



LGPD

LEI GERAL DE
PROTEÇÃO DE DADOS
&
SEGURANÇA DA
INFORMAÇÃO



SkyShield
S A F E



Desde o advento da internet, nunca, na história, se acumulou tanta informação. Com a crescente demanda de circulação da informação, foi necessário desenvolver uma lei que protegesse os dados compartilhados diariamente, sobretudo os dados de pessoa física, com isso, para controlar o uso das informações pessoais, foi criada a

LGPD.

www.skysshield.com.br

TÓPICOS

01

CONCEITOS

02

RESPONSABILIDADES

03

BOAS PRÁTICAS

04

ABRANGENCIA E SANÇÕES



SkyShield
S A F E

CARTILHA INTERATIVA

CLICK NOS TÓPICOS E NOS
BOTÕES PARA AVANÇAR OU
VOLTAR A PÁGINA.



CONCEITOS

O QUE É SEGURANÇA DA INFORMAÇÃO?

É um conjunto de controles que definem procedimentos, responsabilidades e formas de gerenciamento dos riscos, aplicado na proteção da informação.

O QUE É INFORMAÇÃO?

Informações da EMPRESA em sua forma verbal ou escrita, em suporte físico ou digital, armazenada, trafegada ou em trânsito na infraestrutura tecnológica.

Na empresa podem ser de caráter jurídico, comercial, administrativo, estratégico, técnico, financeiro, mercadológico, legal, de recursos humanos ou de qualquer outra natureza, bem como todas as informações adquiridas por associação, aquisição, licença, compra ou confiadas por clientes e terceiros.

O QUE É LGPD?

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, nº 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade de pessoas físicas.

Essa lei estabelece como os dados pessoais devem ser tratados, dispostos em meio físico digital, feito por organizações públicas ou privadas.

CONCEITOS

O QUE É PRIVACIDADE?

É o direito de todo indivíduo de ter suas informações pessoais preservadas, garantindo que ele possa conduzir sua vida de acordo com suas convicções, interesses e prioridades, de forma protegida.

O QUE É ATIVO?

Bens da EMPRESA que possuem valor econômico, incluída a informação e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento (ex.: móveis, servidores, notebooks, tablets, impressoras, scanners, firewalls, switches, softwares etc.).

O QUE É TITULAR DE DADOS?

O titular de dados é toda pessoa a quem se referem os dados em uso.

O QUE É CONTROLADOR?

É a parte interessada na privacidade que determina os objetivos e os meios para o tratamento dos Dados Pessoais e que não é pessoa natural que usa os dados para objetivos pessoais.



CONCEITOS



O QUE É OPERADOR?

É a parte interessada na privacidade, que faz o tratamento dos Dados Pessoais em benefício e de acordo com as instruções de um controlador.

O QUE É TRATAMENTO DE DADOS PESSOAIS?

Qualquer operação que podemos fazer com dados pessoais, tais como a coleta, o armazenamento, o compartilhamento e mesmo a eliminação dos dados.

O QUE É DADO PESSOAL?

Quaisquer dados a partir dos quais podemos identificar uma pessoa natural ou física direta ou indiretamente, a depender do contexto, por exemplo, seu nome, seu endereço e seu CPF.

O QUE É DADO PESSOAL SENSÍVEL?

Dado pessoal sensível são as informações que exigem um pouco mais de atenção, são os dados que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.



CONCEITOS

QUAIS SÃO OS DIREITOS DO TITULAR DE DADOS?

O titular tem muitos direitos, como por exemplo: eles podem querer saber:

- ❖ Se a EMPRESA tem dados dele?
- ❖ Quais os dados que a EMPRESA tem dele?
- ❖ Como ela pode corrigir estes dados?
- ❖ Ela pode pedir para excluir os dados que a EMPRESA tem.
- ❖ Ele pode inclusive querer saber com quem a EMPRESA compartilhou os dados dele.

Em qualquer caso, informe que a EMPRESA se compromete a responder todas as solicitações em conformidade com a legislação, e informe para o seu gestor.

COMO PROTEGER A INFORMAÇÃO DA EMPRESA?

As informações podem existir de muitas maneiras, sendo: escrita em papel, armazenada e transmitida por meios eletrônicos, exibida em áudio e vídeo ou falada em conversas formais ou informais.

Seja qual for a forma ou o meio pelo qual a informação é apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com os controles definidos na política de Segurança da Informação.

AS EMPRESAS SE RESERVAM O DIREITO DE PROTEGER E MONITORAR ADOTANDO ALGUNS PROCEDIMENTOS.



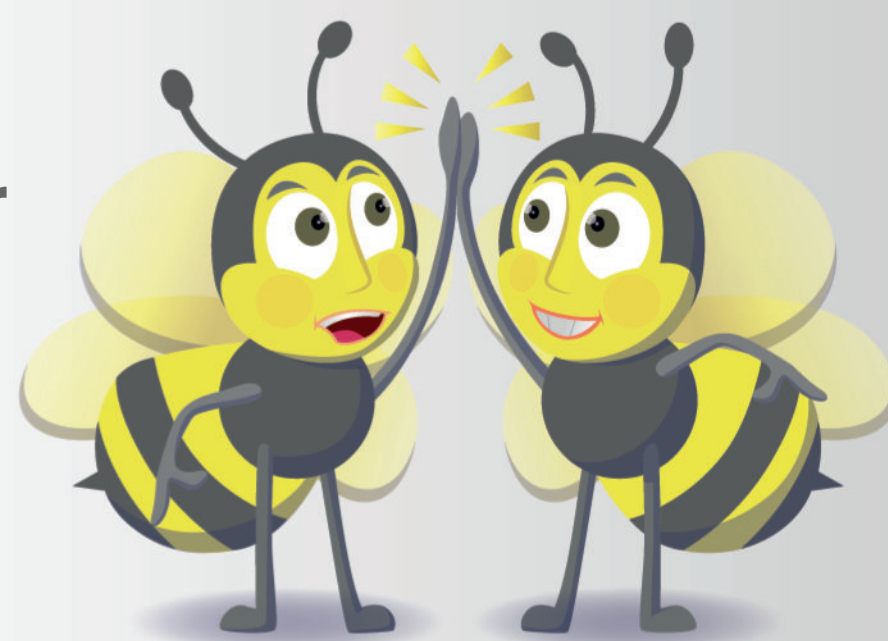
RESPONSABILIDADES

Como objetivo principal, a **SEGURANÇA DA INFORMAÇÃO** vem resguardar a empresa quanto à **confidencialidade, integridade e disponibilidade das informações** sob sua gestão e responsabilidade. Além disso, tem objetivo de:

- ❖ Direcionar a implementação de controles e processos internos;
- ❖ Estabelecer diretrizes para que todos sigam padrões de comportamento aceitáveis de acordo com a Segurança da Informação;
- ❖ Estabelecer formas de proteção da PRIVACIDADE e dos dados pessoais no nosso dia a dia;
- ❖ Gerir de forma segura os ativos de hardware, software, redes e comunicações da empresa e monitorar suas aplicações;
- ❖ Reduzir os riscos de impacto negativo ao negócio, resultado de uma falha de segurança.
- ❖ Orientar a equipe que as informações são de propriedade da EMPRESA e devem ser utilizada somente para os propósitos do negócio.

O QUE CABE A CADA COLABORADOR?

- ❖ O colaborador não pode, em qualquer tempo ou sob qualquer propósito, apropriar-se de informações, tampouco delas se aproveitar, se beneficiar ou divulgar a pessoas que não façam parte da empresa.
- ❖ Todos deverão **manter a privacidade e a confidencialidade** de quaisquer informações sensíveis e/ou privilegiadas obtidas no desempenho de suas funções profissionais.
- ❖ Informações sobre clientes, projetos, parceiros, **não devem ser publicadas** em qualquer site, e-mail, mídias sociais, entre outros. Exceções podem ocorrer quando o material a ser divulgado for devidamente autorizado pelo cliente, parceiro ou responsável da EMPRESA.
- ❖ Todos devem trabalhar de forma **ética e honesta**, e de forma alguma se envolver em ações que possam colocar em risco a sua credibilidade pessoal e profissional ou a credibilidade da EMPRESA.
- ❖ Todos devem relatar as informações completas e adequadas, inerentes aos resultados dos trabalhos, revelando todos os fatos significativos à EMPRESA.





AO TOMAREM CONHECIMENTO DE QUALQUER SUSPEITA OU FRAGILIDADE DE SEGURANÇA, DEVERÃO NOTIFICAR O FATO, FAZENDO CONTATO COM SEU GESTOR OU COMUNICANDO À EQUIPE DE SEGURANÇA DA INFORMAÇÃO IMEDIATAMENTE.

DICAS DE SEGURANÇA DA INFORMAÇÃO.

- ❖ Procure sempre identificar o motivo para cada rotina que precise solicitar dados pessoais e que apenas sejam solicitados os dados indispensáveis para essa atividade;
- ❖ Mantenha os dados pessoais sempre corretos e atualizados de forma que a consulta seja facilitada;
- ❖ Seja sempre transparente sobre as operações com os dados pessoais;
- ❖ Apenas compartilhe os dados pessoais internamente ou com terceiros se isso for estritamente necessário;
- ❖ Em relação aos clientes, lembre-se de que a privacidade e a proteção de dados pessoais são importantes nos nossos serviços e devem ser sempre valorizados.



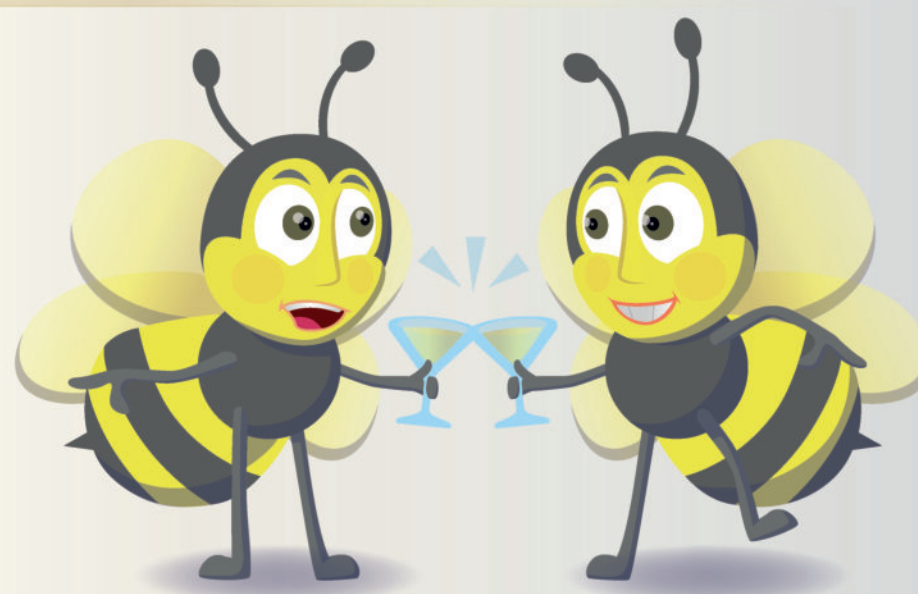


Senhas são pessoais, intransferíveis e de uso exclusivo:

- ❖ Evite a composição de senha com o nome ou sobrenome do usuário, nome da conta de usuário, nome da empresa ou qualquer variação deles; ou com informações do usuário que possam ser facilmente obtidas por terceiros, tais como, mas não se limitando a: RG, CPF, placa de automóvel, número de telefone, data de aniversário e endereço;
- ❖ Recomenda-se que as senhas para os **USUÁRIOS** devem ser compostas por uma quantidade mínima de 8 (oito) caracteres combinando letras (A, B, C, a, b, c...), números (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) e caracteres especiais (@ # \$ % & ...); devendo ser alteradas periodicamente a cada 90 dias, bem como a utilização de duplo fator de autenticação;
- ❖ **Cuidado com as senhas de comércio eletrônico, aplicativos e portais utilizados para compras.** As informações da EMPRESA e dos seus clientes são sigilosas e devem ser utilizadas apenas para a finalidade para a qual foi coletada e o acesso a ela só deve ser realizado mediante autorização.



CUIDADO COM O CONVÍVIO SOCIAL!



Como seres humanos somos sociáveis e muitas vezes falamos sobre assuntos do trabalho e mesmo sem intenção criamos vulnerabilidades.

Para evitá-las por meio deste tipo de contato com outras pessoas, seguem algumas recomendações:

- ❖ Jamais divulgar sua senha, pois ela é utilizada como assinatura eletrônica e deve ser mantida em sigilo;
- ❖ Cuidado ao digitar senhas ou acessar máquinas de terceiros, especialmente fora da empresa;
- ❖ Somente aceitar ajuda técnica de um membro da equipe da área de TI ou de segurança da EMPRESA, previamente apresentado e identificado;
- ❖ Cuidado ao executar procedimentos técnicos duvidosos cujas instruções tenham chegado por pessoa ou e-mail desconhecido;
- ❖ Sempre relate pedidos externos ou internos que venham a discordar dos tópicos anteriores;
- ❖ Organizar sua mesa de trabalho, não deixando visíveis dados escritos ou impressos a terceiros.

BOAS PRÁTICAS



CUIDADO COM O ACESSO FÍSICO DE VISITANTES NA EMPRESA.



O acesso das pessoas nas dependências da empresa deve ser controlado e, quando acessadas, o visitante deverá sempre ser acompanhado por um colaborador da EMPRESA.

CUIDADO COM O USO DOS CELULARES DA EMPRESA!

Para todos os celulares fornecidos aos profissionais para a realização das tarefas e funções diretamente relacionadas ao trabalho, os seguintes cuidados devem ser adotados para que o celular não seja danificado, furtado ou roubado:

- ❖ O colaborador é responsável pela segurança do celular que lhe foi fornecido, devendo mantê-lo em sua posse sempre que possível; quando guardado, deve ser em um local seguro, de preferência fora de vista;
- ❖ Não deixar o celular em veículos estacionados ou na posse de terceiros;
- ❖ Em caso de perda do celular, o responsável deve notificar à administração da empresa o fato imediatamente;
- ❖ Para os casos de furto ou roubo, é necessário que se faça um boletim de ocorrência;
- ❖ Em caso de desligamento do profissional, o celular deverá ser devolvido no momento do desligamento.



BOAS PRÁTICAS



CUIDADO COM O USO DAS MENSAGENS INSTANTÂNEAS.

Todos devem tomar todos os cuidados necessários quanto às mensagens instantâneas, pois o uso de plataformas em nuvem não corporativas em sua maioria para troca de mensagens instantâneas por SMS, WhatsApp®, Telegram® e similares, se tornou muito comum e difundido no mundo entre as pessoas e entre empresa e consumidor.

Deve-se fazer uso consciente e adequado deste tipo de comunicação, pois pode existir muita troca de INFORMAÇÃO através de textos, voz (áudio), imagens (foto e vídeo), documentos (arquivos) etc.;



Pode ocorrer perda acidental, roubo ou furto de equipamento, no qual os dados permanecem na memória do dispositivo, representando um risco para a empresa e/ou para pessoas. Vale lembrar que esse tipo de comunicação passou a ser alvo de ataques e fraudes cibernéticas.

CUIDADO COM O USO DO SEU CELULAR PARTICULAR!

O gestor da área deverá ser avisado e aprovar o uso de celulares pessoais. Este uso está vinculado às necessidades de acordo com a sua função e atividades.

ABRANGÊNCIA E SANÇÕES

Com base na Lei Geral de Proteção de Dados (LGPD), a EMPRESA, em seu entendimento sobre a questão de dados pessoais e privacidade, define que todas as informações pessoais e, principalmente, **DADOS PESSOAIS SENSÍVEIS**, devem ser protegidos com a utilização de medidas técnicas e administrativas de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou divulgação.

**ESCLARECEMOS NESTA CARTILHA
COMO TRATAR OS DADOS PESSOAIS
EM ACORDO COM A LGPD.**



Link da Lei

<https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>

ABRANGÊNCIA E SANÇÕES

ASPECTO TÉCNICO E LEGAL.

Esta cartilha foi escrita como base na Lei Geral de Proteção de Dados (LGPD), nas práticas para a gestão da segurança da informação das normas ABNT ISO/IEC 27001 e 27002; nas práticas de privacidade das normas ABNT ISO/IEC 27018, 27701, 29100 e 29152 e nas práticas de gestão de riscos da norma ABNT ISO/IEC 31000.

A VIOLAÇÃO DESSAS INFORMAÇÕES APONTADAS PODERÁ ACARRETAR, DESDE PENALIDADE DISCIPLINAR, ATÉ CRIMES DE INFRAÇÃO À LEGISLAÇÃO.



CLICK nos ícones
e entre em contato



◀◀ ANTERIOR

TÓPICOS

FIM

