E-fólio B | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Sistemas Computacionais

CÓDIGO: 21174

DOCENTE: Vitor Rocio

A preencher pelo estudante

NOME: Ricardo Ferreira da Conceição Dias Marques

N.º DE ESTUDANTE: 1100281

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 28 de janeiro de 2019

TRABALHO / RESOLUÇÃO:

a) Gestão de utilizadores;

As contas de utilizador, para autenticação e acesso às respetivas estações de trabalho, dos 50 colaboradores da empresa seguradora **deveriam estar registadas num servidor central de serviço de diretório** (tipicamente, num sistema do tipo *Microsoft Active Directory* ou de LDAP). *C*omo é referido em Frisch (2002, pág. 313), está amplamente estabelecido o uso de serviços de diretório (como é o caso do LDAP) para armazenar informação de empregados (incluindo informação das contas associadas de utilizador) e ainda como forma de permitir a autenticação do utilizador em múltiplos sistemas. Se a aplicação centralizada da empresa seguradora o permitisse, seria útil que a autenticação dos utilizadores (colaboradores da seguradora) nessa aplicação usasse o mesmo serviço de diretório.

Uma outra medida seria a definição e a implementação da política de, **quando um funcionário abandona a organização** (empresa seguradora), **proceder à desabilitação (mas NÃO à remoção) das suas contas de utilizador**, por motivos de segurança (para evitar acessos de utilizadores que já não trabalham na organização e/ou por parte de potenciais atacantes que tentem ter acesso ao sistema através de contas de utilizador já não utilizadas). Esta mesma recomendação de desabilitar, mas **SEM** remover, contas de utilizadores que saíram da organização, é dada em Frisch (2002, pág. 254), que argumenta que a conta não deve ser removida, porque o utilizador pode voltar à organização ou outro utilizador que tome o lugar dele pode precisar, em certos casos, de acesso a esses ficheiros.

Outra das medidas seria a definição e a implementação de uma **política de "trancar" automaticamente** (de forma temporária) **as contas de utilizadores para as quais se verifiquem múltiplas tentativas falhadas de autenticação** (o que é sinal de que alguém poderá estar a querer aceder ilegitimamente ao sistema, usando a conta desse utilizador). Este mecanismo é referido, por exemplo em Frisch (2002, pág. 288): "*Automatic account locking after too many failed login attempts".*

b) Segurança e confidencialidade;

Algumas das políticas que indiquei, na resposta à alínea "a)" sobre "*Gestão de utilizadores*" são também, ao mesmo tempo, políticas de segurança.

Adicionalmente – como forma de aumentar os níveis de segurança e de proteger a **confidencialidade** – deveria ser definido um **sistema de autorizações**, associado a perfis / grupos de contas de utilizador, de forma a que cada utilizador apenas aceda aos dados a que deva aceder. Uma implementação típica assenta em ***Access Control Lists (ACLs)*** que, como é referido em Frisch (2002, pág. 353), permitem dar acesso a ficheiros para

utilizadores individuais e/ou grupos de utilizadores. Além disso, outra medida poderia ser, para os dados que sejam classificados como sendo "sensíveis" (como serão os dados dos clientes de uma seguradora), que os mesmos sejam protegidos por **mecanismos de cifra** (***encryption***) – vide, por exemplo, Frisch (2002, pág. 362). Quanto à aplicação centralizada, a viabilidade desta medida de cifra de dados (caso não esteja já implementada), poderá depender, nalguns casos, da forma como a aplicação esteja desenvolvida e, caso a aplicação tenha sido desenvolvida por uma empresa externa, do que o contrato associado permitir em termos de desenvolvimentos adicionais. Dito isso, existem **tecnologias de Bases de Dados** que permitem a **cifra de dados de forma transparente**, como é, por exemplo, o caso da "***T**ransparent **D**ata **E**ncryption"* (TDE) disponível nos motores de Bases de Dados "*Microsoft SQL Server*" e "*Oracle*" - vide Microsoft (2019) e Oracle (2019).

Naturalmente, os Administradores do Sistema deverão respeitar o "**Código de Ética dos Administradores de Sistemas**" (USENIX, 2006) e, neste campo em particular, os requisitos da secção de Privacidade *("**Privacy**"*), em particular as obrigações de os administradores de sistemas acederem a dados privados **apenas** quando as suas tarefas técnicas assim o exigirem e de manter e proteger a confidencialidade da informação a que tenham acesso.

c) Gestão de recursos computacionais;

Deverá haver alguma **standardização do parque informático** das estações de trabalho (*workstations*) dos 50 colaboradores, de forma a facilitar a sua gestão.

Uma das medidas a implementar poderia ser a criação de uma ***checklist* com os passos a realizar na instalação de *software* de uma nova estação de trabalho**. Tal como é referido, por exemplo em Limoncelli et al. (2007), uma boa *checklist* é útil mesmo quando a instalação do Sistema Operativo possa ser completamente automatizada, porque há sempre tarefas associadas que não podem ser automatizadas, por envolverem atos físicos (como seja, por exemplo, testar que o computador imprime bem para a impressora que esteja predefinida – aplicável no caso do enunciado).

No que diz respeito à componente, referida no enunciado, do arquivo pessoal de ficheiros digitais, uma outra medida possível seria a **implementação de uma política de quotas de utilização de espaço em disco** por utilizador (em particular no que diga respeito a *file shares* de rede), de acordo com o espaço em disco disponível - tal como é sugerido, por exemplo, em Frisch (2002, pág. 1012).

d) Ambiente de trabalho e ferramentas do administrador;

Uma medida será a definição e instalação das ferramentas do administrador necessárias para a administração do parque informático.

Frisch (2002, pág. 2) refere que a **automação** continua a ser a salvação do administrador (“*Automation is still the administrator’s salvation*”). Um dos aspetos importantes de automação – e que também é **outra medida** que proponho neste trabalho – diz respeito ao uso de ferramentas de **automação de instalação do S.O.** (Sistema Operativo)**,** em particular, para as estações de trabalho de novos colaboradores**.** Por exemplo, Limoncelli (2007, pág. 32), refere que qualquer S.O. moderno tem uma forma para automatizar a sua instalação que, normalmente, consiste em fazer *boot* a partir da estação de trabalho e que faz *download* de um programa de um servidor que prepara (particiona e formata) o disco, instala o sistema operativo, as aplicações e instala *scripts* localizados de instalação. No caso do nosso enunciado, alguns desses ***scripts* localizados a desenvolver** provavelmente dirão respeito, entre outros aspetos, à **configuração, no Sistema Operativo das estações de trabalho, das impressoras e digitalizadores (*scanners*).**

e) Gestão de dados e ficheiros.

O enunciado do trabalho refere que os utilizadores (50 colaboradores da empresa seguradora) podem fazer o “arquivo pessoal dos respetivos ficheiros digitais”. Para além disso, a aplicação centralizada da seguradora terá os dados dos clientes da seguradora. Em ambos os casos, uma medida muito importante é a **realização de *backups***.

Uma **medida possível** de política é disponibilizar uma ***share* pessoal de rede a cada colaborador** (visível / “mapeada” para a sua estação de trabalho) e informar os colaboradores que os ficheiros que eles queiram que sejam salvaguardados (como seja o tal “arquivo pessoal dos respetivos ficheiros digitais”) deverão ser colocados nessa pasta de rede. Essa medida centraliza os ficheiros num servidor ou até num *cluster* de servidores (o que aumenta os níveis de resiliência a eventuais falhas de *hardware*) e facilita a salvaguarda dos ficheiros / dados, face à alternativa de manter esses ficheiros em cada *workstation*.

Assim, **uma outra medida** importante associada seria a criação de um **plano de *backups*** (ou de “salvaguardas”). Frisch (2002, págs. 708-709) refere que esse plano deverá dar resposta às seguintes questões: Que ficheiros precisam de ser salvaguardados? Qual é a sua localização? Quem vai salvaguardá-los? Onde, quando e como é que os *backups* devem ser realizados? Qual é a frequência com que os ficheiros são alterados? Quão depressa temos de restaurar um ficheiro importante que desapareça ou fique danificado? Durante quanto tempo temos de guardar os ficheiros salvaguardados? Para onde vamos restaurar os ficheiros salvaguardados (para o sistema original e/ou para algum outro destino)?

Referências Bibliográficas

Frisch, Aeleen (2002). *Essential System Administration*. O'Reilly

Limoncelli, Thomas A. et al. (2007). *The practice of system and network administration*. 2nd Edition, Addison-Wesley

Microsoft (2019). "*Transparent Data Encryption (TDE) - SQL Server | Microsoft Docs*". https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sqlallproducts-allversions

Oracle (2019). "*Database Advanced Security Administrator's Guide - Transparent Data Encryption".https://docs.oracle.com/cd/B19306_01/network.102/b14268/asotrans.htm#ASOAG600*

Patterson, David & Hennessy, David (2011) *Computer Organization and Design.* revised 4th edition. Morgan Kaufmann

USENIX (2006). *The System Administrators' Code of Ethics.* https://lopsa.org/CodeOfEthics