Exercício de auditoria ISO27k

Material de Anotações

Estas são modelos de respostas do exercício de auditoria ISO27k. Você pode não concordar com as sugestões e provavelmente está certo. Justamente, porque, cada contexto organizacional, pode modificar vários pontos avaliados (ex: vários riscos identificados e controles necessários por um escritório pequeno de advocacia serão diferentes, por exemplo, de um escritório maior e com mais maturidade).

Lembrete: o objetivo deste exercício é praticar o processo e refinar suas habilidades de auditoria por meio deste aprendizado.

Ao longo da tabela você encontrará diversas anotações.

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impactos	Recomendações
1. Os critérios usados para avaliar os riscos não são atualizados desde o ano passado	6.1.2 (a)(1)	**NC**	Os critérios usados e os próprios riscos avaliados podem não refletir a situação atual do negócio	Revisar os critérios antes do fim do ano
2. O acesso a uma pasta que deveria ser restrita está sendo compartilhada com todos na organização	A.9.2.2	**nc**	Falta de rastreabilidade se algum acesso não autorizado acontecer	Criar/Melhorar a Política de Controle de Acesso dando clareza de quem é responsável por atribuir os acessos a recursos de informação; implementar a política por meio de procedimentos que garantam que os acessos serão atribuídos individualmente

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impactos	Recomendações
3. Auditoria de campo indica que a conscientização no departamento de segurança é baixa (abaixo de 50%, usando como base a própria métrica da organização)	7.3 + A7.2.2	**NC/nc** (auditor decide conforme qualidade das informações apresentadas)	Com conscientização e treinamentos insuficientes, colaboradores tornam-se mais vulneráveis (são alvos fáceis!) para phishing/engenharia social/ malwares, fraudes e etc e são mais prováveis de não respeitarem políticas	Garanta que treinamentos/conscientização sejam fornecidos periodicamente para os colaboradores, de acordo com as necessidades da organização e de cada pessoa; use avaliações, surveys e outras métricas para direcionar o entendimento e redução de vulnerabilidades; ajuste o conteúdo das ações de conscientização e entregue conforme audiência. ex: apresente exemplos de incidentes no ramo financeiro no material de treinamento para os colaboradores da área Financeira
4. Alguns softwares que estão em uso não foram adequadamente testados, devido à ausência de requisitos pré-estabelecidos de segurança	A.14.2.5	**obs**	As implicações dependem da natureza do software em uso e de suas possíveis falhas	Identifique e priorize testes nas aplicações críticas; revise os riscos da área; formalize o aceite dos riscos residuais com os donos das aplicações
5. Políticas do Sistema de Gestão não possuem um controle de versão e registro de distribuição de acesso	7.5.3	**NC**	Pessoas podem estar usando políticas desatualizadas e não estarem por dentro das mudanças recentes	Implemente um processo que garante que qualquer nova/atualização de políticas, procedimentos e normas relacionadas sejam utilizadas somente pelas pessoas autorizadas e as versões sejam devidamente controlados, por exemplo, na intranet
6. O departamento de Marketing está trabalhando no lançamento de um produto em conjunto com um fornecedor (agência de propaganda) a qual não	A.13.2.4	**nc**	Informações sensíveis estão sendo fornecida ao fornecedor sem a adoção de controles apropriados; a divulgação inapropriada e pré-matura de informações pode causar	De acordo com a política de segurança, partes externas devem se comprometer por meio de um NDA antes de ter acesso a informações classificadas como "confidencial"; controles também devem ser adotados para garantir a proteção e o uso apropriado das informações; esta não conformidade deve ser tratado

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impactos	Recomendações
tem um NDA assinado			danos a reputação e perda de receitas	por meio do processo de Gestão de incidentes
7. O fornecimento de recursos ao Sistema de Gestão de Segurança da Informação (SGSI) é muito restrito	5.1 (c)	**NC**	O SGSI não pode alcançar os seus objetivos	Em conjunto com a Alta Direção, revise os objetivos e o propósito do SGSI. Desta forma, os objetivos serão mais realistas e recursos podem ser definidos de forma adequada para alcançá-los
8. Contas inativas de rede não são desabilitadas conforme políticas e procedimentos interno	A.9.2.1	**nc**	Ex-colaboradores podem manter e explorar o acesso deles na rede	Mensure e direcione a conformidade com políticas e procedimentos por meio de treinamentos, possíveis penalidades por não conformidade e etc.
9. O uso de senhas fracas é comum	A.9.4.3	**obs**	O objetivo do controle de acesso e prestação de contas são difíceis de serem alcançados, deixando os riscos a informação tratados de forma inadequada	Estabeleça e formalize uma política de senhas; como complemento a política, realize ações de conscientização e treinamento para usuários e administradores de sistemas; periodicamente revise a conformidade com a política, a fim de encontrar qualquer gap no processo
10. O controle de versão do documento "Registro de Ativos de Informação" mostra que a última atualização do documento foi há 5 anos atrás	6.1.2(b) + A.8.1.1	**NC**	O "Registro de Ativos de Informação" está desatualizado e provavelmente não estão compreendendo ativos que devem ser identificados, ter seus riscos avaliados e tratados	Revise periodicamente os seus ativos de informação e seus riscos associados (ex: entre 1-3 anos dependendo da volatilidade) de acordo com os requisitos do SGSI, mantendo os registros atualizados

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impactos	Recomendações
11. Documentos confidenciais são armazenados em notebooks pessoais ao invés de ser guardados no meio de armazenamento corporativo autorizado	A.8.1.1	**nc**	Incidentes como roubo, perda, falha de hardware ou infecção de malware no notebook pode possibilitar divulgação não apropriada ou impossibilitar o acesso legítimo as informações, causando perdas e prejuízos ao negócio; riscos poderiam ser menores se o armazenamento corporativo estivesse sendo usado como esperado	Revise os riscos e controles de segurança aplicados aos documentos 'confidenciais; fortaleça a conformidade por meio de conscientização, treinamento, auditoria etc.
12. Nenhuma evidência da execução da avaliação de riscos à segurança da informação foi apresentada	8.2	**NC**	Possibilidade de riscos a informação estarem sendo tratadas de forma inadequada	Revise o processo de Gestão de riscos para avaliar todos os riscos existentes e mantenha as evidências desta avaliação (formalize o processo)
13. Contas inativas de rede não são desabilitadas e permanecem ativas de forma indefinida	A.9.2.1	**Obs**	Ex-colaboradores podem manter e explorar o acesso deles na rede	Revise, avalie e trate os riscos relacionado aos ex-colaboradores por meio de políticas, procedimentos e controles técnicos apropriados
14. Nenhuma solução de antivírus está sendo usada	A.12.2	**Obs**	Aumenta-se o risco de infecções por malware – há a possibilidade de acontecer incidentes mais críticos	Revise, avalie e trate os riscos relacionados a malware, mantendo as evidências da decisão tomada

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impactos	Recomendações
15. Embora a organização não processe dados de cartões, não realiza auditoria de conformidade com o PCI para indicar um possíveis falhas no tratamento de dados pessoais	Nenhuma ou possivelmente A.12.6.1 e A.18.1.4	**irr**	[Este é um exemplo de apontamento que reflete a expectativa pessoal do auditor(a), ao invés do requisito ou recomendação da norma]	[Este tipo de apontamento vale a discussão, mas não é relevante para o SGSI e para certificação, pois está fora do escopo da auditoria da ISO27k. A Alta Direção pode escolher ignorá-lo, considerá-lo de forma separada e/ou até lembrar ao auditor qual o escopo e propósito da atual auditoria.]
16. Quando questionados, alguns colaboradores mostram desconhecimento da política de segurança da organização	7.3 + A.7.2.1	**NC/nc** (auditor decide conforme qualidade das informações apresentadas)	Colaboradores e a organização como um todo estão expostos a riscos de segurança como perda de dados ou outros ativos importantes	Por meio de diversas ações (*ex:* surveys, testes, avaliações), a alta direção deve garantir que todos os seus colaboradores estão conscientizados o suficiente sobre as políticas e suas obrigações
17. A organização não possui contato com grupos especiais (fóruns, boletins, newsletter, eventos e etc) para se atualizar sobre assuntos relacionados à segurança da informação	4.1 + A.6.1.4	**NC**	A organização provavelmente não está atualizada em relação aos recentes incidentes e mudanças na área e na indústria	Entender o contexto da organização, tanto interno como externo, é uma parte fundamental da Gestão de riscos e segurança, portanto, estabeleça relações sociais, participe de fóruns e se engaje com a comunidade
18. Ao menos uma NC não foi tratada desde a última auditoria	10.1 + A.18.2.2	**NC**	A organização não pode se (re)certificar com não conformidades maiores	A Alta Direção deve priorizar recursos para solucionar as NCs de forma adequada, reafirmando a importância e o seu apoio ao SGSI

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impactos	Recomendações
19. Alguns incidentes relacionados a privacidade identificados não foram reportados conforme processo estabelecido internamente	A.16.1.2	**Obs**	A demora em responder a incidentes reduz a eficiência e eficácia. Ex: limitando as escolhas da Alta Direção em como respondê-los	Sabe-se que responder de forma imediata a todos os incidentes é difícil, mas, priorizar a resposta de incidentes mais críticos pode melhorar a velocidade e eficiência das respostas aos incidentes; este apontamento sugere uma oportunidade de melhoria para o SGSI

Sobre a redação do relatório

Alguns apontamentos, impactos e recomendações da tabela, estão escritos de forma vaga e, sem contexto, podem ser mal interpretados ou questionado pela alta direção. Os apontamentos geralmente são suportados por evidências analisadas e referenciadas no relatório de auditoria. Apresentar e discutir o rascunho do relatório com a alta direção é uma excelente oportunidade de esclarecer todas as dúvidas e de ganhar o comprometimento da organização as ações que precisam ser feitas, antes de finalizá-lo.

Sobre as categorias

- **NC** = falha em não atender de forma completa exigências de um requisito da ISO/IEC 27001. **DEVEM** ser tratadas de forma prioritária para que a organização possa se certificar, pois, indica que o SGSI não está estruturado e funcionando conforme especificado pela norma;
- **nc** = uma falha de menor relevância da organização frente a algum requisito da ISO/IEC 27001. DEVE ser tratada em um prazo maior do que a NC, mas, não é impeditivo para obter a certificação;
- **obs** = não é uma não conformidade, trata-se mais de um comentário ou sugestão de oportunidade de melhoria. O auditor pode ter uma opinião, e o 'Anexo A da ISO 27001' ou outros catálogos de controles podem sugerir outra abordagem, mas, a Alta Direção, têm o direito de decidir. Neste caso, os processos para atender os requisitos do SGSI da 27001 estão sendo seguidos, mas, com uma abordagem diferente, o que não impede alcançar a certificação.
- **irr** = irrelevante e provavelmente fora do escopo da auditoria da ISO27k. A Gestão da Segurança da Informação é um assunto tão abrangente que qualquer coisa relacionada a proteção da informação se torna relevante, mas não, se o propósito da auditoria é revisar a conformidade com a '27001'. Esses tipos de apontamentos podem servir de distração e devem ser tratados informalmente e talvez considerado em outros tipos de auditoria, revisões e etc.

Sobre os impactos

Lembre-se que o objetivo principal do SGSI é ajudar a organização a ter uma estrutura necessária para proteger informações de riscos, de forma que o negócio possa ser beneficiado. A conformidade com '27001' é um meio de alcançar esse objetivo, mas não o fim. Descrever os impactos ao negócio reforça para a Alta Direção toda a atenção que deve ser dada ao que for reportado.

Sobre as recomendações

A Alta Direção/cliente (não o auditor(a)!) decide como os apontamentos serão tratados..., mas, se o auditor(a) na Auditoria de Certificação não estiver satisfeito(a) com a resposta, ele/ela pode não recomendar a certificação a autoridade certificadora, enquanto os pontos (particulamente **NCs**) não forem solucionadas.