Imagem: Freepik.com / evening_tao

ISO 27001: O PODER DA INFORMAÇÃO ASSENTA NA SEGURANÇA

POR MARIA BEATRIZ FERNANDES

O COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO ESTÁ UNIFICADO NA NORMA ISO 27001, QUE AJUDA A MITIGAR E GERIR O RISCO TECNOLÓGICO DAS ORGANIZAÇÕES DE FORMA CONTINUADA.

Entre tecnologias de ponta, sistemas e processos complexos e mercados polivalentes, a informação é o fator comum que dá corpo às infraestruturas societais e um dos maiores recursos que desenham as operações diárias das organizações. Seja no setor público ou privado, a informação suporta uma grande variedade de processos pelo que a confidencialidade deve ser assegurada por todas as partes integrantes do negócio.

A segurança da informação é repartida em três grandes pilares - confidencialidade, integridade e disponibilidade - que ajudam a proteger as organizações de potenciais riscos. Assim, não basta implementar processos seguros; é uma prioridade sensibilizar as partes integrantes para o significado de segurança da informação.

O compromisso com a segurança da informação foi unificado na reconhecida ISO 27001, norma que ajuda as organizações a definir, adotar e manter um Sistema de Gestão de Segurança de Informação (SGSI). A matéria passa por um CISO que vai fazer a gestão do programa.

Tendo em conta que os processos de gestão e operação da segurança de informação não estão sistematizados dentro das organizações, são necessárias facilitadoras da certificação. A Integrity presta serviços de consultoria na preparação e implementação da norma. Com uma certificação ativa, a empresa presta ainda serviços de índole continuada, porque "a segurança não pode ser um projeto, mas um processo", afirma Aurélio Maia, Consulting Service Director na Integrity, completando que as práticas implementadas "têm que ser interiorizadas na cultura da organização".


AURÉLIO MAIA, INTEGRITY

IMPLEMENTAR E LANÇAR DIRETRIZES

Segundo Maia, o ISO 27001 pode ser dividido em três componentes. Em primeiro lu-

gar, a componente documental, pelo que são "elaboradas e operacionalizadas as políticas e procedimentos dos registos". A segunda componente define a metodologia de gestão de risco e a respetiva operacionalização na organização", em duas fases - uma de avaliação de risco e uma de tratamento, que passa por entender e enquadrar as vulnerabilidades da organização em causa e, a partir daí, seguir um caminho sustentável de melhoria contínua, em que, em função dos riscos, se implementa um conjunto de controlos tecnológicos, organizacionais e humanos.


BRUNO MARQUES, CIIWA

A SEGURANÇA DA INFORMAÇÃO É REPARTIDA EM TRÊS GRANDES PILARES - CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE - QUE AJUDAM A PROTEGER AS ORGANIZAÇÕES DE POTENCIAIS RISCOS

Por último, a terceira componente diz respeito ao "conjunto das atividades de gestão e operação, que têm uma realimentação para a gestão de risco", fazendo a "medição da eficácia e da eficiência das ações em curso".

O *roadmap* de implementação tem como requisito uma auditoria ao sistema, para detetar possíveis falhas, que, segundo Maia, são "naturais que ocorram" porque "não há sistemas perfeitos". Reitera, ainda, que se não houver não conformidades "é um sinal de que o sistema não está bem operacionalizado, porque são sempre as não conformidades os gatilhos da melhoria dos próprios sistemas - é uma prova de maturidade".

A norma não certifica tecnologias, locais ou grupos de pessoas, mas um ou vários processos de gestão e operação, que variam consoante a natureza do negócio da organização. A Integrity advoga "que se deve começar por um processo mais simples e eventualmente aumentar o âmbito", uma vez que "é mais fácil evoluir do que implementar um sistema enorme à partida".

Tradicionalmente, os âmbitos são definidos pelas localizações onde o processo assenta a atividade, as pessoas envolvidas e "as unida-

des de proteção". Apesar de existir um conjunto de vantagens garantidas pela norma, também existe uma série de "inércias" que as organizações encontram na implementação e a definição do âmbito constitui um dos primeiros desafios.

VALOR E INÉRCIA

Numa segunda instância, o compromisso da gestão de topo pelo projeto - que a norma define como requisito - costuma causar constrangimentos. Bruno Marques, Vice-Presidente da Direção da CIIWA – que oferece cursos de formação para o ISO 27001 –, acredita que o processo depende da "adesão e sensibilização desde a gestão de topo", pelo que "o executivo tem de fazer mudanças de gestão", que atendam à componente das tecnologias da segurança, da privacidade e da transformação digital". Marques conclui que "para termos uma cultura de segurança de informação e gestão de riscos, sem dúvida que a liderança tem que dar o exemplo", numa abordagem *top down*.


RICARDO MADEIRA SIMÕES, CÂMARA MUNICIPAL DA AMADORA

Nos processos de negócio estão envolvidas pessoas que, no dia a dia, não estão habituadas a ter a processos embebidos em segurança da informação. Como tal, os recursos humanos podem causar aquilo que Ricardo Madeira Simões, Chefe de Divisão de Sistemas e TIC da Câmara Municipal da Amadora – que detém a certificação desde 2016 –, define como "resistências internas" e que devem ser ultrapassadas. Contudo, como Bruno Marques diz, "um dos pilares da segurança são as pessoas e as suas competências – que podem ser o elo mais fraco ou o elo mais valioso".

As resistências dependem da perceção da norma: "se é um tema que importa ou se não os mobiliza", explica Marques, assegurando que na experiência da CIIWA "as pessoas estão cada vez mais sensíveis para o tema e aderem muito facilmente". Apesar do esforço acrescido, as equipas "conseguem adequar os comportamentos quando é explicado o enquadramento e quando é passada a mensagem de que a certificação não é apenas um requisito legal, mas que é fundamental para a sociedade, a organização e famílias".

É de notar, ainda, que a disponibilização de recursos garante a capacidade de manter o sistema ativo. Com a certificação a sofrer constantes auditorias internas e externas e a ser renovada a cada três anos, devem existir ferramentas adequadas de suporte.

Alcançar a certificação não é automático e linear. Madeira Simões conta que tiveram

> O COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO FOI UNIFICADO NA RECONHECIDA ISO 27001, NORMA QUE AJUDA AS ORGANIZAÇÕES A DEFINIR, ADOTAR E MANTER UM SISTEMA DE GESTÃO DE SEGURANÇA DE INFORMAÇÃO (SGSI).

de seguir todas as cláusulas da norma que se aplicavam ao âmbito que estabeleceram e à Declaração de Aplicabilidade do ISO 27001, a principal ligação entre a avaliação de riscos e o tratamento e a implementação da segurança da informação.

Para a CM Amadora, o ISO 27001 veio na sequência do ISO 9001 (qualidade de serviço). "Com a experiência que adquirimos, vimos que havia potencial para melhorar as condições do serviço e resolvemos dar um passo à frente e ir para um *standard* especificamente virado para a segurança da informação".

Aos esforços mencionados, acrescem os custos do processo de *setup* do projeto e da própria certificação, que passa por duas fases de auditoria – interna e externa. O custo é contextual e tem de ser calculado em função do volume de negócios, do número de pessoas envolvidas e da maturidade da entidade. Aurélio Maia conta que para o caso da Integrity, o esforço em termos de consultoria é diretamente proporcional ao envolvimento no projeto e "varia entre os 30 mil euros para os projetos mais pequenos e os 120 mil para os maiores". O tempo de implementação pode variar entre os seis meses e um ano.

TRABALHAR PARA UMA ORGANIZAÇÃO RESILIENTE

Avançando para a última fase - a auditoria de certificação - as empresas têm de apresentar evidências de que possuem um conjunto de mecanismos internos em linha com a norma. A segurança e a gestão da privacidade são pilares de confiança do mercado e "as empresas que não entrarem no jogo correm o risco de ficar sem mercados significativos", explica Marques, acrescentando que "o certificado é mais importante do que nunca porque há dois *drivers*. Por um lado, a resposta operacional que a pandemia criou nas empresas" e, por outro, "o fator de confiança que é necessário transparecer para o mercado".

A ISO 27001 é uma arma de competição e serve como "uma *baseline* para os negócios", infere o representante da CIIWA. O certificado acaba por ser parte integrante da sobrevivência e do crescimento do negócio, uma mais-valia para todo o ecossistema e "sem dúvida que se ganha mais credibilidade e reputação" e acrescenta valor às organizações.