ATA DE AUDITORIA DE REVISÃO

SPRINT: «*intervalo do sprint*»

NÚMERO: «*numero da ata*»

DATA: «*data*»

Aos «*data por extenso*», na sede da empresa «*nome da empresa*» (ORGANIZAÇÃO), na «*morada*», freguesia de «*freguesia*», concelho de «*concelho*», estiveram reunidas «*nome do gerente*» e «*nome do auditor*» na qualidade de gerente (RESPONSÁVEL PELO TRATAMENTO) e auditora (AUDITOR) respetivamente.

A reunião teve como objetivo apresentar os resultados obtidos com a auditoria de revisão interna efetuada ao sistema informático da ORGANIZAÇÃO, levada a cabo a seis de junho de dois mil e dezoito, considerando as regras e objetivos definidos no Regulamento de Sistema elaborado e aprovado pelo RESPONSÁVEL PELO TRATAMENTO. Com esta auditoria, pretende-se dar continuidade à implementação de regras e boas práticas conducentes à conformidade com o Regulamento Geral de Proteção de Dados (RGPD), demonstrando a preocupação da ORGANIZAÇÃO e do RESPONSÁVEL PELO TRATAMENTO com a segurança, privacidade e integridade dos dados e com a disponibilidade do sistema informático.

Posto isto, a reunião teve como base a seguinte ordem de trabalhos:

**Ponto 1** – Resumo das vulnerabilidades identificadas na auditoria anterior, fazendo referência às vulnerabilidades corrigidas e não corrigidas, frisando o impacto que podem significar ao nível da segurança ou disponibilidade do SISTEMA.

**Ponto 2** – Analisar as novas vulnerabilidades identificadas durante a auditoria realizada e respetivas medidas corretivas propostas.

**Ponto 3** – Verificar e analisar acidentes de violação de dados ocorridos no sprint em auditoria.

**Ponto 4** – Verificar o cumprimento dos compromissos do sprint anterior e compilar os compromissos de cronograma identificados que devem ser atendidos até à próxima auditoria.

**Ponto 5** – Agendar a próxima auditoria de revisão.

Assumiu a presidência da reunião o AUDITOR, que deu início aos trabalhos, passando a ser analisados e discutidos pela ordem indicada.

**Ponto 1** – O AUDITOR, começou por apresentar ao RESPONSÁVEL PELO TRATAMENTO o resumo das vulnerabilidades detetadas no SISTEMA durante a auditoria anterior, que foram alvo das medidas corretivas propostas e as vulnerabilidades que permaneceram em estado pendente.

De cinquenta e quatro vulnerabilidades detetadas no sistema informático na auditoria de diagnóstico, foram corrigidas dezasseis vulnerabilidades, ficando ainda em estado pendente trinta e quatro, vinte e três de categoria crítica e quinze de categoria severa. Duas das vulnerabilidades identificadas foram assumidas como necessárias pelo RESPONSÁVEL PELO TRATAMENTO, sendo que outras duas encontram-se em estado pendente com medidas de mitigação de risco provisórias implementadas. Foi verificado ainda que, parte das vulnerabilidades em estado pendente encontram-se já implementadas em alguns dos equipamentos da ORGANIZAÇÃO, nomeadamente no que se refere à alteração das palavra-chave e excesso de privilégios de utilizadores.

De entre as vulnerabilidades não corrigidas, salientou as que considerou necessário dar mais enfase, as quais são apresentadas de seguida:

* Verificou-se que os utilizadores continuam a utilizar mecanismos automáticos para guardar palavras-chave de forma a facilitar o acesso a *sites* ou recursos nos dispositivos. O AUDITOR alertou que, no caso de invasão do computador, estas autenticações automáticas facilitam o acesso descontrolado à informação desses sites ou recursos. Sensibilizou ainda, para o facto de as palavras-chave guardadas pertencerem a clientes da ORGANIZAÇÃO e que no caso de um incidente de violação de dados, estes seriam lesados, o que provocaria danos graves para a imagem da ORGANIZAÇÃO. Para o caso de assumir esta vulnerabilidade como necessária para as operações da ORGANIZAÇÃO, o AUDITOR informou que existe software gratuito para gestão de credenciais de utilizador, pelo que se recomenda a consulta ao administrador do sistema para mitigar o risco. No entanto, existem ferramentas incluídas nas licenças de antivírus, que são consideradas mais seguras e mais usáveis, pelo que na próxima renovação do antivírus, foi recomendado a substituição do *software*.
* A versão do *firmware* dos computadores encontram-se desatualizadas. Embora a correção desta vulnerabilidade possa deixar o equipamento inoperável, recomenda-se aconselhamento do administrador do sistema, com objetivo de medir o risco deste facto acontecer e de forma a equacionar a hipótese de considera-la como assumida.
* Verificou-se que ainda não foram implementados quaisquer mecanismos de controlo de DEA nos dispositivos existentes. Da mesma forma que no ponto anterior, na próxima renovação do antivírus instalado, recomenda-se a aquisição de *software* que controle o uso deste tipo de dispositivos nos equipamentos.
* Existem dispositivos que saem fora da esfera física da ORGANIZAÇÃO, cujo conteúdo pode ser alvo de consulta não autorizada por terceiros. Recomenda-se o uso de um *software* que coloque a informação contida nestes dispositivos ilegível, ou seja cifrada. De notar que existe software gratuito para proceder à encriptação desta informação.
* Foram tomadas medidas temporárias para mitigação de risco relativo a acessos externos autorizados. No entanto, de forma a garantir que o risco seja reduzido, recomendou-se a implementação de uma VPN (rede virtual privada) para este tido de acesso. Verificou-se ainda que a porta de acesso remoto do CPF002 (ver Caracterização do Sistema) encontra-se aberta, e que, uma vez não autorizado o acesso remoto a este equipamento, deve-se solicitar ao administrador do sistema que esta seja fechada.
* Verificou-se que foi implementada uma *firewall* para gestão exclusiva da rede interna da ORGANIZAÇÃO. No entanto, verificou-se que a sua configuração ainda permite que qualquer equipamento se consiga ligar à rede através de fio. Recomenda-se que o administrador do sistema, configure a *firewall* de modo a permitir que somente os equipamentos registados na Caracterização do Sistema se possam ligar à rede sem fios.
* Continuam a existir ficheiros nos computadores dos utilizadores com necessidade de avaliação quanto à sua necessidade de manutenção no sistema ou que não são alvo de cópias de segurança. A existência de informação em excesso e dispersa no sistema dificulta o cumprimento de obrigações legais por parte da ORGANIZAÇÃO. Recomenda-se que seja seguida a estratégia de recursos definida no Regulamento de Sistema e que apenas sejam mantidos os ficheiros necessários, e se necessários que sejam colocados num repositório centralizado (servidor) alvo de cópias de segurança de forma a promover o bom funcionamento da ORGANIZAÇÃO.

Ainda das vulnerabilidades detetadas na auditoria anterior, duas foram assumidas como necessárias de existir pelo RESPONSÁVEL PELO TRATAMENTO de dados, tendo este justificado esta necessidade expondo o seguinte:

* O facto de não existir nenhum dispositivo que funcione como primeiro nível de proteção de infraestrutura e, embora os computadores do SISTEMA estejam protegidos com aplicações de segurança de sistema operativo, o RESPONSÁVEL PELO TRATAMENTO reconhece a importância da 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 informático. No entanto, o custo de implementação para resolução desta vulnerabilidade é demasiado elevado para a ORGANIZAÇÃO, tendo já sido tomadas outras medidas de mitigação deste risco, tais como implementação de uma *firewall* com administração interna exclusiva.
* Atendendo ao facto que o servidor em produção na ORGANIZAÇÃO não está abrangido por garantia ou contrato de suporte do fabricante, e uma avaria pode condicionar ou inviabilizar o acesso às aplicações ou dados existentes no mesmo, o RESPONSÁVEL PELO TRATAMENTO assume que o mesmo é alvo de manutenção permanente e encontra-se instalado num ambiente adequado que promove o seu bom funcionamento e a sua durabilidade. Assume ainda que, assim que aconselhável pelo administrador do sistema, este equipamento será substituído.

As vulnerabilidades assumidas acima identificadas voltarão a ser reavaliadas deste ponto a um ano.

A implementação das medidas corretivas propostas para correção das vulnerabilidades identificadas no sistema informático foi superior a trinta e cinco por cento, o que demonstra a preocupação e a importância que a ORGANIZAÇÃO entrega à segurança, integridade e disponibilidade dos dados pelos quais é responsável. Desta forma, pode-se concluir que a ORGANIZAÇÃO está no bom caminho à conformidade com o RGPD.

**Ponto 2** – Durante a auditoria efetuada, não foram detetadas novas vulnerabilidades no sistema informático.

**Ponto 3** – Durante a auditoria efetuada, não foram registados quaisquer acidentes de violação de dados pessoais.

**Ponto 4** – Tendo por base o Regulamento de Sistema e o cronograma do DSPI, o AUDITOR informou o RESPONSÁVEL PELO TRATAMENTO acerca dos compromissos a atender até à data auditoria seguinte:

* Limpar dados das cópias de segurança;
* Mudar as palavras-chave de utilizador nos computadores (CPF002, CPF003, CPF004 e SVR001);
* Mudar as palavras-chave de configuração do dispositivo de infraestrutura ESS001;
* Mudar a palavra-chave de acesso à rede *wi-fi*.
* Substituir consumíveis do CPF001, CPF002, CPF003 e CPF004.

Relativamente aos compromissos agendados para o sprint em auditoria, foram avaliadas a regras de exceção à rede e que foram alteradas as palavras-chave do CPF001 e CPP001, não se tendo verificado qualquer intervenção a nível de limpeza de cópias de segurança. A alteração de palavras-chave nos equipamentos ainda pendentes e o compromisso de limpeza de cópias de segurança, passa assim, para compromisso do sprint seguinte.

Relativamente à sugestão de substituição dos consumíveis dos computadores acima identificados, uma vez que não foi adotada, recomenda-se a consulta de opinião ao administrador do sistema relativamente a este compromisso, passando este também para o sprint seguinte.

**Ponto 4** – Como último ponto da agenda, o AUDITOR e o RESPONSÁVEL PELO TRATAMENTO, acordaram que a próxima auditoria ao sistema informático ficaria agendada para o dia dez de setembro de dois mil e dezoito.

Nada mais havendo a tratar, deu-se por encerrada a reunião e dela foi lavrada a presente ata que, depois de lida vai ser assinada por todos os presentes.

«*local*»,, «*dia*», de «*mês*», de «*ano*»,.

O RESPONSÁVEL PELO TRATAMENTO,

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

O AUDITOR,

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

FIM