POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

HU-UFGD

Sumário

1. ESCOPO

1.1. OBJETIVO

E estabelecer os objetivos do HU-UFGD para o gerenciamento da segurança da informação. A segurança da informação é definida como a preservação da confidencialidade, integridade e disponibilidade de informações.

Os princípios de segurança da informação descrevem as regras gerais relacionadas à segurança da informação dentro de uma organização. Esses princípios tentam explicar aos usuários o que é o correto e o comportamento incorreto na organização em relação a vários tópicos e conceitos. Alguns desses princípios estarão intimamente ligados à cultura de uma organização ou aos requisitos regulamentares que regem o setor em que a organização está funcionando. Outros, no entanto, serão aplicáveis a todas as organizações e serão encontrados em qualquer política de segurança da informação, como a proteção contra vírus e a conscientização e educação dos usuários.

1.2. ABRANGÊNCIA

O conhecimento desta POSIC aplica-se ao HU-UFGD, sendo de responsabilidade de todos os servidores, empregados, colaboradores internos ou externos, bem como a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do HU-UFGD Todos esses atores são responsáveis por garantir a segurança das informações a que tenham acesso.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta POSIC são estabelecidos os seguintes conceitos e definições:

a) **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;
b) **Ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
c) **Análise de riscos**: uso sistemático de informações para identificar fontes e estimar o risco;
d) **Atividade**: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
e) **Ativo**: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou

mais atividades e que tenha ou gere valor para a organização;

f) **Ativos de Informação**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

g) **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

h) **Avaliação de riscos**: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

i) **Celeridade**: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;

j) **Classificação da informação**: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

k) **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

l) **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

m) **Custodiante do ativo de informação:** é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

n) **Desastre:** evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais ou críticos, por um período de tempo superior ao prazo de recuperação;

o) **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

p) **Descarte:** eliminação correta de informações, documentos, mídias e acervos digitais;

q) **Ética**: os direitos dos agentes públicos devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;

r) **Evento de segurança da informação**: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação, ou falta de controle, ou situação previamente desconhecida que possa ser relevante para a segurança da informação;

s) **Gerenciamento de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

t) **Gestão de continuidade dos negócios:** processo de gestão que identifica ameaças potenciais para uma organização, bem como os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo prevê a definição de estrutura para o aprimoramento da resiliência

organizacional, de modo a se responder efetivamente às ameaças e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, assim como suas atividades de valor agregado

u) **Gerenciamento 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;

v) **Gestão de segurança da informação e comunicações:** ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

w) **Identificação de riscos:** processo para localizar, listar e caracterizar elementos do risco;

x) **Incidente de SIC:** evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

y) **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

z) **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

aa) **Política de Segurança da Informação e Comunicações**: documento aprovado pelo SGSIC, CGTI e CGSIC, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

bb) **Proprietário de ativos de informação:** unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

cc) **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

dd) **Resiliência**: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

ee) **Responsabilidade**: os usuários dos recursos tecnológicos devem conhecer e respeitar todas as normas de segurança da informação e comunicações da instituição;

ff) **Risco de SIC**: potencial associado à exploração de uma ou 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;

gg) **Segurança física e do ambiente:** processo referente à proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização estiver presente;

hh) **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à Ebserh;

ii) **Tratamento da informação:** conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

jj) **Tratamento de incidentes**: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas; e realizar as prováveis correções dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

kk) **Tratamento dos riscos:** processo e implementação de ações de segurança da informação e comunicações, com o objetivo de evitar, reduzir, reter ou transferir um risco;

ll) **Usuário:** qualquer pessoa que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação;

mm) **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

3. REFERÊNCIAS LEGAIS E NORMATIVAS

Esta POSIC está em conformidade com a POSIC da EBSERH, seguindo as mesmas referências legais e normativas, conforme Item 3 da POSIC da EBSERH e aplica-se no âmbito do HU-UFGD, filial da EBSERH.

4. PRINCÍPIOS

Esta POSIC e suas ações serão norteadas pelos seguintes princípios, assim definidos:

a) **Celeridade**: As ações de SIC devem oferecer respostas rápidas à incidentes e falhas de segurança;

b) **Ética**: Os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIC;

c) **Clareza:** As regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

d) **Legalidade**: As ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do HU-UFGD EBSERH e Universidade Federal da Grande Dourados.
e) **Publicidade:** Transparência no trato da informação, observados os critérios legais.

5. DIRETRIZES GERAIS

As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo HU-UFGD, e que devem ser seguidas pelos usuários de recursos tecnológicos, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, será sempre protegida adequadamente, de acordo com esta política. Os recursos de Tecnologia da Informação e Comunicação (TIC) Disponibilizados pelo HU-UFGD serão utilizados estritamente para seu propósito.

É vedado, a qualquer usuário do HU-UFGD, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

As diretrizes desta POSIC constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração dos seguintes documentos:

a) Norma Geral de POSIC do HU-UFGD: destinado aos usuários.
b) Norma Técnica de POSIC do HU-UFGD: destinado ao SGPTI
c) Plano de Gerenciamento de Riscos (PGR).
d) Plano de Gerenciamento de Incidentes (PGI).

Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta POSIC, devem ser direcionados ao Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC).

6. DIRETRIZES E ESPECÍFICAS

6.1. Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC)

Deve ser formalmente constituído por colaboradores nomeados pela Superintendência do HU-UFGD. A composição mínima deve incluir:

a) 1 representante indicado pela Superintendência para presidir o Subcomitê;
b) 1 representante e suplente indicado pela Gerência Administrativa;
c) 1 representante e suplente indicado pela Gerência de Atenção à Saúde;
d) 1 representante e suplente indicado pela Gerência de Ensino e Pesquisa;
e) 1 representante e suplente indicado pela Unidade de Comunicação Social
f) 1 representante e suplente indicado do Setor de Gestão de Processos e Tecnologia da Informação.

O SGSIC deverá reunir-se semestralmente. Reuniões adicionais devem ser realizadas sempre que for necessário, para deliberar sobre algum incidente grave ou definição relevante para o HU-UFGD. O SGSIC poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico.

Cabe ao SGSIC:

a) Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
b) Propor alterações nas versões da POSIC e a inclusão, a eliminação ou a mudança de normas complementares;
c) Avaliar os incidentes de segurança e propor ações corretivas;
d) Definir as medidas cabíveis nos casos de descumprimento da POSIC e/ou das Normas de Segurança da Informação complementares;

6.2. Gerenciamento de Segurança da Informação e Comunicações (GESIC)

Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade do negócio. As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Os requisitos de SIC do HU-UFGD devem ser explicitamente citados em todos os termos celebrados entre a instituição e terceiros, através de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política, bem como deverá ser exigido o "Termo de compromisso de uso dos ativos de tecnologia da informação do HU-UFGD".

6.3. Gerenciamento de Riscos de Segurança da Informação e Comunicações (GRSIC)

A GRSIC é um conjunto de processos que permite 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.

Qualquer instância administrativa, assistencial ou técnica do HU-UFGD torna-se uma área responsável por ativos de informação. A GRSIC deve ser realizado no âmbito do HU-UFGD, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizado periodicamente, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades.

Trata-se de um instrumento do programa de Gerenciamento de Riscos que deve incluir um Plano de Gerenciamento de Riscos (PGR) e um Plano de Gerenciamento de Incidentes (PGI).

O PGR consiste no processo de identificar, avaliar e administrar eventos diante de incertezas críticas.

O PGI definirá responsabilidade e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

6.4. Plano de Gerenciamento de Riscos (PGR)

A gestão de riscos é um processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos positivos ou negativos capazes de afetar os objetivos, programas, projetos ou processos de trabalho do Hospital Universitário (HU-UFGD) nos níveis estratégico, tático e operacional.

Seu objetivo é aumentar a probabilidade e o impacto dos riscos positivos (oportunidades) e reduzir a probabilidade e o impacto dos riscos negativos (ameaças)

6.5. Plano de Gerenciamento de Incidentes (PGI)

O gerenciamento efetivo e a resposta aos incidentes de Segurança da Informação para manter operações seguras dentro do HU-UFGD. Para isso deve:

a) Estabelecer e manter um incidente de segurança da informação e registro de resposta e registrar todos os incidentes
b) Garantir que todos os incidentes de Segurança da Informação sejam reportados e escalados (quando aplicável) através de canais de gerenciamento e / ou autoridades adequadas
c) Garantir que os incidentes sejam investigados e aplicar processos disciplinares formais
d) Garantir responsabilidades e procedimentos para a notificação atempada de eventos e incidentes de segurança, incluindo violações, ameaças e deficiências de segurança, são comunicados a todos os membros do HU-UFGD.

e) A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do HU-UFGD.

6.6. Gerenciamento de Ativos de Informação

O gerenciamento de ativos de informação deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua. Os ativos de informação do HU-UFGD deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de SIC e são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação. É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo HU-UFGD.

6.7. Tratamento da Informação

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do HU-UFGD. Os dados, as informações e os sistemas de informação do HU-UFGD devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade classificando a informação.

6.8. Classificação da Informação

Toda informação criada, manuseada, armazenada, transportada ou descartada do HU-UFGD será classificada de acordo com a Lei nº 12.527, de 18 de novembro 2011. O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo HU-UFGD e a partir dela conhecer e obedecer às restrições de acesso e divulgação associadas. As informações sob gestão do HU-UFGD terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento com o objetivo de limitar a exploração às informações exclusivas da instituição.

6.9. Monitoramento, Auditoria e Conformidade

O monitoramento, auditoria e conformidade observará o seguinte:

a) O uso dos recursos de TIC disponibilizados pelo HU-UFGD é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;
b) A entrada e saída de ativos de informação do HU-UFGD serão registradas e autorizadas por autoridade competente mediante procedimento formal;
c) Qualquer instância do HU-UFGD poderá ser um canal de comunicação para receber denúncias de infração a qualquer parte desta POSIC.

6.10. Controle de Acesso

A política e os procedimentos são consistentes com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, padrões e orientação. As regras de controle de acesso a todos os sistemas institucionais, intranet e internet, informações, dados e as instações físcas do HU-UFGD deverão ser definidas e regulamentadas, por meio de normas internas, com objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

6.11. Uso de e-mail

O correio eletrônico é um recurso de comunicação corporativa do HU-UFGD e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta POSIC e da "Norma Geral de SIC", além

das demais diretrizes do governo. O e-mail é para fins corporativos e relacionados às atividades do colaborador relacionado a sua atividade fim. As mensagens de correio eletrônico deverão incluir assinatura com o seguinte formato:

a) Nome do colaborador;
b) Gerência ou departamento;
c) Nome da Instituição;
d) Telefones;
e) Correio Eletrônico;

6.12. Acesso à internet

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por meio da "Norma Geral de SIC", atendendo as determinações dessa POSIC, e demais orientações governamentais e legislação em vigor. Deverá existir no mínimo os grupos a serem configurados:

a) Grupo 0: acesso irrestrito, de uso exclusivo aos administradores de rede (SGPTI), devendo ser utilizado apenas para fins de manutenção, teste e atualização dos servidores/ativos da rede, devendo ser nominal e seus acessos deverão estar registrados no relatório de acessos.

b) Grupo 1: acesso limitado, a critério do Chefe/Gerente e respeitando as presentes normas, para os colaboradores do HU UFGD EBSERH.

c) Grupo 2: acesso restrito somente a sites com assuntos de interesse do HU UFGD EBSERH.

6.13. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação são restritas ao SGPTI e devem observar critérios e controles de segurança para garantir o respeito aos atributos básicos de segurança da informação. Os sistemas legados anteriores a esta norma deverão ser:

Auditados para fins de documentação (inclui descrições narrativas, flowcharts, definição de ferramentas usadas para seu desenvolvimento, contribuição e formas de produção;

a) Listings de programa de fonte, dados de testes, contribuições e produção, arquivos detalhados e planos de registro, pedidos de mudança, instruções de operador e controles;
b) Elaboração de planejamento do setor SGPTI para que estes sistemas legados sejam substituídos a fim de se adequarem as normas vigentes tais como:

- **ISO 9001-2008:** certificação de padrão internacional que garante um confiável sistema de controle das etapas de desenvolvimento, elaboração e execução dos serviços.
- **CMMI – Nível 5:** baseado nas melhores práticas de desenvolvimento e manutenção, o CMMI – Capability Maturity Model Integration é um modelo de referência de práticas necessárias à maturidade da empresa, que busca estabelecer um modelo único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas. O nível 5 do CMMI é o mais alto grau de maturidade que a certificação reconhece.
- **MPS.BR:** desenvolvido pela Softex, pelo governo e por universidades para a melhoria da qualidade de processos, o MPS.BR, ou Melhoria de Processos do Software Brasileiro, engloba referência, avaliação e modelo de negócio para melhoria do processo de software no Brasil.

6.14. Conscientização, sensibilização e capacitação em SIC

O HU-UFGD deverá promover conscientização dos colaboradores em relação à relevância da segurança da informação, mediante campanhas, palestras, treinamentos e outros meios de marketing.

6.15. Investimentos em SIC

Os investimentos em SIC deverão ser avaliados quando houver necessidade e então haverá integrar o PDTI e deverá ser aprovado pelo CGTI.

6.16. Propriedade Intelectual

As informações produzidas por usuários internos ou externos, no exercício de suas funções, são patrimônio intelectual do HU-UFGD e não cabe a seus criadores qualquer forma de direito autoral, ressalvando o direito de autoria, se for o caso. É vedada a utilização de patrimônio intelectual do HU-UFGD em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

6.17. Contratos, Convênios, Acordos, Instrumentos e Congêneres

Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter clausulas que estabeleçam a obrigatoriedade de observância desta POSIC. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar essa POSIC e suas normas complementares aos empregados, prepostos e todos os envolvidos em atividades vinculadas ao HU-UFGD.

6.18. Uso de Computação em Nuvem

O uso de recursos de Computação em Nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo à determinações desta POSIC e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

6.19. Uso de Dispositivos Móveis

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações, internet e e-mail do HU-UFGD, devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a essa POSIC e regida por meio da "Norma Geral de SIC.

7. PENALIDADES

Ações que violem essa POSIC ou quaisquer de suas diretrizes, normas ou procedimentos ou que quebrem os controles de Segurança da Informação e Comunicações serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor. O usuário poderá responder a processo administrativo ou disciplinar pelo prejuízo que vier a ocasionar à instituição.

8. COMPETÊNCIAS E RESPONSABILIDADES

8.1. Superintendência do HU-UFGD:

a) Promover a cultura de segurança da informação e comunicações;
b) Aprovar a Política de Segurança da Informação e Comunicações (POSIC);
c) Nomear o Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC).

8.2. Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC):

a) Promover a cultura de SIC;
b) Elaborar, avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do HU-UFGD e às legislações vigentes;
c) Coordenar as ações de segurança da informação e comunicações;
d) Aprovar a abertura de processo administrativo mediante constatação de quebra e segurança da informação;
e) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Superintendência do HU-UFGD os resultados consolidados de tais investigações e avaliações;
f) Propor recursos necessários às ações de Segurança da Informação e Comunicações;
a) Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;
b) Propor e atualizar normas relativas à Segurança da Informação e Comunicações;
c) Prover os meios necessários para capacitação, o aperfeiçoamento técnico dos usuários do HU-UFGD, bem como prover a infraestrutura necessária para o seu funcionamento;
d) Divulgar no âmbito do HU-UFGD essa POSIC.

8.3. Setor De Gestão De Processos E Tecnologia Da Informação (SGPTI):

Ao SGPTI, como mantenedor dos ativos de TIC, cabe norma própria descrita na “Norma Técnica de SIC”.

8.4. Proprietário de Ativos de informação:

a) Proteger e manter os ativos de informação;
b) Seguir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com essa POSIC;
c) Garantir a segurança dos ativos de informação sob sua responsabilidade através de monitoramento contínuo;
d) Comunicar as exigências de SIC a todos os usuários sob sua responsabilidade;
e) Conceder e revogar acessos aos ativos de informação;
f) Comunicar ao SGPTI e/ou SGSIC a ocorrência de incidentes de SIC; e
g) Designar custodiante dos ativos de informação, quando aplicável.

8.5. Custodiante dos Ativos de Informação:

a) Proteger e manter os ativos de informação;
b) Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com essa POSIC.
c) Seguir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com essa POSIC.

8.6. Terceiros e Fornecedores:

a) Tomar conhecimento dessa POSIC;
b) Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
c) Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

8.7. Usuários:

a) Proteger e manter os ativos de informação sob sua responsabilidade;
b) Conhecer e cumprir essa POSIC;
c) Assinar o "Termo de compromisso de uso dos ativos de TIC do HU-UFGD";
d) Comunicar os incidentes que afetam à segurança dos ativos de informação e comunicações à chefia imediata.

9. DIVULGAÇÃO E CONSCIENTIZAÇÃO

A divulgação das regras e orientações de segurança aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança da informação no âmbito do HU-UFGD. Cabe ao SGSIC providenciar a divulgação interna dessa POSIC e das normas, inclusive com publicação permanente na página do HU-UFGD, para que seu conteúdo possa ser consultado a qualquer momento e desenvolver processo permanente de divulgação, sensibilização conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIC.

10. ATUALIZAÇÃO

A segurança da informação e comunicações, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos. Os instrumentos normativos gerados a partir dessa POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas da EBSERH Sede conforme os seguintes critérios:

10.2. Política de Segurança da Informação e Comunicações (POSIC):

a) Nível de Aprovação: Superintendência do HU-UFGD
b) Periodicidade de Revisão: Anual

10.3. Normas e Planos de SIC:

a) Nível de Aprovação: SGSIC
b) Periodicidade de Revisão: Semestral

10.4. Procedimentos Operacionais:

a) Nível de Aprovação: SGPTI
b) Periodicidade de Revisão: Semestral

10.5. Validade:

Essa POSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

11. PRINCIPAIS SIGLAS

ABNT Associação Brasileira de Normas Técnicas

CGSIC Comitê Gestor de Segurança da Informação e Comunicações

ETIR Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

GETIR Gestão de Tratamento de Incidentes de Segurança em Rede Computacional

GECON Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações

GESIC Gestão de Segurança da Informação e Comunicações

GRSIC Gestão de Riscos de Segurança da Informação e Comunicações

GSI/PR Gabinete de Segurança Institucional da Presidência da República

IEC International Electrotechnical Commission

ISO International Organization for Standardization

POSIC Política de Segurança da Informação e Comunicações

SGSIC Subcomitê Gestor de Segurança da Informação e Comunicações

SIC Segurança da Informação e Comunicações

SISP Sistema de Administração dos Recursos de Informação e Informática

TI Tecnologia da Informação

TIC Tecnologia da Informação e Comunicações

DGPTI Diretoria de Gestão de Processos e Tecnologia da Informação

PDTIC Plano Diretor de Tecnologia da Informação e Comunicações

12. CONTROLE DE VERSÃO

VERSÃO	DATA	DESCRIÇÃO DAS ATUALIZAÇÕES	AUTOR(ES)
1.0	27.02.18	Elaboração	Alessandro Carvalho, Alessandro Teixeira, André Pereira, André Rogério, Filipe Martins, Jonathas Júnior, Junio Eduvirgem, Leandro Santos, Márcia Strassburger, Thiago Hilgert