA

Nesta secção identificam-se os dispositivos com necessidades regulares de atualizações de segurança.

* + 1. Versões de SO e outras aplicações

O quadro seguinte permite rastrear as aplicações por dispositivo com necessidades de atualizações de segurança regulares. Para facilitar a leitura, o SO é sempre a primeira aplicação mencionada por dispositivo. Apesar das atualizações de aplicações profissionais serem maioritariamente não relacionadas com a segurança e disponibilidade, serão também aqui consideradas pelo facto de lidarem com DADOS PESSOAIS e poderem haver atualizações de segurança a este nível.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | APLICAÇÃO | VERSÃO |
| SVR001 |  |  |
|  | APP001 | 10.0.16299.371 |
|  | APP003 | 9.0 |
|  | APP004 | 12.0.2569.0 |
| CPF001 |  |  |
|  | APP001 | 10.0.16299.371 |
|  | APP002 | 12.0.6612.1000 |
|  | APP003 | 9.0 |
|  | APP005 |  |
|  | APP006 | 11.0.0 |
| CPF002 |  |  |
|  | APP001 | 10.0.16299.371 |
|  | APP003 | 9.0 |
|  | APP005 | 15.0.4989.1000 |
|  | APP006 | 11.0.0 |
| CPF003 |  |  |
|  | APP001 | 10.0.16299.371 |
|  | APP003 | 9.0 |
|  | APP005 | 15.0.5023.1000 |
|  | APP006 | 11.0.0 |
| CPP001 |  |  |
|  | APP001 | 10.0.16299.371 |
|  | APP003 | 9.0 |

* + 1. Versões de *firmware*

O quadro seguinte resume os dispositivos com necessidade de atualizações de *firmware*. As versões representam as últimas atualizações de segurança disponibilizadas por cada fabricante. As versões indicadas em dispositivos do tipo computador fixo ou móvel referem-se à BIOS do equipamento.

|  |  |
| --- | --- |
| DISPOSITIVO | VERSÃO |
| ESS001 | 10.2.1.L |
| SVR001 | 3.40 |
| CPF001 | A05 |
| CPF002 | A11 |
| CPF003 | A10 |
| CPP001 | 3.40 |
| IMP001 | 20071203 |
| IMP002 | WBP2CN1803AR |

* 1. DISPONIBILIDADE E INTEGRIDADE DOS DADOS

Nesta secção enumeram-se os mecanismos implementados no SISTEMA que promovem a disponibilidade e integridade dos dados.

* + 1. Redundância elétrica

Nesta secção são registados os tipos de redundância elétrica implementados no SISTEMA. As responsabilidades de verificação dos equipamentos de redundância são atribuídas aos UTILIZADORES pelo RESPONSAVEL PELO TRATAMENTO em ata.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | DESCRIÇÃO | RESPONSABILIDADE DE VERIFICAÇÃO |
| REE001 | FUNÇÃO: Estabilização de energia dos dispositivos elegíveis a serem estabilizados.  MANUTENÇÃO: Substituição das baterias a cada 3 anos. | UTILIZADOR: USR002  PERIODICIDADE: Todas as sextas-feiras |

* + 1. Redundância de servidores

Nesta secção incluem-se os servidores que podem entrar em produção em caso de inoperabilidade ou falha dos que se encontram em produtivo. As verificações de redundância de servidores são da responsabilidade dos UTILIZADORES de SISTEMA designados pelo RESPONSÁVEL DO TRATAMENTO de dados em ata.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | DESCRIÇÃO | RESPONSABILIDADE DE VERIFICAÇÃO |
| (vazio) | ATUALIZAÇÃO DE DADOS: (vazio)  DISPOSITIVOS ORIGEM DOS DADOS: (vazio) | UTILIZADOR: (vazio)  PERIODICIDADE: (vazio) |

* + 1. Redundância de discos

Nesta secção são descritos os sistemas de redundância de discos utilizados pela ORGANIZAÇÃO (e.g. RAID 0, 1, 5, etc.). As verificações de bom funcionamento dos mecanismos de redundância são da responsabilidade dos UTILIZADORES de SISTEMA designados pelo RESPONSÁVEL DO TRATAMENTO de dados em ata.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO | DESCRIÇÃO | RESPONSABILIDADE DE VERIFICAÇÃO |
| (vazio) | TIPO DE REDUNDÂNCIA: (vazio) | UTILIZADOR: (vazio)  PERIODICIDADE: (vazio) |

* + 1. Cópias de segurança

Nesta secção estão descritas todas as tarefas existentes para execução de cópias de segurança. São mantidos os registos de verificação de execução de cópias de segurança. Quando designado pelo RESPONSÁVEL PELO TRATAMENTO, podem também existir tarefas de validação de conteúdo de cópias de segurança. Os registos de verificação e validação (se aplicável) de cópias de segurança são da responsabilidade dos UTILIZADORES de SISTEMA designados pelo RESPONSÁVEL DO TRATAMENTO de dados em ata. A coluna destino identifica o dispositivo e pasta destino para o qual é feita a cópia de segurança.

|  |  |  |
| --- | --- | --- |
| DESTINO | DESCRIÇÃO | RESPONSABILIDADE DE VERIFICAÇÃO |
| [REC002]\  CopiasPrimavera | EXECUTANTE: Primavera Windows Services  ORIGEM DOS DADOS: REC001  TIPO: Completo  TIPO DE VERIFICAÇÃO: Visual (data de criação do ficheiro resultado das cópias) | UTILIZADOR:N/A  PERIODICIDADE: N/A |
| [DEA001]  \Trabalho | EXECUTANTE: USR002  ORIGEM DOS DADOS: REC002  TIPO: Incremental, sem apagamento no destino.  TIPO DE VERIFICAÇÃO: Visual (abertura aleatória de 2 ficheiros (e.g. Excel, Word, etc.) para análise da atualidade de conteúdo). | UTILIZADOR: USR002  PERIODICIDADE: Todas as terças e quintas-feiras |
| [DEA002]  \Trabalho | EXECUTANTE: USR003  ORIGEM DOS DADOS:REC002  TIPO: Incremental, sem apagamento no destino.  TIPO DE VERIFICAÇÃO: Visual (abertura aleatória de 2 ficheiros (e.g. Excel, Word, etc.) para análise da atualidade de conteúdo). | UTILIZADOR: USR003  PERIODICIDADE: Todas as segundas, quartas e sextas-feiras |

* 1. SUPORTE E CONTRATOS
     1. Parcerias

Nesta secção apresentam-se as parceiras existentes por dispositivo ou aplicação. A cada parceria é indicada também o tipo de parceria existente. Utilizam-se os seguintes tipos de parceira: i) garantia – que representa uma parceria com o fabricante da aplicação ou dispositivo; ii) suporte protocolado – para os dispositivos ou aplicações em que o suporte está abrangido por um contrato formal ou acordo informal (i.e. não existem impedimentos comerciais ou financeiros prévios para acesso ao suporte); iii) suporte não protocolado – em que o suporte está sujeito a impedimentos comerciais ou financeiros prévios (e.g. pagamento antecipado de um valor a orçamentar); e iv) suporte inativo – em que existem impedimentos definitivos que impossibilitam o acesso ao suporte (e.g. parceiro de suporte encerrou atividade).

Uma parceria não protocolada ou inativa pode representar uma vulnerabilidade para a ORGANIZAÇÃO. O facto de existirem impedimentos, temporários ou definitivos, de acesso ao suporte, pode por em causa a segurança, privacidade, integridade e disponibilidade dos dados e do SISTEMA.

|  |  |  |
| --- | --- | --- |
| DISPOSITIVO OU APLICAÇÃO | PARCEIRO | TIPO PARCERIA |
| ESS001 |  |  |
|  | PAR002 | Suporte protocolado |
| DRD001 |  |  |
|  | PAR001 | Suporte protocolado |
| DRD002 |  |  |
|  | PAR001 | Suporte protocolado |
| REE001 |  |  |
|  | PAR001 | Suporte protocolado |
| SVR001 |  |  |
|  | PAR001 | Suporte protocolado |
| CPF001 |  |  |
|  | PAR001 | Suporte protocolado |
| CPF002 |  |  |
|  | PAR001 | Suporte protocolado |
| CPF003 |  |  |
|  | PAR001 | Suporte protocolado |
| CPP001 |  |  |
|  | PAR001 | Suporte protocolado |
| IMP001 |  |  |
|  | PAR001 | Suporte protocolado |
| IMP002 |  |  |
|  | PAR001 | Suporte protocolado |
|  | PAR004 | Garantia |
| APS001 |  |  |
|  | PAR001 | Suporte protocolado |
| APP001 |  |  |
|  | PAR001 | Suporte protocolado |
| APP002 |  |  |
|  | PAR001 | Suporte protocolado |
| APP003 |  |  |
|  | PAR001 | Suporte protocolado |
| APP004 |  |  |
|  | PAR001 | Suporte protocolado |
| APP005 |  |  |
|  | PAR001 | Suporte protocolado |
| APP006 |  |  |
|  | PAR003 | Suporte protocolado |
| APP007 |  |  |
|  | PAR001 | Suporte protocolado |

* + 1. Renovação de subscrições e contratos

Nesta secção resumem-se os licenciamentos ou contratos com necessidade de renovação periódica (e.g. antivírus, Microsoft Office 365, garantias ou contratos de suporte a servidores, contratos de suporte a UPS, etc.). O AUDITOR lembra em ata a cada auditoria as renovações de subscrições e contratos a renovar para o próximo SPRINT. Aqui deve constar informação acerca da aplicação/dispositivo e a próxima renovação.

|  |  |
| --- | --- |
| DISPOSITIVO OU APLICAÇÃO | RENOVAÇÃO |
| APS001 | 2017-12-25 |
| APP003 | 2018-04-17 |

1. VULNERABILIDADES E AUDITORIAS

Nesta secção são apresentadas as vulnerabilidades identificadas que podem ter impacto no SISTEMA, e a documentação relacionada com as auditorias internas e externas.

Além das vulnerabilidades diretamente relacionadas com a segurança, são também indicadas as operacionais (i.e. as que podem condicionar a produtividade ou até operacionalidade da ORGANIZAÇÃO). Para cada vulnerabilidade são propostas medidas corretivas com o objetivo de a resolver de forma temporária ou definitiva.

Para cada auditoria realizada (interna ou externa) são aqui arquivados documentos diversos (e.g. atas de encerramento ou relatórios) resultantes da mesma.

* 1. VULNERABILIDADES IDENTIFICADAS

A manutenção do conteúdo dos quadros desta secção é feita a cada auditoria. As novas vulnerabilidades detetadas devem ser inseridas e as já existentes ainda pendentes devem ser revistas com o objetivo de validar se já foram ou não resolvidas. Quando uma vulnerabilidade é resolvida o seu estado deve ser atualizado. Caso a solução implementada impacte o Cronograma, Caracterização do SISTEMA ou PSD, essas alterações devem ser refletidas nos módulos e quadros respetivos (e.g. implementação de uma nova versão de *firmware* num dispositivo, instalação de uma nova aplicação de segurança, etc.).

Com o objetivo de promover a eficácia do processo de auditoria, a deteção de vulnerabilidades é feita com base em listas de vulnerabilidades e exposições comuns (ver anexo 4).

Nesta secção são enumeradas as vulnerabilidades identificadas: i) ainda não corrigidas e que podem pôr em causa o PSD definido; e ii) as vulnerabilidades corrigidas que são apenas mantidas para registo futuro do histórico. O impacto de cada vulnerabilidade é definido pelo AUDITOR, utilizando o bom senso na avaliação do risco que cada uma pode representar para o SISTEMA.

As vulnerabilidades podem ser categorizadas em dois níveis de impacto:

* SEVERO – que indica a necessidade de encontrar formas de resolver ou mitigar de forma imediata;
* CRÍTICO – que indica a necessidade de resolução logo que possível.

A coluna ESTADO dos quadros seguintes pode assumir um dos seguintes valores: i) Pendente; ii) Pendente, com medida temporária (mitigação); iii) Implementada; e iv) obsoleta ou sem significado (para quando uma vulnerabilidade deixou de fazer sentido ou deixou de existir a necessidade de correção).

Uma vulnerabilidade apenas pode ser classificada num dos quadros seguintes: i) segurança; ii) operacionais; e iii) assumidas.

* + 1. Segurança

O quadro seguinte resume as vulnerabilidades identificadas e classifica-as quanto ao seu possível impacto no SISTEMA. O campo DATA identifica a data de identificação da vulnerabilidade.

|  |  |  |
| --- | --- | --- |
| ID | VULNERABILIDADE E MEDIDA CORRETIVA | ESTADO |
| V000001  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000002  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: N/A.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000003  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000004  DATA:  2018-05-04  IMPACTO:  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  DISPOSITIVOS: N/A.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000005  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: N/A  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000006  DATA:  2018-05-04  IMPACTO:  Critico | 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.  DISPOSITIVOS: N/A  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000007  DATA:  2018-05-04  IMPACTO:  Severo | VULNERABILIDADE:  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  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000008  DATA:  2018-05-04  IMPACTO:  Severo | VULNERABILIDADE:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000009  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000010  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V0000011  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V0000012  DATA:  2018-05-04  IMPACTO:  Critico | VULNERABILIDADE:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000013  DATA:  2018-05-04  IMPACTO:  Critico | VULNERABILIDADE:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000014  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001; CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000015  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001; CPF002; CPF003.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V0000016  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001; CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V0000017  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001; CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000018  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001; CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000019  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000020  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001; CPF002; CPF003.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000021  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF002; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000022  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001; CPF001; CPF002; CPF003.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000023  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001; CPF001; CPF002; CPF003.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000024  DATA:  2018-05-04  IMPACTO:  Critico | 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.  DISPOSITIVOS: SVR001; CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000025  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001/APP004.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000026  DATA:  2018-05-04  IMPACTO:  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 (Cert. Oracle America, Inc. 07/02/2016).  DISPOSITIVOS: CPF001; CPF003.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000027  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001; CPF002; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000028  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000029  DATA:  2018-05-04  IMPACTO:  Crítico | 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.  DISPOSITIVOS: CPF002.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000030  DATA:  2018-05-04  IMPACTO:  Crítico | 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.  DISPOSITIVOS: CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000031  DATA:  2018-05-04  IMPACTO:  Crítico | 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.  DISPOSITIVOS: CPF001; CPF002; CPF003; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000032  DATA:  2018-05-04  IMPACTO:  Crítico | 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.  DISPOSITIVOS: SVR001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000033  DATA:  2018-05-04  IMPACTO:  Crítico | 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.  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000034  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: N/A.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000035  DATA:  2018-05-04  IMPACTO:  Critico | 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.  DISPOSITIVOS: CPF001; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000036  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001; CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000037  DATA:  2018-05-04  IMPACTO:  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).  DISPOSITIVOS: CPF002, CPP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000038  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001; CPF002.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000039  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: REE001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
|  | 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.  DISPOSITIVOS: DEA001; DEA002.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000040  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: DEA001; DEA002; REC001 e REC002.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000041  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: N/A.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000042  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: IMP002.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000043  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: N/A.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000044  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |

* + 1. Operacionais

O quadro seguinte apresenta as vulnerabilidades identificadas não relacionadas diretamente com a segurança e privacidade, mas que podem vir a representar constrangimentos à disponibilidade ou integridade dos dados (e.g. uma NAS antiga que aparenta estar em fim de vida; uma aplicação instalada num SO antigo e que não é possível instalar num SO mais recente;), ou podem por em causa a operabilidade da ORGANIZAÇÃO influenciando negativamente a sua normal atividade (e.g. máquina de corte sem parceiro de suporte; um produto utilizado sem licença apropriada que pode inviabilizar o funcionamento do equipamento em resultado de uma apreensão por uma entidade fiscalizadora).

|  |  |  |
| --- | --- | --- |
| ID | VULNERABILIDADE E MEDIDA CORRETIVA | ESTADO |
| V000045  DATA:  2018-05-04  IMPACTO:  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.  DISPOSITIVOS: SVR001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |

* + 1. Assumidas

Esta secção identifica vulnerabilidades de segurança assumidas como necessárias de existir pelo RESPONSÁVEL PELO TRATAMENTO de dados. Ainda assim, devem ser indicadas as medidas para diminuir o risco sobre o sistema (e.g. acesso externo é uma vulnerabilidade mas é utilizado um protocolo para encriptação de dados na internet; a necessidade de existir cópias de segurança desligadas e transportadas para fora da empresa por causa de incêndios ou assaltos, mas encriptadas; necessário utilizar *pendrive* para levar trabalhos para máquinas de produção, mas estão identificadas; utilização de *wireless* corporativo atendendo a existência de dispositivos de recolha móveis, mas com chave desconhecida e complexa; utilização de um portátil fora da empresa (e.g. vendedor externo); é necessário utilizar uma *pendrive* para passar desenhos para a determinada máquina de produção; etc.).

|  |  |  |  |
| --- | --- | --- | --- |
| ID | DESCRIÇÃO | ASSUNÇÃO | PRÓXIMA REAVALIAÇÃO |
| (vazio) | (vazio) | (vazio) | (vazio) |

* 1. AUDITORIAS INTERNAS

Nesta secção são documentadas as auditorias de revisão. É utilizado o termo SPRINT para designar o tempo decorrido entre duas auditorias seguidas.

As auditorias de revisão têm por objetivo acompanhar a evolução do SISTEMA ao longo do tempo, nomeadamente através do relato contínuo das vulnerabilidades identificadas, medidas corretivas propostas e recomendações. Funcionam como pontos de controlo promotores da privacidade e segurança, e da integridade e disponibilidade dos dados e do SISTEMA. Pretende-se demonstrar a preocupação da ORGANIZAÇÃO para com os dados pessoais, aumentar iterativamente o nível de conformidade do SISTEMA com o RGPD, e facilitar as possíveis auditorias inspetivas.

Cada auditoria inicia com a verificação de conformidade e arquivo dos registos produzidos durante o SPRINT em encerramento, e do cumprimento dos compromissos definidos no calendário para esse período. De seguida o AUDITOR verifica a entrada e saída de UTILIZADORES do SISTEMA, com o objetivo de detetar necessidades de reconfiguração de permissões ou de formação. Depois efetua o levantamento de alterações ocorridas no SISTEMA e que podem ferir ou por em causa o PSD definido. Por fim faz um levantamento dos compromissos a atender para o próximo SPRINT e elabora a ata de encerramento a ser assinada pelo RESPONSÁVEL PELO TRATAMENTO.

* + 1. Diagnóstico inicial

Nesta secção é arquivada a ata e restante documentação produzida durante o diagnóstico inicial.

* + 1. Auditorias de Revisão

Nesta secção são arquivadas as atas relacionadas com cada auditoria de revisão e é através destas que o RESPONSÁVEL PELO TRATAMENTO toma conhecimento de informações de relevo para a segurança e disponibilidade do SISTEMA. Pretende-se que as atas demonstrem a preocupação com as questões de segurança e da evolução das medidas conducentes à conformidade com o RGPD tomadas ao longo do tempo.

A ata de encerramento deve:

* + - * 1. Referenciar as alterações de estado ocorridas na secção de vulnerabilidades identificadas e medidas corretivas, frisando as não resolvidas e o impacto que podem significar ao nível da segurança ou disponibilidade do SISTEMA;
        2. Referenciar as novas vulnerabilidades identificadas com referência às medidas corretivas sugeridas, frisando o impacto que podem ter no contexto do PSD definido;
        3. Avaliar o cumprimento dos compromissos do SPRINT anteriores, e mencionar os compromissos previstos para o próximo SPRINT salientando a importância que têm para a segurança ou disponibilidade do SISTEMA;
        4. Se necessário, atribuir ou rever responsabilidades de tarefas aos UTILIZADORES;
        5. Mencionar os IVD, a informação acerca da decisão do RESPONSÁVEL PELO TRATAMENTO de comunicar à AUTORIDADE DE CONTROLO e aos TITULARES DOS DADOS, e as medidas propostas para evitar que se repita o incidente em causa;
        6. Resumir as autorizações ou revisão de alterações com impacto no PSD; e
        7. Agendamento da próxima auditoria de revisão.

Cada ata deve terminar indicando a apreciação do RESPONSÁVEL PELO TRATAMENTO de dados, caso este pretenda fazê-lo.

* 1. AUDITORIAS EXTERNAS

Esta secção contém a documentação relacionada com auditorias externas, tais como da AUTORIDADE DE CONTROLO e de outras entidades.

* + 1. Autoridade de controlo

Nesta secção devem constar os relatórios de inspeções realizadas pela AUTORIDADE DE CONTROLO.

* + 1. Outras entidades

Nesta secção devem existir os relatórios de inspeções realizadas por outras entidades externas.

1. REGISTOS

Neste módulo são arquivados os registos produzidos pelos UTILIZADORES e AUDITOR no decurso das suas auditorias de revisão. São também registados os incidentes nomeadamente os de violação de dados ocorridos no SISTEMA. É utilizado o termo SPRINT para designar o tempo decorrido entre duas auditorias seguidas.

* 1. REGISTOS DE UTILIZADOR

Nesta secção constam os registos criados por UTILIZADORES durante o último SPRINT.

* + 1. Redundância

Nesta subsecção constam os registos relacionados com a redundância elétrica, de servidores e de discos.

* + - 1. Redundância elétrica

Nesta subsecção constam os registos relacionados com a redundância elétrica.

* + - 1. Redundância de servidores

Nesta subsecção constam os registos relacionados com a redundância de servidores.

* + - 1. Redundância de discos

Nesta subsecção constam os registos relacionados com a redundância de discos.

* + 1. Cópias de segurança

Nesta subsecção constam os registos relacionados com a verificação de execução de cópias de segurança, e validação de conteúdo de cópias de segurança (se aplicável).

* + - 1. Verificação de cópias de segurança

Nesta subsecção constam os registos relacionados com a verificação de cópias de segurança.

* + - 1. Validação de conteúdo de cópias de segurança

Nesta subsecção constam os registos relacionados com a validação de conteúdo das cópias de segurança.

* + 1. Outros

Nesta subsecção constam os registos relacionados com o registo de intervenções técnicas e registos de formação prestada aos UTILIZADORES relacionada com o SISTEMA.

* + - 1. Registos de intervenções técnicas

Nesta subsecção constam os registos relacionados com as intervenções técnicas.

* + - 1. Registos de formação

Nesta subsecção constam os registos relacionados com formação de UTILIZADORES.

* + - 1. Outros

Nesta subsecção constam outros registos relacionados com o SISTEMA.

* 1. REGISTOS DO AUDITOR

Nesta secção constam os registos criados ou utilizados pelo próprio AUDITOR ao longo das auditorias.

* + 1. Computadores, servidores ou equivalentes

Nesta subsecção encontram-se os registos utilizados para a recolha ou alteração de informação relativa a computadores, servidores ou equivalentes.

* + - 1. SVR001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe

* + - 1. CPF001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. CPF002

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. CPF003

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. CPP001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + 1. Equipamentos de rede

Nesta subsecção encontram-se os registos utilizados para a recolha ou alteração de informação relativa a equipamentos de rede.

* + - 1. ESS001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. DRD001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. DRD002

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + 1. Recursos de rede

Nesta subsecção encontram-se os registos utilizados para a recolha ou alteração de informação relativa a recursos de rede.

* + - 1. REC001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. REC002

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. REC003

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + 1. DEA

Nesta subsecção encontram-se os registos utilizados para a recolha ou alteração de informação relativa a DAEs.

* + - 1. DEA001

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + - 1. DEA002

Nesta subsecção encontram-se os registos relacionados com o dispositivo em epígrafe.

* + 1. Outros Dispositivos

Nesta secção encontram-se os registos relacionados com outros dispositivo existentes no SISTEMA.

* + 1. Utilizadores

Nesta subsecção encontram-se os registos utilizados para a recolha ou alteração de informação relativa a utilizadores.

* + - 1. USR001

Nesta subsecção encontram-se os registos relacionados com o utilizador em epígrafe.

* + - 1. USR002

Nesta subsecção encontram-se os registos relacionados com o utilizador em epígrafe.

* + - 1. USR003

Nesta subsecção encontram-se os registos relacionados com o utilizador em epígrafe.

* + - 1. [PAR001]

Nesta subsecção encontram-se os registos relacionados com o utilizador em epígrafe.

* + 1. Outros registos

Nesta subsecção encontram-se os registos utilizados para a recolha ou alteração de informação relativa a outros registos.

* + - 1. Registos de auditoria

Nesta subsecção encontram-se os registos relacionados com a conformidade de registos e da própria auditoria.

* 1. REGISTOS DE INCIDENTES
     1. Violação de dados

O registo de incidentes de violação de dados é obrigatório, e deve resumir e documentar todos os incidentes ocorridos com os dados tratados pelo RESPONSÁVEL PELO TRATAMENTO. Este registo não dispensa a comunicação à AUTORIDADE DE CONTROLO e aos TITULARES DOS DADOS nos casos em que se aplique o RGPD.

Nesta secção serão arquivados todos os registos de violação de dados relacionados com o SISTEMA ocorridos.

* + 1. Outros incidentes

Nesta secção serão arquivados registos de outros incidentes relacionados com o SISTEMA.

1. ANEXOS DA ORGANIZAÇÃO
   1. DOCUMENTAÇÃO
      1. Regulamento do SISTEMA

Nesta secção pode ser consultado o Regulamento do SISTEMA em vigor na ORGANIZAÇÃO. Para que seja válido deve estar assinado pelo RESPONSÁVEL PELO TRATAMENTO. Todos os UTILIZADORES devem também assinar indicando que tomaram conhecimento.

* + 1. Política de Segurança e Confidencialidade

Nesta secção pode ser consultada a Política de Segurança e Confidencialidade da ORGANIZAÇÃO.

* 1. COMPROVATIVOS DE COMPRA, RENOVAÇÕES E REVISÕES

Nesta secção devem constar os comprovativos de: i) compra ou licenciamento de dispositivos ou aplicações do SISTEMA (e.g. faturas, licenças, certificados, etc.); ii) renovações das subscrições (e.g. renovações das aplicações de segurança); iii) contratos e respetivas renovações se aplicável (e.g. extensões de garantia, contratos de assistência ou prolongação de garantia); iv) revisões técnicas dos dispositivos sujeitos; e v) restante documentação de relevo para o SISTEMA ou que comprove a execução de tarefas controladas pelo auditor no Calendário.

A estrutura desta secção é orientada ao dispositivo ou aplicação. Cada subsecção representa apenas um dispositivo ou aplicação individualmente. Se for necessário, podem ser utilizadas micas para facilitar o processo de arquivo.

* + 1. SVR001

Nesta subsecção encontra-se a documentação relacionada com o dispositivo em epígrafe.

* + 1. CPF001

Nesta subsecção encontra-se a documentação relacionada com o dispositivo em epígrafe.

* + 1. CPF002

Nesta subsecção encontra-se a documentação relacionada com o dispositivo em epígrafe.

* + 1. CPF003

Nesta subsecção encontra-se a documentação relacionada com o dispositivo em epígrafe.

* + 1. CPP001

Nesta subsecção encontra-se a documentação relacionada com o dispositivo em epígrafe.

* + 1. REE001

Nesta subsecção encontra-se a documentação relacionada com o dispositivo em epígrafe.

* + 1. APS001

Nesta subsecção encontra-se a documentação relacionada com a aplicação em epígrafe.

* + 1. APP003

Nesta subsecção encontra-se a documentação relacionada com a aplicação em epígrafe.

* + 1. Outros

Nesta subsecção encontra-se a documentação relacionada com outros dispositivos e aplicação existentes no SISTEMA.

* 1. CREDENCIAIS E FICHEIROS ORIGINAIS

Esta secção é composta por uma mica com um envelope contendo as credenciais de SISTEMA e uma *pendrive* com os ficheiros originais para facilitar a edição do conteúdo deste DOSSIER. Essa *pendrive* não consta da Caracterização do SISTEMA nem do PSD porque é apenas utilizada para este fim e para evitar entropia na análise do DSPI. Apenas contém ficheiros relacionados com o DSPI ou cumprimento do Regulamento do SISTEMA. O seu conteúdo está encriptado, e não pode ser utilizada para outros fins que não os atrás descritos.

1. ANEXOS DE AUDITORIA

Este módulo contém os anexos de suporte às auditorias.

* 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:  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:  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:  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:  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:  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:  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. |

* 1. MATRIZES
     1. Utilizador

Nesta secção devem ser arquivadas as matrizes dos diferentes formulários de registo utilizados na ORGANIZAÇÃO pelo UTILIZADOR (i.e. registos e formulários vazios). Os registos a serem preenchidos pelos UTILIZADORES devem ser designados em ata pelo RESPONSÁVEL PELO TRATAMENTO de dados.

* + - 1. Redundância
         1. Registo de verificação da redundância elétrica

Este anexo deve conter o *template* de registo de verificação de funcionamento da redundância elétrica de um determinado equipamento.

**REGISTO DE VERIFICAÇÃO DA REDUNDÂNCIA ELÉTRICA**

Neste mapa devem ser registadas todas as verificações de redundância elétrica efetuadas ao dispositivo REE abaixo identificado.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO:  REE:  PERIODICIDADE DE VERIFICAÇÃO: | INÍCIO:  FIM:  MOD: DSPI-RVRE-V1.0A |

No quadro seguinte devem ser registados os momentos de verificação. Cada linha representa uma verificação efetuada. Caso responda afirmativamente à questão da coluna 3, deve informar de imediato o administrador do sistema, o técnico responsável pela infraestrutura e o RESPONSÁVEL PELO TRATAMENTO de dados. Esta informação deve ser prestada oralmente e também por escrito via e-mail.

|  |  |  |
| --- | --- | --- |
| DATA | RELATÓRIO BREVE | IMPACTO NO SISTEMA? 1) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1) O estado pode ter impacto na segurança ou disponibilidade do SISTEMA?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + - * 1. Registo de verificação da redundância de servidores

Este anexo deve conter o *template* de registo de verificação de funcionamento da redundância de servidores de um determinado *datacenter* ou servidor de *backup*.

**REGISTO DE VERIFICAÇÃO DA REDUNDÂNCIA DE SERVIDORES**

Neste mapa devem ser registadas todas as verificações de redundância de servidores efetuadas ao equipamento abaixo identificado.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO:  DISPOSITIVO:  PERIODICIDADE DE VERIFICAÇÃO: | INÍCIO:  FIM:  MOD: DSPI-RVRS-V1.0A |

No quadro seguinte devem ser registados os momentos de verificação. Cada linha representa uma verificação efetuada. Caso responda afirmativamente à questão da coluna 3, deve informar de imediato o administrador do sistema, o técnico responsável pela infraestrutura e o RESPONSÁVEL PELO TRATAMENTO de dados. Esta informação deve ser prestada oralmente e também por escrito via e-mail.

|  |  |  |
| --- | --- | --- |
| DATA | RELATÓRIO BREVE | IMPACTO NO SISTEMA? 1) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1) O estado pode ter impacto na segurança ou disponibilidade do SISTEMA?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + - * 1. Registo de verificação da redundância de discos

Este anexo deve conter o *template* de registo de verificação de funcionamento da redundância de discos (RAID) de um determinado servidor ou servidor de *backup*.

**REGISTO DE VERIFICAÇÃO DA REDUNDÂNCIA DE DISCOS**

Neste mapa devem ser registadas todas as verificações de redundância de discos efetuadas ao equipamento abaixo identificado.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO:  BAK:  PERIODICIDADE DE VERIFICAÇÃO: | INÍCIO:  FIM:  MOD: DSPI-RVRD-V1.0A |

No quadro seguinte devem ser registados os momentos de verificação. Cada linha representa uma verificação efetuada. Caso responda afirmativamente à questão da coluna 3, deve informar de imediato o administrador do sistema, o técnico responsável pela infraestrutura e o RESPONSÁVEL PELO TRATAMENTO de dados. Esta informação deve ser prestada oralmente e também por escrito via e-mail.

|  |  |  |
| --- | --- | --- |
| DATA | RELATÓRIO BREVE | IMPACTO NO SISTEMA? 1) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1) O estado pode ter impacto na segurança ou disponibilidade do SISTEMA?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + - 1. Cópias de segurança
         1. Registo de verificação de execução de cópias de segurança

Este anexo deve conter o *template* de registo de verificação de execução de cópias de segurança de uma determinada tarefa de cópias de segurança.

**REGISTO DE VERIFICAÇÃO DE EXECUÇÃO DE CÓPIAS DE SEGURANÇA**

Neste mapa deve estar registadas todas as verificações de execução da tarefa de cópias abaixo indicada. Deve existir um registo diferente por cada tarefa de cópias de segurança.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO:  TAREFA:  PERIODICIDADE DE VERIFICAÇÃO: | INÍCIO:  FIM:  MOD: DSPI-RVECS-V1.0A |

No quadro seguinte devem ser registados os momentos de verificação. Cada linha representa uma verificação efetuada. Caso responda afirmativamente à questão da coluna 3, deve informar de imediato o administrador do sistema, o técnico responsável pela infraestrutura e o RESPONSÁVEL PELO TRATAMENTO de dados. Esta informação deve ser prestada oralmente e também por escrito via e-mail.

|  |  |  |
| --- | --- | --- |
| DATA | RELATÓRIO BREVE 1) | IMPACTO NO SISTEMA? 2) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1) Incluir o tipo de verificação executada (e.g. abertura e verificação de conteúdo dos ficheiros e )  
2) O estado pode ter impacto na segurança ou disponibilidade do SISTEMA?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + - * 1. Registo de validação de conteúdo em cópias de segurança (se aplicável)

Este anexo deve conter o *template* de registo de validação de conteúdo de cópias de segurança de uma determinada tarefa de cópias de segurança.

**REGISTO DE VALIDAÇÃO DE CONTEÚDO DE CÓPIAS DE SEGURANÇA**

Neste mapa devem ser registadas todas as validações de conteúdo de cópias de segurança. Deve existir um registo diferente por conteúdo.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO:  TAREFA:  PERIODICIDADE DE VERIFICAÇÃO: | INÍCIO:  FIM:  MOD: DSPI-RVCCS-V1.0A |

No quadro seguinte devem ser registados os momentos de verificação. Cada linha representa uma verificação efetuada. Caso responda afirmativamente à questão da coluna 3, deve informar de imediato o administrador do sistema, o técnico responsável pela infraestrutura e o RESPONSÁVEL PELO TRATAMENTO de dados. Esta informação deve ser prestada oralmente e também por escrito via e-mail.

|  |  |  |
| --- | --- | --- |
| DATA | RELATÓRIO BREVE 1) | IMPACTO NO SISTEMA? 2) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1) Incluir o tipo de validação executada (e.g. reposição da e confirmação de conteúdo)  
2) O estado pode ter impacto na segurança ou disponibilidade do SISTEMA?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + - 1. Outros
         1. Registo de intervenções técnicas

Este anexo deve conter o *template* de registo das intervenções técnicas feitas na ORGANIZAÇÃO.

**REGISTO DE INTERVENÇÕES TÉCNICAS**

Este registo permite documentar as intervenções técnicas ocorridas na ORGANIZAÇÃO. A cada intervenção deve ser preenchida uma linha de registo.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO: | INÍCIO:  FIM:  MOD: DSPI-RIT-V1.0A |

No quadro seguinte devem ser efetuados os registos. Cada linha representa uma intervenção técnica efetuada.

|  |  |  |
| --- | --- | --- |
| INTERVENÇÃO | | IMPACTO |
| DATA:  TÉCNICO: | DISPOSITIVOS E APLICAÇÕES ENVOLVIDAS:  RESUMO BREVE DA INTERVENÇÃO: | CALENDÁRIO: 1)  CARACTERIZAÇÃO DO SISTEMA: 2)  PLANO DE SEGURANÇA E DISPONIBILIDADE: 3) |
| DATA:  TÉCNICO: | DISPOSITIVOS E APLICAÇÕES ENVOLVIDAS:  RESUMO BREVE DA INTERVENÇÃO: | CALENDÁRIO: 1)  CARACTERIZAÇÃO DO SISTEMA: 2)  PLANO DE SEGURANÇA E DISPONIBILIDADE: 3) |
| DATA:  PARCEIRO: | DISPOSITIVOS E APLICAÇÕES ENVOLVIDAS:  RESUMO BREVE DA INTERVENÇÃO: | CALENDÁRIO: 1)  CARACTERIZAÇÃO DO SISTEMA: 2)  PLANO DE SEGURANÇA E DISPONIBILIDADE: 3) |

1) A intervenção impacta o calendário (cronograma) da ORGANIZAÇÃO, porquê?  
2) A intervenção impacta a caracterização do SISTEMA, em que medida?  
3) A intervenção impacta o PSD da ORGANIZAÇÃO, como?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + - * 1. Registo de formação relacionada com o SISTEMA

Este anexo deve conter o *template* de registo da formação relacionada com a segurança, privacidade, integridade e disponibilidade, prestada aos UTILIZADORES do SISTEMA. O registo deve ser orientado à ação de formação e deve ser assinada por todos os UTILIZADORES participantes.

**REGISTO DE FORMAÇÃO RELACIONADA COM O SISTEMA**

Este registo confirma a participação dos UTILIZADORES na ação de formação abaixo identificada. A cada ação de formação deve ser preenchida um destes registos.

O quadro seguinte resume a ordem de atribuição da responsabilidade de preenchimento deste registo.

|  |  |
| --- | --- |
| ATRIBUIÇÃO DA RESPONSABILIDADE DE PREENCHIMENTO | REGISTO |
| ATA:  DATA:  RESPONSÁVEL PELO TRATAMENTO:  UTILIZADOR DESIGNADO: | INÍCIO:  FIM:  MOD: DSPI-RFRS-V1.0A |

O quadro seguinte identifica a ação de formação em que participaram os UTILIZADORES assinantes.

|  |  |
| --- | --- |
| AÇÃO DE FORMAÇÃO | PERIODO DE FORMAÇÃO |
| DATA:  IDENTIFICAÇÃO DA AÇÃO: | INICIO:  FIM: |

Cada UTILIZADOR participante na ação de formação deve assinar o quadro abaixo confirmando a sua presença.

|  |  |
| --- | --- |
| NOME LEGÍVEL | RÚBRICA |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(UTILIZADOR designado)

* + 1. Auditor

Nesta secção podem ser encontrados as matrizes dos registos que podem ser utilizados pelo AUDITOR.

* + - 1. Auditoria
         1. Registo de conformidade dos registos dos UTILIZADORES.

**REGISTO DE CONFORMIDADE DOS REGISTOS DOS UTILIZADORES**

Este registo é utilizado pelo AUDITOR na verificação de conformidade dos registos preenchidos pelos UTILIZADORES.

O quadro seguinte identifica a auditoria e o AUDITOR responsável.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO:  DATA:  AUDITOR: | **INICIO:**  **FIM:**  **MOD:** DSPI-RCRU-V1.0A |

Cada linha do quadro seguinte representa uma verificação de conformidade pelo AUDITOR.

|  |  |
| --- | --- |
| REGISTO | CONFORMIDADE |
| REGISTO: 1)  INICIO:  FIM:  UTILIZADOR: | CONFORME OU NÃO CONFORME [sim, não]:  VULNERABILIDADES:  MEDIDA CORRETIVA: |
| REGISTO: 1)  INICIO:  FIM:  UTILIZADOR: | CONFORME OU NÃO CONFORME [sim, não]:  VULNERABILIDADES:  MEDIDA CORRETIVA: |
| REGISTO: 1)  INICIO:  FIM:  UTILIZADOR: | CONFORME OU NÃO CONFORME [sim, não]:  VULNERABILIDADES:  MEDIDA CORRETIVA: |
| REGISTO: 1)  INICIO:  FIM:  UTILIZADOR: | CONFORME OU NÃO CONFORME [sim, não]:  VULNERABILIDADES:  MEDIDA CORRETIVA: |

1) Indicar o código e nome do registo (e.g. DSPI-RVRE, Registo de Verificação de Redundância Elétrica)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

* + - * 1. Conformidade da auditoria

Este anexo deve ser utilizado para garantir o cumprimento de todas as tarefas do AUDITOR associadas à auditoria e respetivo encerramento.

**REGISTO DE CONTROLO DA AUDITORIA**

Este registo é utilizado para apoiar o controlo das tarefas a desempenhar pelo AUDITOR em cada auditoria.

|  |  |
| --- | --- |
| AUDITORIA | SPRINT EM ENCERRAMENTO |
| NÚMERO:  DATA:  AUDITOR: | **INICIO:**  **FIM:**  **MOD:** DSPI-RCA-V1.0A |

O quadro seguinte contém um conjunto de itens a verificar com o objetivo de garantir a execução de todas as tarefas relacionadas com uma auditoria.

|  |  |
| --- | --- |
| TAREFA | NOTAS |
| INICIO |  |
| Atualizar o módulo Anexos de Auditoria. |  |
| ENTRADA E SAÍDA DE UTILIZADORES |  |
| Avaliar a necessidade de reconfiguração de permissões. |  |
| Assinar Regulamento do SISTEMA (novos UTILIZADORES). |  |
| Avaliar necessidades de formação. |  |
| RESPONSABILIDADES DOS UTILIZADORES |  |
| Atribuir ou rever a atribuição de responsabilidades de registo. |  |
| Recolher registos preenchidos e distribuir registos limpos. |  |
| CALENDÁRIO |  |
| Reconfigurar os compromissos atendidos durante o último SPRINT. |  |
| Resumir os compromissos não atendidos do último SPRINT. | Incluir na ata enfatizando o impacto de não se ter atendido ao compromisso. |
| Levantar os compromissos a atender no próximo SPRINT. | Incluir na ata. |
| Atender aos compromissos do AUDITOR (revisão de autorizações, atribuição de responsabilidades, utilização de *wireless*, etc.). | Incluir em ata as decisões tomadas (e.g. continua a existir a necessidade de *wireless*…). |
| VULNERABILIDADES |  |
| Avaliar a correção de vulnerabilidades pendentes e atualizar o respetivo estado se aplicável. |  |
| Avaliar o impacto da não correção das vulnerabilidades não resolvidas. | Incluir na ata de encerramento o impacto das mais graves. |
| Levantar novas vulnerabilidades do SISTEMA. | Incluir na ata de encerramento o resumo das mais importantes. |
| INCIDENTES |  |
| Avaliar os IVD ocorridos e as decisões de comunicação assumidas pelo RESPONSÁVEL PELO TRATAMENTO. | Incluir na ata resumo das decisões de comunicação. |
| Avaliar a implementação de medidas adicionais de controlo. | Incluir um resumo em ata. |
| OUTROS |  |
| Avaliar conformidade e arquivar dos registos de UTILIZADORES. |  |
| Avaliar as alterações ocorridas que possam impactar a Caracterização do SISTEMA e o PSD. |  |
| FIM |  |
| Agendar da próxima Auditoria de Revisão. |  |
| Encriptar *pendrive* com conteúdo das auditorias. |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

* + - 1. Computadores, servidores ou equivalentes
         1. Registo de computador, servidor ou equivalente

Este anexo contém o formulário a preencher quando ocorre uma entrada ou alteração de um computador, servidor ou equivalente no SISTEMA.

**REGISTO DE COMPUTADOR, SERVIDOR OU EQUIVALENTE**

Este registo é utilizado pelo AUDITOR registar a entrada ou alteração de um computador, servidor ou equivalente no SISTEMA.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do dispositivo no SISTEMA. | **Modelo** | Modelo do dispositivo. |
| Data | Data do registo. | **Processador** | Descrição do processador do dispositivo. |
| Tipo de equipamento | Tipo de dispositivo a registar | **Memória principal** | Tamanho total da memória principal do dispositivo. |
| Data de compra | Data de aquisição do dispositivo pela ORGANIZAÇÃO. | **Memória secundária** | Tamanho total da memória secundária do dispositivo. |
| Inativo | Se o dispositivo ainda se encontra em uso pela ORGANIZAÇÃO. | **SO** | Sistema operativo instalado no dispositivo. |
| Data de inatividade | Se o dispositivo estiver fora de uso, registar data de inatividade. | **Endereço IP** | Endereço IP do dispositivo. |
| Descrição | Descrição do dispositivo. | **Versão de *firmware* da BIOS** | Versão de *firmware* da BIOS do dispositivo. |
| Função | Função do dispositivo da ORGANIZAÇÃO. | **Localização** | Localização do dispositivo na ORGANIZAÇÃO. |
| Marca | Marca do dispositivo. |  |  |
| SUPORTE TÉCNICO | | | |
| Id | Identificador do parceiro responsável pelo suporte ou fabricante do dispositivo no SISTEMA. | **Periodicidade** | Periodicidade de atualização de contratos de suporte. |
| Tipo de PAR | Se é parceiro ou fabricante. | **Antecedência** | Com que antecedência se deve proceder à renovação do contrato. |
| Inativo | Se o suporte ao dispositivo ainda se encontra ativo no SISTEMA. | **Contactos** | Contactos para pedido de suporte. |
| Data de inatividade | Se o suporte estiver inativo, registar a data de inatividade. | **Horário** | Horário disponível para contacto. |
| Designação | Designação do parceiro/fabricante. | **Observações** | Observações (e.g. motivo da inatividade do suporte) |
| Tipo de parceria | Descrição do processador do dispositivo. |  |  |
| APLICAÇÕES DE SEGURANÇA | | | |
| Id | Identificador da aplicação de segurança no SISTEMA. | **Versão** | Versão da aplicação instalada. |
| Tipo de aplicação | Tipo de aplicação. | **Data de aquisição de licença** | Data da última aquisição da licença para uso da aplicação. |
| Suporte | Identificador do parceiro/fabricante que fornece suporte à aplicação no SISTEMA. | **Periodicidade** | Periodicidade de renovação da aplicação. |
| Inativo | Se a aplicação ainda está ativa no dispositivo. | **Antecedência** | Com que antecedência se deve proceder à renovação. |
| Data de inatividade | Se a aplicação estiver inativa, registar a data de inatividade. | **Regras** | Descrever as barreiras ou regras de exceção de acesso ao equipamento. |
| Descrição | Descrição da aplicação. | **Motivo de inativação** | No caso de a aplicação for inativada registar o motivo. |
| RECURSOS DE REDE | | | |
| Id | Identificador do recurso disponibilizado pelo dispositivo no sistema. | **Partilha** | Descrição da partilha. |
| Inativo | Se o recurso ainda se encontra ativo, ou seja, se ainda é partilhado pelo dispositivo. | **Descrição do conteúdo** | Descrição do conteúdo da partilha. |
| Data de inatividade | Se o recurso estiver inativo, registar a data de inatividade. | **Justificação** | Justificação da existência do recurso. |
| Tipo de recurso | Tipo de recurso disponibilizado pelo dispositivo (e.g pasta partilhada) | **Motivo de inativação** | No caso de a aplicação for inativada registar o motivo. |
| UTILIZADORES | | | |
| Id | Identificador do UTILIZADOR autorizado a operar no equipamento. | **Perfil do UTILIZADOR** | O perfil atribuído ao UTILIZADOR para operar no dispositivo. |
| Acesso externo | Se o UTILIZADOR tem permissão para acesso remoto ao equipamento. | **Descrição do perfil** | Descrição do perfil atribuído. |
| Inativo | Se o UTILIZADOR foi inativado. | **Tipo de acesso externo** | Se tem autorização de acesso externo, indicar o tipo de acesso. |
| Data de inatividade | Se a aplicação estiver inativa, registar a data de inatividade. | **Justificação** | Justificar a permissão de acesso externo ao dispositivo. |
| Nome | Nome do utilizador. |  |  |

Nos quadros seguintes deve ser registado o dispositivo, juntamente com toda a informação a si relacionada.

|  |  |  |
| --- | --- | --- |
| **DADOS GERAIS** | | |
| ID: (vazio)  DATA: (vazio) | TIPO DE EQUIPAMENTO:  COMPUTADOR  Portátil  SERVIDOR  NAS  Backup | DATA COMPRA: (vazio)  INATIVO DATA DE INATIVIDADE: (vazio) |
| DESCRIÇÃO: (vazio) | | |
| FUNÇÃO: (vazio) | | |
| MARCA: (vazio) | | |
| MODELO: (vazio) | | |
| PROCESSADOR: (vazio) | | |
| MEMÓRIA PRINCIPAL: (vazio) | | |
| MEMÓRIA SECUNDÁRIA: (vazio) | | |
| SO: (vazio) | | |
| ENDEREÇO IP: (vazio) | | |
| LOCALIZAÇÃO: (vazio) | | |

|  |  |  |
| --- | --- | --- |
| **SUPORTE TÉCNICO** | | |
| ID: (vazio) | TIPO DE PAR:  PARCEIRO  FABRICANTE | INATIVO DATA DE INATIVIDADE: (vazio) |
| NOME: (vazio) | | |
| TIPO DE PARCERIA: (vazio) | | |
| PERIODICIDADE: (vazio) | | |
| ANTECEDÊNCIA: (vazio) | | |
| CONTACTOS: (vazio) | | |
| HORÁRIO: (vazio) | | |
| OBSERVAÇÕES: (vazio) | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **APLICAÇÕES** | | | | | | | |
| ID: (vazio) | | TIPO DE APLICAÇÃO:  SEGURANÇA  OUTRA  SO  PRODUTIVIDADE  OPERACIONAIS | | SUPORTE: (vazio)  INATIVO DATA DE INATIVIDADE: (vazio) | | | |
| DESCRIÇÃO: (vazio) | | | | | | | |
| VERSÃO: (vazio) | | | | | | | |
| DATA DA AQUISIÇÃO DE LICENÇA: (vazio) | | | | | | | |
| PERIODICIDADE: (vazio) | | | | | | | |
| ANTECEDÊNCIA: (vazio) | | | | | | | |
| REGRAS: | | | | | | |  |
|  | DESCRIÇÃO | | REGRA/BARREIRA | | ESTADO | DATA VERIFICAÇÃO |
|  | |  | |  |  |
|  | |  | |  |  |
|  | |  | |  |  |
| MOTIVO INATIVAÇÃO: (vazio) | | | | | | | |

|  |  |
| --- | --- |
| **RECURSOS DE REDE** | |
| ID: (vazio) | INATIVO DATA DE INATIVIDADE: (vazio) |
| TIPO: (vazio) | |
| PARTILHA: (vazio) | |
| DESCRIÇÃO DE CONTEÚDO: (vazio) | |
| CREDENCIAIS: (vazio) | |
| JUSTIFICAÇÃO: (vazio) | |
| MOTIVO INATIVAÇÃO: (vazio) | |

|  |  |  |
| --- | --- | --- |
| **UTILIZADORES** | | |
| ID: (vazio) | ACESSO EXTERNO | INATIVO DATA DE INATIVIDADE: (vazio) |
| NOME: (vazio) | | |
| PERFIL: (vazio) | | |
| DESCRIÇÃO PERFIL: (vazio) | | |
| TIPO DE ACESSO EXTERNO: (vazio) | | |
| JUSTIFICAÇÃO PARA ACESSO EXTERNO: (vazio) | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte pode ser consultado o impacto que o preenchimento do DSPI-RCSE pode ter no DSPI.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Rosto do Dossier | |
| Calendário / compromissos | Inserir registo de compromisso. |
| Calendário / cronograma | Registar compromisso no cronograma. |
| DSPI / Caracterização do SISTEMA | |
| Suporte técnico / (todos) | Inserir ou remover registo de parceiro. |
| Infraestrutura /segmento / diagrama | Alterar diagrama se necessário |
| Infraestrutura /segmento / servidores ou equivalentes ou dispositivos de backup ou computadores fixos ou computadores portáteis. | Inserir ou alterar registo. |
| Aplicações de segurança / (todos) | Inserir ou remover registo de uma aplicação de segurança na respetiva subseção de acordo com o nível. |
| Outras aplicações / (todos) | Inserir ou remover registo de uma aplicação de segurança na respetiva subseção de acordo com o tipo de aplicação. Registar o dispositivo no ponto |
| Outras aplicações / aplicações por dispositivo. | Registar as aplicações que estão instaladas no dispositivo. |
| Recursos de rede / (todos) | Registar ou remover recursos de rede disponibilizados pelo dispositivo. |
| UTILIZADORES / Perfis | Registar permissões do UTILIZADOR (ficha de utilizador). |
| DSPI / Plano de Segurança e Disponibilidade | |
| Controlo de acesso à infraestrutura / barreiras de acesso / SO | Atualizar se necessário. |
| Controlo de acesso à infraestrutura / exceções de acesso / rede local com fios; rede local sem fios; SO | Atualizar se necessário. |
| Controlo de acesso à infraestrutura / acessos externos / autorizações | Atualizar se necessário. |
| *Malware* e atualizações de segurança / proteções de *malware* de SO | Atualizar se necessário. |
| *Malware* e atualizações de segurança / atualizações de segurança de outras aplicações e SO | Atualizar se necessário. |
| *Malware* e atualizações de segurança / atualizações de *firware* | Atualizar se necessário. |
| OUTROS | |
| Registo de utilizadores | Se houver alguma alteração a nível de permissões no dispositivo, ou se o UTILIZADOR ainda não tiver registo, alterar ou preencher um DSPI-RU |
| Inatividade do dispositivo | Se o dispositivo for retirado do SISTEMA preencher um DSPI-RSCSE |

* + - * 1. Registo de saída de computadores, servidor ou equivalente

Este anexo contém o formulário a preencher quando ocorre a saída de um servidor do SISTEMA.

(garantir que a informação foi apagada de forma definita ou o disco removido do equipamento).

* + - 1. Equipamentos de rede
         1. Registo de router ou distribuidor de rede

Este anexo contém o formulário a preencher quando ocorre a entrada ou alteração de um equipamento de rede (e.g. routers, *appliances*, *firewalls*, *switch*, etc.).

**REGISTO DE ROUTER OU DISTRIBUIDOR DE REDE**

Este registo é utilizado pelo AUDITOR registar a entrada ou alteração de equipamentos de rede no SISTEMA.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do dispositivo no SISTEMA. | Marca | Marca do dispositivo. |
| Data | Data do registo. | **Modelo** | Modelo do dispositivo. |
| Tipo | Tipo de dispositivo a registar | **Versão do *firmware*** | Versão do *firmware* instalado no dispositivo. |
| Data de compra | Data de aquisição do dispositivo pela ORGANIZAÇÃO. | **Endereço IP** | Endereço IP do dispositivo. |
| Inativo | Se o dispositivo ainda se encontra em uso pela ORGANIZAÇÃO. | **Localização** | Localização do dispositivo na ORGANIZAÇÃO. |
| Data de inatividade | Se o dispositivo estiver fora de uso, registar data de inatividade. | **Justificação** | Justificar a existência de um equipamento *wireless* no SISTEMA. |
| Função | Função do dispositivo da ORGANIZAÇÃO. |  |  |
| SUPORTE TÉCNICO | | | |
| Id | Identificador do parceiro responsável pelo suporte ou fabricante do dispositivo no SISTEMA. | **Periodicidade** | Periodicidade de atualização de contratos de suporte. |
| Tipo de PAR | Se é parceiro ou fabricante. | **Antecedência** | Com que antecedência se deve proceder à renovação do contrato. |
| Inativo | Se o suporte ao dispositivo ainda se encontra ativo no SISTEMA. | **Contactos** | Contactos para pedido de suporte. |
| Data de inatividade | Se o suporte estiver inativo, registar a data de inatividade. | **Horário** | Horário disponível para contacto. |
| Designação | Designação do parceiro/fabricante. | **Observações** | Observações (e.g. motivo da inatividade do suporte) |
| Tipo de parceria | Descrição do processador do dispositivo. |  |  |
| APLICAÇÕES DE SEGURANÇA | | | |
| Id | Identificador da aplicação de segurança no SISTEMA. | **Versão** | Versão da aplicação instalada. |
| Tipo de aplicação | Tipo de aplicação. | **Data de aquisição de licença** | Data da última aquisição da licença para uso da aplicação. |
| Suporte | Identificador do parceiro/fabricante que fornece suporte à aplicação no SISTEMA. | **Periodicidade** | Periodicidade de renovação da aplicação. |
| Inativo | Se a aplicação ainda está ativa no dispositivo. | **Antecedência** | Com que antecedência se deve proceder à renovação. |
| Data de inatividade | Se a aplicação estiver inativa, registar a data de inatividade. | **Motivo de inativação** | No caso de a aplicação for inativada registar o motivo. |
| Descrição | Descrição da aplicação. |  |  |
| EXCEÇÕES DE ACESSO | | | |
| Tipo de exceção | Tipo de exceção de acesso à rede. | Regras | Descrição e estado das regras de acesso à rede. |
| Descrição | Descrição da exceção disponibilizada pelo dispositivo. | **Dispositivos permitidos** | Dispositivos permitidos na rede. |

No quadro seguinte deve ser efetuado o registo da informação de um router ou distribuidor de rede.

|  |  |  |
| --- | --- | --- |
| **DADOS GERAIS** | | |
| ID: (vazio)  DATA: (vazio) | Tipo:  ROUTER  DISTRIBUIDOR DE REDE  WIRELESS | DATA COMPRA: (vazio)  INATIVO DATA DE INATIVAÇÃO: (vazio) |
| MARCA: (vazio) | | |
| MODELO: (vazio) | | |
| FUNÇÃO: (vazio) | | |
| VERSÃO DO *FIRMWARE*: (vazio) | | |
| ENDEREÇO IP: (vazio) | | |
| LOCALIZAÇÃO: (vazio) | | |
| JUSTIFICAÇÃO: (vazio) | | |

|  |  |  |
| --- | --- | --- |
| **SUPORTE TÉCNICO** | | |
| ID: (vazio) | TIPO DE PAR:  PARCEIRO  FABRICANTE | INATIVO DATA DE INATIVAÇÃO: (vazio) |
| NOME: (vazio) | | |
| TIPO DE PARCERIA: (vazio) | | |
| PERIODICIDADE: (vazio) | | |
| ANTECEDÊNCIA: (vazio) | | |
| CONTACTOS: (vazio) | | |
| HORÁRIO: (vazio) | | |
| OBSERVAÇÕES: (vazio) | | |

|  |  |  |
| --- | --- | --- |
| **APLICAÇÕES DE SEGURANÇA** | | |
| ID: (vazio) |  | SUPORTE: (vazio)  INATIVO DATA DE INATIVAÇÃO: (vazio) |
| DESCRIÇÃO: (vazio) | | |
| VERSÃO: (vazio) | | |
| DATA DA AQUISIÇÃO DE LICENÇA: (vazio) | | |
| PERIODICIDADE: (vazio) | | |
| ANTECEDÊNCIA: (vazio) | | |
| MOTIVO INATIVAÇÃO: (vazio) | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EXCEÇÕES DE ACESSO** | | | | | | | | |
| TIPO DE EXCEÇÃO:  INTERNET  REDE LOCAL  WIRELESS | | | | |  | | | |
| DESCRIÇÃO: (vazio) | | | | | | | | |
| REGRAS: (vazio) | | | | | | | |  |
|  |  | | | | | |  | |
|  | REGRAS | | | | | ESTADO | |  |
|  | | | | |  | |
|  | | | | |  | |
|  | | | | |  | |
|  | | | | | | | | |
| DISPOSITIVOS PERMITIDOS: (vazio) | | | | | | | |  |
|  |  | | | | | |  | |
|  | DISPOSITIVO | ADMISSÃO | REVISÃO | JUSTIFICAÇÃO | | ESTADO | |  |
|  |  |  |  | |  | |
|  |  |  |  | |  | |
|  |  |  |  | |  | |
|  | | | | | | | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte pode ser consultado o impacto que o preenchimento do DSPI-RRDR pode ter no DSPI.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Rosto do Dossier | |
| Calendário / compromissos | Inserir registo de compromisso. |
| Calendário / cronograma | Registar compromisso no cronograma. |
| DSPI / Caracterização do SISTEMA | |
| Suporte técnico / (todos) | Inserir ou alterar registo de parceiro. |
| Infraestrutura / equipamentos de segmentação de rede | Inserir ou remover registo |
| Infraestrutura /segmento / diagrama | Alterar diagrama se necessário |
| Infraestrutura /segmento / distribuidores de rede *wired*; distribuidores de rede *wireless* | Inserir ou alterar registo. |
| Aplicações de segurança / nível de infraestrutura | Inserir ou remover registo de uma aplicação de segurança. |
| DSPI / Plano de Segurança e Disponibilidade | |
| Controlo de acesso à infraestrutura / exceções de acesso / internet; rede local com fios; rede local sem fios | Atualizar se necessário. |
| *Malware* e atualizações de segurança / proteções de *malware* de infraestrutura | Atualizar se necessário. |
| *Malware* e atualizações de segurança / atualizações de firmware | Atualizar se necessário. |
| OUTROS | |
| Inatividade do dispositivo | Se o dispositivo for retirado do SISTEMA preencher um DSPI-RSRDR |

* + - * 1. Registo de saída de routers ou distribuidores de rede

Este anexo contém o formulário a preencher quando ocorre a saída de um equipamento de rede (se aplicável, garantir a eliminação de configurações específicas da ORGANIZAÇÃO).

* + - 1. Redundância Elétrica
         1. Registo de recurso

Este anexo contém o formulário a preencher quando ocorre a disponibilização ou alteração de um recurso no SISTEMA.

**REGISTO DE REDUNDÂNCIA ELÉTRICA**

Este registo é utilizado pelo AUDITOR registar a entrada ou alteração de redundância elétrica no SISTEMA.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do dispositivo de redundância elétrica no SISTEMA. | **Modelo** | Modelo do dispositivo. |
| Data | Data do registo. | **Função** | Função do dispositivo da ORGANIZAÇÃO. |
| Tipo | Tipo de dispositivo a registar | **Manutenção** | Tipo de manutenção que o dispositivo requer. |
| Data de compra | Data de aquisição do dispositivo pela ORGANIZAÇÃO. | **UTILIZADOR responsável** | UTILIZADOR do SISTEMA responsável pela verificação do funcionamento do dispositivo. |
| Inativo | Se o dispositivo ainda se encontra em uso pela ORGANIZAÇÃO. | **Ultima verificação** | Data da última intervenção no dispositivo. |
| Data de inatividade | Se o dispositivo estiver fora de uso, registar data de inatividade. | **Periodicidade** | Periodicidade da verificação. |
| DESCRIÇÃO | Descrição do dispositivo de redundância | **Localização** | Localização do dispositivo na ORGANIZAÇÃO. |
| Marca | Marca do dispositivo. |  |  |
| SUPORTE TÉCNICO | | | |
| Id | Identificador do parceiro responsável pelo suporte ou fabricante do dispositivo no SISTEMA. | **Periodicidade** | Periodicidade de atualização de contratos de suporte. |
| Tipo de PAR | Se é parceiro ou fabricante. | **Antecedência** | Com que antecedência se deve proceder à renovação do contrato. |
| Inativo | Se o suporte ao dispositivo ainda se encontra ativo no SISTEMA. | **Contactos** | Contactos para pedido de suporte. |
| Data de inatividade | Se o suporte estiver inativo, registar a data de inatividade. | **Horário** | Horário disponível para contacto. |
| Designação | Designação do parceiro/fabricante. | **Observações** | Observações (e.g. motivo da inatividade do suporte) |
| Tipo de parceria | Descrição do processador do dispositivo. |  |  |

No quadro seguinte deve ser efetuado o registo da informação de redundância elétrica.

|  |  |  |
| --- | --- | --- |
| **DADOS GERAIS** | | |
| ID: (vazio)  DATA: (vazio) |  | DATA COMPRA: (vazio)  INATIVO DATA DE INATIVAÇÃO: (vazio) |
| DESCRIÇÃO: (vazio) | | |
| MARCA: (vazio) | | |
| MODELO: (vazio) | | |
| FUNÇÃO: (vazio) | | |
| MANUTENÇÃO: (vazio) | | |
| UTILIZADOR RESPONSÁVEL: (vazio) | | |
| ULTIMA VERIFICAÇÃO: (vazio) | | |
| PERIODICIDADE: (vazio) | | |
| LOCALIZAÇÃO: (vazio) | | |

|  |  |  |
| --- | --- | --- |
| **SUPORTE TÉCNICO** | | |
| ID: (vazio) | TIPO DE PAR:  PARCEIRO  FABRICANTE | INATIVO DATA DE INATIVAÇÃO: (vazio) |
| NOME: (vazio) | | |
| TIPO DE PARCERIA: (vazio) | | |
| PERIODICIDADE: (vazio) | | |
| ANTECEDÊNCIA: (vazio) | | |
| CONTACTOS: (vazio) | | |
| HORÁRIO: (vazio) | | |
| OBSERVAÇÕES: (vazio) | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte pode ser consultado o impacto que o preenchimento do DSPI-RRE pode ter no DSPI.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Rosto do Dossier | |
| Calendário / compromissos | Inserir registo de compromisso. |
| Calendário / cronograma | Registar compromisso no cronograma. |
| DSPI / Caracterização do SISTEMA | |
| Suporte técnico / (todos) | Inserir ou alterar registo de parceiro. |
| Infraestrutura /segmento / diagrama | Alterar diagrama se necessário |
| Infraestrutura /segmento / redundância elétrica | Inserir ou alterar registo. |
| DSPI / Plano de Segurança e Disponibilidade | |
| Disponibilidade e integridade de dados / redundância elétrica | Atualizar se necessário. |
| OUTROS | |
| Responsabilidades no SISTEMA | Se houverem responsabilidades a atribuir preencher um DSPI-RARU |
| Inatividade do dispositivo | Se o dispositivo for retirado do SISTEMA preencher um DSPI-RSRDR |

* + - * 1. Registo de extinção de recurso

Este anexo contém o formulário a preencher quando ocorre a saída de uma aplicação do SISTEMA.

* + - 1. Recursos
         1. Registo de recurso

Este anexo contém o formulário a preencher quando ocorre a disponibilização ou alteração de um recurso no SISTEMA.

**REGISTO DE RECURSO DE SISTEMA**

Este registo é utilizado pelo AUDITOR registar a entrada ou alteração de um recurso de sistema no SISTEMA.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do recurso no SISTEMA. | **Descrição** | Descrição do recurso de sistema. |
| Data | Data do registo. | **Tipo** | Tipo de recurso. |
| Inativo | Se o recurso ainda se encontra ativo no SISTEMA. | **Descrição de conteúdo** | Descrição do conteúdo existente no recurso. |
| Data de inatividade | Se o recurso estiver fora de uso, registar data de inatividade. | **Utilizadores** | Permissões por utilizador. |
| Tipo de recurso | Se o recurso é de servidor, externo ou outro |  |  |

No quadro seguinte devem ser efetuados os registos de um recurso de sistema no SISTEMA.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **DADOS GERAIS** | | | | | | | |
| ID: (vazio)  DATA: (vazio) | | | TIPO DE RECURSO:  SERVIDORES  EXTERNOS  OUTRO | | INATIVO DATA DE INATIVAÇÃO: (vazio) | | |
| DESCRIÇÃO: (vazio) | | | | | | | |
| TIPO: (vazio) | | | | | | | |
| PARTILHA: (vazio) | | | | | | | |
| DESCRIÇÃO DE CONTEÚDO: (vazio) | | | | | | | |
| UTILIZADORES: (vazio) | | | | | | |  |
|  |  | | | | |  | |
|  | ID | PERMISSÃO | | JUSTIFICAÇÃO | | CREDENCIAIS |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  | | | | | | | |
| ID: (vazio)  DATA: (vazio) | | | TIPO DE RECURSO:  SERVIDORES  EXTERNOS  OUTRO | | INATIVO DATA DE INATIVAÇÃO: (vazio) | | |
| DESCRIÇÃO: (vazio) | | | | | | | |
| TIPO: (vazio) | | | | | | | |
| PARTILHA: (vazio) | | | | | | | |
| DESCRIÇÃO DE CONTEÚDO: (vazio) | | | | | | | |
| UTILIZADORES: (vazio) | | | | | | |  |
|  |  | | | | |  | |
|  | ID | PERMISSÃO | | JUSTIFICAÇÃO | | CREDENCIAIS |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  | | | | | | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte pode ser consultado o impacto que o preenchimento do DSPI-RRS pode ter no DSPI.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Caracterização do SISTEMA | |
| Infraestrutura /segmento / recursos de rede | Registar ou remover recursos de rede disponibilizados pelo dispositivo. |
| DSPI / Plano de Segurança e Disponibilidade | |
| Permissões dos utilizadores / UTILIZADORES autorizados por DEA | Atualizar se necessário. |

* + - * 1. Registo de extinção de recurso

Este anexo contém o formulário a preencher quando ocorre a saída de uma aplicação do SISTEMA.

* + - 1. DAE
         1. Registo de DAE

Este anexo contém o formulário a preencher quando ocorre uma entrada ou alteração de um DAE no SISTEMA.

…justificação, localizações autorizadas, lista de UTILIZADORES que podem manusear e declaração de responsabilidade pela utilização e apenas para os fins aqui descritos assinada por cada um.

**REGISTO DE DAE**

Este registo é utilizado pelo AUDITOR registar a entrada ou alteração de um DAE no SISTEMA.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do equipamento no SISTEMA. | **Tipo** | Tipo de DEA. |
| Data | Data do registo. | Descrição de conteúdo | Descrição do conteúdo existente no dispositivo. |
| Inativo | Se o dispositivo ainda se encontra em uso pela ORGANIZAÇÃO. | **Autorizações** | Autorizações por utilizador. |
| Data de inatividade | Se o equipamento estiver fora de uso, registar data de inatividade. | **Localizações autorizadas** | Localizações autorizadas para o dispositivo. |

No quadro seguinte devem ser efetuados os registos de um DEA no SISTEMA.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DADOS GERAIS** | | | | | | | | |
| ID: (vazio)  DATA: (vazio) | | |  | | INATIVO DATA DE INATIVAÇÃO: (vazio) | | | |
| TIPO: (vazio) | | | | | | | | |
| DESCRIÇÃO DE CONTEÚDO: (vazio) | | | | | | | | |
| AUTORIZAÇÕES: (vazio) | | | | | | | |  |
|  |  | | | | | |  | |
|  | DISPOSITIVO | UTILIZADOR | | JUSTIFICAÇÃO | | ESTADO | |  |
|  |  | |  | |  | |
|  |  | |  | |  | |
|  |  | |  | |  | |
|  | | | | | | | | |
| LOCALIZAÇÕES AUTORIZADAS: (vazio) | | | | | | | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte pode ser consultado o impacto que o preenchimento do DSPI-RDAE pode ter no DSPI.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Caracterização do SISTEMA | |
| Infraestrutura /segmento / diagrama | Alterar diagrama se necessário |
| Infraestrutura /segmento / dispositivos de armazenamento externo | Inserir ou alterar registo. |
| Recursos de rede / (todos) | Registar ou remover recursos de rede disponibilizados pelo dispositivo. |
| DSPI / Plano de Segurança e Disponibilidade | |
| *Controlo dos DEA* / dispositivos/UTILIZADORES autorizados por DEA | Atualizar se necessário. |
| Disponibilidade e integridade de dados / redundância elétrica | Atualizar se necessário. |
| OUTROS | |
| Inatividade do dispositivo | Se o dispositivo for retirado do SISTEMA preencher um DSPI-RDEA |

* + - * 1. Registo de saída de DAE

Este anexo contém o formulário a preencher quando ocorre a saída de um DAE no SISTEMA.

(garantir que a informação foi apagada de forma definita ou o disco removido do equipamento).

* + - 1. Outros Equipamentos
         1. Registo de outros equipamentos

Este anexo contém o formulário a preencher quando ocorre uma entrada ou alteração de um equipamento (e.g impressoras, máquinas de produção) no SISTEMA.

**REGISTO DE OUTROS EQUIPAMENTOS**

Este registo é utilizado pelo AUDITOR registar a entrada ou alteração de um computador, servidor ou equivalente no SISTEMA.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do equipamento no SISTEMA. | **Tipo de ligação ao sistema** | Ligação que o equipamento disponibiliza para ligação ao SISTEMA. |
| Data | Data do registo. | **Tipo de impressora** | Tipo de impressora. Preencher no caso do equipamento ser uma impressora |
| Tipo de equipamento | Tipo de dispositivo a registar. | **Tecnologia** | Tecnologia usada pelo equipamento. |
| Data de compra | Data de aquisição do equipamento pela ORGANIZAÇÃO. | **Interfaces de comunicação** | Interfaces de comunicação que o equipamento disponibiliza. |
| Inativo | Se o dispositivo ainda se encontra em uso pela ORGANIZAÇÃO. | **Cor** | No caso do equipamento ser uma impressora, indicar se imprime a cores. |
| Data de inatividade | Se o equipamento estiver fora de uso, registar data de inatividade. | **Atualização de *firmware*** | Versão do *firmware* instalado no equipamento. |
| DESCRIÇÃO | Descrição do equipamento. | **Endereço IP** | Endereço IP do equipamento. |
| Marca | Marca do equipamento. | **Localização** | Localização do dispositivo na ORGANIZAÇÃO. |
| Modelo | Modelo do equipamento. | **Recurso** | Se for recurso do sistema |
| SUPORTE TÉCNICO | | | |
| Id | Identificador do parceiro responsável pelo suporte ou fabricante do dispositivo no SISTEMA. | **Periodicidade** | Periodicidade de atualização de contratos de suporte. |
| Tipo de PAR | Se é parceiro ou fabricante. | **Antecedência** | Com que antecedência se deve proceder à renovação do contrato. |
| Inativo | Se o suporte ao dispositivo ainda se encontra ativo no SISTEMA. | **Contactos** | Contactos para pedido de suporte. |
| Data de inatividade | Se o suporte estiver inativo, registar a data de inatividade. | **Horário** | Horário disponível para contacto. |
| Designação | Designação do parceiro/fabricante. | **Observações** | Observações (e.g. motivo da inatividade do suporte) |
| Tipo de parceria | Descrição do processador do dispositivo. |  |  |

No quadro seguinte devem ser efetuados os registos de um equipamento no SISTEMA.

|  |  |  |
| --- | --- | --- |
| **DADOS GERAIS** | | |
| ID: (vazio)  DATA: (vazio) | TIPO DE EQUIPAMENTO:  IMPRESSORA  EQUIPAMENTO DE PRODUÇÃO  OUTRO | DATA COMPRA: (vazio)  INATIVO DATA DE INATIVAÇÃO: (vazio) |
| DESCRIÇÃO: (vazio) | | |
| MARCA: (vazio) | | |
| MODELO: (vazio) | | |
| TIPO DE LIGAÇÃO AO SISTEMA: (vazio) | | |
| TIPO DE IMPRESSORA: (vazio) | | |
| TECNOLOGIA: (vazio) | | |
| INTERFACES DE COMUNICAÇÃO: (vazio) | | |
| COR: (vazio) | | |
| VERSÃO DE FIRMWARE: (vazio) | | |
| ENDEREÇO IP: (vazio) | | |
| LOCALIZAÇÃO: (vazio) | | |

|  |  |  |
| --- | --- | --- |
| **SUPORTE TÉCNICO** | | |
| ID: (vazio) | TIPO DE PAR:  PARCEIRO  FABRICANTE | INATIVO DATA DE INATIVAÇÃO: (vazio) |
| NOME: (vazio) | | |
| TIPO DE PARCERIA: (vazio) | | |
| PERIODICIDADE: (vazio) | | |
| ANTECEDÊNCIA: (vazio) | | |
| CONTACTOS: (vazio) | | |
| HORÁRIO: (vazio) | | |
| OBSERVAÇÕES: (vazio) | | |

|  |  |
| --- | --- |
| **RECURSOS DE REDE** | |
| ID: (vazio) | INATIVO DATA DE INATIVAÇÃO: (vazio) |
| Descrição: (vazio) | |
| TIPO: (vazio) | |
| JUSTIFICAÇÃO: (vazio) | |
| MOTIVO INATIVAÇÃO: (vazio) | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte pode ser consultado o impacto que o preenchimento do DSPI-ROE pode ter no DSPI.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Caracterização do SISTEMA | |
| Suporte técnico / (todos) | Inserir ou alterar registo de parceiro. |
| Infraestrutura /segmento / diagrama | Alterar diagrama se necessário |
| Infraestrutura /segmento / outros equipamentos | Inserir ou alterar registo. |
| Recursos de rede / (todos) | Registar ou remover recursos de rede disponibilizados pelo dispositivo. |
| DSPI / Plano de Segurança e Disponibilidade | |
| *Malware* e atualizações de segurança / atualizações de firmware | Atualizar se necessário. |
| Disponibilidade e integridade de dados / redundância elétrica | Atualizar se necessário. |
| OUTROS | |
| Inatividade do dispositivo | Se o dispositivo for retirado do SISTEMA preencher um DSPI-ROE |

* + - * 1. Registo de saída de outros equipamentos

Este anexo contém o formulário a preencher quando ocorre a saída de um DAE no SISTEMA.

(garantir que a informação foi apagada de forma definita ou o disco removido do equipamento).

* + - 1. Utilizadores
         1. Registo de utilizador

Este anexo contém o formulário a preencher para acompanhar a entrada ou alteração de um UTILIZADOR no SISTEMA. Contém uma lista de sugestões para acompanhar a entrada de um novo utilizador.

**REGISTO DE UTILIZADOR**

Este documento é preenchido pelo AUDITOR para registar a entrada de um UTILIZADOR do SISTEMA. A sua forma *checklist* permite ajudar a integração do novo utilizador, e identificar mais facilmente as necessidades de reconfiguração do DSPI motivadas pela entrada do utilizador. O documento é assinado em conjunto com o RESPONSÁVEL PELO TRATAMENTO de dados pelo facto de atribuir permissões a dispositivos, aplicações e recursos.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. Identifica também o UTILIZADOR que entra no SISTEMA. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte apresenta as instruções de leitura e preenchimento de cada campo que pertence ao registo.

|  |  |  |  |
| --- | --- | --- | --- |
| CAMPO | INSTRUÇÕES | CAMPO | INSTRUÇÕES |
| DADOS GERAIS | | | |
| Id | Identificador do UTILIZADOR no SISTEMA. | Inativo | Se o dispositivo ainda se encontra em uso pela ORGANIZAÇÃO. |
| Nome | Nome do utilizador. | Data de inatividade | Se o equipamento estiver fora de uso, registar data de inatividade. |
| Data | Data de entrada do utilizador. |  |  |
| PERMISSÕES OU AUTORIZAÇÕES | | | |
| Id | Identificador da permissão ou autorização. | **Descrição** | Descrição da parceria ou permissão. |
| Tipo | Se é uma permissão ou uma autorização. | **Designação** | Designação da parceria ou autorização. |
| Inativo | Se a permissão ou autorização ainda está ativa no SISTEMA. | **Justificação** | Justificação da existência do recurso. |
| Data de inatividade | Se a permissão ou autorização estiver inativa, registar a data de inatividade. | **Motivo de inativação** | No caso de a aplicação for inativada registar o motivo. |
| Dispositivo ... | Dispositivo, DEA, aplicação ou recurso do SISTEMA autorizado. |  |  |

O quadro seguinte especifica as permissões atribuídas ao novo UTILIZADOR por dispositivo ou DAE, aplicação e recurso.

|  |  |  |
| --- | --- | --- |
| DADOS GERAIS | | |
| ID: (vazio) |  | INATIVO DATA DE INATIVAÇÃO: (vazio) |
| NOME: (vazio) |  |  |
| DATA (ENTRADA): (vazio |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PERMISSÕES OU AUTORIZAÇÕES | | | | |
| ID: (vazio) | | TIPO:  PERMISSÃO  AUTORIZAÇÃO | | INATIVO DATA DE INATIVAÇÃO: (vazio) | |
| DISPOSITIVO/DEA/APLICAÇÃO/RECURSO: (vazio) | | | | |
| DESCRIÇÃO: (vazio) | | | | |
| DESIGNAÇÃO: (vazio) | | | | |
| JUSTIFICAÇÃO: (vazio) | | | | |
| MOTIVO DE INATIVAÇÃO: (vazio) | | |  | |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

O quadro seguinte tem a forma de uma lista com itens a verificar aquando da entrada de um novo utilizador. O preenchimento facilita a identificação de necessidades decorrentes da entrada de um utilizador. A coluna “Impacto” deve ser preenchida com uma das palavras: i) Sim; ou ii) Não. As colunas “Medidas propostas” e “Vulnerabilidade” podem ser personalizada para melhor documentar as alterações a efetuar e os riscos de não efetuar.

|  |  |
| --- | --- |
| ITEM | MEDIDAS PROPOSTAS |
| DSPI / Caracterização do SISTEMA | |
| UTILIZADORES / ativos | Inserir registo. |
| (vazio) | (vazio) |
| DSPI / Plano de Segurança e Disponibilidade | |
| Controlo dos DEA / Dispositivos/UTILIZADORES autorizados por DEA | Atualizar DSPI se necessário. |
| Permissões dos UTILIZADORES / (todos) | Atualizar DSPI se necessário. |
| (vazio) | (vazio) |
| DOCUMENTAÇÃO (Aplicabilidade: Admin, User, Operador) | |
| Leitura da política de privacidade e segurança do SISTEMA | UTILIZADOR deve assinar documento comprovativo da leitura. |
| Leitura do regulamento de utilização do SI | UTILIZADOR deve assinar documento comprovativo da leitura. |
| Assinatura do compromisso de confidencialidade (dados pessoais e outros) | UTILIZADOR deve assinar documento comprovativo da leitura. |
| (vazio) | (vazio) |
| DOCUMENTAÇÃO (Aplicabilidade: Admin, User) | |
| Leitura do documento de boas práticas para utilização do email | UTILIZADOR deve assinar documento comprovativo da leitura. |
| Leitura do documento de boas práticas para utilização dos recursos e arquivo de documentos. | UTILIZADOR deve assinar documento comprovativo da leitura. |
| (vazio) | (vazio) |
| FORMAÇÃO (Aplicabilidade: Admin, User) | |
| Formação na utilização correta dos recursos de rede | Folha de presenças na formação. |
| (vazio) | (vazio) |
| OUTROS | |
| Responsabilidades no SISTEMA | Se houverem responsabilidades a atribuir preencher um DSPI-RARU |
| (vazio) | (vazio) |

* + - * 1. Registo de saída de utilizador

Este anexo contém o formulário a preencher para acompanhar a saída e inativação de um UTILIZADOR no SISTEMA. Contém uma lista de verificação de alterações a efetuar aquando da saída de um utilizador.

**REGISTO DE SAÍDA DE UTILIZADOR**

Este documento é preenchido pelo AUDITOR para registar a saída de um UTILIZADOR do SISTEMA. A sua forma *checklist* permite identificar mais facilmente as necessidades de reconfiguração do DSPI, motivadas pela saída do utilizador.

O quadro seguinte identifica a auditoria e o AUDITOR responsável pela mesma. Identifica também o UTILIZADOR que sai do SISTEMA. É utilizado o termo SPRINT para representar o tempo decorrido entre duas auditorias seguidas.

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

O quadro seguinte tem a forma de uma lista com itens a verificar que podem ser impactados pela saída de um utilizador. O seu preenchimento facilita a identificação das alterações necessárias a efetuar no DSPI decorrentes da saída do utilizador. A coluna “Impacto” deve ser preenchida com uma das palavras: i) Sim; ou ii) Não. As colunas “Medidas propostas” e “Vulnerabilidade” podem ser personalizada para melhor documentar as alterações a efetuar e os riscos de não efetuar.

|  |  |  |  |
| --- | --- | --- | --- |
| ITEM | MEDIDAS PROPOSTAS | IMPACTO | VULERABILIDADE |
| DSPI / Caracterização do SISTEMA | | |  |
| UTILIZADORES / ativos | Reconfigurar para inativo. | Sim | Severa |
| (vazio) | (vazio) | (vazio) | (vazio) |
| DSPI / Plano de Segurança e Disponibilidade | | |  |
| Controlo de acesso à infraestrutura / Acessos externos / Autorizações | Cancelar o acesso externo. |  | Severa |
| Controlo dos DEA / Dispositivos/UTILIZADORES autorizados por DEA | Cancelar a autorização. |  | Critica |
| Permissões dos UTILIZADORES / UTILIZADORES autorizados por dispositivo | Cancelar a autorização. |  | Severa |
| Permissões dos UTILIZADORES / UTILIZADORES autorizados por aplicação | Cancelar a autorização. |  | Severa |
| Permissões dos UTILIZADORES / UTILIZADORES autorizados por recurso | Cancelar a autorização. |  | Severa |
| Disponibilidade e Integridade dos Dados / (todos) | Rever UTILIZADORES responsáveis |  | Severa |
| (vazio) | (vazio) | (vazio) | (vazio) |
| OUTROS | | |  |
| Responsabilidades no SISTEMA | Se houverem responsabilidades a alterar preencher um DSPI-RARU |  | Critica |
| (vazio) | (vazio) | (vazio) | (vazio) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUDITOR)

* + 1. Outros registos
       1. Incidentes
          1. Registo de incidentes de violação de dados

Este anexo deve ser utilizado para registar os incidentes de violação de dados ocorridos, relacionados com o SISTEMA.

**REGISTO DE INCIDENTE DE VIOLAÇÃO DE DADOS**

**(IVD** N.º 99999)

Este documento é preenchido pelo DPO, ADMINISTRADOR DE SISTEMA ou AUDITOR e serve para registar incidentes de violação de dados ocorridos, relacionados com o SISTEMA. Deve ser assinado pelo autor e pelo RESPONSÁVEL PELO TRATAMENTO. Cada formulário deve registar apenas um incidente de violação de dados.

|  |  |
| --- | --- |
| RESPONSÁVEL PELO TRATAMENTO e DPO (se aplicável) | OUTROS DADOS |
| IDENTIFICAÇÃO (nome / designação):  (vazio)  ENCARREGADO DE PROTEÇÃO DE DADOS (*Data Protection Officer* (DPO)):  N/A | AUTOR:  (vazio)  DATA E HORA:  (vazio) |

|  |
| --- |
| INCIDENTE |
| RESUMO |
| RESUMO (descrição breve (uma linha)): (vazio)  DATA E HORA DO INCIDENTE (se não for conhecida, indicar uma estimativa): (vazio)  DATA E HORA É UMA ESTIMATIVA [sim, não]: (vazio)  TIPO DE INCIDENTE [destruição, perda, alteração, acesso não autorizado, outro]: (vazio)  CAUSA [acidental, intencional]: (vazio) |
| DESCRIÇÃO COMPLETA |
| (vazio) |
| DADOS AFETADOS |
| ENVOLVE DADOS PESSOAIS [sim, não]: (vazio)  ENVOLVE DADOS PESSOAIS DE CATEGORIA ESPECIAL [sim, não]: (vazio)  DADOS AFETADOS (e.g. e-mail, telefone, etc.):  (vazio) |
| TITULARES DOS DADOS AFETADOS |
| QUANTIDADE DE TITULARES DOS DADOS: (vazio)  IDENTIFICAÇÃO DOS TITULARES DOS DADOS:  (vazio) |
| CONSEQUÊNCIAS POSSÍVEIS |
| PARA OS TITULARES DOS DADOS:  (vazio)  PARA O RESPONSÁVEL PELO TRATAMENTO:  (vazio) |
| RECOMENDAÇÕES DO AUTOR E PROPOSTAS DE MELHORIA |
| COMUNICAÇÃO À AUTORIDADE DE CONTROLO (RGPD, Art.º 33) [sim, não]: (vazio)  COMUNICAÇÃO AOS TITULARES DOS DADOS (RGPD, Art.º 34) [sim, não]: (vazio)  PROPOSTAS DE MELHORIA (sugestões):  (vazio) |
| DECISÕES DO RESPONSÁVEL PELO TRATAMENTO |
| COMUNICAÇÃO À AUTORIDADE DE CONTROLO (RGPD, Art.º 33) [efetuar, não efetuar]: (vazio)  COMUNICAÇÃO AOS TITULARES DOS DADOS (RGPD, Art.º 34) [efetuar, não efetuar]: (vazio)  IMPLEMENTAR AS PROPOSTAS DE MELHORIA [sim, não]:  OUTRAS CONSIDERAÇÕES OU PROPOSTAS DE MELHORIA:  (vazio) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUTOR) (RESPONSÁVEL PELO TRATAMENTO)

* + - * 1. Registo de outros incidentes

Este anexo deve ser utilizado para registar outros incidentes ocorridos, relacionados com o SISTEMA.

**REGISTO DE OUTROS INCIDENTES**

Este documento é preenchido pelo DPO, ADMINISTRADOR DE SISTEMA ou AUDITOR e serve para registar outros incidentes ocorridos, relacionados com o SISTEMA. Deve ser assinado pelo autor e pelo RESPONSÁVEL PELO TRATAMENTO. Cada formulário deve registar apenas um incidente.

|  |  |
| --- | --- |
| RESPONSÁVEL PELO TRATAMENTO e DPO (se aplicável) | OUTROS DADOS |
| IDENTIFICAÇÃO (nome / designação):  (vazio)  ENCARREGADO DE PROTEÇÃO DE DADOS (*Data Protection Officer* (DPO)):  N/A | AUTOR:  (vazio)  DATA E HORA:  (vazio) |

|  |
| --- |
| INCIDENTE |
| RESUMO |
| RESUMO (descrição breve (uma linha)): (vazio)  DATA E HORA DO INCIDENTE (se não for conhecida, indicar uma estimativa): (vazio)  DATA E HORA É UMA ESTIMATIVA [sim, não]: (vazio)  CAUSA [acidental, intencional]: (vazio) |
| RELATÓRIO DO AUTOR |
| (vazio) |
| RELATÓRIO DO AUTOR |
| (vazio) |
| DECISÕES DO RESPONSÁVEL PELO TRATAMENTO |
| (vazio) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(AUTOR) (RESPONSÁVEL PELO TRATAMENTO)

* + - 1. Minutas
         1. Ata de encerramento do Diagnóstico Inicial

Nesta secção pode consultar-se a minuta da ata para encerramento do Diagnóstico Inicial.

* + - * 1. Ata de encerramento de Auditoria de Revisão

Nesta secção pode ser consultada a minuta da ata de encerramento das Auditorias de Revisão.