DO'S & DONT'S - I

Tomada de decisões para os riscos de tecnologia e informação

Certifique-se de que você...	Assegure-se de que não...
 ... compreende o que a organização busca alcançar para fornecer contexto para uma avaliação de riscos útil e boas decisões de gestão de riscos.	... vai conduzir a avaliação de riscos e tomar decisões de gestão de riscos isoladamente e sem compreender o contexto empresarial.
 ... vai realizar avaliação de risco e gerenciar riscos para todo o desenvolvimento, design, implementação e todo o ciclo de vida de uso de um sistema ou serviço.	... recicla avaliação de risco e gestão para soluções onde as decisões de projeto relevantes já foram tomadas. Não assuma que uma vez que um serviço ou sistema está em operação de que não há necessidade de continuar a gerenciar riscos.
 ... entenda os bens e serviços da sua organização e com o que o negócio se preocupa. Considere o que mais é importante para a organização (ou seja, reputação, confiabilidade do serviço, privacidade do cliente, bem-estar do cliente e segurança).	... basta pensar sobre a confidencialidade, integridade e disponibilidade de ativos de informação
 ... tenha pessoas com o necessário conhecimento técnico, de segurança e uso de ferramentas bem como as competências empresariais para avaliar objetivamente os riscos e comunicá-los à organização.	...emprega recursos para usar métodos de avaliação de riscos e gerar listas inúteis de riscos que nã levam em conta as necessidades da organização.

DO'S & DONT'S - II

Tomada de decisões para os riscos de tecnologia e informação

Certifique-se de que você...	Assegure-se de que não...
 ... realiza a avaliação de risco para gerar informações que subsidiem as decisões de gerenciamento de riscos de TI.	... realiza uma avaliação de risco simplesmente para satisfazer uma etapa do projeto.
 ... escala suas atividades de avaliação de risco conforme necessário para apoiar diferentes decisões de gerenciamento de riscos em toda a organização	... suponha que você pode usar a mesma abordagem para identificar, analisar e avaliar o risco em toda a organização. Um tamanho não serve para todos.
 ... comunica as entradas e saídas e os produtos de sua avaliação de risco de forma significativa e clara.	... inseriu palavras sem sentido ou números em formulários, planilhas ou ferramentas. Não gerar saídas sem sentido de métodos ou ferramentas, e esperar que eles sejam compreendidos e consistentes.
 ... comunica riscos no nível apropriado de detalhe exigido pelo público, traduzindo em linguagem significativa, quando necessário.	... suponha que todos que precisam entender seus riscos. Não use jargão de segurança ao descrever os riscos para os decisores, e não use linguagem de negócios para fornecedores e desenvolvedores se eles precisam entender os detalhes técnicos.

DO'S & DONT'S - III

Tomada de decisões para os riscos de tecnologia e informação

Certifique-se de que você...	Assegure-se de que não...
 ... reutilizou informações de avaliação de risco disponíveis para soluções comuns.	... refaz avaliações de risco se não houver diferença entre a solução comum e o que a organização está fazendo.
 ... criou linhas de base para as entradas de avaliação de risco (por exemplo, ameaça) com base nas melhores informações disponíveis, e usá-los até que algo significativo muda.	... confiou em analistas de risco e pseudo- especialistas para tomar decisões isoladas sobre os parâmetros de avaliação de risco enquanto espera que a saída seja consistente.
 ... priorizou a produção de avaliações de risco baseadas é importante para a organização e o impacto nele considerado.	... inseriu palavras sem sentido ou números em formulários, planilhas ou ferramentas. Não gerar saídas sem sentido de métodos ou ferramentas, e esperar que eles sejam compreendidos e consistentes.
 ... comunicou riscos no nível apropriado de detalhe exigido pelo público, traduzindo em linguagem significativa, quando necessário.	... suponha que todos que precisam entender seus riscos. Não use jargão de segurança ao descrever os riscos para os decisores, e não use linguagem de negócios para fornecedores e desenvolvedores se eles precisam entender os detalhes técnicos.

DO'S & DONT'S - IV

Tomada de decisões para os riscos de tecnologia e informação

Certifique-se de que você...	Assegure-se de que não...
 ... incorporou e aplicou medidas de segurança reais em soluções tecnológicas como resultado de uma boa avaliação de risco e decisões de gestão de riscos desde o início	... espera que simplesmente por estar seguindo um processo de gerenciamento de risco irá fornecer segurança real sem ação pró-ativa, engajada e inteligente de gestão de risco e tomada de decisão em todo.
 ... vertificou-se de que os requisitos de segurança em contratos e acordos de nível de serviço são informados e rastreáveis a riscos reais.	... vai simplesmente dizer em contratos e acordos de nível de serviço que os sistemas ou serviços devem ser credenciados ou complacentes com um padrão específico.
 ... documentou as avaliações de risco e as principais decisões de gestão de risco para fins de rastreabilidade e responsabilização.	... criou conjuntos de documentos grandes e desnecessários e listas inúteis ou inutilizáveis de riscos