



POLÍTICA DE PRIVACIDADE DE DADOS

SUMÁRIO

Controle do Documento	3
Registro de Alterações	3
Revisores	3
Justificativa	6
Escopo	6
Conceitos e Siglas	6
Cultura de Privacidade e Proteção de Dados	6
Os pilares da nossa cultura de privacidade	7
Diretrizes	8
Dados de Funcionários	8
Dados de Terceiros	9
Dados dos nossos clientes	9
Ações de Coleta de Dados	10
Ciclo de vida dos dados de colaboradores	10
Área Comercial (Pré e Pós-venda)	11
Área Financeira	11
Área de Gestão de Pessoas	11
Área de TI	11
Contratos	12
Papéis e Responsabilidades	12
Comitê de Privacidade e Proteção de Dados	12
Direitos do titular	13
Em caso de violação	13
Nossa estratégia, missão e próximos passos	14
Questões em aberto	15
Questões finalizadas	15



Justificativa

Esta política se faz necessária, pois a **Green Iluminação** considera que a privacidade e a proteção de dados são valores importantes que fazem parte da sua cultura organizacional. Faz parte da nossa missão desenvolver soluções tecnológicas que englobam a privacidade desde a concepção e ajudar nossos clientes com as necessidades de proteção de dados.

Desde o anúncio da Lei Geral de Proteção de Dados, a **Green** mantém seus processos, procedimentos e políticas para estar adequada.

Escopo

A Green está comprometida a somente tratar dados pessoais, sejam de seus colaboradores, seus clientes, fornecedores, parceiros e terceiros, com o mais alto nível de cuidado, confidencialidade e conformidade com as legislações aplicáveis.

Nossos colaboradores, gestores e administradores devem sempre, no exercício de suas atividades, garantir que dados pessoais são tratados em conformidade com a lei e com esta Política.

Caso você tenha alguma dúvida em relação às suas obrigações, direitos e deveres em relação ao tratamento de dados pessoais, entre em contato com nosso Encarregado pela Proteção de Dados Pessoais por meio do e-mail: **contato@greenengbrasil.com.br**

Conceito e Siglas

Abaixo listamos um pequeno glossário, onde você verá os significados de alguns conceitos adotados para a LGPD e que são usados em alguns pontos dessa política.

Privacidade: Direito de ser protegido de uma interferência em assuntos pessoais e familiares.

Privacy by Design: Privacidade desde a concepção e longo do ciclo de vida de todo o projeto. Garantir que novos produtos e serviços, já nasçam com as questões de privacidade e proteção de dados contemplados.

Fake News: Compartilhamento de notícias que são falsas.

DPO: Data Protection Officer ou Encarregado de dados, é o profissional que, dentro de uma organização, é encarregado de cuidar das questões referentes à proteção de dados pessoais da organização.

A presente política foi elaborada com base nos documentos:

- Lei federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, "LGPD" - Disponível em: http://www.planalto.gov.br/ccivil_03/Ato2015-2018/2018/Lei/L13709.htm



- Lei Federal nº 13.853/2019, responsável por alterar a Lei Geral de Proteção de Dados, “LGPD” – Disponível em: http://www.planalto.gov.br/ccivil_03/Atos2019-2022/2019/Lei/L13853.htm

Dados Pessoais	<p>Qualquer informação relativa a uma pessoa singular identificada ou identificável (“Titular”).</p> <p>É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.</p>
-----------------------	--

Dados Pessoais Sensíveis	Qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.
Anonimização	Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento.
Encarregado (Data Protection Officer)	Pessoa responsável pela Proteção de Dados Pessoais na Companhia e pela comunicação com a ANPD e com os titulares, contatável pelo e-mail: contato@greenengbrasil.com.br
Titular	Pessoa a quem os dados pessoais se referem.
Tratamento	Qualquer operação efetuada sobre dados pessoais, por meio automatizados ou não automatizados, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
Controlador (a)	Pessoa a quem competem as decisões sobre o tratamento dos dados pessoais.
Operador (a)	Pessoa que realiza o tratamento de dados pessoais em nome do(a) controlador(a).
ANPD	Autoridade Nacional de Proteção de Dados.



Cultura de Privacidade e Proteção de Dados

Inspirados na cultura Privacy by Design, na Green, entendemos que privacidade e a proteção de dados, deve ser algo a ser encarado como uma cultura dentro e fora da empresa. Ao encarar este tema como cultura, elevamos seu nível de importância e ao mesmo tempo que o tornamos um hábito, sem burocracias, regras engessadas e letras miúdas.

Os pilares de nossa cultura de privacidade:

Nos comprometemos a proporcionar segurança e proteger os dados dos nossos clientes, dando controle e trazendo facilidades para o manuseio dos seus dados pessoais no dia a dia.

Faz parte da nossa cultura os seguintes itens:

- Consultar, divulgar e compartilhar somente informações conhecidas como públicas e verdadeiras: O que você encontrar em nossas redes sociais e site da empresa, fique à vontade para repassar adiante. Outras fontes, mesmo que mídias conhecidas, sugerimos que analise com cuidado a autenticidade, pois não desejamos que você caia nas famosas *Fake News*.
- **Os dados pessoais dentro da empresa:** dados dos nossos clientes, consumidores, funcionários ou terceiros, devem ser guardados a “7 chaves” e somente acessado por perfis correspondentes. Se você considera que está vendo informações além do seu perfil, não deixe de entrar em contato com a Segurança da Informação: para contato@greenengbrasil.com.br
- **Aplicações Corporativas e Chat Interno:** Nós sabemos que a comunicação é um dos pilares mais importantes para o sucesso dos nossos projetos, por isso, utilizamos as seguintes aplicações para gerenciarmos nossas atividades, projetos e comunicados: Para o colaborador temos um canal direto com o RH da empresa, para contato@geenengbrasil.com.br.
- **Facebook, LinkedIn, Whatsapp e etc:** Você já deve ter percebido, que estes canais utilizam suas informações pessoais, portanto, não é adequado misturá-las com as informações da empresa, não recomendamos nenhuma troca de informações da empresa, dentro destes canais de uso público e pessoais. Agora se for para tratar alguma coisa informação, orçamento, fique tranquilo(a), a nossa equipe entrará em contato, contamos com seu apoio, para fiscalizar estas ocorrências. E se você vir informações da empresa, dos nossos clientes e projetos sendo trocados nestes aplicativos, não deixe de entrar em contato conosco, envie um e-mail para: contato@greenengbrasil.com.br



- **Privacidade 360:** A Green se preocupa com a privacidade e proteção de dados dos seus clientes e parceiros. Se você encontrar alguma empresa parceira, desrespeitando ou violando a privacidade dos clientes, não deixe de nos comunicar. Envie um e-mail para: contato@greenengbrasil.com.br

Diretrizes

As seguintes diretrizes, devem ser respeitadas para os tipos de dados, conforme abaixo:

Dados de funcionários

Os dados de funcionários, são necessários para realizar a admissão no Departamento Pessoal e cumprir as exigências de órgãos regulatórios como ministério do trabalho e CLT. A **Green** não coleta nenhum dado além do solicitado para cumprir os protocolos de admissão previsto nos regulamentos trabalhistas e as informações necessárias para distribuição dos benefícios, como por exemplo: plano de saúde, odontológico, transporte e outros.

- Dados que são coletados pela **Green:**

- 1.Nome completo;
- 2.CTPS;
- 3.Certidão de Nascimento/Casamento;
- 4.CPF, RG, PIS;
- 5.Nome da mãe e do pai;
- 6.Endereço completo;
- 7.Escolaridade, Certificados e Títulos;
- 8.Caderneta de vacinação dos filhos.

- Não devem ser coletados: A Green apoia a diversidade no ambiente organizacional, contudo, podemos fazer isto sem coletar dados pessoais sensíveis. Evite coletar ou questionar os dados abaixo:

- 1.Raça;
- 2.Religião;
- 3.Opção sexual;
- 4.Filiação a sindicatos, opiniões filosóficas/políticas ou organização de caráter religioso;
- 5.Dado referente à saúde ou à vida sexual;
- 6.Dado genético ou biométrico, quando vinculado a uma pessoa natural.

Atenção! Se você encontrar qualquer um destes dados sendo coletados em nome da Green ou evento vinculado nos informe. Envie um e-mail para contato@greenengbrasil.com.br
Ficaremos gratos(as) e tomaremos as devidas ações;



Dados de terceiros

Nossa política de privacidade e proteção de dados tem equivalência igual para funcionários e terceiros, desta forma, todas as normas e procedimentos são aplicadas em ambos os casos e precisam ser assinadas.

Assim como os funcionários, os terceiros possuem as mesmas responsabilidades com a confidencialidade, privacidade e a proteção de dados. Da mesma forma, ao se comprometerem com esta política e as diretrizes da **Green**, assinam o Acordo de Confidencialidade.

Dados dos nossos clientes

Devemos coletar somente o mínimo necessário para as finalidades pretendidas e de acordo com as nossas bases legais. Coletamos dados pessoais: Nome completo, Endereço, Telefone, E-mail, CPF e RG. Somente estes dados podem ser coletados para fins de cadastro, contrato e por finalidade de segurança.

Ao falarmos de segurança, podemos citar a base legal:

Art. 11 g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Tratamos os dados pessoais com sigilo absoluto, com confidencialidade e devem ser protegidos desde o momento da coleta até o seu descarte. Esses dados não devem de forma alguma ser compartilhados, transmitidos ou armazenados sem atender aos critérios exigidos na política de segurança.

Nós da **Green** temos por objetivo ter o máximo de responsabilidade, prezando pela privacidade e proteção desses dados, por isso é estritamente proibido o uso de dados de qualquer sistema interno para outra finalidade que não esteja envolvida no dia a dia da **Green**.

O que se faz na Green fica na Green.



Princípios norteadores da proteção de dados pessoais

A Green cuidará para que todas as atividades de tratamento de dados pessoais estejam em conformidade com os 08 (oito) princípios trazidos pela legislação sobre privacidade e proteção de dados. São eles:

Princípio da boa-fé: todas as operações de tratamento deverão ser pautadas em boas intenções, na moral e bons costumes aceitos pela sociedade.

Princípio da finalidade e adequação: O tratamento de dados pessoais deve se limitar aos propósitos legítimos, específicos, explícitos e informados ao Titular, e somente deve ocorrer de formas compatíveis com estas finalidades. Dados pessoais não poderão ser coletados/obtidos para uma finalidade, e depois utilizados para outra. Todos os usos de um dado devem ser compatíveis com o motivo original da coleta/obtenção.

Princípio da necessidade: A coleta e utilização de dados pessoais deverá ser limitada ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular, garantindo também, que tais informações sejam armazenadas pelo menor tempo possível/necessário.

Princípio do livre acesso e qualidade dos dados: Aos titulares deverá ser garantida a consulta facilitada e gratuita quanto à forma e duração do tratamento e integralidade de seus dados pessoais, estando assegurada a exatidão, clareza, relevância e atualização destes.

Princípio da transparência: Serão garantidas aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes, observados os segredos comercial e industrial.

Princípio da segurança e prevenção: A segurança e confidencialidade dos dados pessoais devem ser garantidas por meio de medidas técnicas e organizacionais, abaixo delimitadas, a fim de prevenir a ocorrência de incidentes de segurança envolvendo dados pessoais.

Princípio da não discriminação: As atividades de tratamento de dados pessoais jamais poderão objetivar fins discriminatórios, ilícitos ou abusivos.

Princípio da responsabilização: A Green deverá armazenar registros de todas as atividades de tratamento de dados pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados pessoais, comprovando sua eficácia e eficiência.

Ações de Coleta de Dados

Ciclo de vida dos dados de colaboradores

Considere o fluxo abaixo para compreender como os dados podem “nascer”, serem armazenados por um determinado período, até serem inativados ou cancelados, dentro da **Green**



- 1. Planejamento:** Antes de levantar quaisquer dados, você deve realizar um planejamento e estar embasado em algum processo/norma da empresa. Para dados pessoais sensíveis, consultar o(a) DPO, pois não estamos autorizados a coletar estes dados. Enviar e-mail para: contato@greenengbrasil.com.br
- 2. Coleta:** Momento em que o cliente interno: funcionários e terceiros, enviam seus dados para a **Green**;
- 3. Ativação:** Após devidas análises é realizado o processo de admissão e criadas as contas de acesso aos sistemas;
- 4. Alteração:** Ao longo do tempo estes dados podem sofrer alterações cadastrais ou mudanças na conta, como por exemplo: mudança de nome, alteração de cargo, mudança de perfis, autorizações e outros.
- 5. Inativação ou exclusão:** Dependendo de cada processo, o colaborador em caso de demissão, férias ou afastamento, poderá ter seu cadastro inativo ou até mesmo excluído.

As áreas abaixo estão autorizadas (de acordo com perfis de acesso correspondentes), a trabalhar com os dados pessoais durante seu ciclo de vida:



Área Comercial (Pré e Pós-Venda)

Coleta dados para elaboração de propostas comerciais, contratos de clientes da **Green**, campanha de e-mail marketing para clientes já cadastrados, atualização de cadastros e pesquisa de satisfação. O trabalho é realizado respeitando as diretrizes, de coletar sobre os dados para elaboração do contrato: **CNPJ, sócios e testemunhas (Nome e CPF)**. Dados adicionais, não devem ser coletados, em quaisquer hipóteses.

Área Financeira

A área financeira, segue as diretrizes desta política. Poderá consultar as informações pertinentes aos dados pessoais e necessários para fins administrativos (benefícios, salário e informações trabalhistas) de acordo com a função de trabalho e perfil relacionado. O sigilo das informações financeiras dos nossos clientes e colaboradores é mandatório.

Área de Gestão de Pessoas

A área de Gestão de Pessoas, segue as diretrizes de clientes internos-funcionários e terceiras, desta política. Deve estar atenta aos dados coletados no pré-seleção, admissão e eventos organizados pela empresa ou que é convidada. É responsável também por ser a principal agente fiscalizadora e disseminadora, da cultura de privacidade da **Green**.

Área de TI

A área de TI é o coração da privacidade e proteção de dados na **Green**. Responsável por definir e aplicar as políticas que garantam a privacidade e a proteção de dados, durante todo o ciclo de vida de desenvolvimento das aplicações, tornando como pré-requisito a proteção de dados by design (desde o início).

Nos procedimentos técnicos são detalhadas as medidas organizacionais, modelos de arquitetura, configurações e ferramentas, que derivam das práticas de privacidade proteção de dados mencionadas neste política.

A área de TI tem um papel fundamental para garantir que a proteção de dados aconteça na prática e que os serviços fornecidos pela **Green** sejam seguros e eficazes de acordo, com as medidas de segurança de informação e governança de TI, disseminada pela empresa e exigidos pela Lei Geral de Proteção de Dados.



Contratos

Todos os contratos da **Green** são revisados e negociados com seus parceiros, clientes e prestadores de serviços, para garantia da privacidade e proteção de dados, bem como, adequação as medidas e padrões de segurança, exigidos pela LGPD.

Esta revisão ocorre no início do contrato e periodicamente sob atualização/revisão das leis.

Não recomendamos em qualquer hipótese assinatura e/ou renovação de contratos, com empresas que não estejam adequadas às exigências pela LGPD. É prudente consultar o DPO da empresa em caso de dúvidas.

Papéis e Responsabilidades

- **Funcionários/terceiros/fornecedores:** Devem considerar os itens desta política na execução dos serviços e atuar como agentes fiscalizadores e disseminadores.
- **Gerência e alta direção:** Prover os recursos necessários e apoio para os projetos de privacidade e proteção de dados; garantir as auditorias periódicas de adequação a LGPD e treinamentos necessários;
- **DPO:** Auxiliar na adequação de processos para cumprimento da LGPD, treinamento, orientações e auditoria interna.

Programa de privacidade Green

- Para que o programa de privacidade da Green se mostre efetivo e produza resultados positivos, é importante que os pilares e procedimentos abaixo sejam constantemente observados durante as operações de tratamento de dados pessoais.

Comitê de Privacidade e Proteção de Dados

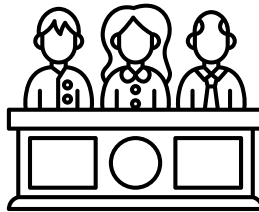
O comitê de privacidade e proteção de dados da **Green** têm um papel fundamental para continuidade e melhoria contínua dos serviços e projetos, incluindo a privacidade desde a concepção. Faz parte das responsabilidades do Comitê:

- Propor políticas e atuar sendo o porta-voz da necessidade de seu cumprimento;
- Conscientização de todos os agentes internos envolvidos com tratamento de dados pessoais;
- Gerenciar atividades relativas ao tratamento de dados;
- Fiscalizar os processos que envolvem tratamento de dados.

Fazem parte do comitê:

Ronyeri Junior

- O Comitê de Privacidade deve se reunir a cada 30 (trinta) dias, para apresentação e acompanhamento do programa de privacidade da Green e deve ser composto por integrantes de áreas-chave da Companhia, capazes de deliberar e decidir sobre assuntos relacionados à privacidade e proteção de dados.
- Os objetivos do comitê são, principalmente, garantir a comunicação e cumprimento do programa de privacidade e discutir e tomar decisões sobre novas atividades de tratamento, atividade regulamentada pela Política de Privacy by Design, com base nos riscos levantados por meio de Relatórios de Impacto à Proteção de Dados Pessoais.
- Adicionalmente, o Comitê de Privacidade deverá sempre ser envolvido na tomada de decisões a respeito de atividades de tratamento que envolvem riscos avaliados como altos e muitos altos, reportando-se diretamente ao Comitê Executivo da Companhia.



Encarregado de Proteção de Dados (DPO)

- O Encarregado de Proteção de Dados (DPO ou Data Protection Officer) deve possuir conhecimentos jurídicos e técnicos relacionados à proteção de dados pessoais e experiência na área que sejam proporcionais ao nível de complexidade e sensibilidade das operações de tratamento de dados pessoais que a empresa realiza.
- O Encarregado de Proteção de Dados deve gozar de um grau razoável de independência em relação ao restante da administração, de modo a lhe permitir assegurar os direitos dos titulares de dados cujas informações pessoais são tratadas pela Companhia. Suas funções não devem incluir atividades ou responsabilidades que possam conflitar com a responsabilidade da empresa para com os titulares de dados pessoais.
- A atuação do Encarregado de Proteção de Dados deve garantir a conformidade da Companhia em relação às leis e demais normas de privacidade e proteção de dados aplicáveis aos seus negócios, por meio do programa de privacidade.

- Suas principais atribuições envolvem, sem prejuízo de demais atividades estabelecidas em políticas e procedimentos que compõem o programa de privacidade:
 1. Gestão do programa de privacidade;
 2. Desenvolvimento, manutenção e propositura de revisão das Políticas de Privacidade da organização, inclusive desta política;
 3. Fiscalização do cumprimento das Políticas de Privacidade da organização;
 4. Monitoramento do nível de conformidade da organização, por meio de análises de diagnósticos trimestrais, com a definição de planos de ação para melhorar o treinamento e a clareza das Políticas de Privacidade;
 5. Atuação como ponto de contato para autoridade nacional de proteção de dados e os titulares dos dados.
- Recepção de requisições dos titulares de dados pessoais, com o imediato atendimento a tais requerimentos, quando aplicável.
- Discussão e definição, junto ao Comitê de Privacidade, sobre eventuais situações a respeito das requisições realizadas por titulares de dados pessoais.
- Preparo dos Relatórios de Impacto à Proteção de Dados Pessoais, com apuração e revisão dos riscos das atividades nele relatadas.
- Cabe ao encarregado a decisão, em casos de risco baixo a moderado, sobre as atividades de tratamento de dados pessoais conduzidas pela empresa. Caso o risco seja considerado alto ou muito alto, a decisão deverá ser escalada ao Comitê de Privacidade.
- Por fim, o Encarregado deve auxiliar no esclarecimento de dúvidas e orientar demais membros da empresa, durante a execução de suas atividades, quando envolverem operações de tratamento de dados pessoais.

Direitos do titular

Você como titular dos dados pessoais (dono dos seus dados) tem direito a obter da **Green**, uma relação aos dados do titular por ele tratados, a qualquer momento e mediante a requisição, conforme ações abaixo:

- Quero solicitar acesso aos meus dados pessoais que são tratados pela **Green**;
- Quero solicitar correção dos meus dados pessoais;
- Quero me opor ao tratamento de meus dados pessoais;
- Quero solicitar a exclusão permanente dos meus dados pessoais, entendendo que eles não são mais necessários para as finalidades pretendidas;
- Quero levantar as minhas restrições sobre o tratamento, permitindo somente aquilo que considero necessário, inclusive com o meu consentimento;
- Quero solicitar a portabilidade dos meus dados pessoais: receber uma cópia para levar para outro controlador.
- Outros.

Todos estes itens você pode solicitar enviando um e-mail para contato@greenengbrasil.com.br

A **Green** irá analisar sua solicitação com atenção e te responder com todas as informações necessárias, dentro do prazo de até **15 dias**. Conforme previsto, na Lei Geral de Proteção de Dados.



Em caso de violação

Estamos atentos para cumprimento da Lei Geral de Proteção de Dados, desta forma, se ocorrer uma violação da segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada **relacionada a dados pessoais**, temos um cenário de **violação de dados pessoais**. Se este tipo de incidente ocorrer, você deve nos informar o mais breve possível, seguindo as etapas.

Incidentes podem ser definidos como qualquer falha na observância dos pontos descritos nesta política, que podem gerar risco de dano aos titulares de dados pessoais.

A comunicação de acidentes, não conformidades com esta política e de dúvidas deverão ser feitas diretamente para **contato@greenenbrasil.com.br**

Probabilidade

O pilar da probabilidade objetiva mensurar as chances que uma determinada atividade de tratamento de dados pessoais possui em ser submetida a uma situação não desejada, a qual, inclusive, possa acarretar na ocorrência de incidentes de segurança ou posterior aplicação de sanções pela Autoridade Nacional de Proteção de Dados, por conta da inobservância de normas específicas trazidas pela Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados). O cálculo deste pilar será realizado com base na incidência de fatores que possam gerar um ponto de atenção para a atividade. Abaixo trazemos alguns exemplos comuns de acordo com a criticidade apresentada.

Baixo - Atividades que não observam as boas práticas da legislação de proteção de dados, contudo não descumprem as suas diretrizes;

Médio - Atividades que, pontualmente e de forma isolada, possam descumprir a legislação de proteção de dados ou tornas os dados pessoais tratados, levemente vulneráveis;

Alto - Atividades se utilizam de métodos pouco ou não recomendáveis ou até mesmo contrários às diretrizes da legislação de proteção de dados, levando ao seu provável descumprimento e conseqüente surgimento de altas vulnerabilidade atreladas às informações pessoais tratados.

Impactos

1. Baixo - Os titulares sujeitos ao tratamento não serão afetados ou caso afetados, enfrentarão pequenos inconvenientes;
2. Médio - Os titulares sujeitos ao tratamento possivelmente serão afetados por situações significativamente inconvenientes;
3. Alto - Os titulares sujeitos ao tratamento encontrarão significativas consequências, as quais poderão ser superadas mediante sérias dificuldades, ou até mesmo consequências irreversíveis;

Para cada risco identificado, para além da indicação das medidas mitigadores aplicáveis, avaliar a probabilidade e o impacto e encontrar dentre os exemplos apontados, os que melhor acomodam a situação, realizando a multiplicação de ambos os fatores.

Classificação da Atividade

Seguindo a Classificação realizada na “Análise de Risco”, de acordo com a quantidade de riscos apurados e a criticidade de cada um destes, recomenda-se a classificação final da atividade, de acordo com os critérios abaixo:



Quaisquer riscos abaixo de nível 2.	A partir de um risco de nível 2, até um ou mais riscos de nível 6.	A partir de dois ou mais atividades com risco de nível 6, independentemente da aplicação de medidas necessárias.
-------------------------------------	--	--