Política de Segregação de Funções e Confidencialidade da Informação

Elaborador: Roberto Stricher | **Revisor:** Grupo de Trabalho Deliberativo

Aprovador: Política aprovada pelo CONSUNI – Conselho Superior Universitário em xx/xx/xxxx pela ata nºxx | Versão: 01

UNIPAR
UNIVERSIDADE PARANAENSE

Sumário

1. OBJETIVO

Segregação de funções refere-se a práticas onde o conhecimento e/ou privilégios necessários para se completar um processo são quebrados e divididos entre múltiplos usuários de forma a coibir que apenas um seja capaz de executá-lo ou controla-lo sozinho.

A principal razão de se aplicar a segregação de funções é prevenir a realização e ocultação de fraude e erro no curso normal das atividades, uma vez que havendo mais de uma pessoa para realizar uma atividade se minimiza a oportunidade de transgressões e aumenta as chances de se detectá-la, assim como de se detectam erros não intencionais.

2. DEFINIÇÕES

- **Tipos de Segregação de Funções:**
  - **Separação sequencial:** quando uma atividade é quebrada em etapas realizadas por diferentes pessoas (ex.: solicitação, autorização e implementação de direitos de acesso)
  - **Separação individual:** quando pelo menos 2 pessoas precisam atuar para aprovar (ex. quem prepara não revisa, quem revisa não aprova)
  - **Separação espacial:** quando existe a necessidade de realizar atividades diferentes em locais diferentes (ex.: localizações diferentes para receber e armazenar matéria prima)
  - **Separação fatorial:** quando vários fatores contribuem para se completar a atividade (ex.: acesso por autenticação de dois fatores)
- **Conflito de Interesses:** eventos nos quais os objetivos pessoais dos tomadores de decisão, por qualquer razão, não estejam alinhados aos objetivos da entidade, alunos e de seus clientes
- **Confidencialidade**: somente as pessoas devidamente autorizadas podem ter acesso à informação
- **Integridade:** apenas alterações autorizadas podem ser realizadas nas informações;
- **Disponibilidade:** a informação deve estar disponível sempre que necessário as pessoas autorizadas.

3. DIRETRIZES / REGRAMENTOS

Segregação de Funções

- Divisão da função em etapas separadas, considerando tanto o conhecimento necessário para a função trabalhar como os privilégios que possibilitam que a função seja abusada;

- Definição de um ou mais princípios de segregação a serem aplicados. Exemplos de funções e princípios de segregação a serem aplicados são:
    - Funções de autorização (ex.: duas pessoas precisam autorizar um pagamento)
    - Funções de documentação (ex.: uma pessoa cria um documento e outra o aprova)
    - Custódia de ativos (ex.: criação e armazenamento de cópia de segurança em sites diferentes)
    - Ambientes de desenvolvimento e produção dos sistemas aplicativos, no qual somente pessoas de TI possam ter acesso na área de desenvolvimento e somente pessoas das áreas operacionais ao ambiente de produção dos sistemas aplicativos (ex.: colaborador dada área de TI realizar mudança na versão do sistema aplicativo que está em produção);
- Atividades desempenhadas por pessoas que tenham conflito de interesses devem ser identificadas suas responsabilidades redistribuídas de forma a eliminar a exposição a esse risco;
- Controles compensatórios deveriam estar implementados para assegurar que mesmo sem a segregação de funções os riscos identificados estão sendo apropriadamente tratados. Exemplos de controles de compensação são:
    - **Monitoramento de atividades**: este permite que as atividades sejam supervisionadas enquanto em progresso, como uma forma de assegurar que elas estão sendo realizadas adequadamente.
    - **Trilhas de auditoria**: estas permitem a organização recriar os reais eventos desde o início até a sua situação atual (ex.: quem iniciou o evento, a hora do dia e data, etc.).
    - **Supervisão pela gestão**: isto permite avaliação e tratativa apropriada e em tempo hábil de situações excepcionais.

Confidencialidade das Informações

- As informações confidenciais devem ser tratadas de forma ética e sigilosa e de acordo com os procedimentos, códigos, manuais e políticas vigentes, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- Segregação de instalações, equipamentos e informações comuns, quando aplicável.
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

- Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao Gerente de GRC – Governança, Riscos e Compliance;

4. PAPÉIS E RESPONSABILIDADES

4.1 – GRC – Governança, Riscos e Compliance

- Identificar funções que são indispensáveis para as atividades da organização, e potencialmente sujeitas a abuso, considerando tanto os direcionadores de negócio como a conformidade regulatória (ex.: Matriz de Riscos e Controles Internos);
- Monitorar as áreas da Unipar que possuem funções indispensáveis e sujeitas aos riscos da falta de segregação e fomentar que os responsáveis distribuam as funções de forma a mitigar o risco ou implementar controles compensatórios para mitiga-los.
- Incluir na matriz de riscos e controles todas as funções consideradas indispensáveis para avaliar a efetividade dos mesmos.

4.2 – Áreas identificadas por GRC

- Manter uma distribuição de atividades que permita uma segregação de funções apropriada e efetiva;
- No caso de não ser possível uma segregação apropriada de funções, implementar controles compensatórios para mitigar esse risco;

4.3 – Todas as áreas / colaboradores da Unipar

- Seguir todas as diretrizes dessa política sobre Segregação de Funções e Confidencialidade das Informações;
- Implementar controles compensatórios nos casos em que a segregação de funções não for viável;
- Sempre que houver necessidade de compartilhar informações internas, ou sob responsabilidade da Unipar com alguma pessoa Jurídica / Física terceira, deverá:
    - Obter aprovação de GRC – Governança, Riscos e Compliance de que a informação pode ser compartilhada com terceiros;
    - Uma vez que for autorizado, deverá solicitar a assinatura de um NDA (*Non Disclosure Agreement* – Acordo de Não Divulgação) antes de compartilhar a informação.
- **Importante:** serão aplicados sansões aos colaboradores pela não observância dos direcionamento e regras dispostos nessa Política. Estas podem varia de uma simples advertência verbal à uma demissão por justa causa, no caso de se identificar a facilitação/descuido que possa gerar o vazamento de informações e ou documentos sem a devida autorização;

5. REGULAMENTAÇÃO INTERNA / EXTERNA

Política de Controles Internos e Política de Cadastro de Fornecedores.

6. VIGÊNCIA E HISTÓRICO DE APROVAÇÃO

A presente Política de Segregação de Funções e Confidencialidade da Informação, contendo os direcionamentos e regramentos, passa a vigorar a partir de sua aprovação.

DATA	DESCRIÇÃO	APROVADOR
21/07/2021	Criação da atual política	Conselho Superior Universitário na Ata #
DD/MM/AAAA	2ª Versão – Revisão e atualização do documento.	Conselho Superior Universitário na Ata #

CONSELHO SUPERIOR UNIVERSITÁRIO DA UNIPAR
CONSUNI