**DSPI**

**DOSSIER DE SEGURANÇA E PRIVACIDADE INFORMÁTICA**

(Firjó-Fios e Malhas, 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. Ancecont - Contabilidades, 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 Firjó - Fios e Malhas, Lda. é constituída pelas empresas enumeradas no quadro abaixo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | EMPRESA | DEPARTAMENTO | | LOCALIZAÇÃO |
| EMP001 | Firjó - Fios e Malhas, Lda. |  |  | Rua Esqueiro 1263, 4750-685 SILVA BCL |
|  |  | DEP001 | Sede | Rua Esqueiro 1263, 4750-685 SILVA BCL |

* + 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 DOS DADOS não considerou necessário nomear um DPO para a ORGANIZAÇÃO conforme registado na ata 2018/1 de 2018-04-04 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 |
| Cristiana Monteiro | RESPONSÁVEL DOS DADOS | 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 |  |  |  |
| Revisão da UPS SEG001 | Cada 3 anos |  |  | 2016-12-22 |
| Renovação de licença ERP Primavera | Cada 12 meses |  |  | 2017-10-10 |
| Renovação das licenças do antivírus | Cada 12 meses |  |  | 01-01-2018 |
| Mudar palavras-chave de utilizador | Cada 12 meses |  |  |  |
| Reavaliação dos DEA | Cada 12 meses |  |  |  |
| Limpar destino de cópias de segurança para garantir a minimização de ficheiros | Cada 12 meses |  |  |  |
| Rever responsabilidades atribuídas aos utilizadores | Cada 12 meses |  |  |  |
| Reavaliação de regras de exceção de acesso à infraestrutura | Cada 12 meses |  |  |  |

*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.

|  |  |  |  |
| --- | --- | --- | --- |
| MARCO | DESCRIÇÃO | COMPONENTES | ESTADO |
|  |  |  |  |
| 2022 | | | |
| Dezembro | Revisão da UPS SEG001 | REE001 |  |
| Outubro | Renovação de licença ERP Primavera | APP003 |  |
| Abril | Substituir consumíveis de dispositivo | CPF001 |  |
| Abril | Rever responsabilidades atribuídas aos utilizadores | N/A |  |
| Abril | Limpar dados de cópias de segurança | DEA001, CPF001 |  |
| Abril | Reavaliação de DEA | DEA001 |  |
| Abril | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001 |  |
| Janeiro | Renovação de antivírus | APS001 |  |
| 2021 | | | |
| Outubro | Renovação de licença ERP Primavera | APP003 |  |
| Abril | Rever responsabilidades atribuídas aos utilizadores | N/A |  |
| Abril | Limpar dados de cópias de segurança | DEA001, CPF001 |  |
| Abril | Reavaliação de DEA | DEA001 |  |
| Abril | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001 |  |
| Janeiro | Renovação de antivírus | APS001 |  |
| 2020 | | | |
| Outubro | Renovação de licença ERP Primavera | APP003 |  |
| Abril | Rever responsabilidades atribuídas aos utilizadores | N/A |  |
| Abril | Limpar dados de cópias de segurança | DEA001, CPF001 |  |
| Abril | Reavaliação de DEA | DEA001 |  |
| Abril | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001 |  |
| Janeiro | Renovação de antivírus | APS001 |  |
| 2019 | | | |
| Dezembro | Revisão da UPS SEG001 | REE001 |  |
| Outubro | Renovação de licença ERP Primavera | APP003 |  |
| Abril | Rever responsabilidades atribuídas aos utilizadores | N/A |  |
| Abril | Limpar dados de cópias de segurança | DEA001, CPF001 |  |
| Abril | Reavaliação de DEA | DEA001 |  |
| Abril | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001 |  |
| Janeiro | Renovação de antivírus | APS001 |  |
| 2018 | | | |
| Outubro | Renovação de licença ERP Primavera | APP003 |  |
| Abril | Substituir consumíveis de dispositivo | CPF001 |  |
| Abril | Limpar dados de cópias de segurança | DEA001, CPF001 |  |
| Abril | Mudar palavras-chave de UTILIZADOR nos computadores | CPF001 |  |

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 |
| PAR003 | HP | TELEFONE: (vazio)  HORÁRIO: 24x7x365 |

* + 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 | MEO | TELEFONE: 16200  HORÁRIO: 24x7x365 |

* + 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: Router Technicolor – TG784nV3  (equipamento cedido e assistido pela MEO)  AQUISIÇÃO: N/A | 192.168.1.254  192.168.1.253 1) | EMP001.DEP001 |

1) Servidor FTP interno do router;

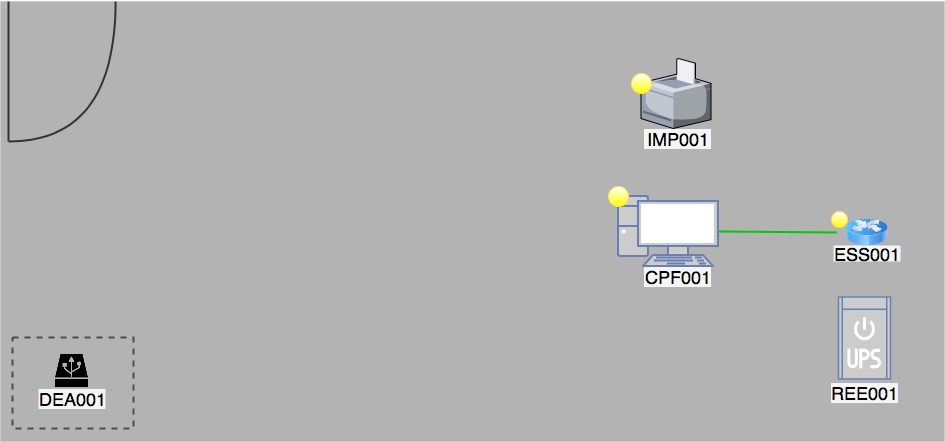
* + - 1. Segmentos de rede

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 0 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:  UPS – Smart UPS online interativa 700VA  (APC Smart-UPS 700)  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 |
| (vazio) | NOME NETBIOS: (vazio)  MARCA / MODELO: (vazio)  TIPO: (vazio)  PROCESSADOR: (vazio)  MEMÓRIA PRINCIPAL: (vazio)  MEMÓRIA SECUNDÁRIA: (vazio)  FUNÇÃO: (vazio)  AQUISIÇÃO: (vazio) | (vazio) | (vazio) |

* + - 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 |
| 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: ADMIN-PC  MARCA / MODELO: DELL FK6M022  PROCESSADOR: Intel Core i3 – 4130 3.4 GHz  MEMÓRIA PRINCIPAL: 8 GB  MEMÓRIA SECUNDÁRIA: 240 GB (SSD) 465 GB  AQUISIÇÃO: 2014-10-10 | 192.168.1.91  (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 |
| (vazio) | NOME NETBIOS: (vazio)  MARCA / MODELO: (vazio)  PROCESSADOR: (vazio)  MEMÓRIA PRINCIPAL: (vazio)  MEMÓRIA SECUNDÁRIA: 4(vazio)  AQUISIÇÃO: (vazio) | (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: HP Deskjet 3639  TECNOLOGIA DE IMPRESSÃO: Jato de tinta  TIPO: Multifunções  INTERFACES DISPONÍVEIS: Ethernet e USB  INTERFACE ATUAL: Ethernet  LEITOR DE USB OU CARTÕES: Não | 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. |

* + 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 8.1 Pro 64 bits |

* + 1. Aplicações de produtividade

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

|  |  |
| --- | --- |
| ID | DESCRIÇÃO |
| APP002 | Microsoft Office Home and Business 2013 |
| APP004 | Microsoft SQL Server 2014 |

* + 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 |

* + 1. Aplicações por dispositivo

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

|  |  |
| --- | --- |
| DISPOSITIVO | APLICAÇÕES |
| CPF001 | APP001, APP002, APP003, APP004 |

* + 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: ADMIN-PC\Primavera  CREDENCIAIS: ANEXO VI -3 | Base de dados onde consta informação operacional do ERP Primavera (APP003, APP004). |

* + 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 |
| REC002 | DESCRIÇÃO: Google Drive  CREDENCIAIS: anexo VI - 3 | Cópias de segurança onde consta informação operacional do ERP Primavera e dos restantes ficheiros da ORGANIZAÇÃO. |

* + 1. Outros recursos

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

|  |  |  |
| --- | --- | --- |
| ID | TIPO | DESCRIÇÃO |
| (vazio) | (vazio) | (vazio) |

* + 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. |

* + 1. Utilizadores ativos

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

|  |  |
| --- | --- |
| ID | Nome |
| USR001 | Cristiana Monteiro |
| USR004 | Célio Carvalho |

* + 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 as medidas de segurança e disponibilidade implementadas no SISTEMA ao nível da infraestrutura, rede local e sistemas operativos. São também mencionados os dispositivos que executam *software* e que, por esse motivo, devem ser objeto de atenção para revisão de versões e aplicação de *patches* de segurança. Além disso são apresentadas as proteções implementadas para prevenção de *malware*, controlo de DEA, cópias de segurança e permissões dos utilizadores.

Os dados constantes deste plano são atualizados pelo AUDITOR sempre que exista a necessidade de atualização nomeadamente quando existe a correção ou mitigação de vulnerabilidades identificadas.

Alguns dos quadros apresentados nos itens seguintes solicitam um estado individual. Este estado pode ser utilizado pelo AUDITOR para definir uma regra provisoriamente inativa até decisão definitiva de eliminação.

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

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 |
| ESS001 | *Router* para a internet | PAR002 |

* + - 1. Rede local

Neste ponto constam as barreiras de admissão à rede 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 nos SO, tais como *firewalls* por *software* (SO, KIS, etc.), conta de convidado desativada, acesso apenas com UTILIZADOR e palavra-chave a todos os recursos, etc.

|  |  |
| --- | --- |
| DISPOSITIVO / APLICAÇÃO | BARREIRAS |
| CPF001.APP001 |  |
|  | Conta de convidado desativada |
|  | Autenticação com nome de UTILIZADOR e palavra-chave |
| CPF001.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 configuradas por dispositivo.

|  |  |  |  |
| --- | --- | --- | --- |
| DISPOSITIVO | REGRA | DESCRIÇÃO | ESTADO |
| ESS001 |  |  |  |
|  | Rede pública (80) 🡪 ESS001 (80) | Suporte técnico remoto do parceiro | Ativo |
|  | Rede pública (21) 🡪 ESS001 (21) | 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 definidas 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 definidas 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 |
| (vazio) |  |  |  |
|  | PORTAS / DESCRIÇÃO: (vazio) | (vazio) | (vazio) |
|  | PORTAS / DESCRIÇÃO: (vazio) | (vazio) | (vazio) |

* + 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 |
| (vazio) |  |  |
|  | (vazio) | (vazio) |

* + 1. Dispositivos/UTILIZADORES autorizados por DEA

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

|  |  |  |  |
| --- | --- | --- | --- |
| DEA | DISPOSITIVOS/UTILIZADORES |  | ESTADO |
| DEA001 |  |  |  |
|  | CPF001/USR001 | ATA: 2018/1 de 2018-04-04  JUSTIFICAÇÃO: Dispositivo utilizado para cópias de segurança onde consta informação operacional do ERP Primavera e dos restantes ficheiros da ORGANIZAÇÃO. | Ativo |

* + 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 inseridas 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 |  |
| (vazio) | (vazio) |  |
|  |  | ATA: (vazio)  JUSTIFICAÇÃO: (vazio)  LOCALIZAÇÕES AUTORIZADAS: (vazio)  MEDIDAS DE PROTEÇÃO ADICIONAL: (vazio) |

* + 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 |
| (vazio) | (vazio) |

* 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 |
| CPF001 |  |  |
|  | USR001 | APP001.PER001 |
| CPF001 |  |  |
|  | USR004 | 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 |
| APP004 |  |  |
|  | USR001 | PER003 |

* + 1. Utilizadores autorizados por recurso

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

|  |  |  |  |
| --- | --- | --- | --- |
| RECURSO | UTILIZADOR | AUTORIZAÇÃO | PERMISSÕES |
| (vazio) |  |  |  |
|  | (vazio) | ATA: (vazio)  JUSTIFICAÇÃO: (vazio) | (vazio) |

* + 1. Utilizadores autorizados por recurso externo

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

|  |  |  |  |
| --- | --- | --- | --- |
| RECURSO | UTILIZADOR | AUTORIZAÇÃO | PERMISSÕES |
| REC001 |  |  |  |
|  | USR001 | ATA: 2018/1  JUSTIFICAÇÃO: Utilizado para cópias de segurança *online* onde consta informação operacional do ERP Primavera.  CONHECE AS CREDENCIAIS [S/N]: Sim | R |

* 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 |
| (vazio) |  |  |
|  | (vazio) | (vazio) |

* + 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) |
| DISPOSITIVO |  |  |
| (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 |
| CPF001 |  |  |
|  | 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 |
| CPF001 |  |  |
|  | APP001 | 6.3.9600 |
|  | APP002 | 15.05007.1000 |
|  | APP003 | 9.0 |
|  | APP004 | 12.0.2269.0 |

* + 1. Versões de *firmware*

O quadro seguinte permite rastrear os dispositivos com necessidade de atualizações de *firmware*. Deve ser mantida informação acerca da versão do *firmware* atual para que o AUDITOR possa confrontar com as últimas versões disponibilizadas com cada fabricante em sede de auditoria. As versões indicadas em dispositivos de tipo computador fixo ou móvel referem-se à BIOS da máquina.

|  |  |
| --- | --- |
| DISPOSITIVO | VERSÃO |
| ESS001 | 10.2.1.L |
| CPF001 | A02 |
| IMP001 | 040.011.1107.1739 |

* 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: USR001  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 devem ser 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 |
| [CPF001]\CopiasSQL | EXECUTANTE: Primavera Windows Services  ORIGEM DOS DADOS: REC001  TIPO: Completo  TIPO DE VERIFICAÇÃO: Visual (data de criação do ficheiro das resultado das cópias) | UTILIZADOR: USR001  PERIODICIDADE: Todos os dias |
| [REC002]\CopiasSQL | EXECUTANTE: Pastas sincronizadas  ORIGEM DOS DADOS:  [CPF001]\CopiasSQL  TIPO: Completo  TIPO DE VERIFICAÇÃO: Visual (data de criação do ficheiro das resultado das cópias) | UTILIZADOR: USR001  PERIODICIDADE: Todos os dias |
| [DEA001] | EXECUTANTE: USR001  ORIGEM DOS DADOS:  [CPF001]\CopiasSQL  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: USR001  PERIODICIDADE: Todas as sextas-feiras |
| [DEA001] | EXECUTANTE: USR001  ORIGEM DOS DADOS:  [CPF001]\Utilizadores\user  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: USR001  PERIODICIDADE: Todas as 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 |
| CPF001 |  |  |
|  | PAR001 | Suporte protocolado |
| IMP001 |  |  |
|  | PAR001 | Suporte protocolado |
|  | PAR003 | Garantia |

* + 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 | 2017-12-13 |
| APP003 | 2018-01-16 |

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 |
| V000035  DATA:  2018-04-04  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 |
| V000034  DATA:  2018-04-04  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 |
| V000033  DATA:  2018-04-04  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: IMP001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000032  DATA:  2018-04-04  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 e REC002.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000031  DATA:  2018-04-04  IMPACTO:  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..  DISPOSITIVOS: DEA001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000030  DATA:  2018-04-04  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.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000029  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000028  DATA:  2018-04-04  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.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000027  DATA:  2018-04-04  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 |
| V000026  DATA:  2018-04-04  IMPACTO:  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.  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000025  DATA:  2018-04-04  IMPACTO:  Critico | 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.  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000024  DATA:  2018-04-04  IMPACTO:  Critico | 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.  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000023  DATA:  2018-04-04  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 (APP004 - SQL Server 2014).  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000022  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000021  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000020  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000019  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000018  DATA:  2018-04-04  IMPACTO:  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.  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000017  DATA:  2018-04-04  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.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000016  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V0000015  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V0000014  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000013  DATA:  2018-04-04  IMPACTO:  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 (Windows 8.1).  DISPOSITIVOS: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000012  DATA:  2018-04-04  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: CPF001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000011  DATA:  2018-04-04  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 |
| V0000010  DATA:  2018-04-04  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 |
| V000009  DATA:  2018-04-04  IMPACTO:  Critico | 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 |
| V000008  DATA:  2018-04-04  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 |
| V000007  DATA:  2018-04-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000006  DATA:  2018-04-04  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 |
| V000005  DATA:  2018-04-04  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 |
| V000004  DATA:  2018-04-04  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 |
| V000003  DATA:  2018-04-04  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 |
| V000002  DATA:  2018-04-04  IMPACTO:  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.  DISPOSITIVOS: ESS001.  DATA DE RESOLUÇÃO: (vazio) | Pendente |
| V000001  DATA:  2018-04-04  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 |

* + 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 |
| V000036  DATA:  2018-04-04  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: CPP001.  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) |