Opice BLUM

Redefinindo os limites do possível.

cert.br nic.br cgi.br

Tiago Neves Furtado

Sócio das áreas de Proteção de Dados e Resposta a Incidentes no Opice Blum. Membro do Conselho Consultivo de Publicações da *International Association of Privacy Professionals* - IAPP e reconhecido *Fellow of Information Privacy* – FIP pela mesma associação. Professor em Cursos de Pós-Graduação e Educação Executiva em Direito Digital, Proteção de Dados, Resposta a Incidentes e Inteligência Artificial.

https://br.linkedin.com/in/tnfurtado

Vinicius Azevedo

Doutor (PhD) e Mestre em Direito pela USP. Especialista em Direito Digital pelo ITS e pela FGV. Certificado em Cibersegurança pela ISC2 e pela HarvardX. Advogado Gestor do Time de Resposta a Incidentes no Opice Blum e Professor em Cursos de Pós-Graduação em Direito Digital.

https://br.linkedin.com/in/viniciusazevedocoelho

Guilherme Ochsendorf de Freitas

Especialista em Direito e Tecnologia da Informação pela POLI-USP e em Gestão Estratégica em Tecnologia da Informação pela FEA-RP - USP. Certificado em Cibersegurança pelo ISC2 e Resposta a Incidente pela Carnegie Mellon University (CERT.br) e FGV. Advogado do Time de Resposta a Incidentes no Opice Blum e Professor em Cursos de Pós-Graduação em Direito Digital.

https://br.linkedin.com/in/guilhermeochsendorf

TLP:CLEAR

13º Fórum Brasileiro de CSIRTs

Decisões da ANPD: Lições Práticas de Incidentes de Segurança para CSIRTs.

São Paulo, 28 e 29 de julho de 2025

Resumo

1. Conceitos Introdutórios

- 1. Olhar do regulador
- 2. Alinhamento estratégico da legislação com Frameworks.

2. Lições Práticas para CSIRTs

- Infrações mais recorrentes na ANPD
- Lições 1 a 4.
- Como as decisões da ANPD moldam a atuação dos Times de CSIRTs.

3. Recomendações para CSIRTs

T

TLP:CLEAR

Conceitos introdutórios:

O que é um incidente de segurança e dados pessoais para ANPD?

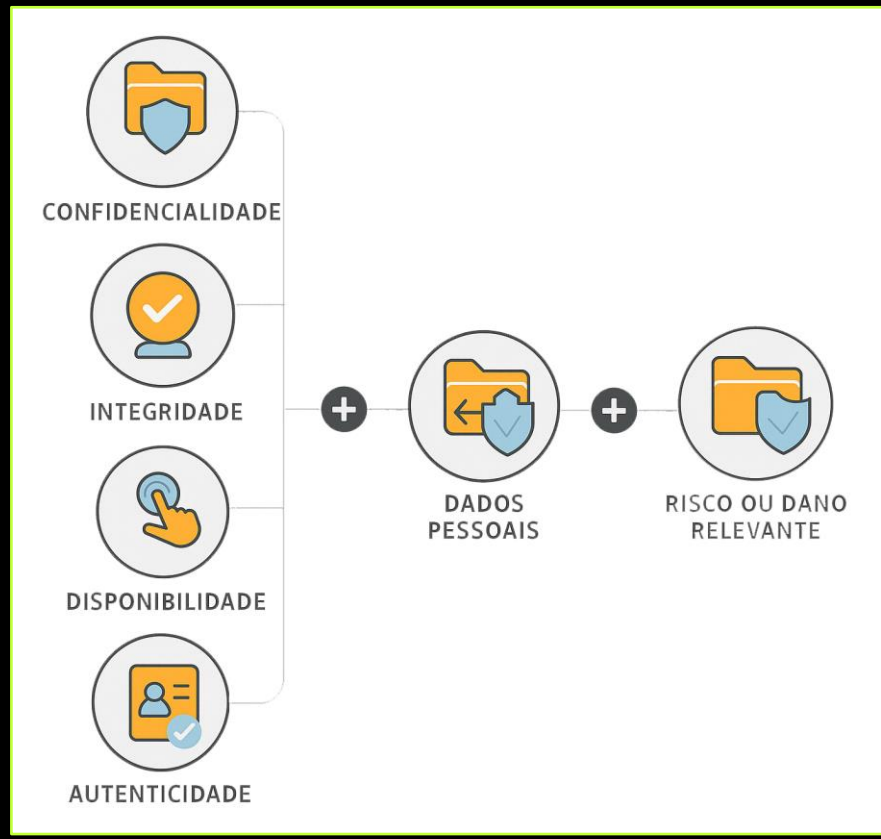
Ele abrange qualquer evento adverso confirmado que comprometa as propriedades de *confidencialidade, integridade, disponibilidade* ou *autenticidade dos dados pessoais*.

Isso inclui situações acidentais ou ilícitas de destruição, perda, alteração ou acesso não autorizado. Mesmo a indisponibilidade prolongada de sistemas que tratam dados pessoais pode configurar um incidente de segurança que acarreta risco ou dano relevante aos titulares.

A mera existência de uma vulnerabilidade em um sistema não é um incidente, mas sua exploração pode resultar em um incidente de segurança.

Dados pessoais são definidos como: qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Dados anonimizados não são considerados dados pessoais para os fins da LGPD, a menos que o processo de anonimização possa ser revertido com meios razoáveis.



T

TLP:CLEAR

Conceitos introdutórios:

O que é risco ou dano relevante?

Um incidente pode acarretar risco ou dano relevante quando "puder afetar significativamente interesses e direitos fundamentais dos titulares".

Isso inclui situações em que a atividade de tratamento puder:

- impedir o exercício de direitos ou a utilização de um serviço;
- ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Esta obrigação se manifesta pela possibilidade de risco ou dano relevante, não exigindo a concretização do dano e isso deve ser levado para avaliação do risco.

Resolução nº. 15/2024 da ANPD

Art. 5º O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;
II - dados de crianças, de adolescentes ou de idosos;
III - dados financeiros;
IV - dados de autenticação em sistemas;
V - dados protegidos por sigilo legal, judicial ou profissional; ou
VI - dados em larga escala.

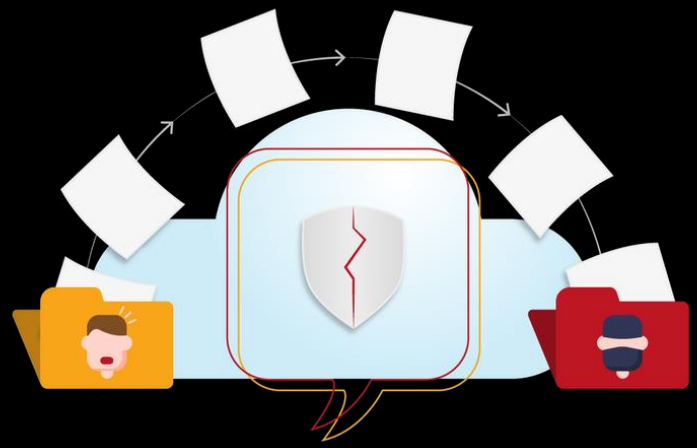
§ 1º O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Conceitos introdutórios:

O que considerar para avaliação do risco do incidente?

Na avaliação de risco do incidente, devem ser considerados, dentre outros aspectos:

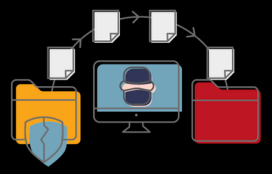
- O contexto da atividade de tratamento de dados;
- As categorias e quantidades de titulares afetados;
- As naturezas, as categorias e a quantidade de dados violados;
- Os potenciais danos materiais, morais, reputacionais causados aos titulares;
- Se os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares;
- As medidas de mitigação adotadas pelo controlador após o incidente.



Um mesmo tipo incidente pode ou não ser considerado capaz de causar risco ou dano relevante em função da combinação desses critérios.

Conceitos introdutórios:

Exemplos de incidentes capazes de gerar risco ou dano relevante aos titulares:



A invasão de uma instituição financeira por um agente malicioso que realize a cópia não autorizada de uma base de dados contendo dados pessoais dos correntistas, tais como extratos bancários, números de cartões de crédito e senhas viola o sigilo bancário dos titulares e os expõe a risco de fraudes e danos morais e materiais.

A indisponibilidade prolongada de um sistema utilizado por uma rede hospitalar em razão de um incidente de sequestro de dados (*ransomware*), impedindo o acesso aos dados dos pacientes ou a realização de procedimentos médicos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos ou danos à saúde.

A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

Conceitos introdutórios:

Prazo e formas de comunicação:

A comunicação à ANPD e ao(s) titular(es) deverá ser realizada pelo Controlador no prazo de três (3) dias úteis.

Excepcionalmente, na hipótese de o controlador não dispor de informações completas a respeito do incidente ou não conseguir notificar a todos os titulares no prazo recomendado, a comunicação à ANPD poderá ser realizada em etapas: preliminar e complementar.

A impossibilidade de realizar a comunicação completa deve ser devidamente justificada pelo controlador. As informações poderão ser complementadas, de maneira fundamentada no prazo de vinte (20) dias úteis, a contar da data da comunicação.

Comunicação titulares:

A comunicação aos titulares é regulada (art. 9) e deve, preferencialmente, usar linguagem simples e de fácil entendimento e ocorrer de forma direta e individualizada.

Se a comunicação individualizada for inviável ou os titulares não puderem ser identificados, o controlador deve usar meios de divulgação amplos (sítio eletrônico, aplicativos, mídias sociais, canais de atendimento) por, no mínimo, três meses.

1. Olhar do regulador

Construindo a história de um incidente.

- Identificar o que aconteceu (causa raiz);
- Corrigir as falhas e implementar soluções;
- Comunicar reguladores + Stakeholders + titulares de dados; e
- Implementar medidas de mitigação de danos.

T

TLP:CLEAR

1. Olhar do regulador.

Alinhamento estratégico da legislação com Frameworks:

Exigência da ANPD / LGPD	Mapeamento no NIST CSF v2.0	Mapeamento no ISO/IEC 27002:2022
Comunicação do Incidente (Art. 48 LGPD, Res. 15/2024)	**RS.CO-02:** Stakeholders internos e externos são notificados sobre incidentes **RS.MA-01:** O plano de resposta a incidentes é executado em coordenação.	**Cláusula 7.4:** Comunicação **A.5.26:** Gestão de incidentes de segurança da informação. **A.5.24:** Planejamento e preparação da gestão de incidentes.
Análise de Risco e Dano Relevante (Art. 48 LGPD, Res. 15/2024)	**DE.AE-04:** O impacto e escopo estimados de eventos adversos são compreendidos. **RS.AN-03:** A análise é realizada para estabelecer a causa raiz do incidente. **RS.AN-08:** A magnitude de um incidente é estimada e validada.	**A.5.25:** Avaliação e decisão sobre eventos de segurança da informação. **A.5.27:** Lições aprendidas com incidentes de segurança da informação.
Medidas de Segurança para Proteger os Dados (Art. 48, § 3º e art. 49)	**PR.DS-01:** A confidencialidade, integridade e disponibilidade dos dados em repouso são protegidas. **PR.DS-02:** A confidencialidade, integridade e disponibilidade dos dados em trânsito são protegidas. **PR.DS-10:** A confidencialidade, integridade e disponibilidade dos dados em uso são protegidas.	**A.8.24:** Uso de Criptografia. **A.8.11:** Mascaramento de dados. **A.5.14:** Prevenção contra vazamento de dados.
Registro de Operações / Logs (Art. 15 MCI)	**PR.PS-04:** Registros de log são gerados e disponibilizados para monitoramento contínuo. **DE.CM-03:** A atividade de pessoal e o uso de tecnologia são monitorados para encontrar eventos adversos. **RS.AN-07:** Dados e metadados de incidentes são coletados e sua integridade preservada.	**A.8.15:** Logging. **A.5.28:** Coleta de evidências. **A.8.16:** Atividades de monitoramento.

T

TLP:CLEAR

2. Lições Práticas para CSIRTs:

Infrações mais recorrentes na ANPD:

- não manter registro das operações de tratamento de dados pessoais (ROT) (Art. 37 da LGPD) - 1 processo.
- falta de comprovação da indicação do encarregado (Art. 41 da LGPD) - 1 processo;
- ausência de comprovação de hipótese legal de tratamento de dados pessoais (Art. 7º da LGPD) – 1 processo;
- falta de comprovação da indicação do encarregado de dados pessoais (Art. 23, III da LGPD)- 1 processo;
- não atendimento às requisições da ANPD / obstrução à atividade de fiscalização (Art. 5º do regulamento de fiscalização) - 3 processos;
- ausência de envio do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) após solicitação da ANPD (Art. 38 da LGPD) - 3 processos;

- os sistemas utilizados não atendem aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios da LGPD (Art. 49 da LGPD).

- Esta infração ocorreu em 4 (quatro) processos;

- não comunicar aos titulares a ocorrência de incidente de segurança que possa lhes acarretar risco ou dano relevante (Art. 48 da LGPD e Resolução nº 15/2024).

Esta infração foi identificada em 6 (seis) dos processos.

2. Lições Práticas para CSIRTs:

Lição 1 - A importância dos Logs na resposta a incidentes

Por que os logs são essenciais?

- Permitem identificar a causa e a extensão do incidente.
- Ajudam a delimitar o impacto real: o que ocorreu, o que foi acessado ou exfiltrado, quais dados foram violados.
- São fundamentais para a avaliação do risco e definição da obrigação de notificação à ANPD e aos titulares.

Exemplo prático:

Ambiente de gestão de pessoas acessado indevidamente. Possíveis dados: contato, cargo, salário, atestados médicos, em diferentes arquivos.

- Cenário com logs:
  - Registros indicam que apenas dados de contato foram acessados.
  - Risco está limitado a abordagens indevidas.
  - Comunicação pode ser dispensada.
- Cenário sem logs:
  - Considerar o pior cenário de impacto: dados críticos como financeiros e de saúde.
  - Risco relevante de discriminação, danos morrais e reputacionais.
  - Necessidade de comunicar ANPD, titulares.

TLP:CLEAR

2. Lições Práticas para CSIRTs:

Lição 2 – Medidas técnicas como argumentos de defesa

O dever de comunicação aos titulares só existe quando o incidente for capaz de "acarretar risco ou dano relevante".

Adotar medidas técnicas eficazes podem eliminar ou reduzir drasticamente esse risco, afastando o dever de comunicação.

- Criptografia
- Monitoramento
- Remoção do conteúdo
- Pagamento de resgate?

Exemplo prático:

Ambiente de gestão de pessoas acessado indevidamente.
Possíveis dados: contato, cargo, salário, atestados médicos.

- Medidas técnicas adotadas:
  - Revogação imediata de credenciais comprometidas.
  - Bloqueio do IP utilizado no acesso indevido.
  - Monitoramento de vazamentos e publicações em fóruns DW.
  - Análise dos logs para confirmar impacto limitado.
- Resultados:
  - Risco reduzido.
  - Ausência de impacto a dados sensíveis ou financeiros.
  - Comunicação pode ser dispensada com base na mitigação do risco.

TLP:CLEAR

2. Lições Práticas para CSIRTs:

Lição 3 – Validação técnica: exfiltração da amostra de dados

Os CSIRTs lidam constantemente com a dúvida: o adversário realmente exfiltrou os dados que alega ter? Para a ANPD, a publicação de amostras cria presunção de veracidade.

Lógica Regulatória.

Inversão do ônus da prova. Quando um grupo de ransomware publica amostras de dados consistentes com as informações do controlador (por exemplo: dados de funcionários, trechos de e-mails corporativos), o ônus da prova se inverte.

- Não cabe à ANPD provar que os dados são verdadeiros, mas ao controlador provar que são falsos ou que o vazamento não se originou de seus sistemas.

Decisões (não públicas): A postura da ANPD em casos de "ausência de delimitação" (assumir o pior) e "falta de evidência de exfiltração" indica que a evidência (amostra na Dark Web) será tratada com seriedade. A recusa em investigar ou a negação sem provas será vista como falta de cooperação..

Lição para o CSIRT:

Monitoramento Contínuo. Implementar serviços de monitoramento da Dark Web e canais de Threat Intel.

Análise Rápida. Ao receber uma ameaça de extorsão, a primeira ação é buscar evidências de exfiltração e amostras publicadas e acompanhar o *countdown*.

Validação Técnica. Analisar as amostras para verificar sua autenticidade e correlacioná-las com os logs de acesso e de fluxo de dados. O resultado dessa análise é fundamental para o parecer jurídico.

TLP:CLEAR

2. Lições Práticas para CSIRTs:

Lição 4 - Identificação dos dados e titulares: dados não estruturados

A análise em ataques que comprometem servidores de arquivos (documentos, planilhas, e-mails) é complexa. Como avaliar o risco em milhares de arquivos .docx, .pdf e .xlsx?

Nossa abordagem:

Amostragem. Utilizar ferramentas de e-Discovery, scripts ou análise manual para fazer uma amostragem relevante dos arquivos afetados.

Classificação e análise da amostra. Analisar a amostra manualmente ou com ferramentas de IA para identificar a prevalência de dados pessoais e sensíveis.

Criação da matriz de risco. Identificar, na amostra, os tipos de dados presentes e classificar o risco para cada tipo de dado e titular.

Decisão de comunicação. Com base na análise da amostra, tomar uma decisão informada, que pode ser:

- comunicar a todos (obrigação legal quando não se sabe quem foi impactado);
- comunicar apenas aos grupos de risco identificados ou;
- documentar a decisão de não comunicar com base na inexistência de dano ou risco relevante.

O papel do CSIRT na avaliação:

Natureza dos dados. Identificar os tipos de dados nos sistemas comprometidos (exemplo: o banco de dados 'X' continha CPF, nome e dados de saúde).

Volume de titulares. Precisar o número de titulares afetados. Se os logs não permitem delimitar, deve-se considerar a base inteira.

Medidas de proteção. Informar se os dados estavam criptografados, anonimizados ou de outra forma protegidos para auxiliar na tomada de decisão e avaliação de risco.

2. Lições Práticas para CSIRTs:

Exemplo de Matriz com Dados:

		Dados Pessoais																	
Nome	**CPF**	CPF	Nome	Cópias de documentos de identificação oficial.	Endereço	Data de Nascimento	Gênero-Sexo	Telefone	RG	Filiação	CNH	Passaporte	Cargo	Estado Civil	Email	ID Profissional	Imagem, áudio e video	Nacionalidade	Dados protegidos por sigilo profissional/legal.	Dados de Geolocalização	PIS
Nome do titular	Número de CPF		x		x		x		x		x		x		x		x		x		x

2. Lições Práticas para CSIRTs:

Exemplo de Matriz com Dados:

Dados Pessoais Sensíveis									Dados Pessoais Sensíveis: Referente à saúde.			Dado financeiro ou econômico								Dados de Autenticação de Sistemas	
Origem racial ou étnica.	Convicção religiosa.	Opinião política.	Referente à saúde.	Filiação a organização sindical, religiosa, filosófica ou política.	Referente à vida sexual.	Biométrico.	Genético.	Dados pessoais que podem revelar dados pessoais sensíveis	Atestado Médico	Exames e laudos	Receituário Médico	Banco, agência ou conta	Extrato de pagamento/transações	Boleto	Dados de meios de pagamento (número de cartão de crédito)	Salário	Informes de rendimento	IRPF	PIX	Nomes de usuário de sistemas de informação.	Dado de autenticação de sistema
	x		x		x		x		x		x		x		x		x		x		x

2. Lições Práticas para CSIRTs:

Exemplo de Matriz com Dados:

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?	Probabilidade de dano/risco relacionado ao dado pessoal		Teste de violação a interesses e direitos fundamentais										
integralmente protegidos por criptografia / pseudonimização?	Indicar a provável consequência de utilização indevida de cada dado pessoal crítico identificado (Exemplo: PIS com CPF e dado de contato: Informações completas para a execução de fraudes previdenciárias. Permite que o criminoso entre em contato com a vítima (por telefone, SMS, WhatsApp) se passando por uma instituição (Caixa, Governo Federal), usando dados reais (PIS, CPF) para obter senhas, códigos de segurança ou induzir a vítima a clicar em links maliciosos.	Indicar a provável consequência de utilização indevida de cada dado pessoal crítico identificado	Danos Materiais	Danos Morais	Fraudes Financeiras / Engenharia Social	Roubo de identidade	Violação a integridade física	Discriminação Social	Danos Reputacionais	Limitação de acesso a um serviço	Exposição dos dados protegidos por sigilo profissional/legal	Restrições de Direitos	Perda de acesso dos dados

TLP:CLEAR

2. Lições Práticas para CSIRTs:

Exemplo de Matriz com Dados:

Teste de critérios por categorias e tipos de dados afetados.						Violação da Segurança da Informação dos Dados Pessoais						
Dados pessoais sensíveis	Dados de crianças, adolescentes ou idosos	Dados financeiros	Dados de autenticação em sistemas	Dados em larga escala	Dados protegidos por sigilo legal	Confidencialidade	Integridade	Disponibilidade	Autenticidade	Dever de comunicação à ANPD e aos titulares	Nome do Arquivo	Localização/ Caminho da Pasta	Hash
Sim		Não		Sim		Não		Sim		Sim			
										Não			

2. Lições Práticas para CSIRTs:

Como as decisões da ANPD moldam a atuação dos times de CSIRTs:

As decisões da ANPD direcionam que o trabalho do CSIRT não termina na contenção do incidente. Ele se estende à produção de evidências e relatórios técnicos que subsidiarão a análise jurídica e a tomada de decisão da companhia.

A resposta a um incidente de segurança com dados pessoais deixou de ser uma atividade puramente técnica. Hoje, é um processo técnico-jurídico regulado, com prazos e consequências legais diretas. A resposta a incidentes não é mais apenas sobre conter a ameaça, é sobre gerenciar o risco legal e regulatório.

Fonte: FRIST CSIRT Services Framework Version 2.1

TLP:CLEAR

3. Recomendações para CSIRTs:

O que muda no dia a dia do time de resposta a incidentes?

1. Logs são ativos críticos: trate os logs como um ativo de negócio essencial. A ausência ou a má qualidade deles tem impacto legal e financeiro direto. Garanta a retenção por no mínimo seis meses. Audite, centralize e proteja seus logs, pois o futuro da empresa depende deles legalmente.

2. Mitigação é defesa: a implementação de controles não é apenas uma boa prática de segurança, mas também uma estratégia de defesa legal. Essa ação pode ser um elemento redutor de risco, podendo afastar o dever de comunicação.

3. Integre-se o jurídico com o time técnico: a integração do DPO e do departamento jurídico deve ser uma etapa obrigatória e imediata. Crie um manual de resposta a incidentes que inclua os acionamentos e as informações necessárias para as equipes de conformidade e jurídica. A resposta não é mais apenas técnica. A contratação de um membro do CSIRT com conhecimento jurídico e técnico tem otimizado o tempo de resposta a incidentes.

4. Utilize frameworks de referência e documente: a adoção de boas práticas e de modelos como NIST e ISO ajuda a demonstrar a responsabilidade e a diligência na proteção de dados. Cada ação técnica durante um incidente, como contenção, erradicação, recuperação e análise, gera evidências. Documente cada passo, pois o relatório será a peça central da defesa e tomada de decisão da companhia.

G

TLP:CLEAR

cert.br nic.br cgi.br

Opice BLUM

Tiago Neves Furtado
tiago.furtado@opiceblum.com.br

Vinicius Azevedo
vinicius.azevedo@opiceblum.com.br

Guilherme Ochsendorf de Freitas
guilherme.freitas@opiceblum.com.br