



S3GURANÇA
DA INFORMAÇÃO

* * * *

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Segurança da Informação

■ Segurança da Informação

É uma área bastante ampla e tem o fornecimento de proteção de ativos como objetivo. Neste contexto, ativo é todo elemento que possa trazer algum prejuízo para seu dono, responsável, empregador, se porventura, sofrer ou gerar algum tipo de dano. Note que pessoas, hardware ou software podem ser citados como exemplos de ativos aos olhos da segurança, uma vez que todos possuem potencial danoso.

No emprego de proteção, a Segurança da Informação conta com controles tanto físicos quanto lógicos.

São exemplos de controles físicos de segurança o uso de blindagens, cofres, paredes dentre outros e para controles lógicos podemos citar o uso de software, políticas e normas.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

A Segurança da Informação possui sólidos pilares, que norteiam todos os seus métodos e abordagens de proteção.

São 3 (três):

- » Confidencialidade – Assegura que o acesso a informações reconhecidamente sensíveis, ocorra apenas por meio de pessoas autorizadas. Este pilar parte do princípio de que não haverá outra pessoa, a não ser o proprietário e (ou) pessoas autorizadas por ele, com possibilidade de acesso às suas informações.
- » Integridade – Visa garantir que a informação não sofrerá alterações indesejadas pelo proprietário (ou) responsável. Sejam elas acidentais (deleção, perda, cópia etc.) ou maliciosas (fraudes, roubos, sequestros etc.).
- » Disponibilidade – Respeitados os demais pilares, este objetiva manter a informação disponível durante todo o tempo em que se precisa dela.

Por ter uma abordagem mais holística, a Segurança da Informação irá ofertar tudo que é requerido para garantir que a informação permaneça **confidencial, íntegra e disponível**, sempre que necessário.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Para fazer isso, ela agrega metodologias, processos, normas, técnicas, ferramentas, estruturas organizacionais, tecnologias e outros elementos, que são alicerces para os métodos de proteção, nas várias maneiras em que a informação se apresenta.

Aplica-se Segurança da Informação para qualquer aspecto de proteção da informação ou dados, em qualquer forma. O nível de proteção será proporcionalmente relativo, ao valor da informação e aos prejuízos inerentes ao uso impróprio desta. Devemos lembrar que, uma informação sensível e que deve ser privada, nem sempre está em formato digital, portanto, a Segurança da Informação não se limita apenas a oferecer proteções digitais.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

■ Cibersegurança

Dentro da esfera de Segurança da Informação, a cibersegurança fornece todos os elementos digitais de proteção que a informação necessita.

Em uma intensidade cada vez maior, empresas, indústrias e governos interconectam sistemas digitais em busca de mais eficiência. Neste cenário, riscos de várias naturezas começam a se elevar.

Por exemplo:

- » Corrompimento da integridade ou perda dos dados;
- » Captura de senhas, credenciais ou vazamento de dados sensíveis;
- » Extorsão por meio de cobrança de resgate de informações sigilosas (sequestro de dados);
- » Espionagem de dados/industrial;
- » Adulteração de informações;

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

- » Exposição pública de dados confidenciais;
- » Propagação de SPAM.

Os prejuízos inerentes a cada um destes incidentes digitais são muitas vezes intangíveis, dependendo da relevância da informação comprometida, para a organização.

Proteger informações sempre foi a função básica da Segurança da Informação. Com o advento da Lei Geral de Proteção de Dados – LGPD, esta proteção passa a ser mandatória e a não obediência, juntamente aos vários cuidados que a proteção de informações pessoais, poderá custar caro para as organizações.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Protegendo dados em sua Infraestrutura Local e na Nuvem

É vasta a lista de barreiras e cuidados que podem e devem ser tomados para proteger os dados que tratamos. Vejamos alguns.

Cuidados para a Infraestrutura Local

■ Controles de acesso

Além das informações estarem bem mapeadas e classificadas (sensíveis, sigilosas, etc.) com seus respectivos responsáveis declarados, o acesso a ela deve ocorrer de maneira controlada, ou seja, além de ser privilégio exclusivo de quem realmente necessita, precisa passar por alguma análise estratégica. Isto criará barreiras para possíveis privilégios impertinentes.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

É um erro armazenar informações sem ter controle sobre quem tem acesso e poderes sobre elas. Este cenário dá margem para várias possibilidades nocivas para a organização, como vazamento ou destruição de dados, por exemplo. É extremamente eficaz revisar permanentemente os controles, validando e testando limitações de acesso.

■ Ciclo de vida de contas

É preciso que as contas de acesso dos colaboradores estejam vinculadas ao controlador de domínio, este é um excelente passo, uma vez que contas locais facilmente poderão ser esquecidas e permanecer existentes sem necessidade.

Sabe aquele usuário e senha que utilizamos para nos identificarmos na rede? Em resumo, o controlador de domínio, é responsável por armazenar estas contas e senhas de usuários, que são válidas e permitidas pelos administradores da rede.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Feito isto, o ideal é que os sistemas de registro/cadastro de pessoas, da área de Recursos Humanos esteja interligado ao controlador de domínio, pois uma vez que determinado colaborador perde ou ganha vínculo com a organização, isto é automaticamente refletido no controlador de domínio.

■ Riscos da rede sem fio

Principalmente quando disponibilizado para visitantes, o controle de acesso já citado, torna-se ainda mais fundamental. Deve-se ter a rede de visitantes isolada e sem possibilidade de se comunicar com outros serviços e sistemas internos restritos aos colaboradores.

Segmentar a rede, isolando a rede sem fio, o famoso *wi-fi*, em um segmento limitado, é um ótimo meio para proteger informações restritas. Nunca utilizar protocolos de encriptação antigos e inseguros como o WEP e dar preferência a WPA2 que apesar de mais pesado, é moderno e seguro. Estes protocolos são responsáveis por manter segura e livre de captura de informações, a conexão do dispositivo (notebook, smatphone etc.) com o equipamento de *wi-fi*.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

■ Backups

O backup não é considerado um recurso de prevenção no contexto de ataques, porém, ele lhe dará a saída em casos onde a informação foi destruída ou mesmo sequestrada, como no caso de um ransomware.

Seus backups devem estar armazenados em local ainda mais restrito (digital e fisicamente) e com rígidas políticas de controle de acesso.

Mas, é necessário que se estabeleçam períodos de testes nos backups realizados. Isto irá validar a integridade e eficácia dos backups que vem sendo realizados, evitando surpresas em um momento de crise onde de fato ele será necessário.

■ Firewall

A Internet é uma rede mundial sem leis específicas e sua rede local precisa estar isolada e com as garantias corretas.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Dê preferência por *firewalls* de mercado, com suporte e garantias. Ter um *firewall* licenciado significa atualizações constantes e correções mais rápidas para bugs (erros de sistema) e brechas de segurança. Caso você opte por um Firewall não licenciado e sem suporte, dependerá da velocidade que os responsáveis pela sua administração terão de se manter atualizados sobre falhas publicadas e seu conhecimento do produto para aplicação da correção.

■ Conscientização

Falhas humanas podem causar grandes transtornos para a organização. Muitas vezes isto se dá simplesmente por desconhecimento da conduta correta.

Promova o tema Segurança da Informação dentro da organização, por meio de palestras, cursos, treinamentos, webcasts etc. Um usuário desinformado sob o aspecto de segurança, pode se tornar um ofensor, independente de sua área ou cargo.

Suas informações estarão mais seguras quando seus colaboradores também estiverem de fato se importando com isto.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Cuidados para a Nuvem

■ Nuvens privadas X nuvens públicas

As redes privadas nos oferecem recursos de uso exclusivo. Isso significa que ao contratar uma nuvem privada, teremos ativos dedicados apenas ao nosso uso. Nas nuvens públicas, estaremos compartilhando recursos com outros usuários. Quanto menor o compartilhamento de recursos, menor a chance de vazamentos.

■ Criptografia

O provedor de nuvem deve entregar garantias de que estes dados estarão codificados todo o tempo. Estas garantias devem explicitar que apenas o contratante do serviço possui a chave de decodificação dos dados armazenados em sua nuvem.

Uma outra opção, ainda mais segura, é armazenarmos os dados na nuvem já codificados, criando com isso mais uma camada de segurança.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

■ Recurso de backup

Observe se o provedor escolhido dá opções que viabilizem realizar backup em outros locais de sua escolha, fora da nuvem. Assim você não estará limitado apenas aos recursos padronizados oferecidos por ele.

Ter cópias em mais de um lugar seguro é gerar menor possibilidade de perda de dados.

■ Controle de acessos

Assim como na Infraestrutura Local, é vital que este tema lhe seja relevante na nuvem. Busque sempre optar por provedores que ofereçam vastas opções de autenticação e restrições para o acesso aos dados ou infraestrutura.

Busque serviços que possibilitem a autenticação em duas etapas, que geralmente consiste no cadastro de um celular ou um e-mail para o qual o sistema irá enviar um número de confirmação toda vez que houver um acesso ao serviço.

Verifique a possibilidade de criação de perfis com privilégios distintos, pois isto dará aos administradores maior poder de gerenciar a proteção das informações ali contidas.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?

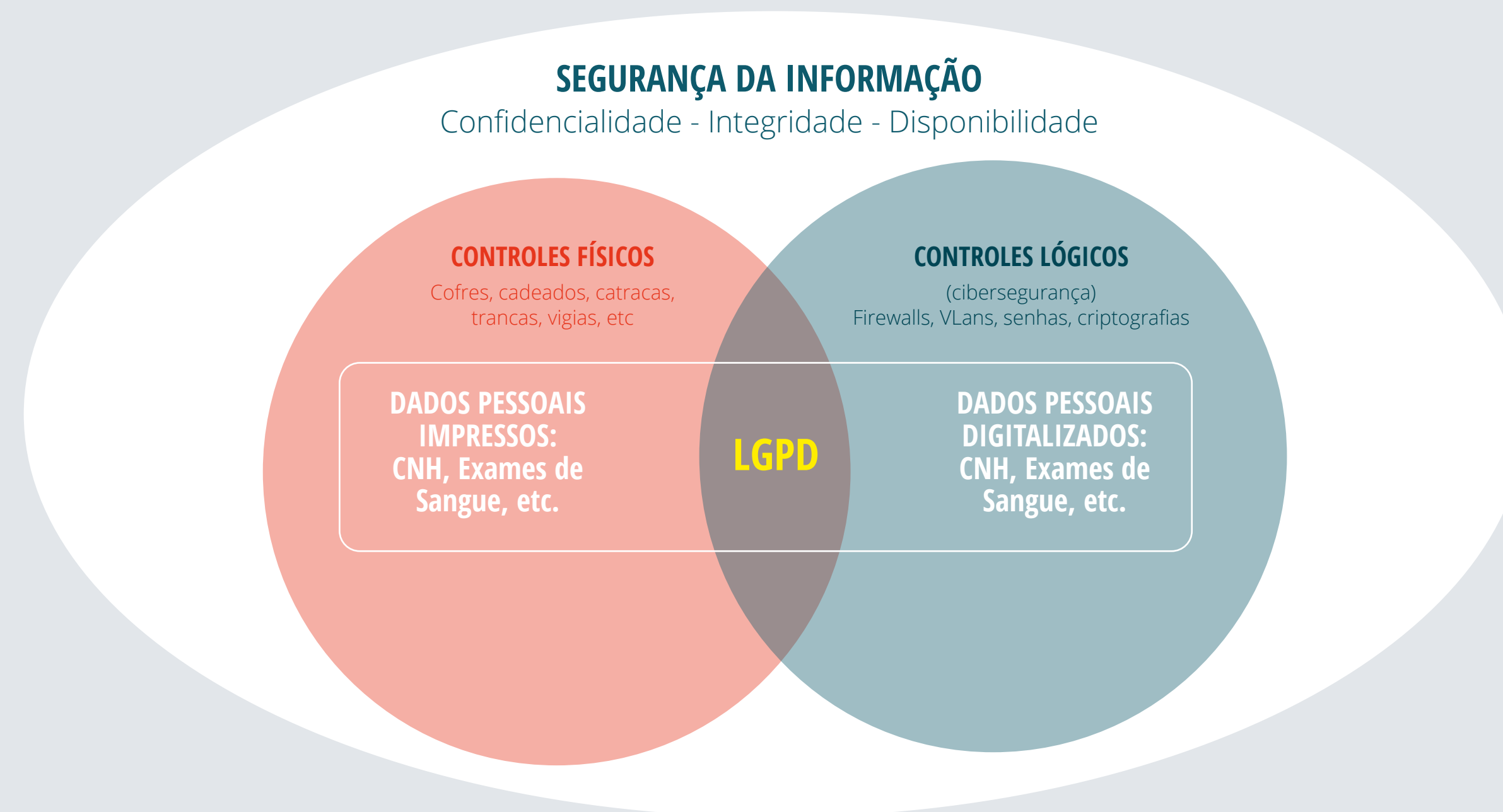


S3GURANÇA
DA INFORMAÇÃO

* * * *

Segurança da Informação, Cibersegurança e LGPD

Esta tríade tem em comum a busca pela proteção da informação.



Na tríade em questão, a LGPD é a mais específica, pois trata exclusivamente da informação em formato de dados pessoais.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Em síntese, a LGPD busca garantias ao dono do dado pessoal – o titular - de que aquela sua informação só será utilizada por quem recebeu autorização (*do dono*) formalmente. Proteger dados pessoais – o foco da LGPD – requer tanto controles físicos como lógicos. Estar em conformidade com a LGPD, inevitavelmente exigirá elementos advindos tanto da segurança da informação quanto da cibersegurança.

Resumindo...

Proteger dados pessoais, que são o foco da LGPD nos dias atuais, exigirá em grande parte controles lógicos fornecidos pela Cibersegurança, que é uma vertente da Segurança da Informação.

Por este motivo, pode-se afirmar que, não há possibilidade de garantir adequação à LGPD sem o emprego da Segurança da Informação.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



**S3GURANÇA
DA INFORMAÇÃO**

* * * *

Mas, se eu me preocupar apenas com a Segurança, automaticamente estarei atendendo ao que a LGPD exige?

Não! Lembre-se, a Segurança da Informação é uma área que emprega tecnologia, onde muitos elementos são opcionais, a organização pode entender que não precisa de um ou outro elemento para se considerar segura.

A LGPD é uma lei e não há nada de opcional nela, ou seja, se você estiver focado apenas na Segurança da Informação, não implementará todas as regras que a LGPD exige, portanto, respondendo à pergunta, não estará automaticamente atendendo ao que a LGPD exige.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Mas...

Caso a organização não esteja buscando criar estruturas internas de segurança instintivamente, baseada apenas no feeling da equipe técnica, mas sim em um framework de mercado com estas estruturas consolidadas, que abrangem parte das entregas que a LGPD exige, terá mais garantias de estar em conformidade com a segurança da informação e com a lei.

Com isto, além de basear a criação da estrutura interna de segurança em um framework já validado, estará também cuidando de aspectos de proteção de dados que a LGPD exige.

Isto significa que, no caso de ter um framework como guia para criação de uma estrutura de segurança, possivelmente este fará menção para que sejam obedecidas as legislações vigentes relativas às informações que estão sendo protegidas.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



**S3GURANÇA
DA INFORMAÇÃO**

* * * *

Que framework
posso utilizar?

ISO/IEC 27001.

Utilizada por gigantes como Google, IBM, Microsoft, etc., a ISO 27001 é uma norma de segurança da informação que foi publicada em 2005 e revisada em 2013. A publicação se deu pela International Organization for Standardization (ISO).

Sua adoção não é obrigatória, apesar disso, é reconhecida em vários países como sendo um dos principais frameworks para implementação de segurança da informação / cibersegurança.

Ela fornece controles que visam estruturar a maneira como a organização se previne, trata e responde a questões de segurança.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



**S3GURANÇA
DA INFORMAÇÃO**

* * * *

Adotando a Norma ISO 27001, quais aspectos da proteção de dados estarei reforçando perante a LGPD ?

Analisando as exigências da LGPD, é possível perceber que diversos pontos são abordados pela ISO 27001. Podemos dizer que existem convergências entre a Norma e a lei, uma vez que, há uma espécie de cruzamento entre algumas exigências da Lei e ofertas de controle da Norma.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

2 Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

Conformidade

Caso a organização esteja trabalhando na implementação da ISO 27001, ela já precisará por exigência da própria norma, a obediência a LGPD.

Isto se dá por conta do controle **A.18.1.1** que pede a *“Identificação de legislação e requisitos contratuais aplicáveis”*.

Para tanto, é mandatório que se tenha uma lista de requisitos legislativos, estatutários, regulatórios e contratuais relevantes ao tratamento da informação.

Uma vez que a organização precisa estar em conformidade com a LGPD, esta regulamentação entra automaticamente nesta lista.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Já não bastasse isso, observe o que é exigido no controle **A.18.1.4** da norma: *“Privacidade e proteção de informações pessoais”*.

Mais uma vez a implementação da Norma, irá trazer conformidade com a lei. Agora por meio de exigir que as organizações implementem uma política de privacidade e proteção de informações de dados pessoais, também previstas na LGPD.

Notificação de violação

A LGPD exige que as organizações notifiquem a Autoridade Nacional de Proteção de Dados (ANPD) cumprindo “prazo razoável” (a definir), acerca da ocorrência de incidente de segurança da informação.

Antes de avançarmos, perceba primeiro que, o vazamento de um dado pessoal nada mais é que um incidente de segurança, tecnicamente falando.

Portanto, não nos causaria nenhuma estranheza se a ISO 27001 contivesse uma estrutura para este tratamento. Correto?

Sim!

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

A “*Gestão de incidentes de segurança da informação*” não deixará de ser abordada durante a implementação da Norma, pois o controle **A.16.1** demanda: “*uma abordagem consistente e eficaz para a gestão de incidentes de segurança da informação, incluindo a comunicação de eventos de segurança*”.

Por consequência, esta abordagem também contempla a notificação das “*pessoas naturais*”, ou simplesmente titulares dos dados pessoais, exigida pela LGPD.

Gestão de ativos

Na visão da Segurança da Informação, qualquer elemento que impacte em valor ao negócio é considerado um ativo e este pode existir de diversas formas.

Por exemplo, uma informação física ou digital, um software, um hardware, uma pessoa ou mesmo um ambiente físico, ou qualquer outra coisa que caso sofra comprometimento dos pilares da Segurança da Informação (*lembra? confidencialidade, integridade ou disponibilidade.*) traz prejuízo ao negócio.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Quando a LGPD e a ISO 27001 se conversam sobre isso? Quando se considera dados pessoais como ativos de Segurança da Informação.

Dentro do controle **A.8** da ISO 27001 é abordada a “Gestão de Ativos”. Nele é feita a inclusão de dados pessoais como ativo de segurança da informação e auxiliando ainda a organização durante o mapeamento dos dados pessoais. O controle vai além, e dá diretrizes quanto ao seu armazenamento, processamento e também tratamento.

Através desta gestão, poderão ser fomentados no Artigo 6º da LGPD, os 10 (dez) princípios para o tratamento de dados pessoais.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Privacy by Design e Privacy by Default

Assegurar aos titulares dos dados que haja privacidade durante todo o ciclo de vida dos seus dados, portanto, desde o momento em que ele é coletado, tratado e compartilhado, até o momento de sua exclusão é o que buscam os princípios da LGPD. Este também é o conceito denominado como *Privacy by Design* ou Privacidade desde a Concepção.

O conceito *Privacy by Design* também segue a ideia de incorporar garantias de privacidade para dados pessoais, em todos os projetos/produtos desenvolvidos, o que dá origem ao *Privacy by Default*.

Privacidade por Padrão ou *Privacy by Default* insere como mandatório que o usuário não deva necessitar configurar ou tomar qualquer ação para que tenha privacidade dos seus dados. Ela tem que ser automática, como uma configuração padrão.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Desta maneira, dentro da organização não seria permitido desenvolver nenhum projeto, produto ou serviço sem inserir como prioritário neste processo, a proteção da privacidade e a obediência ao correto ciclo de vida já citado.

A ISO 27001 possui também abordagem para este tema, onde diretrizes são dadas para “Aquisições, desenvolvimento e manutenção do sistema” e também faz a seguinte citação: “A segurança da informação é uma parte integrante dos sistemas de informação em todo o ciclo de vida”, em seu controle **A.14**.

Relação com fornecedores

A LGPD fala sobre papéis de controlador e operador no contexto do tratamento de dados pessoais. Qualquer atividade de tratamento realizada pelo fornecedor (operador) deve seguir todos os requisitos de conformidade com as regulamentações envolvidas acordadas via formalização contratual com o contratante (controlador).

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Durante o processo de implementação da Norma ISO 27001 o tema em questão também será tratado, uma vez que em seu controle **A.15.1** há diretrizes para a “Segurança da Informação na relação com fornecedores, onde serão tratadas proteções para os ativos da organização que são acessíveis pelos fornecedores.

Avaliação dos riscos

É prática básica na busca de adequação a LGPD, que se tenha real noção dos riscos a privacidade. Para tanto, é necessário que as organizações desenvolvam um relatório de impacto à proteção de dados pessoais (RIPD).

Este mesmo relatório, que em essência, é uma análise de riscos, também é requerido pela ISO 27001 e sua implementação fornece suporte em sua elaboração.

O controle **A.8.2.1** da Norma, trata sobre *Classificação da informação* e direciona: “A informação deve ser classificada em termos de requisitos legais, valor, criticidade e sensibilidade com relação a divulgação ou modificação não autorizada”.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Aqui a Norma em si, já pede atenção para obediências legais e sobre definição de valor, criticidade da informação.



1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?

É sempre mais complexo tratar um problema antes de ter real noção de suas dimensões, então antes de qualquer ação na busca por mais proteção para informações, é necessário que haja uma avaliação do grau de riscos e impactos que a organização possui. Só assim, poderão ser traçados planos para agir.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Gerenciando riscos você obtém:

■ Serviços resilientes

Menos paradas e interrupções serão percebidas durante atividades do cotidiano antes geradas por panes, perdas ou furtos de dados ou mesmo instabilidades na própria rede decorrentes de ataques cibernéticos, aumentando assim a eficiência e evitando retrabalhos;

■ Melhor prevenção de vazamentos

Durante análise de riscos de Segurança um dos maiores ofensores passa a ser dados pessoais sem o devido cuidado. Identificar esta fraqueza trará maior proteção contra vazamento de informações sensíveis ou dados digitais que podem provocar prejuízos;

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

■ Melhor proteção contra de perda de dados

Proteger e guardar dados importantes de clientes e funcionários durante todo ciclo de vida explicitado em acordos, consentimentos formais ou contratos, evita que a empresa tenha sérios prejuízos. Devemos lembrar que a perda de um dado é um incidente de Segurança e caso se trate de um dado pessoal está sujeita às sanções previstas na LGPD;

■ Precauções contra causas naturais ou mesmo acidentes

Sim, a Segurança das informações não pode ser ameaçada apenas por ofensores digitais. Acidentes e desastres naturais (tempestades, desmoronamentos, inundações etc.) ou criminosos (destruição ou dano de equipamento, incêndios, etc.), podem facilmente ocasionar prejuízos intangíveis, caso estes riscos não tenham sido gerenciados;

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

■ Ações específicas para manter o acesso mais controlado aos dados

Informações e dados só devem estar acessíveis para quem realmente precisa. Novamente, se o cenário envolve dados pessoais, a questão ganha outro patamar de relevância por conta da privacidade. Além disso, ter os dados apenas sob domínio necessário pode evitar, por exemplo, espionagens por parte de concorrentes ou qualquer outro ofensor mal-intencionado;

■ Alta credibilidade

Manter-se resiliente com boa saúde operacional, sem interrupções na produção, reduz o real impacto da perda de credibilidade. Ataques cibernéticos, captura e (ou) roubos de dados, tendem a prejudicar a reputação da organização, pondo em sério risco a confiança do usuário, consumidor, etc.

1

Segurança da Informação

2

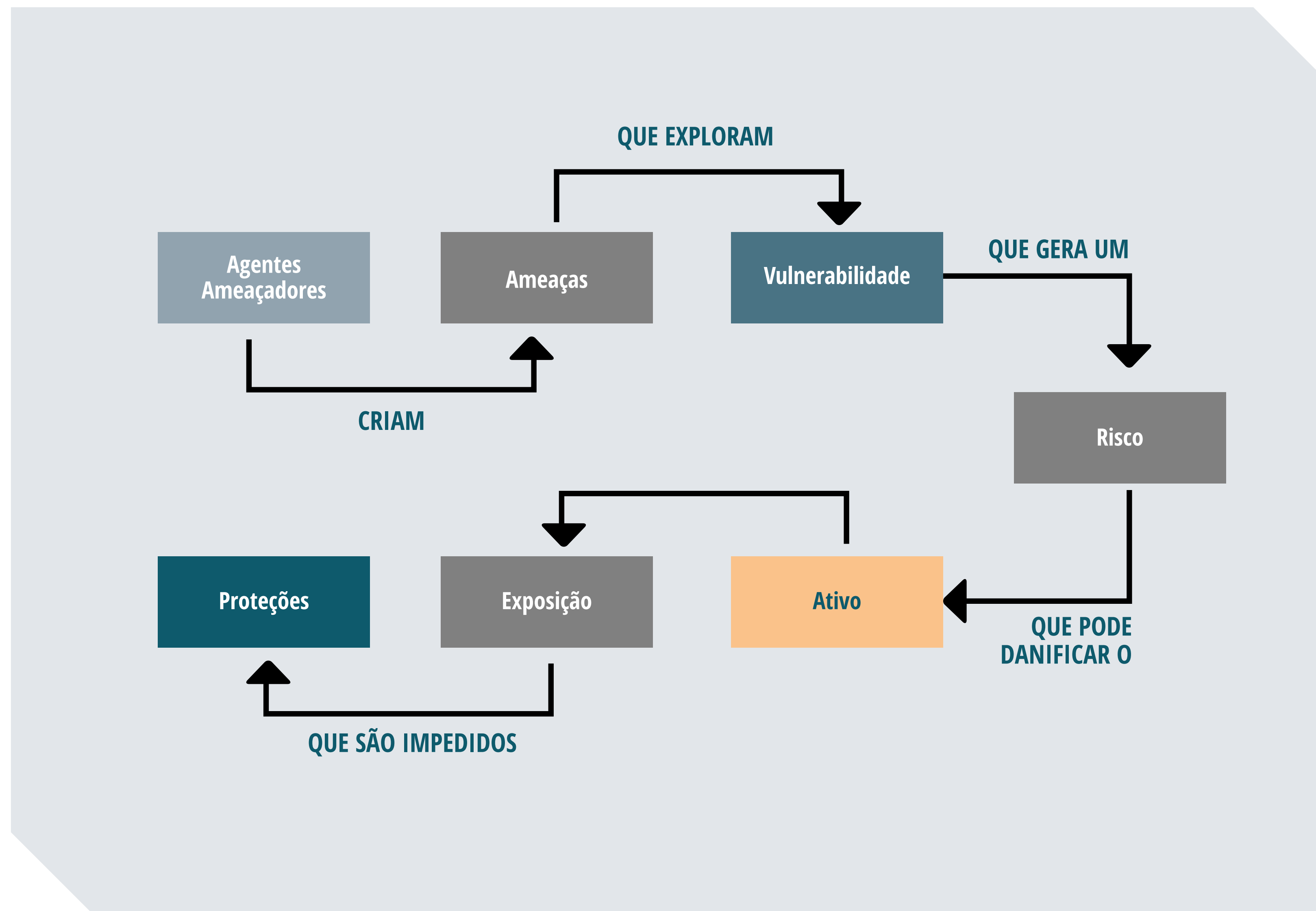
Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO



1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Síntese

A Segurança da Informação busca proteger com controles físicos e lógicos, qualquer tipo de informação cujo comprometimento de sua confidencialidade, integridade ou disponibilidade signifique prejuízo para seu dono ou responsável.

O fato da informação atualmente transitar cada vez mais em formato digital, faz com que a Cibersegurança seja a principal responsável pelo emprego das garantias que estas informações necessitam, por ser o braço da segurança da informação com elementos digitais de proteção.

Identificar riscos é eficaz para aplicar medidas adequadas de segurança na proteção das informações, ou seja, evitando esforços excessivos ou insuficientes, perda de tempo.

1

Segurança da Informação

2

Como os projetos de adequação à LGPD podem se beneficiar adotando a ISO 27001?

3

Qual é a relevância do Gerenciamento de Riscos para proteção de informações?



S3GURANÇA
DA INFORMAÇÃO

* * * *

Uma opção que as organizações possuem para nortear um trabalho de estruturação interna de segurança é a adoção de metodologias específicas já experimentadas pelo mercado.

Neste caso, a Norma ISO/IEC 27001 é uma excelente alternativa, bastando que a organização adapte as orientações para sua realidade. A norma também inclui abordagens que serão úteis durante uma iniciativa de adequação a Lei Geral de Proteção de Dados – LGPD, que colocou em outro patamar a proteção de dados pessoais, por estabelecer diversas exigências no trato de informações de cunho pessoal.

SOBRE O AUTOR

Renier Ponciano é gerente técnico do Time Hepta na Advocaica Geral da União. Membro da ANPPD, Auditor interno ISO 27001 e DPO, é um profundo conhecedor e ávido estudioso de tudo relacionado a segurança da informação.

SOBRE A HEPTA TECNOLOGIA

Há quase 30 anos atuando na prestação de serviços de tecnologia da informação, a Hepta tem como missão potencializar as competências e investimentos de TI de seus clientes para que possam focar em seu negócio. Por isso, está sempre em busca de soluções ágeis e inteligentes para resolver problemas, otimizar negócios e criar oportunidades.

Sua Central de Serviços Compartilhados (CSC) reúne especialistas das mais diversas áreas, somando cerca de 150 competências técnicas diferentes. Atua na elaboração e execução de projetos e consultorias especializadas para apoiar a governança de TI, tanto na adequação à LGPD como

Vamos bater um papo sobre
a sua estratégia digital de negócios?



contato@hepta.com.br



[hepta-informatica-ltda](https://www.linkedin.com/company/hepta-informatica-ltda)



[/heptatecnologia](https://www.facebook.com/heptatecnologia)



<http://bit.ly/hepta-wap-business>