UNIVERSIDADE FEDERAL DE LAVRAS
PRÓ-REITORIA DE PLANEJAMENTO E GESTÃO
Diretoria de Gestão da Tecnologia da Informação

PROCESSO DE GERENCIAMENTO DE RISCOS

A Coordenadoria de Segurança da Informação da Diretoria de Gestão de Tecnologia da Informação – DGTI, em conformidade com a Norma Complementar nº 04, da Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República – GSIPR de 15/02/2013, institui o seguinte processo de gerenciamento de riscos:

CAPITULO I – OBJETIVOS E ESCOPO

Art 1º. Este documento estabelece as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC na Universidade Federal de Lavras – UFLA, em conformidade com o Art. 7º da Política de Segurança da Informação e Comunicações – PSIC/UFLA, visando manter os riscos em níveis aceitáveis.

Art 2º. O processo de GRSIC deve estar alinhado aos planos estratégicos institucionais da UFLA, buscando identificar as necessidades da instituição em relação aos requisitos de segurança da informação e comunicações, bem como estabelecer um Sistema de Gestão de Segurança da Informação – SGSI eficaz e alinhado com as melhores práticas de segurança e a Norma ABNT NBR ISO/IEC 27005.

Art 3º. O processo de GRSIC está limitado ao escopo das ações de Segurança da Informação e Comunicações e tais ações compreendem apenas as medidas de proteção dos ativos de informação, conforme definido neste documento.

Art 4º. Para fins da execução do processo de GRSIC/UFLA aplicam-se os seguintes conceitos:

I. Ativo de Informação – qualquer recurso que faça parte dos sistemas de informação e meios para geração de documentos que tenham valor para a UFLA;
II. Ativo de Sistema – patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução de sistemas e processos da UFLA;
III. Ativo de Processamento – patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura ou instalações físicas necessários para a execução de sistemas e processos da UFLA, tanto aqueles produzidos internamente quanto os adquiridos pela universidade;
IV. Controle de Acesso – restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação da UFLA;
V. Custódia – consiste na responsabilidade de se guardar um ativo para terceiros sem, contudo, permitir automaticamente o acesso ao ativo ou o direito de conceder acesso a outros;

VI. Direito de Acesso – privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;
VII. Ferramentas – conjunto de equipamentos, programas, procedimentos, normas e demais recursos por meio dos quais se aplica a Política de Segurança da Informação da UFLA;
VIII. Incidente de Segurança – qualquer evento ou ocorrência que promova uma ou mais ações que comprometa, ou que seja uma ameaça à integridade, autenticidade ou disponibilidade de qualquer ativo da UFLA;
IX. Proteção dos Ativos – processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade, sendo que o meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;
X. Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
XI. Análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco;
XII. Análise/avaliação de riscos – processo completo de análise e avaliação de riscos;
XIII. Avaliação de riscos – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;
XIV. Comunicação do risco – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;
XV. Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e consequências de um risco;
XVI. Evitar risco – uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;
XVII. Gestão de Riscos de Segurança da Informação e Comunicações – conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
XVIII. Identificação de riscos – processo para localizar, lista r e caracterizar elementos do risco;
XIX. Reduzir risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;
XX. Reter risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;
XXI. Riscos de Segurança da Informação e Comunicações – potencial associado à exploração de uma o u mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
XXII. Transferir risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

XXIII. Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;
XXIV. Vulnerabilidade – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.
XXV. Responsabilidade – obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

CAPITULO II – PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art 5º. O processo de GRSIC deverá considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais, a PSIC/UFLA e a estrutura da UFLA.

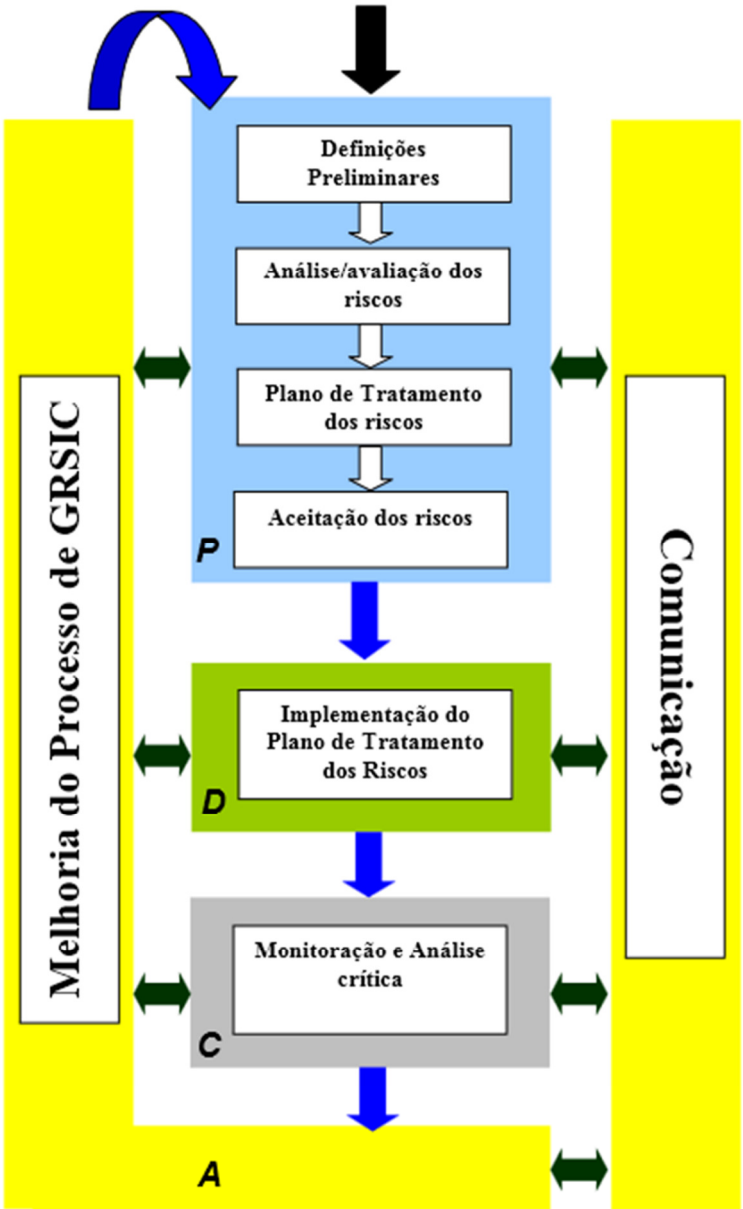
Art 6º. O processo de GRSIC está alinhado ao modelo denominado PDCA (Plan-Do-Check-Act), conforme definido na Norma Complementar nº 02/GSIPR, publicada no Diário Oficial da União nº 199, Seção1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua, estabelecido pelo Anexo A da Norma Complementar nº 04/GSIPR.

Art 7º. O processo de GRSIC é composto pelas seguintes etapas:

I. Definições Preliminares / Escopo – deve-se realizar uma análise do órgão, segmento, processo, sistema, recurso, ativo de informação ou da instituição como um todo, visando estruturar o processo de gestão de riscos de segurança da informação e comunicações, sendo consideradas as características do órgão ou entidade e as restrições a que estão sujeitas, a fim de delimitar o âmbito de atuação;
II. Análise/avaliação dos riscos – deve-se realizar o inventário e mapeamento dos ativos de informação, com o intuito de identificar os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados;
III. Plano de Tratamento dos Riscos – determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, considerando a análise custo/benefício, às restrições organizacionais, técnicas e estruturais, os requisitos legais e políticas existentes, estabelecendo ações de Segurança da Informação e Comunicações – SIC, responsáveis, prioridades e prazos de execução necessários à sua implantação;
IV. Aceitação do Risco – deve-se verificar os resultados obtidos pelo processo de executado, considerando o plano de tratamento, realizando seu aceite ou submetendo os ativos de informação à uma nova avaliação de riscos;
V. Implementação do Plano de Tratamento dos Riscos - executar as ações de Segurança da Informação e Comunicações – SIC incluídas no Plano de Tratamento dos Riscos aprovado.

VI. Monitoração e análise crítica - detectar possíveis falhas nos resultados, monitorar os riscos, as ações de SIC e verificar a eficácia do processo de GRSIC, a fim de mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades da instituição e a mudanças no ambiente e nos fatores de riscos na qual a organização está sujeita;
VII. Melhoria do Processo de GRSIC – executar as ações corretivas ou preventivas aprovadas e assegurar a implantação das melhorias, a fim de atingir os objetivos traçados.

Art 8º. O Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios deverão ser baseados em informações geradas pelo processo de GRSIC.



CAPITULO III – RESPONSABILIDADES

Art 9º. A Coordenadoria de Segurança da Informação da DGTI, no âmbito de suas atribuições, é responsável pela coordenação de Gestão de Riscos de Segurança da Informação e Comunicações, com anuência do Comitê de Segurança da Informação e Comunicações - CSIC.

Art 10º A Coordenadoria de Segurança da Informação da DGTI deverá submeter os resultados obtidos pelo processo de GRSIC ao CSIC, que baseado nessas informações, deverá elaborar e submeter para aprovação do Conselho Universitário – CUNI o plano de Gerenciamento de Incidentes e da Ação e Resposta a Incidentes, bem como, o Plano de Continuidade de Negócio da UFLA.

Lavras, 29 de agosto de 2014.

CLAYTON FERREIRA SANTOS
Coordenador de Segurança de Informação e Comunicações

ERASMO EVANGELISTA DE OLIVEIRA
Diretor de Gestão de Tecnologia da Informação