TOPCERTIFIER
www.topcertifier.com

METODOLOGIA DE ATENDIMENTO ISO 27001:2013

INFORMAÇÃO GESTÃO DE SEGURANÇA SISTEMA (SGSI)

TOPCERTIFIER
www.topcertifier.com

INTRODUÇÃO À ISO 27001:2013

A ISO 27001:2013 permite a uma organização identificar os Riscos de Segurança da Informação. Tendo em conta as ameaças, vulnerabilidades, os impactos e protegendo a organização sem comprometer a sua CIA (Confidencialidade, Integridade, Disponibilidade) de informação, adotando Sistema adequado de gestão da segurança da informação A agenda geral da ISO 27001:2013 é cobrir os aspetos abaixo.

- Fornecer um modelo para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um Sistema de Gestão da Segurança da Informação com controlos físicos e técnicos.

- Garantir que o SGSI está integrado nos processos de negócio das organizações.

- Criar uma cultura organizacional que incentive a participação ativa dos colaboradores na Sistema de gestão da segurança da informação.

COMEÇO

A reunião de kickoff é uma ferramenta essencial para comunicar e planear a execução do projeto com obstrução mínima e concluir o projeto dentro do tempo e custo planeados.
A agenda da reunião inicial é:

- Discussão do plano do projeto: Inclui discussão sobre a prestação de contas e a responsabilidade da estaca titulares. marcos e entregas no projeto

- Âmbito dos serviços e âmbito da certificação

- Requisitos legais e regulamentares

CRIAÇÃO DA EQUIPA NÚCLEO

- Nomeação do CISO
- Nomeação do Comité de Gestão da Segurança da Informação
- Nomeação de Auditores Internos
- Gestor do BCP
- Nomeação do Líder ISO

TOPCERTIFIER
www.topcertifier.com

ANÁLISE DE GAP

Durante esta fase, realizámos uma análise de lacunas para verificar o quanto das suas práticas atuais estão em conformidade de acordo com os requisitos padrão. práticas são verificadas em relação a estes quatro critérios de referência

- Requisitos da norma ISO 27001:2013
- SOA
- Requisitos legais, estatutários e regulamentares
- Requisitos do cliente
- Políticas e procedimentos internos

Os resultados desta análise são apresentados sob a forma de um Relatório de Análise de Gap. Este relatório atua como a lista de itens de ação para o lembrete do projeto.

FORMAÇÃO DE CONSCIENTIZAÇÃO DE ISMS

O treino de sensibilização do SGSI será realizado para os colaboradores da sua organização. O treinamento sessão é ajudar os colaboradores a adquirir conhecimento, compreender os conceitos da ISO 27001:2013, e alinhar processos e práticas para alcançar um ambiente de trabalho seguro e livre de ameaças. Quando a equipa tiver sido formada, poderá pensar e agir e contribuir para atingir o objetivo. objetivos.

REGISTO DE RISCOS E SOA

Um procedimento de Gestão de Risco deve ser documentado e utilizado como referência para gerir o riscos identificados em consulta com todos os donos de processos e chefes funcionais. Utilizamos ISO 31000 & Técnicas padrão de gestão de risco ISO 27005 para identificar, analisar, avaliar, documentar, priorizar, tratar e quantificar os riscos identificados. Esta etapa cria um Registo de Riscos. Risco Adequado os planos de tratamento são identificados com base no nível de apetite ao risco e no fator CIA da empresa. Os resultados de tais ações são calculados, registados, avaliados e documentados. O A Declaração de Aplicabilidade (SOA) define e identifica os controlos físicos e técnicos aplicável à sua organização com base nos seus processos e requisitos de negócio.

TOPCERTIFIER
www.topcertifier.com

GESTÃO DE ATIVOS

Auxiliamos no desenvolvimento de políticas e procedimentos de gestão de ativos, em coordenação com o chefes funcionais e compreensão sobre o processo. O principal objetivo do ativo gestão é:

- Para identificar os ativos organizacionais e definir as responsabilidades de proteção adequadas
- Para evitar a divulgação, modificação, remoção ou destruição não autorizada da informação armazenada na mídia
- Para garantir que a informação recebe um nível adequado de proteção de acordo com a sua importância para a organização

SEGURANÇA DE REDE / COMUNICAÇÃO:

Ajudamos no desenvolvimento de políticas e procedimentos de gestão de segurança de rede, coordenando com os responsáveis funcionais e compreensão do processo. O principal objetivo da segurança de rede é:

- Garantir a proteção da informação nas redes e o seu suporte ao tratamento da informação instalações
- Para manter a segurança da informação transferida dentro de uma organização e com qualquer entidade externa

GESTÃO DE INCIDENTES

Auxiliamos no desenvolvimento de políticas e procedimentos de gestão de incidentes, em coordenação com o chefes funcionais e compreensão sobre o processo. O principal objetivo do incidente gestão é:

- Garantir uma abordagem consistente e eficaz à gestão da segurança da informação incidentes, incluindo a comunicação sobre eventos e pontos fracos de segurança

TOPCERTIFIER
www.topcertifier.com

GESTÃO DE CONTINUIDADE EMPRESARIAL

Auxiliamos no desenvolvimento de políticas e procedimentos de gestão de continuidade de negócio, coordenação com os chefes funcionais e compreensão do processo. O principal objetivo da gestão da continuidade de negócio é a seguinte:

- Para garantir que a continuidade da segurança da informação é incorporada no negócio da organização sistemas de gestão da continuidade

- Para garantir a disponibilidade de instalações de processamento de informação

SEGURANÇA FÍSICA:

Auxiliamos no desenvolvimento de políticas e procedimentos de segurança física, em coordenação com o chefes funcionais e compreensão sobre o processo. O principal objetivo do Físico segurança é:

- Para evitar o acesso físico não autorizado, danos e interferências nos recursos da organização instalações de processamento de informação e informação

- Para evitar a perda, dano, roubo ou comprometimento de bens e interrupção do funcionamento da organização operações

SEGURANÇA DOS RECURSOS HUMANOS:

Auxiliamos no desenvolvimento de políticas e procedimentos de RH, em coordenação com os chefes funcionais e compreensão sobre o processo. O principal objetivo da segurança de RH é:

- Para garantir que os colaboradores e os contratados compreendem as suas responsabilidades e são adequados para as funções para as quais são considerados

- Para proteger os interesses da organização como parte do processo de mudança ou rescisão emprego

- Garantir que foi dada formação adequada a todos os funcionários e fornecedores com respeito à segurança da informação

TOPCERTIFIER
www.topcertifier.com

DOCUMENTAÇÃO

Os nossos especialistas listarão as políticas, processos, POPs, SOA aplicável e registos que precisam de ser definido e documentado de acordo com os requisitos da ISO 27001:2013, discutindo com cada chefes de departamento e função auxiliamos na criação da documentação necessária.

ESTABELECER CONTROLES DE ISMOS

Uma vez que as políticas, processos, Declaração de Aplicabilidade (SOA), os seus controlos e SOPs tenham sido foi documentada e a lista de registos a recolher foi listada e o pessoal foi identificados e formados em tais atividades, então a necessidade é operar, monitorizar e rever o eficiência de tais processos.

FORMAÇÃO DE AUDITORES INTERNOS

A formação de Auditor Interno (IA) ISO 27001:2013 será ministrada ao pessoal identificado. Esta formação irá capacitar este pessoal para analisar a necessidade de AI, planear e programar AI, preparar listas de verificação de auditoria e conduzir uma IA e documentar e reportar as suas observações ao topo gestão.

AUDITORIA INTERNA

Os nossos especialistas supervisionarão a condução da auditoria interna pela sua equipa de auditoria interna. Esta auditoria interna identificará lacunas ainda existentes no sistema e demonstrará o nível de preparação para enfrentar a auditoria de certificação. Esta auditoria dá à organização a oportunidade de identificar e retificar todas as não conformidades antes de avançar para a auditoria de certificação. O topoa gestão é informada das conclusões da auditoria interna.

TOPCERTIFIER
www.topcertifier.com

ANÁLISE DE CAUSA RAIZ (RCA) E AÇÕES CORRETIVAS

Todas as não conformidades identificadas durante a auditoria interna, auditorias de clientes ou de terceiros, ou de Avaliação de riscos e metodologia de tratamento de riscos, registo de riscos Registo de Incidentes, Vulnerabilidade Relatório de avaliação e teste de penetração (VAPT), ataques de malware, registo de tempo de inatividade, rede questões, controlos de acesso, registo de ativos, relatórios de avaliação de risco de terceiros, CIA-Information classificação, ataques internos e externos e quaisquer outras fontes devem ser listados. A RCA será realizado com recurso a técnicas como o Brainstorming e os métodos Fish-Bone. O corretor ideal ações são implementadas. A eficácia de tais ações é documentada e revista através de um Relatório de Ações Corretivas (CAR).

REUNIÃO DE AVALIAÇÃO DA GESTÃO (MRM)

O MRM é uma oportunidade para todas as partes interessadas do SGSI se reunirem em intervalos programados para rever, discutir e planear ações sobre os pontos da agenda abaixo.

- Eficácia do atual Sistema de Gestão em relação ao SGSI
- Planos e registos de avaliação de riscos e tratamento de riscos
- Resultados sobre CIA (Confidencialidade, Integridade e Disponibilidade) da informação
- Resultados de auditoria e não conformidades de todas as fontes
- Plano de ação corretiva para resolver quaisquer itens em aberto
- Melhorias contínuas efetuadas no sistema
- Recursos e formação necessários
- Aspetos estatutários e de conformidade

AUDITORIA DE CERTIFICAÇÃO: ETAPA 1

Quando o nível de preparação atingir níveis adequados, o processo de certificação começa. Um auditor nomeado pelo Organismo de Certificação (OC) verifica a Norma requisitos através de uma auditoria de estágio 1. Isto envolve a revisão pelo auditor das políticas, processos, SOPs, SOA, registos operacionais críticos, registos IA e MRM. Quaisquer desvios importantes das recomendações do BC as expectativas serão notificadas neste momento para trazer as correções necessárias. Isso reduz as probabilidades de não conformidades graves durante a auditoria de certificação. O Certificador TOP entrará em contacto com todas as partes interessadas e supervisionar a conclusão tranquila da auditoria.

TOPCERTIFIER
www.topcertifier.com

AUDITORIA DE CERTIFICAÇÃO: ETAPA 2

Após a conclusão bem-sucedida da auditoria do Estágio 1, o auditor concentra-se numa auditoria detalhada do relatório e documentação do Sistema de Gestão da Segurança da Informação da organização. A TOPCertifier teria formado o seu pessoal nos requisitos de auditoria e em enfrentando a auditoria. Os nossos especialistas estarão presentes para auxiliar em todos os meios necessários ao bom andamento funcionamento da auditoria. O TOPCertifier ajudará a sua equipa a resolver quaisquer não conformidades identificados durante a auditoria. Após a conclusão com sucesso da auditoria de certificação, o TOPCertifier entrará em contacto com todas as partes interessadas para redigir, aprovar e divulgar o certificado final.

CONTINUAÇÃO DA CONFORMIDADE

O TOPCertifier fará parte da jornada de conformidade da sua organização e irá ajudá-lo regularmente intervalos com formação necessária, suporte e atualizações de sistemas, auditorias internas e externas e renovação regular da sua certificação.