Uma discussão sobre "acessibilidade e segurança para o sucesso das organizações" …

José Borbinha
INESC-ID / Instituto Superior Técnico
jlb@tecnico.ulisboa.pt

Resumo

Considerando acessibilidade como sendo a garantia de acesso à informação, propomos começar por abordar isso aqui numa perspetiva da segurança de informação, evocando a chamada tríade da confidencialidade, integridade e disponibilidade ("CIA" na literatura de língua inglesa, de "Confidentiality, Integrity and Availability").

Confidencialidade é o objetivo de que apenas os atores quem têm necessidade legítima para acesso à informação tem isso previsto, implicando que tentativas de acesso por outros devem ser consideradas ilegítimas, e assim prevenidas (tal engloba os objetivos do RGPD, mas pode ser mais vasto que apenas a privacidade, considerando por exemplo, segredos de negócio, etc.).

Integridade implica que a informação acedida pelos atores é verdadeira, sendo o que diz ser e se foi alterada isso está devidamente assinalado, e é a adequada, isto é, corresponde ao que diz ser.

Disponibilidade é a garantia de que a informação está acessível aos atores quando necessário e numa forma em que pode ser usufruída (quando isto é referido em relação a atores com necessidades especiais de, por exemplo, visão ou som, tal é geralmente também referido como "acessibilidade", mas aqui estamos usando esse termo num significado mais vasto).

Aborda esta tríade no âmbito de uma organização grande ou média com foco apenas nas operações não basta. A complexidade do desafio implica um foco especial no planeamento das atividades e dos recursos para que os objetivos sejam atingidos da forma mais efetiva e eficiente possível, ao que chamamos gestão. Isto é, precisamos agir com base em conhecimento explícito e partilhado, e não em conhecimento e implícito e "experiência prática".

Somos assim levados a considerar os chamados "sistemas de gestão", o que em relação à qualidade nos faz recordar a norma ISO 9001. Em relação à segurança de informação, a referência atual é a ISO 2701. Referenciais deste tipo são especialmente importantes quando o desafio é colocado em cenários com fortes requisitos de conformidade. Entendendo conformidade como o estado em que estamos em relação a especificações ou regulamentações estabelecidas, o que raramente é garantido, o desafio geralmente apresenta-se como o de se ter a consciência do estado em que se está, o que falta para o ideal, o que decidir em relação a isso (ação urgente? planear a prazo? aceitar e nada fazer?) e como se explica isso. A isso costuma chama-se maturidade, tema para se abordar também em relação a esta discussão.

No entanto nada disto será efetivo sem o papel da governança da organização. Isto é, esses objetivos devem ser assumidos de forma clara pelas estruturas de topo da organização, que devem disponibilizar os recursos necessários e mandatar os agentes internos que devem tornar isso realidade. Sendo os recursos sempre limitados, é necessário ser claro nos objetivos e expetativas que se geram de acordo com isso, o que se costuma chama "alinhamento".

Finalmente, uma última palavra ao tema da capacitação, sem a qual tudo não passa de palavras sem significado, o que irá ser ilustrado num exemplo concreto em relação à preservação digital, um aspeto muito particular deste tema.