ISO/IEC 27001:2022 – SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO – LIDERANÇA

2. Liderança

2.1. Liderança e comprometimento

A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estejam estabelecidos e sejam compatíveis com a direção estratégica da organização;

b) assegurando a integração dos requisitos do sistema de gestão da segurança da informação nos processos da organização;

c) assegurando que os recursos necessários para o sistema de gestão da segurança da informação estejam disponíveis;

d) comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;

e) assegurando que o sistema de gestão da segurança da informação alcance seus resultados pretendidos;

f) orientando e apoiando pessoas a contribuir para a eficácia do sistema de gestão da segurança da informação;

g) promovendo a melhoria contínua; e

h) apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade.

A alta direção desempenha um papel crucial no que diz respeito ao Sistema de Gestão da Segurança da Informação (SGSI) de uma organização. A norma enfatiza que a alta direção deve demonstrar liderança e comprometimento nesse contexto. Isso implica uma série de responsabilidades fundamentais.

Primeiro, a alta direção deve garantir que a política de segurança e os objetivos de segurança da informação sejam claramente estabelecidos e alinhados com a estratégia global da organização. Isso assegura que a segurança da informação seja uma parte integral das atividades organizacionais.

Além disso, a alta direção deve garantir que os requisitos do SGSI estejam integrados nos processos da organização, tornando a segurança da informação parte integrante de todas as operações.

A disponibilidade de recursos é igualmente essencial, e a alta direção deve assegurar que os recursos necessários para o SGSI, sejam eles recursos humanos, materiais ou financeiros, estejam sempre disponíveis.

Comunicação é outra responsabilidade-chave. A alta direção deve comunicar a importância da segurança da informação e da conformidade com os requisitos do SGSI a todos os níveis da organização.

Liderança também envolve orientar e apoiar as pessoas para garantir que contribuam para a eficácia do SGSI, incentivando práticas seguras.

5m

Além disso, a alta direção deve promover a melhoria contínua do SGSI, assegurando que o sistema permaneça eficaz ao longo do tempo.

Finalmente, a alta direção deve apoiar outros papéis de gestão, demonstrando como sua liderança se aplica às áreas sob sua responsabilidade.

A liderança e o comprometimento da alta direção são vitais para assegurar que o SGSI seja eficaz e esteja alinhado com os objetivos estratégicos da organização, promovendo uma cultura de segurança contínua e eficaz na gestão da informação.

2.2. Política

A Alta Direção deve estabelecer uma política de segurança da informação que:

a) seja apropriada ao propósito da organização;

b) inclua os objetivos de segurança da informação (ver 6.2) ou forneça a estrutura para estabelecer os objetivos de segurança da informação;

c) inclua o comprometimento de satisfazer os requisitos aplicáveis relacionados com a segurança da informação;

d) inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

A política de segurança da informação desempenha um papel central na Norma 27001:2022, e a alta direção é encarregada de estabelecê-la. Essa política deve ser específica e adequada ao propósito da organização, sendo único para aquela entidade e não um documento genérico ou copiado de outra fonte.

Além disso, a política de segurança da informação deve incluir os objetivos de segurança da informação, que são discutidos mais detalhadamente na Seção 6.2 da norma. A política deve fornecer a estrutura e o comprometimento para atender aos requisitos relacionados à segurança da informação.

Também é crucial que a política de segurança da informação inclua o comprometimento com a melhoria contínua. Isso significa que a organização está comprometida em aprimorar constantemente seus processos e práticas de segurança da informação, alinhando-os com os objetivos da organização.

Portanto, a política de segurança da informação é uma parte vital do Sistema de Gestão da Segurança da Informação (SGSI) e deve ser única e adaptada às necessidades e metas específicas da organização, garantindo o compromisso com a segurança e a busca constante pela melhoria.

A política da segurança da informação deve:

e) estar disponível como informação documentada;
f) ser comunicada dentro da organização;
g) estar disponível para as partes interessadas, conforme apropriado.

A política de segurança da informação é um componente crítico no Sistema de Gestão da Segurança da Informação (SGSI), e deve ser disponibilizada como informação documentada, o que significa que deve ser documentada de forma que seja facilmente acessível a todos os envolvidos.

Isso inclui tanto o público interno, como os colaboradores da organização, quanto o público externo, que engloba as partes interessadas, tais como clientes, fornecedores e outras entidades que possam estar relacionadas com as operações da organização.

10m

Portanto, a política de segurança da informação não é uma informação confinada apenas ao público interno da organização, mas deve ser comunicada e disponibilizada a todas as partes interessadas, garantindo a transparência e o comprometimento com os princípios de segurança da informação. Esse entendimento é crucial, especialmente em contextos de questões de exames ou avaliações, como no caso do SEBRAE em 2023, onde é fundamental reconhecer que as partes interessadas incluem um público mais amplo além do pessoal interno da organização.

2.3. Papéis, responsabilidades e autoridades organizacionais

A Alta Direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados dentro da organização. A Alta Direção deve atribuir a responsabilidade e autoridade para:

a) assegurar que o sistema de gestão da segurança da informação esteja em conformidade com os requisitos deste documento;

b) relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção.

Dentro do contexto do Sistema de Gestão de Segurança da Informação (SGSI), é crucial estabelecer papéis, responsabilidades e autoridades de forma clara e eficaz. A alta direção da organização tem a responsabilidade de garantir que essas designações sejam feitas e comunicadas de maneira apropriada.

15m

Isso envolve a atribuição de responsabilidades e autoridades para assegurar que o SGSI cumpra com todos os requisitos estabelecidos pela norma. O objetivo é garantir que o sistema esteja em conformidade com as diretrizes e regulamentos do SGSI.

Os indivíduos que ocupam esses papéis relevantes são encarregados de relatar o desempenho do SGSI à alta direção. Isso é essencial para avaliar se o sistema está funcionando eficazmente e cumprindo seus objetivos.

Portanto, a clareza na definição desses papéis e na comunicação das responsabilidades e autoridades é fundamental para o sucesso do SGSI e para garantir que ele opere em conformidade com a norma. Isso assegura que a alta direção tenha as informações necessárias para monitorar e melhorar continuamente o sistema.

DIRETO DO CONCURSO

1. (IFSP/IFSP/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2022) Trabalhar com a gestão de dados perpassa demandas associadas à segurança e à privacidade. A ABNT NBR ISO/IEC 27001 é um padrão que especifica os requisitos para a implementação, manutenção e continuidade na melhoria dos sistemas de segurança da informação. Essa norma aborda esses conceitos sob diferentes níveis institucionais. Com isso, assinale a opção que recomenda práticas incorretas de liderança e comprometimento da alta direção quanto ao Sistema de Gestão de Segurança da Informação (SGSI).

a. Garantir a integração dos requisitos dos sistemas de gestão de segurança da informação dentro dos processos da organização.
b. Orientar e apoiar pessoas para que contribuam para a eficácia do SGSI.
c. Assegurar que os recursos de SGSI estejam disponíveis.
d. Limitar as informações sobre a política do SGSI na empresa, para evitar incidentes.

A questão de 2022 do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo aborda práticas de liderança e comprometimento da alta direção em relação ao Sistema de Gestão de Segurança da Informação (SGSI). É importante notar que a questão solicita a identificação de práticas incorretas.

Dentre as alternativas apresentadas, a primeira menciona "garantir que a integração do sistema de gestão de informação dentro dos processos da organização". No entanto, essa não é uma prática incorreta, pois a integração do SGSI com os processos organizacionais é uma ação recomendada.

A segunda alternativa menciona "orientar e apoiar pessoas para que contribuam para a eficácia do SGSI". Essa é uma prática correta, pois a liderança e o comprometimento da alta direção envolvem exatamente isso: orientar e apoiar as pessoas para que o SGSI seja eficaz.

A terceira alternativa fala em "assegurar que os recursos estejam disponíveis". Isso também é uma prática correta, pois a alta direção deve garantir que os recursos, sejam eles humanos, materiais ou financeiros, estejam disponíveis para o funcionamento eficaz do SGSI.
A quarta alternativa menciona "limitar informações sobre a política da empresa para evitar incidentes". Essa é a prática incorreta, pois a política de segurança da informação não deve ser limitada, mas sim comunicada e disponibilizada para as partes interessadas, tanto internas quanto externas. Portanto, essa alternativa apresenta uma prática que vai contra os princípios de liderança e comprometimento da alta direção no contexto do SGSI.
Portanto, a alternativa correta, que indica uma prática incorreta de liderança e comprometimento da alta direção, é a quarta alternativa que menciona a limitação das informações sobre a política da empresa para evitar incidentes. Isso não está alinhado com as boas práticas de gestão de segurança da informação.

20m

---

2. (INSTITUTO AOCP/SEAD GO/ANALISTA DE GESTÃO GOVERNAMENTAL - ÁREA: TECNOLOGIA DA INFORMAÇÃO/2022/1º SIMULADO) O objetivo da ISO 27001 é prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). Apesar da ISO 27001 não citar explicitamente o ciclo PDCA, podemos associar os verbos estabelecer, implementar, manter e melhorar continuamente às etapas do ciclo PDCA (Plan, Do, Check, Act), respectivamente. Dentre as etapas estabelecidas pelo SGSI, quais fazem parte da etapa de Check?

a. Contexto da Organização e Liderança.
b. Planejamento e Apoio.
c. Apoio e Operação.
d. Melhoria.
e. Avaliação do Desempenho

A ISO 27001 tem como objetivo estabelecer requisitos para que as organizações possam criar, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Embora a norma não mencione explicitamente o ciclo PDCA (Plan-Do-Check-Act), podemos associar os verbos "estabelecer", "implementar", "manter" e "melhorar continuamente" às etapas desse ciclo.
O ciclo PDCA consiste nas etapas de Planejar (Plan), Executar (Do), Verificar (Check) e Agir (Act). Na etapa de "Verificar" (Check), você avalia o que foi feito, ou seja, verifica se as ações executadas estão de acordo com o planejamento. Isso faz parte da fase de "Check" do ciclo PDCA, que envolve a avaliação do desempenho.
Portanto, a questão menciona os verbos "estabelecer", "implementar", "manter" e "melhorar continuamente" e associa essas ações às etapas do ciclo PDCA. No contexto da questão, a

correspondência direta é com a etapa de "Verificar" (Check) do ciclo PDCA, que envolve a avaliação do desempenho. Isso demonstra como a ISO 27001 incorpora a ideia de melhoria contínua no processo de gestão da segurança da informação.

EXERCÍCIOS DE FIXAÇÃO

3. Como a Alta Direção pode demonstrar sua liderança e comprometimento com o sistema de gestão da segurança da informação?

a. Desconsiderando a política de segurança da informação.
b. Ignorando a integração dos requisitos do sistema de gestão da segurança da informação nos processos da organização.
c. Assegurando que os recursos necessários para o sistema de gestão da segurança da informação estejam disponíveis.
d. Não comunicando a importância de uma gestão eficaz da segurança da informação.
e. Ignorando a melhoria contínua do sistema de gestão da segurança da informação.

A questão aborda como a alta direção pode demonstrar sua liderança e comprometimento com o Sistema de Gestão de Segurança da Informação (SGSI). A alta direção desempenha um papel fundamental na promoção da cultura de segurança da informação na organização. Vamos analisar as opções:

A. "Desconsiderando a política de segurança da informação." - Esta opção não está alinhada com a demonstração de liderança e comprometimento. A alta direção deve considerar a política de segurança da informação e, na verdade, é responsável por estabelecê-la.

B. "Ignorando a integração dos requisitos do sistema de gestão de segurança da informação nos processos da organização." - Esta opção sugere ignorar um dos princípios essenciais da segurança da informação, que é a integração dos requisitos do SGSI nos processos organizacionais. A alta direção deve assegurar a integração.

C. "Assegurando os recursos necessários para o SGSI estejam disponíveis." - Isso está alinhado com a liderança e o comprometimento da alta direção. Assegurar que os recursos necessários para o SGSI estejam disponíveis demonstra compromisso com a segurança da informação.

D. "Comunicando a importância de uma gestão eficaz e ignorando a melhoria contínua do SGSI." - Esta opção também está relacionada à liderança e ao comprometimento da alta direção. Comunicar a importância de uma gestão eficaz é uma prática importante, e a alta direção não deve ignorar a melhoria contínua do SGSI.

25m

GABARITO

1. d
2. e
3. c