ATA DE AUDITORIA DE DIAGNÓSTICO

NÚMERO: UNICA

DATA: 2018-04-04

Aos quatro dias do mês de abril do ano dois mil e dezoito, na sede da empresa Ancecont - Contabilidades, Lda. (ORGANIZAÇÃO), na Rua Dom Afonso Henrique, 59 Letra L Loja 5, freguesia de Arcozelo, concelho de Barcelos, estiveram reunidas Angelina Duarte e Marta Martinho na qualidade de gerente (RESPONSÁVEL PELO TRATAMENTO) e auditora (AUDITOR) respetivamente.

A reunião teve como objetivo apresentar os resultados obtidos com a auditoria de diagnóstico interna efetuada ao sistema informático da organização, levada a cabo entre catorze de março de dois mil e dezoito, e vinte e um de março 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 início 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** – Apresentar o Dossier de Segurança e Privacidade Informática (DSPI) cuja abertura ocorreu durante o levantamento efetuado no decurso do diagnóstico inicial.

**Ponto 2** – Analisar as vulnerabilidades identificadas durante a auditoria do diagnóstico inicial e respetivas medidas corretivas propostas.

**Ponto 3** – Compilar os compromissos de cronograma identificados que devem ser atendidos até à próxima auditoria.

**Ponto 4** – Atribuir responsabilidades de registo a utilizadores do sistema.

**Ponto 5** – Aprovar autorizações relacionadas com o sistema informático.

**Ponto 6** – Avaliação de necessidade e nomeação de DPO para a ORGANIZAÇÃO.

**Ponto 7** – Agendar a primeira 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 DSPI resultante do diagnóstico efetuado ao sistema informático, descrevendo todos os trabalhos desenvolvidos e resultados obtidos.

Este trabalho iniciou com o levantamento da arquitetura do sistema, tendo sido registada toda a informação e características dos dispositivos identificados.

De seguida procedeu-se à exploração e análise de cada dispositivo, de forma a tentar extrair vulnerabilidades que pudessem ter impacto na segurança, privacidade, integridade e disponibilidade dos dados e do sistema, tendo em conta o estipulado no Regulamento de Sistema.

Depois de identificadas as vulnerabilidades, foi desenvolvido o DSPI, onde constam todas as especificações dos dispositivos, recursos, utilizadores, parceiros e outros aspetos importantes que compõem o sistema. Além desta informação, o DSPI irá agregar toda a informação relativa às auditorias internas ou externas que podem vir a acontecer (e.g. relatórios, novas vulnerabilidades, novas medidas corretivas, etc.).

O AUDITOR, depois de explicar a organização do documento, fechou este ponto salientando a importância do DSPI para demonstrar a preocupação da ORGANIZAÇÃO em cumprir o Regulamento de Sistema, com o objetivo de promover a conformidade com o RGPD. O DSPI documenta todo o caminho percorrido pela ORGANIZAÇÃO rumo à conformidade com o RGPD.

**Ponto 2** – Durante a auditoria de diagnóstico efetuada, fez-se uma análise a cada equipamento informático existente nas instalações da organização, com o objetivo de encontrar vulnerabilidades que comprometessem a segurança, privacidade e disponibilidade de dados.

Como resultado e em resumo, o AUDITOR informou que, no processo de auditoria, foram identificadas cinquenta e quatro vulnerabilidades no sistema informático, as quais podem ser consultadas do DSPI redigido para a organização. Das vulnerabilidades identificadas, vinte e três foram consideradas severas, tendo o AUDITOR, enfatizado a necessidade de resolução ou mitigação imediata das mesmas. As restantes trinta e uma foram consideradas críticas, havendo necessidade de serem resolvidas logo que possível.

Para todas as vulnerabilidades identificas, foram sugeridas as medidas corretivas consideradas mais adequadas para a sua mitigação ou correção definitiva.

De entre as vulnerabilidades identificadas, foram discutidas as que poderiam necessitar de consciencialização dos utilizadores na utilização do sistema. O AUDITOR recomendou formação com o objetivo de os consciencializar para os riscos de comportamentos como os apresentados de seguida:

* Existem ficheiros nos computadores dos utilizadores com necessidade de avaliação quanto à sua necessidade de manutenção no sistema. A existência de informação em excesso 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 ao funcionamento da ORGANIZAÇÃO.
* Existem dispositivos cujo nome identifica o utilizador direta ou indiretamente. Sabendo quem trabalha com cada dispositivo, torna-se mais fácil um ataque direcionado. Recomenda-se a anonimização do nome dos dispositivos com o objetivo de dificultar a sua procura em caso de invasão de sistema.
* Os utilizadores ou não usam palavra-chave para se autenticarem no sistema operativo ou esta é demasiado fraca. Os utilizadores devem autenticar-se com uma palavra-chave e estas devem ser complexas de forma a dificultar acessos não autorizados ao sistema.
* Todos os utilizadores têm privilégios de administrador no sistema operativo, permitindo que estes possam reconfigurar aplicações e configurações pondo em risco todo o sistema.
* Existem computadores que não bloqueiam automaticamente a sessão de trabalho ao fim de algum tempo de inatividade. De acordo com o Regulamento de Sistema, os computadores devem bloquear ao fim de cinco minutos de inatividade, tendo o utilizador de se autenticar novamente no sistema para retomar a sessão.
* Os utilizadores devem apenas usar as contas de e-mail profissionais para o cumprimento das suas tarefas. Deve-se promover que estas contas de e-mail sejam anonimizadas e que se cumpram as boas práticas respeitantes à não utilização de e-mails para fins não profissionais.
* Existem computadores que não têm qualquer proteção contra *malware* e outros cujas aplicações de segurança não estão atualizadas. Deve-se promover que todos os dispositivos estejam protegidos com aplicações de segurança, e consciencializar os utilizadores a efetuarem as atualizações das aplicações de segurança sempre que necessário.

Depois de discutidas estas e as restantes vulnerabilidades identificadas, estabeleceu-se que até à próxima auditora deveriam ser resolvidas as vulnerabilidades que não exigissem um grande esforço financeiro por parte da empresa, dando prioridade às que significassem mais risco para o sistema e para a ORGANIZAÇÃO.

Relativamente à aquisição de aplicações de segurança (cf. encriptador de ficheiros e controlador de dispositivos externos de armazenamento), e aquisição de um dispositivo para implementação de uma barreira adicional de acesso ao sistema a partir da internet, decidiu-se fazer o investimento de forma faseada no tempo.

**Ponto 3** – 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 da auditoria seguinte:

* Limpar dados das cópias de segurança;
* Reavaliar as regras de exceção de acesso à rede;
* Mudar as palavras-chave de utilizador nos computadores;
* Substituir consumíveis do CPF001, CPF002, CPF003 e CPF004.

**Ponto 4** – Sendo esta a primeira auditoria e havendo a necessidade de cumprir com o estabelecido no Plano de Segurança e Disponibilidade (PSD) do DSPI, procedeu-se à atribuição de responsabilidades de registo aos colaboradores da ORGANIZAÇÃO.

Assim, o RESPONSÁVEL PELO TRATAMENTO decidiu que o USR002 (ver Caracterização do Sistema no DSPI) ficaria responsável por fazer e verificar as cópias de segurança, e monitorizar o equipamento de redundância elétrica. Decidiu também que estas tarefas deveriam ser realizadas todas as sextas-feiras ao final da tarde.

O AUDITOR salientou a importância que estes compromissos têm para a segurança e disponibilidade do sistema, enfatizando a necessidade de se cumprir com zelo as responsabilidades atribuídas.

**Ponto 5** – Apesar de a utilização de alguns dispositivos aumentarem o nível de vulnerabilidade ao sistema, o RESPONSÁVEL PELO TRATAMENTO considerou necessário autorizar a existência de alguns, justificando a sua decisão, e solicitando que sejam tomadas as medidas possíveis para mitigação dos riscos envolvidos. Uma vez identificados e enumerados pelo AUDITOR, O RESPONSÁVEL PELO TRATAMENTO autorizou justificando a utilização dos seguintes dispositivos no sistema:

* O DEA001 (ver Caracterização do Sistema no DSPI), está autorizado a ser utilizado pelo USR002 no SRV001, uma vez que é utilizado para cópias de segurança das bases de dados onde consta a informação operacional do ERP Primavera e dos restantes ficheiros de suporte operacional da ORGANIZAÇÃO.
* O DEA002 (ver Caracterização do Sistema no DSPI), está autorizado a ser utilizado pelo USR001 no CPF001, sendo usado para dados manipular do foro privado deste utilizador.
* Os recursos REC001 e REC002 (ver Caracterização do Sistema no DSPI), podem ser acedidos pelos utilizadores USR001, USR002 e USR003, por ser considerados necessários para que estes colaboradores possam desempenhar as suas funções na ORGANIZAÇÃO. Nestes recursos constam as bases de dados operacionais do ERP Primavera e os ficheiros operacionais da ORGANIZAÇÃO aos quais os utilizadores devem ficar com permissões de leitura e escrita.
* O CPF001 (ver Caracterização do Sistema no DSPI), está autorizado a ser acedido externamente pelo utilizador pelo USR001, com o objetivo de poder aceder à informação operacional fora das instalações da ORGANIZAÇÃO.
* O USR001 (ver Caracterização do Sistema no DSPI), está autorizado mover o CPP001 para fora das instalações da ORGANIZAÇÃO, de forma a ser usado como dispositivo para acesso remoto ao CPF001 aquando fora das instalações da ORGANIZAÇÃO.

Apesar dos riscos associados à mobilidade dos dispositivos externos de armazenamento, o AUDITOR defendeu a necessidade de existirem cópias de segurança *offsite* (i.e. deslocalizadas do espaço físico da ORGANIZAÇÃO) com o objetivo de prevenir roubos e incêndios.

**Ponto 6** – Tendo por base o RGPD, o RESPONSÁVEL PELO TRATAMENTOS não considerou necessário nomear um DPO para a ORGANIZAÇÃO.

**Ponto 7** – 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 um de junho 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.

Barcelos, 4 de abril de 2018.

O RESPONSÁVEL PELO TRATAMENTO,

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

O AUDITOR,

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

FIM