Passo a passo para se adequar à Lei Geral de Proteção de Dados (LGPD)

ÍNDICE

Passo a passo de como se adequar à Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) foi sancionada em 2018, pelo ex-presidente Michel Temer, e tem como objetivo disciplinar o tratamento dos dados pessoais dos brasileiros. É por conta disso que é importante se adequar a essa lei e incluí-la no plano de conformidade da organização.

Por se tratar de algo novo e sobre um tema para o qual, até então, não havia uma especificação clara, muitas empresas ainda não sabem o que precisam fazer para se adequar à Lei Geral de Proteção de Dados e como devem proceder nesse sentido.

Foi pensando nisso que desenvolvemos este post. Elaboramos um passo a passo para que você saiba como proceder para que sua empresa cumpra essa legislação e garanta a segurança dos seus clientes, colaboradores e fornecedores. Ficou interessado em obter essas informações? Então, siga conosco agora mesmo!

1 - Identifique as fontes de coleta de dados

O primeiro passo para se adequar à Lei Geral de Proteção de Dados é identificar as fontes de coleta de dados. Deve-se fazer um mapeamento para que se possa identificar todas as informações dos públicos que são coletadas na organização.

As informações podem ser coletadas em cadastros feitos pelos clientes e fornecedores, em contatos telefônicos, em e-mails trocados etc. É necessário mapear todas essas fontes, para que nada seja negligenciado e nenhum dado seja obtido sem que se tenha conhecimento disso.

2 - Classifique os dados

Para incluir a LGPD no plano de conformidade, também é necessário fazer uma classificação dos dados. Para essa lei, são considerados dados pessoais qualquer informação que possa identificar uma pessoa. Assim sendo, o nome, o telefone, o endereço, entre outros são incluídos nessa classificação.

Existe também os dados considerados sensíveis, que exigem ainda mais cuidado em seu tratamento e sigilo, como:

- Origem racial ou étnica;
- Convicção religiosa;
- Opinião política;
- Filiação a sindicato ou a organização de caráter religioso, filosófico ou político;
- Dado referente à saúde ou à vida sexual;
- Dado genético ou biométrico, quando vinculado a uma pessoa natural.

Por fim, existe o dado anonimizado, relativo ao titular que não possa ser identificado. Essa é uma alternativa para dispensar a necessidade do consentimento, uma vez que os dados que não identificam de forma direta ou indireta o seu titular (ou seja, anonimizados), não podem causar-lhe danos e, portanto, não requerem a proteção da lei.

3 - Verifique os papéis e as responsabilidades

A relação entre compliance e LGPD também precisa ter clareza sobre os papéis e responsabilidades que devem ser cumpridos. A empresa tem o dever de solicitar o consentimento dos seus públicos sempre que forem registrados os seus dados, seja por meios digitais, seja por meios tradicionais.

Também é uma responsabilidade da organização garantir o sigilo e a proteção dos dados. De tal modo, é proibido que a empresa venda, divulgue ou repasse as informações de qualquer pessoa para terceiros, sem a devida autorização.
Para dividir essas responsabilidades de forma clara, está previsto na lei a definição dos agentes de tratamento, que são:

•**Controlador** – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

•**Operador** – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
•**Encarregado** – pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional (também conhecido como Data Protection Officer – DPO);

Esses cargos devem ser ocupados por pessoas que realmente tenham tal competência, onde representaram a organização no caso de um incidente, podendo inclusive, também ser responsabilizados ou punidos.

4 - Realize o Data Discovery e a identificação do ciclo de vida dos dados

O Data Discovery é um processo de levantamento geral de quais informações são coletadas e onde exatamente elas estão armazenadas, consolidando a visualização e identificação desses dados, para que as empresas possam classificá-las, detectando padrões e possíveis anormalidades nas informações.

Em seguida, será necessário mapear o ciclo de vida dos dados, ou seja, saber quando os dados têm início em sua coleta, qual a trajetória deles dentro da sua empresa e seu fim quando não serão mais utilizados. As informações que concluírem seu ciclo de vida e, de acordo com o consentimento e necessidade, devem ser descartadas.

5 - Tenha controle de acesso

Ter o controle de acesso em relação aos dados de seus contatos é uma boa política de compliance e LGPD. Devem ser tomados cuidados para que apenas pessoas autorizadas tenham acesso a dados sigilosos.

Deve ser definido o limite de acesso e de manipulação dos dados de acordo com o seu nível de responsabilidade, finalidade e política de acesso da empresa.

Quando alguém disponibiliza os seus dados para uma empresa, ele está confiando nessa organização. Logo, eles não podem vazar sob nenhuma hipótese! É por isso que investir em segurança da informação, como nos softwares criptografados, é uma alternativa interessante.

6 - Garanta o consentimento

Conforme explicamos, no plano de conformidade de LGPD, é preciso garantir o consentimento das pessoas sempre que um dado for coletado. Este consentimento deverá ser armazenado durante todo ciclo da informação, com opção de consulta e solicitação de revogação por parte do seu titular.

A solicitação do consentimento tem que ser transparente e específica, não gerando confusão para o titular ou induzindo ao erro. A opção de acesso a uma política de privacidade no momento do da coleta do consentimento, detalhando de forma mais completa como e onde será utilizada aquela informação pessoal, é a opção atual mais recomendada.

7 - Faça a revisão de contratos

Para se adequar à Lei Geral de Proteção de Dados, também é recomendado que se faça a revisão de contratos que a empresa tem. Como antigamente não era necessário ter o consentimento das pessoas para que os dados fossem registrados, pode ser que você tenha documentos antigos com irregularidades.

Revisar os contratos, portanto, é uma boa prática para que esses documentos sejam atualizados, de acordo com as especificações da nova legislação.

8 - Conheça as exceções ao consentimento

A LGPD também traz algumas exceções aos consentimentos, ou seja, algumas situações em que eles não se fazem necessários. Isso acontece quando as informações foram tornadas públicas pelo titular por livre e espontânea vontade, em alguns canais, como as redes sociais. São exemplos de exceções:

- Cumprimento de obrigação legal;
- Execução de contrato;
- Interesses legítimos do controlador ou de terceiro;
- Proteção do crédito;
- Proteção da vida;
- Tutela da saúde;
- Processo judicial, administrativo ou arbitral;
- Estudos ou pesquisas; e
- Políticas públicas.

Apesar disso, na relação entre compliance e LGPD, também se deve considerar a boa-fé, a finalidade e o interesse público da coleta e da disponibilização de dados das pessoas , mesmo que eles tenham os tornado públicos.

9- Elaboração do relatório de impacto

É importante que tudo seja documentado na empresa. Assim, evitamos correr riscos, como o uso inadequado dos dados por negligência. Os relatórios de impacto devem atender às questões específicas da LGPD.

A elaboração desse relatório precisará de uma mescla entre conhecimentos técnicos sobre a parte tecnológica e conhecimentos jurídicos para cumprir o formato desejado. Criando a necessidade da comunicação entre os departamentos ou pedir auxílio externo especializado para empresas terceirizadas.

Existem softwares que podem ajudar na emissão e no controle desses relatórios, para que todas as informações possam ser sempre acompanhadas e estar armazenadas de forma segura na empresa.

10 – Monitoramento, avaliação e revisão dos processos

O último passo para se adequar à Lei Geral de Proteção de Dados é fazer o criar os processos de monitoramento, avaliação e revisão dos processos. O objetivo é que o trabalho implementado siga sendo realizado de forma natural, sem que as adequações precisem ser sempre retomadas.

Para isso, é preciso que todo o trabalho realizado seja sempre monitorado e avaliado de forma constante para que esteja dentro das normas de compliance da empresa, e seja revisado quando necessário.

Em novos projetos é importante que o DPO, assim como a área de Risco, estejam envolvidos em todos os projetos de TI, principalmente aqueles que tratem de inovações, visando garantir a conformidade com a lei, e a implementação dos controles adequados.

Uma boa maneira de garantir que tudo isso seja realizado e fazer com que a LGPD esteja no plano de conformidade da organização é contar com um serviço especialização na implementação dessa legislação.

Entendeu como se adequar à Lei Geral de Proteção de Dados? A Athena Security, empresa especializada em segurança da informação, pode ajudar nesse sentido. Para saber mais, entre em contato conosco! Teremos satisfação em contribuir para que a sua empresa saiba como lidar com os dados dos seus clientes, funcionários, fornecedores etc.

A APP LGPPD é uma empresa especializada em segurança da informação, gestão de privacidade de dados, monitoramento e infraestrutura. Possuímos atendimento através de um SOC (Security Operation Center) 24×7, com uma equipe de profissionais certificados nas soluções ofertadas.

Nosso principal diferencial é o atendimento consultivo orientando nossos clientes a seguirem as melhores práticas de mercado, de acordo com a ISO 27000, NIST Cybersecurity Framework, (ISC)², a lei N° 12.965/14 do Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD).

MSS Firewall Gerenciado

Gerenciamento do seu ambiente de firewall garantindo a segurança e disponibilidade do seu negócio.

NOC Monitoramento de TI

Obtenha seu próprio NOC de monitoramento e possua o total controle da sua infraestrutura de tecnologia através do sistema ZABBIX.

Rede Wireless

Deixe de usar soluções caseiras! Profissionalize sua rede WI-FI e aumente a qualidade, desempenho e controle do acesso à internet através de dispositivos sem fio.

Captive Portal com Login Social

Já pensou em fornecer acesso à internet e alcançar novos clientes ao mesmo tempo? Conheça a nossa Solução de Captive Portal integrado com Login Social.

EndPoint Protection

Obtenha a proteção necessária das suas estações e dispositivos móveis, contra ataques de ransomware ou qualquer outro malware.

Estruturação de Redes

Estruture e segmente sua rede de acordo com as melhores práticas, obtendo melhor desempenho e protegendo os seus dados corporativos.

Service Desk e Gerenciamento de Serviços

Centralize as comunicações de suporte entre o TI e seus usuários melhorando o desempenho de sua equipe e a satisfação de seus clientes.

Análise de Vulnerabilidade

Descubra a situação atual de segurança da sua rede, mitigando os riscos de ataques e invasões, elevando o nível de segurança de seus dados.

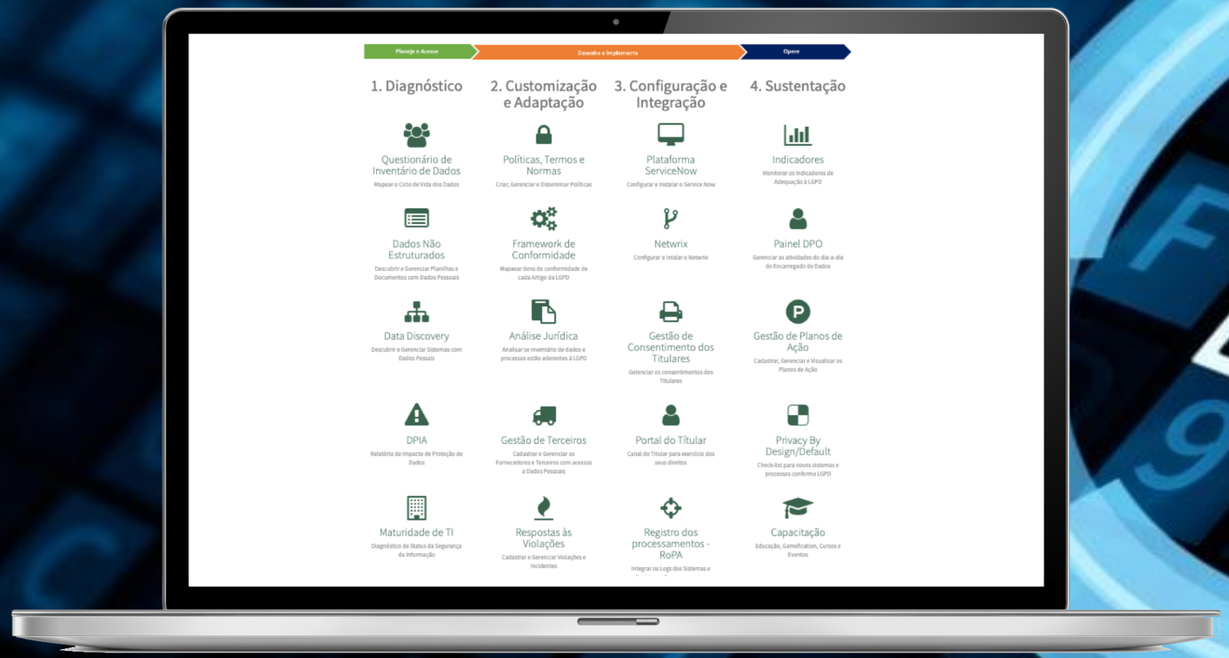
Backup em Nuvem

Nosso serviço de Backup em Nuvem é automatizado, criptografado, compactado, catalogado, e armazenado com segurança em servidores remotos especializados, permitindo acesso imediato 24 horas por dia, 7 dias por semana a seus dados.

Consultoria de Conformidade LGPD

A nova Lei Geral de Proteção de Dados (LGPD) pode influenciar a sua captura de dados de usuários. Por isso, você precisa entender quais os cuidados que deve tomar para não ser penalizado e assim, evitar grandes prejuízos.

Data Discovery



Ações de Gestão do Software:

Deletar, Mover, Quarentenar, Editar Base Legal para tratamento do Dado, Localizar Titular do Dado, Apresentar total por tipo de Dado processado, Anonimizar ou pseudo-anonimizar.

Data Discovery

Descoberta de Arquivos

Classificação do arquivo

Auditoria

Valida propriedade original.

Tratamento e Qualificação

Realizado por tipo de dado

Integração com base de Consentimento

Barra de Progressão

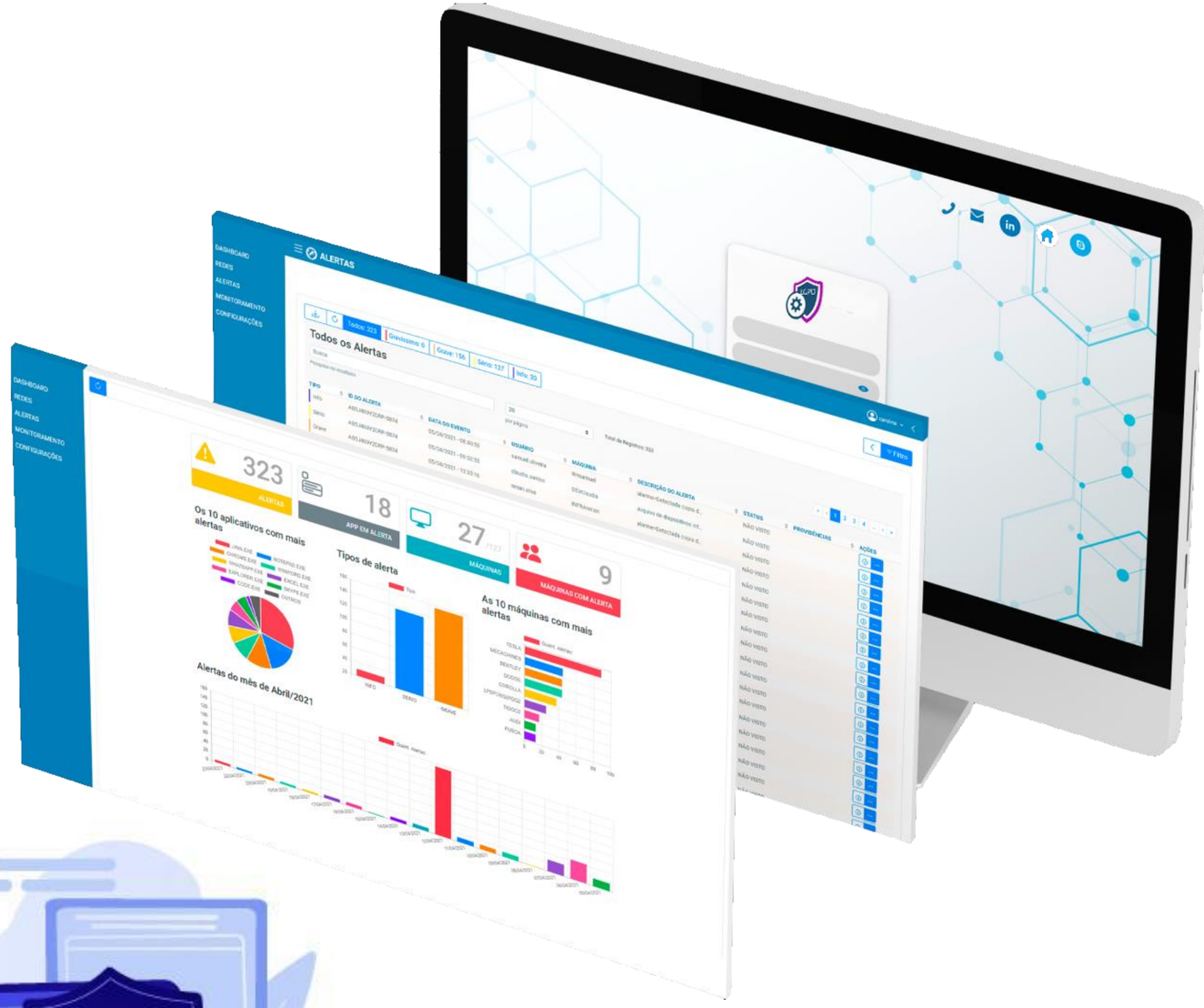
Informações sobre o término do processo.

Identificador único

Rastreabilidade e Governança

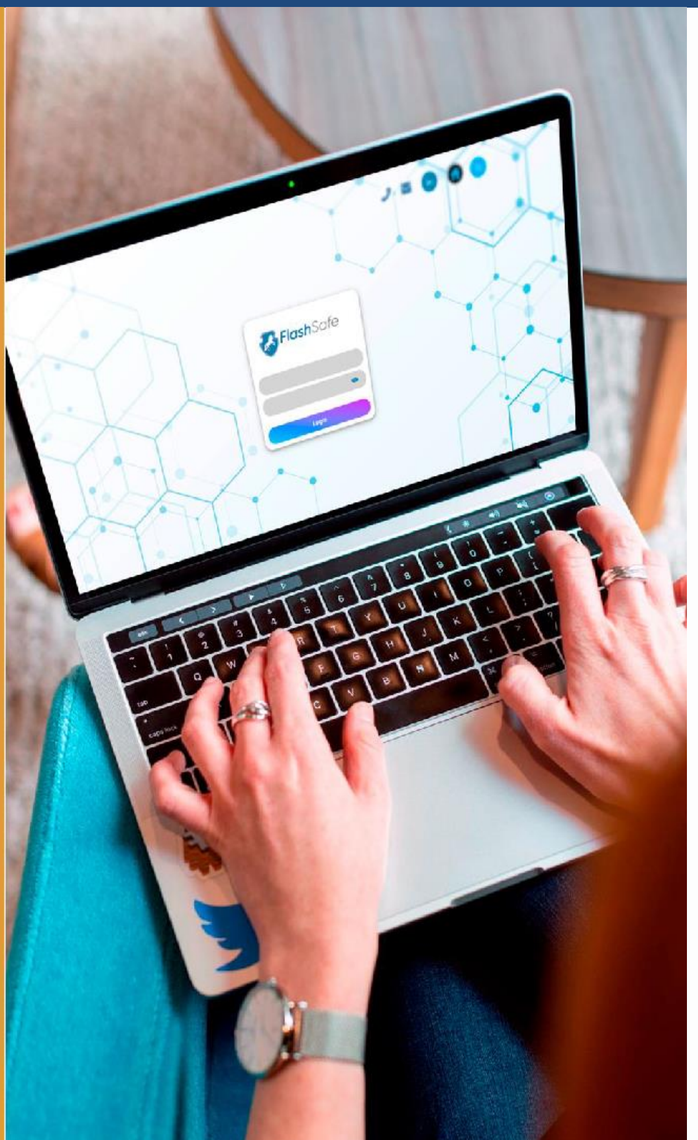
Localizador do titular de dados

Realizado por tipo



APP LGPD

DLP - Data Loss Prevention



O Software é uma solução de Cibersegurança e Produtividade para sua Empresa

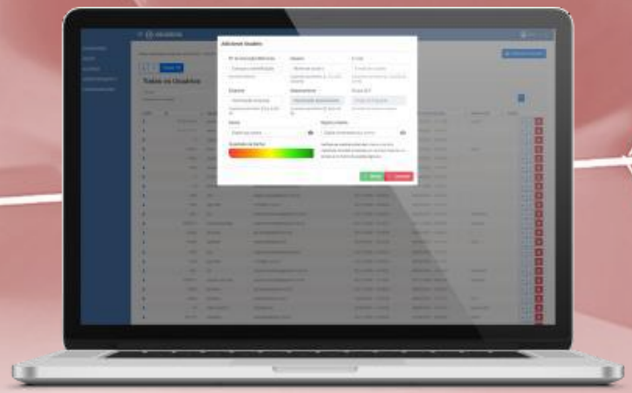
Em conformidade com a LGPD e o contexto do Home Office, o FS é focado na integridade de dados ao evitar que vazamentos ocorram, de dentro para fora das empresas, por colaboradores ou parceiros, de forma intencional ou acidental

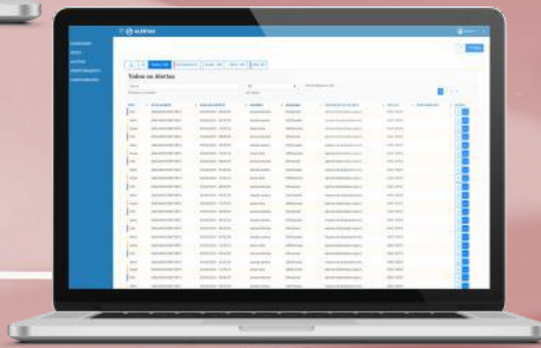
A gestão e interação remota permite o suporte e trabalho em conjunto com os times

1/3 dos dados vazam de dentro para fora!

DLP - Data Loss Prevention

Gestão dos dados de todos
Os departamentos de sua empresa





GERAÇÃO DE EVIDÊNCIA EM TEMPO REAL

A Solução identifica criação do dado sensível e gera evidência para posterior utilização.

NÃO INVASIVO

O foco é o dado sensível e não tudo o que o usuário faz a solução preserva a privacidade do usuário e máquina em tudo o que não está relacionado aos dados sensíveis.

SOFTWARE LEVE

Baixo consumo de CPU e memória, solução desenvolvida para atuar em estações com 4Gb de memória, sem conflitos com o dia a dia de cada usuário. Solução não invasiva.

Obrigado por sua Atenção

Fale com nossos Especialista:
(11) 4134-1720