RESOLUÇÃO Nº. 202 DE 27 DE DEZEMBRO DE 2013.

A PRESIDENTE EM EXERCICIO DO CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DA GRANDE DOURADOS, no uso de suas atribuições legais RESOLVE **ad referendum:**

I) Aprovar a Politica de Segurança da Informação e Comunicação, da Universidade Federal da Grande Dourados – UFGD.

II) Esta Resolução entra em vigor na data da sua assinatura.

Profª. Marlene Estevão Marchetti

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
COORDENADORIA DE DESENVOLVIMENTO DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA UNIVERSIDADE FEDERAL DA GRANDE DOURADOS

1. CONSIDERAÇÕES INICIAIS

A Política de Segurança da Informação e Comunicações assegura o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações. Nesse contexto, a informação é um ativo de grande valor para a instituição e deve ser adequadamente utilizada, armazenada e protegida para a redução do risco de ocorrência de falhas que prejudiquem de qualquer modo a UFGD.

2. OBJETIVO

2.1. Estabelecer diretrizes, responsabilidades, competências e apoio da alta administração na implementação da gestão de segurança da informação e comunicações da Universidade Federal da Grande Dourados (UFGD), de modo a:

2.1.1. Assegurar a disponibilidade, integridade e confidencialidade das informações;

2.1.2. Definir as ações de segurança;

2.1.3. Orientar a adoção de soluções de segurança integradas;

2.1.4. Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3. FUNDAMENTO LEGAL DA POLÍTICA DE SEGURANÇA

3.1. Lei 9.983, de 14 de julho de 2000;

3.2. Decreto nº 4.553, de 27 de dezembro de 2002;

3.3. Decreto nº 3.505, de 13 de junho de 2000;

3.4. Instrução Normativa GSI Nº 1, de 13 de junho de 2008;

3.5. Norma Complementar nº 03/IN01/DSIC/GSIPR;

3.6. Art. 6º da Lei nº 10.683, de 28 de maio de 2003;

3.7. Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006;

3.8. NBR ISSO/IEC 27002:2007;

3.9. NBR ISSO/IEC 27005:2008;

3.10. Decreto nº 1048, de 21 de janeiro de 1994;

3.11. Decreto de 18 de outubro de 2000 – Governo Eletrônico;

3.12. Decreto nº 4.553, de 27 de dezembro de 2002;

3.13. Art. 5º Inciso III da Instrução Normativa nº 04 SLTI/MPOG, de 19 de maio de 2008;

3.14. e-PING – Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008;

3.15. Gabinete de Segurança Institucional/Departamento de Segurança de Informação e Comunicações – Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

4. CONCEITOS E DEFINIÇÕES

4.1. **Comitê Gestor de Tecnologia da Informação (CGTI):** comitê responsável por apreciar e aprovar o Plano Estratégico de Tecnologia da Informação (PETI), o Plano Diretor de Tecnologia da Informação (PDTI) e a Política de Segurança da Informação e Comunicações (PSIC) e demais normas a esta última relacionadas; analisar e aprovar os investimentos na área de Tecnologia da Informação e monitorar o estágio dos projetos e o nível dos serviços, recomendando ações para solução dos problemas de recursos e interesses da área;

4.2. **Comitê Gestor de Segurança da Informação (CGSI):** comitê responsável por elaborar e revisar periodicamente a Política de Segurança da Informação e

Comunicações (PSIC) e normas relacionadas, submetendo à aprovação do Comitê Gestor de Tecnologia da Informação, entre outras competências;

4.3. **Coordenadoria de Desenvolvimento de Tecnologia da Informação (COIN):** setor formalmente instituído na Universidade Federal da Grande Dourados (UFGD) que ficará responsável pela manutenção local dos recursos (RTIC) e planejamento, direção, avaliação e aplicação das políticas, diretrizes e regulamentações de tecnologia da informação e comunicação (TIC) em toda Universidade;

4.4. **Unidade de Ensino (UE):** os campi, unidades, polos e outras estruturas administrativas com atividades pedagógicas que demandem o uso das tecnologias da informação e comunicação;

4.5. **Recursos de Tecnologia da Informação e Comunicação (RTIC):** os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados nas Unidades de Ensino, tais como:

4.5.1. Equipamentos de informática e de telecomunicações de qualquer espécie;

4.5.2. Infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;

4.5.3. Laboratórios de informática de qualquer espécie;

4.5.4. Recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional da UFGD, redes ou outros sistemas de informação.

4.6. **Sistemas de informação:** os sistemas de controle, organização e planejamento acadêmicos e administrativos, bem como seus conteúdos hospedados e/ou armazenados em máquinas servidoras de responsabilidade da COIN ou em máquinas locais com cópias de segurança em máquinas servidoras de responsabilidade da COIN. São partes integrantes do sistema de informação os componentes clientes instalados nas máquinas locais;

4.7. **Serviços de rede:** todos os serviços oferecidos aos usuários por meio da infraestrutura de rede interna e externa, tais como: correio eletrônico, websites (páginas individuais e institucionais de conteúdos para a Internet), aplicações web (sistemas corporativos acessados via rede), repositórios de arquivos em rede, servidores de bancos de dados individuais e corporativos, sistemas de autenticação de usuários de rede, serviços de

segurança e monitoração, entre outros; bem como seus conteúdos (mensagens de correio eletrônico, dados corporativos, documentos, arquivos de configuração) que são hospedados e armazenados em máquinas servidoras de responsabilidade da COIN;

4.8. **Usuário:** qualquer pessoa física ou jurídica com vínculo oficial com a UFGD ou em condição autorizada que utiliza de alguma forma, algum recurso de tecnologia da informação e comunicação (RTIC) da UFGD. Os usuários poderão ser cadastrados ou não no domínio da UFGD e serão classificados, para fins de acesso aos recursos (RTIC), de acordo com os seguintes perfis:

4.8.1. Servidores: qualquer servidor vinculado a UFGD;

4.8.2. Alunos;

4.8.3. Outros:

4.8.3.1. Responsável por entidade externa que utiliza o domínio da UFGD (procuradoria, grupos de pesquisa, e outros afins);

4.8.3.2. Aluno bolsista;

4.8.3.3. Estagiário externo;

4.8.3.4. Servidores terceirizados;

4.8.3.5. Visitante.

4.9. **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. [IN01/DSIC/GSIPR];

4.10. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado. [IN01/DSIC/GSIPR];

4.11. **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. [IN01/DSIC/GSIPR];

4.12. **Não-repúdio:** garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

4.13. **Ativo de Informação:** qualquer recurso que faça parte dos sistemas de informação e meios para geração de documentos que tenham valor para a Instituição;

4.14. **Ativo de Sistema:** patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução de sistemas e processos da Instituição;

4.15. **Ativo de Processamento:** patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura ou instalações físicas necessárias para a execução de sistemas e processos da UFGD, tanto aqueles produzidos internamente quanto os adquiridos pela Universidade;

4.16. **Controle de Acesso:** restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação da UFGD;

4.17. **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;

4.18. **Direito de Acesso:** privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

4.19. **Ferramentas:** conjunto de equipamentos, programas, procedimentos, normas e demais recursos por meio dos quais se aplica a Política de Segurança da Informação da UFGD;

4.20. **Segurança da informação:** conjunto de políticas, normas e procedimentos que objetivam o controle de acesso, a preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade, integridade dos dados e responsabilidade das informações e dos recursos de TIC;

4.21. **Política de Segurança da Informação e Comunicações (PSIC):** documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações. [IN01/DSIC/GSIPR].

5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A Política de Segurança da Informação e Comunicações da Universidade Federal da Grande Dourados consiste na normatização e no disciplinamento de mecanismos que promovam a integridade da estrutura de rede e demais recursos de TIC nos quais trafegam informações e dados comuns ou restritos, neles incluídos os equipamentos que armazenam tais informações.

5.1. A Política de Segurança da Informação:

5.1.1. É constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pela UFGD.

5.1.2. É aplicável a todos os bens e serviços e a todo o pessoal que se utiliza dos recursos de Tecnologia da Informação e Comunicação (TIC), no âmbito da UFGD.

5.2. A Política de Segurança abrange os seguintes aspectos:

5.2.1. Requisitos de Segurança Lógica;

5.2.2. Requisitos de Segurança Física;

5.2.3. Requisitos de Segurança em Recursos Humanos;

5.2.4. Requisitos de Segurança dos Recursos Criptográficos.

5.3. Os requisitos de segurança, dos itens citados em 4.2 serão regulamentados por meio de normas e procedimentos específicos elaborados pelo Comitê Gestor de Segurança da Informação, e avaliados e aprovados pelo Comitê Gestor de Tecnologia da Informação.

6. COMPETÊNCIAS, RESPONSABILIDADES E ESTRUTURA DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

6.1. Ao Comitê Gestor de Tecnologia da Informação compete:

6.1.1. Apreciar e aprovar a Política de Segurança da Informação e Comunicações.

6.2. Aos demais gestores compete: Zelar pelo cumprimento das diretrizes da PSIC.

6.3. A todos os usuários compete:

6.3.1. Conhecer a PSIC e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares;

6.3.2. Adotar comportamento seguro, assumindo atitude pró-ativa e engajada no que diz respeito à proteção das informações da instituição.

6.4. A Pró-Reitoria de Gestão de Pessoas (PROGESP) compete: Obter a assinatura do Termo de Responsabilidade e informar à equipe de Tecnologia da Informação sobre mudanças no quadro funcional da Instituição.

6.5. A todos os setores: Responsabilidade pela garantia da segurança da informação no âmbito da UFGD, ressalvadas as situações em que:

6.5.1. A informação for retirada do âmbito da rede doa UFGD por usuários autorizados;

6.5.2. O usuário autorizado fornecer sua senha de acesso a qualquer outra pessoa;

6.5.3. O acesso à informação for limitado ou indisponibilizado por serviços e estruturas externas a UFGD ou de responsabilidade de outros órgãos ou empresas;

6.5.4. Quando propositadamente ou inadvertidamente o usuário fizer uso inadequado dos recursos (RTIC), seja por inabilidade, conhecimento insuficiente ou intenção de causar dano à instituição ou a outrem.

6.6. Ao Comitê Gestor de Segurança da Informação compete:

6.6.1. Elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (PSIC) e normas relacionadas, submetendo a aprovação do Comitê Gestor de Tecnologia da Informação;

6.6.2. Propor, acompanhar e divulgar os planos de ação para aplicação da PSI, incluindo a conscientização de usuários;

6.6.3. Propor a implantação de soluções para minimização dos riscos;

6.6.4. Observar os boletins de segurança e informativos divulgados pelo Centro de atendimento a Incidentes de Segurança (CAIS/RNP);

6.6.5. Elaborar propostas de normas complementares e políticas de uso dos recursos de informação.

6.7. Ao Presidente do Comitê Gestor de Segurança da Informação, no âmbito de suas atribuições, incumbe:

6.7.1. Promover cultura e segurança da informação e comunicações;

6.7.2. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

6.7.3. Propor recursos necessários às ações de segurança da informação e comunicações;

6.7.4. Coordenar o Comitê Gestor de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRIRC);

6.7.5. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

6.7.6. Manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR) para o trato de assuntos relativos à segurança da informação e comunicações;

6.7.7. Propor normas relativas à segurança da informação e comunicações.

6.8. Ao Conselho Universitário compete:

6.8.1. Aprovar a Política de Segurança da Informação e Comunicações e suas revisões;

6.8.2. Aprovar as Normas e Procedimentos decorrentes da PSIC/UFGD;

7. DIRETRIZES

7.1. TRATAMENTO DA INFORMAÇÃO

7.1.1. Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da instituição de tal forma a garantir a integridade, facilidade de localização e evitar o uso dessas informações por pessoas não autorizadas.

7.1.2. Descarte de informações sensíveis deverá ser realizado através de trituração, incineração ou remoção dos dados de forma segura.

7.1.3. Deverão ser realizadas cópias de segurança das informações tomando como base a norma de gerenciamento de cópias de segurança da informação da UFGD.

7.1.4. As cópias de segurança das informações citadas em 6.1.3 deverão ser testadas, verificadas e armazenadas, local e remotamente, de tal forma a evitar a perda da informação por alguma eventualidade.

7.2. GESTÃO DE RISCOS E TRATAMENTO DE INCIDENTES

7.2.1. Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços da UFGD, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:

7.2.1.1. O que deve ser protegido;

7.2.1.2. Análise de riscos (contra quem ou contra o quê deve ser protegido);

7.2.1.3. Avaliação de riscos (análise da relação custo/benefício).

7.2.2. A COIN apresentará planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê Gestor de Tecnologia da Informação e executados pela COIN.

7.2.3. As normas e procedimentos para implantação e gerenciamento de riscos de Informação serão definidos em documento específico elaborado pelo Comitê Gestor de Segurança da Informação.

7.2.4. A UFGD deverá realizar treinamentos específicos de conscientização para todos os servidores em noções de segurança da informação, visando à implantação e gerenciamento de todos os componentes do Sistema de Gestão de Segurança da Informação (SGSI) e a agilidade da notificação de qualquer evento relacionado a segurança da informação que venha a ocorrer.

7.3. GESTÃO DE CONTINUIDADE

7.3.1. O Plano de Continuidade de Negócio (PCN) tem como objetivo manter em funcionamento os serviços e processos críticos da UFGD na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e qualquer outro tipo de eventualidade que venha a ocorrer.

7.3.2. O PCN da UFGD será definido pelo Comitê Gestor de Segurança da Informação com base na análise de riscos e terá a aprovação do Comitê Gestor de Tecnologia da Informação.

7.4. AUDITORIA E CONFORMIDADE

7.4.1. Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos (RTIC).

7.4.2. Os procedimentos de auditoria e de monitoramento de uso dos recursos (RTIC) serão realizados periodicamente pela COIN, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

7.4.3. Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a PSIC e normas complementares, será permitido à COIN auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário, à Coordenadoria/Diretoria envolvida, e/ou a Reitoria da UFGD dependendo da gravidade. Sendo considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços.

7.4.4. Será mantido pela Ouvidoria da UFGD, canal de comunicação para receber denúncias de infração a qualquer parte desta política de segurança.

7.5. CONTROLE DE ACESSO E UTILIZAÇÃO DOS RECURSOS

7.5.1. Todos os usuários da UFGD têm o direito ao uso dos recursos (RTIC) da UFGD de acordo com as diretrizes de seu perfil, definidas por meio de requisitos técnicos ou por determinação específica da Reitoria ou dos órgãos da administração superior.

7.5.2. O acesso aos serviços de rede da UFGD que necessitam autenticação só será permitido a usuários cadastrados.

7.5.3. O acesso aos recursos (RTIC) será feito por controles físicos ou lógicos, com objetivo de proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. Quando da utilização de nome de usuário e senha, estes serão definidos no momento de ingresso na UFGD.

7.5.4. Todos os usuários deverão, por meio de um termo de responsabilidade específico, assumir o compromisso de:

7.5.4.1. Declarar o conhecimento e aceitação dos termos desta política de segurança e de suas políticas e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

7.5.4.2. Declarar estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria;

7.5.4.3. Manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da COIN.

7.5.5. Todos os usuários, e qualquer outra pessoa que entre na instituição, deverão possuir algum tipo de identificação visível e ter seu acesso registrado, onde possa ser visualizada a data e hora de sua entrada e saída.

7.5.6. Qualquer tipo de informação referente a conteúdos que dizem respeito à instituição deverão ser guardados em lugar seguro como, por exemplo, cofres específicos, armários e mobílias que possuam algum tipo de fechadura quando não estiverem em uso.

7.5.7. Qualquer tipo de equipamento de armazenagem e processamento de informação com tombamento (Ex.: estações de trabalho, notebooks, celulares) só poderão ser utilizados fora das dependências da instituição ou do departamento de sua responsabilidade com autorização prévia, e protegido de forma adequada contra furto, roubo ou perda da informação.

7.5.8. É de total responsabilidade do usuário a proteção das informações institucionais que estejam sob sua responsabilidade, utilizadas no âmbito da instituição ou fora de suas dependências.

7.5.9. O gerenciamento de informações, documentos e materiais sigilosos da UFGD deverão estar em conformidade com a Lei nº 8.159/1991, que dispõe sobre a política

nacional de arquivos públicos e privados e dá outras providências e com o Decreto nº 4.553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

7.6. CORREIO ELETRÔNICO

7.6.1. Os serviços de correio eletrônico hospedados em máquinas servidoras da UFGD, ou em servidores de outras instituições da Administração Pública, são oferecidos como um recurso profissional para apoiar os usuários cadastrados da UFGD no cumprimento dos objetivos institucionais e são passíveis de auditoria.

7.6.2. Os serviços de correio eletrônico citados em 6.6, deverão garantir o sigilo, a confidencialidade, o não-repúdio, a autenticidade, a disponibilidade geral do serviço e, os usuários que o utilizarem, deverão assegurar que o endereçamento da mensagem esteja correto.

7.7. PUBLICAÇÃO E ACESSO À INTERNET

7.7.1. Todos os servidores têm o direito de acesso à internet, conforme as permissões de acesso estipuladas nas normas de segurança da instituição. Esse acesso deverá ser feito exclusivamente para fins diretos e complementares às atividades da instituição, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

7.7.2. Toda informação publicada no portal da UFGD será de responsabilidade do usuário que realizou a publicação.

8. PENALIDADES

A quem descumprir esta política de segurança, as normas e procedimentos estabelecidos pela UFGD serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

8.1. Na Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

8.2. No Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;

8.3. No Código Penal, através do Decreto-Lei nº 2.848/1940;

8.4. Da Lei 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

8.5. No Decreto nº 4.553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

9. DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicações da UFGD devem ser direcionados ao Comitê Gestor de Segurança da Informação, com a interveniência do Comitê Gestor de Tecnologia da Informação.

10. ATUALIZAÇÃO

Todos os instrumentos normativos gerados a partir da PSIC, incluindo a própria PSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 01 (um) ano.

11. VIGÊNCIA

A presente política passa a vigorar a partir da data de sua publicação.