LOBA®

PPRCIC

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Relatório Anual 2025

Entidade: Globaz S.A. (LOBA)

NIF: 504873865

Responsável pelo Cumprimento Normativo (RCN): Equipa interna dedicada

Versão:	**Período de Referência:**	**Elaborado por:**	**Aprovado por:**
1.0	2025	Equipa interna dedicada	Administração: João Gaspar

1. Introdução e Enquadramento

O presente relatório visa avaliar a execução do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPRCIC) da LOBA durante o ano civil de 2025, em estrito cumprimento do **Artigo 6.º do Decreto-Lei n.º 109-E/2021 (RGPC)**.

2. Estrutura Organizacional e Governação

Nos termos e para os efeitos do disposto no Artigo 5.º do Decreto-Lei n.º 109-E/2021 (RGPC), informa-se que, por motivos de ausência temporária do Responsável pelo Cumprimento Normativo (RCN) iniciada em setembro de 2025, as funções de acompanhamento, monitorização e execução do PPRCIC passaram a ser asseguradas, de **forma colegial**, por uma equipa técnica interna dedicada. Todas as validações, controlos operacionais e decisões materiais do Programa de Cumprimento Normativo foram mantidos sob a supervisão direta e assinatura formal do **Conselho de Administração**. Esta transição organizacional garantiu a segregação de funções e a plena eficácia dos mecanismos de controlo previstos no Plano da Globaz, S.A - (LOBA)

3. Monitorização e Reclassificação de Riscos

Ao longo do exercício de 2025, a LOBA manteve uma vigilância ativa sobre a sua Matriz de Riscos e Controlos (MRC). O foco principal incidiu na convergência entre os requisitos do RGPC e os padrões internacionais de segurança da informação, promovendo melhorias contínuas no ambiente de controlo interno.

3.1. Área Tecnológica (CTO) e ISO 27001

No âmbito da presente avaliação, e sob o princípio regulatório da prudência, a

organização optou por **manter a classificação residual de risco no nível Elevado** para os três principais vetores tecnológicos ("Vulnerabilidades de Sistemas", "Gestão de Acessos" e "Disaster Recovery"). Esta decisão fundamenta-se nos seguintes critérios técnicos:

- **Implementação de Controlos e de uma solução de gestão de Passwords para equipas open-source:** Registou-se uma sólida consolidação documental e técnica alinhada com a norma ISO 27001. A este propósito, a gestão de acessos informáticos e a garantia de confidencialidade de credenciais foram significativamente reforçadas através da **institucionalização e uso generalizado de uma solução de gestão de Passwords para equipas open-source** como prática comum e segura de partilha de acessos. Adicionalmente, a criação do Comité de Cibersegurança introduziu uma supervisão mensal sobre os privilégios em plataformas críticas como o CRM e o SGP, sob a execução técnica da equipa de DevOps e supervisão do CTO.
- **Estado do Risco e Prática de Auditoria:** Embora as ações mitigadoras e a governança humana estejam plenamente ativas, determinou-se, por cautela metodológica, manter o nível de risco residual em "Elevado". Rejeitam-se, assim, descidas artificiais de risco antes que os controlos acumulem um histórico operacional robusto e auditável.
- **Perspetiva Futura:** Com a auditoria de concessão da certificação **ISO 27001 agendada para setembro de 2026**, antecipa-se que a conclusão formal deste processo venha a responder, validar e cobrir integralmente todos os pontos identificados nesta área, permitindo então uma reclassificação sustentada do risco residual à medida que o SGSI (Sistema de Gestão de Segurança da Informação) atinge a sua plena maturidade operacional.

4. Formação e Cultura de Integridade

Em 2025, a LOBA continuou a promover a cultura de ética através de:

- Sessões de esclarecimento sobre o Código de Conduta (v1.3).
- Integração de novos colaboradores com foco nas políticas de anticorrupção.
- Manutenção da transparência sobre os canais de reporte interno.
- Encontra-se planeada uma ação de formação obrigatória extensível a toda a

organização, com vista a garantir a universalidade e a consolidação contínua do Programa de Cumprimento Normativo.

5. Canal de Denúncias

Durante o período em análise, o canal de denúncias não registou qualquer comunicação de irregularidades ou infrações, confirmando a eficácia das medidas preventivas implementadas.

6. Conclusão

A LOBA conclui o exercício de 2025 com o seu sistema de compliance reforçado. A integração da gestão de riscos de corrupção com a infraestrutura da ISO 27001 garante uma proteção robusta e sustentável contra riscos de integridade.



Pelo Conselho de Administração: *João Gaspar (CEO) - Globaz, S.A. (LOBA)*

15 de abril de 2026

LOBA®

PPRCIC

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Relatório Intercalar

Entidade: Globaz S.A. (LOBA)

NIF: 504873865

Responsável pelo Cumprimento Normativo (RCN): Equipa interna dedicada

Versão: 1.0	**Ciclo intercalar:** 2025	**Elaborado por:** Equipa Interna Dedicada	**Aprovado por:** Administração: João Gaspar

1. Introdução e Enquadramento Legal

O presente relatório é elaborado em conformidade com o disposto no **Artigo 6.º do Decreto-Lei n.º 109-E/2021 (RGPC)**. O objetivo é proceder à monitorização intercalar da execução do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPRCIC), com foco especial nos riscos identificados com nível de exposição "Elevado".

2. Monitorização do Programa

Em linha com a Matriz de Riscos e Controlos (MRC) em vigor, a infraestrutura e os sistemas informáticos da LOBA foram mapeados como áreas críticas devido ao seu potencial impacto no desvio de informação imaterial ou fraudes.

No âmbito desta avaliação intercalar, e sob o princípio regulatório da prudência, a organização optou por manter a classificação residual de risco no nível "Elevado" para os três principais vetores tecnológicos. Esta decisão fundamenta-se na necessidade de acumular evidências operacionais históricas e consolidar a governança humana antes de proceder a uma reclassificação formal para níveis inferiores.

A gestão de acessos informáticos, particularmente quanto à garantia de confidencialidade de passwords e acessos a sistemas com informações com caráter reservado, foi alvo de atenção. Registou-se a implementação de Autenticação Multi-fator (MFA) em todos os sistemas críticos da LOBA, uma medida que se encontra ativamente em atualização, estando ainda pendente a sua conclusão em alguns sistemas. Adicionalmente, foi executada a centralização de todas as passwords através de uma solução de gestão de Passwords para equipas open-source, eliminando de forma

definitiva as credenciais dispersas e com pouco controlo. Por fim, a introdução da solução de patch management passou a garantir que os postos de trabalho contam com as proteções adequadas para mitigar os riscos de acessos não autorizados.

Risco Mapeado (PPR)	Nível Inerente	Nível Residual Intercalar	Controlos Ativos e Justificação de Eficácia Regulatória (MENAC)
Procedimentos para recuperação da informação e das operações em caso de desastre	Elevado	ELEVADO	As salvaguardas técnicas assentam numa plataforma de patch management em políticas rígidas de backups descentralizados. O controlo mitiga o impacto operacional e o risco de exfiltração de dados por perda ou furto. Retém-se o nível elevado reconhecendo que o fator humano de suborno não é anulável de forma absoluta pela barreira tecnológica. O risco será reavaliado após a auditoria formal da norma ISO/IEC 27001 agendada para setembro de 2026.
Vulnerabilidades dos sites a intrusões (Disponibilidade, Confidencialidade e Integridade)	Elevado	ELEVADO	Implementação em produção de uma ferramenta automática de CodeReview a cada commit e introdução de análise dinâmica de vulnerabilidades alinhada com o referencial OWASP Top 10. Os sistemas funcionam como segregação tecnológica de funções, impedindo a introdução dolosa de vulnerabilidades (backdoors) no código por programadores condicionados por terceiros (Prevenção de Corrupção no Setor Privado, Art.º 8.º). O risco residual mantém-se elevado enquanto o fluxo de DevOps cumpre os testes de maturidade operacional.
Gestão dos acessos informáticos e passwords (Sistemas Críticos: SGP / CRM)	Elevado	ELEVADO	Implementação de Autenticação Multi-fator (MFA) em todos os sistemas considerados críticos para a organização. Esta medida encontra-se em fase ativa de atualização, estando ainda pendente a sua conclusão em alguns sistemas. Centralização integral das passwords numa instância privada da plataformaatravés de uma solução de gestão de Passwords para equipas open-source, eliminando de forma definitiva as credenciais dispersas e com baixo nível de controlo. Implementação de uma solução *patch management* diretamente nos postos de trabalho dos colaboradores, garantindo as proteções adequadas para mitigar os riscos de

			acessos não autorizados.

3. Atividades de Formação, Sensibilização e Cultura Ética

O pilar da formação contínua foi assegurado de forma proporcional e dirigida, cumprindo os ditames de disseminação de uma cultura de integridade:

- Realizou-se em **02/10/2024** uma formação presencial focada no tema *"Prevenção de Riscos de Corrupção e Infrações Conexas"*, ministrada com o apoio de consultoria especializada, contando com a participação ativa de **18 colaboradores estratégicos**, incluindo membros da Administração e Direção.
- Como medida complementar para garantir a abrangência total, os conteúdos formativos em formato vídeo e a documentação de suporte foram disponibilizados de forma permanente na intranet da empresa.
- Encontra-se ainda planeada uma ação de formação obrigatória extensível a toda a organização, com vista a garantir a universalidade e a consolidação contínua do Programa de Cumprimento Normativo.

4. Canais de Denúncia e Instrumentos Gerais de Controlo

Durante o período de referência, os mecanismos transversais do Programa de Cumprimento Normativo mantiveram a sua plena operacionalidade:

- A **versão 1.3** do Código de Conduta manteve-se plenamente em vigor, servindo de referencial ético obrigatório para colaboradores e *stakeholders*. Não se identificou a necessidade de introduzir revisões materiais nesta fase intercalar.
- **Canal de Denúncias (Portal da Denúncia):** Em estrito cumprimento da **Lei n.º 93/2021** (Proteção de Denunciantes), o canal digital alojado no rodapé do *website* oficial manteve-se ativo e monitorizado tecnicamente.

Não foi registada qualquer comunicação de irregularidades, infrações ou denúncias de corrupção durante o intervalo monitorizado, o que indicia a eficácia do ambiente preventivo e do tom de integridade emanado pela gestão.

5. Conclusão

A avaliação intercalar demonstra que o PPRCIC da LOBA está a ser executado de forma empenhada e transparente. Ao assumir a retenção dos riscos de TI no nível **Elevado**, a organização demonstra um compromisso inequívoco com a verdade regulatória, rejeitando descidas artificiais de risco antes de testada a sua plena maturidade.

Como determinações para o próximo ciclo de planeamento, o RCN estabelece o acompanhamento dos trabalhos do Sistema de Gestão de Segurança da Informação (SGSI) rumo à certificação **ISO 27001** em setembro de 2026.

*__Nota de Atualização Estrutural (Setembro de 2025):__ Informa-se que, por motivos de ausência temporária do Responsável pelo Cumprimento Normativo (RCN) iniciada em setembro de 2025, as funções de acompanhamento e execução do PPR passaram a ser asseguradas, de **forma colegial**, por uma equipa técnica interna dedicada. Todas as validações, controlos e decisões materiais do Programa de Cumprimento Normativo mantêm-se sob a supervisão direta e assinatura formal do **Conselho de Administração**, garantindo a total continuidade e eficácia dos controlos previstos no Decreto-Lei n.º 109-E/2021.



Pelo Conselho de Administração: *João Gaspar (CEO) - LOBA*

30 de novembro de 2025