Tipo de documento:	**POLÍTICA**	**PO.SUP.CSI.001**	
Título do documento:	**Política de Segurança da Informação e Comunicação (POSIC)**	Emissão: 16/04/2024 Versão: 1ª	Próxima revisão: 16/04/2028
Lotação:	SUP/ Comitê de Segurança da Informação (CSI)		
Responsável pela execução do procedimento:	Comitê de Segurança da Informação		

CAPÍTULO I

DO OBJETIVO E ÂMBITO DE APLICAÇÃO

OBJETIVOS

Estabelecer, a nível macro, diretrizes, critérios e suporte administrativo para a manutenção da segurança da informação e, portanto, da autenticidade, confidencialidade, disponibilidade e integridade de dados e informações produzidas e/ou tratadas no Complexo do Hospital de Clínicas da Universidade Federal do Paraná/Empresa Brasileira de Serviços Hospitalares (CHC-UFPR/EBSERH).

Art. 1º A Política de Segurança da Informação e Comunicações (POSIC) tem por objetivo estabelecer diretrizes, critérios e suporte administrativo para a implementação da Segurança da Informação e Comunicações (SIC) visando a garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações no âmbito do Complexo Hospital de Clínicas da Universidade Federal do Paraná (CHC-UFPR/Ebserh).

Art. 2º A POSIC trata do uso e do compartilhamento de dados, informações e documentos no âmbito do CHC-UFPR/Ebserh em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando a continuidade de seus processos críticos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicação.

Art. 3º Implantação do Comitê de Segurança da Informação (CSI), com a participação por indicação dos seguintes representantes na posição de titulares e suplentes:

I. Gestor de Segurança da Informação (GSI);

II. Superintendência;
III. Gerência Administrativa;
IV. Gerência de Atenção à Saúde;
V. Gerência de Ensino e Pesquisa;
VI. Setor de Tecnologia da Informação e Saúde Digital;
VII. Ouvidoria;
VIII. Setor Jurídico;
IX. Unidade de Comunicação Regional;
X. Comitê de Implantação da Lei Geral de proteção de Dados Pessoais, comitê que o substitua ou, na falta de ambos, Encarregado de Dados Pessoais do CHC-UFPR/Ebserh.

Art. 4º Integram também a POSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Art. 5º A presente política subordina-se à Política de Segurança da Informação e Comunicação da Ebserh Sede e qualquer dispositivo aqui presente só é válido no que não conflitar com a POSIC da Sede.

Art. 6º Aplica-se a todos que possuam vínculo laboral, acadêmico ou contratual e a todos que utilizem quaisquer dos recursos de informação ou comunicação fornecidos e/ou gerenciados pelo CHC-UFPR/Ebserh, incluindo, mas não se limitando a funcionários (independente de vínculo), acadêmicos, professores, prestadores de serviço, terceirizados, e, no que couber, visitante e pacientes.

CAPÍTULO II

DA DESCRIÇÃO

Art. 7º Esta política descreve os conceitos, estratégias, ações e métodos para a implementação da segurança da informação, contendo instruções de caráter geral e apresentando boas práticas.

CAPÍTULO III

CONCEITOS E DEFINIÇÕES

Art. 8º Para os efeitos desta Política de Segurança entende-se por:

I. **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;

II. **Ameaça**: qualquer evento que explore vulnerabilidades ou seja causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III. **Análise de riscos**: uso sistemático de informações para identificar fontes e avaliar riscos;

IV. **Assinatura digital:** conjunto de dados criptografados, associados a determinado documento ou arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;

V. **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;

VI. **Ativo**: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha valor para a organização;

VII. **Ativo de informação:** patrimônio composto por dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;

VIII. **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;

IX. **Banco de Dados (ou Base de Dados):** é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

X. **Classificação da informação**: identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;

XI. **Cópia de Segurança (Backup):** copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade;

XII. **Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC):** Comitê responsável pela aprovação desta POSIC;

XIII. **Comitê de Segurança da Informação (CSI):** Comitê responsável pela deliberação de assuntos relacionados com a segurança da informação;

XIV. **Computação em nuvem:** modelo computacional que permite acesso, por demanda e independentemente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

XV. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada ou não credenciada;

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

XVII. **Custodiante da informação:** usuário que atua em uma ou mais fases do tratamento da informação, ou seja, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

XVIII. **Dado anonimizado:** é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa.

XIX. **Dados pessoais sensíveis:** aqueles relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a um indivíduo;

XX. **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;

XXI. **Descarte:** eliminação correta de informações, documentos, mídias e acervos digitais ou físicos;

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

XXIII. **Dispositivos móveis:** equipamentos portáteis, dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, dentre eles, laptops, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

XXIV. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):** grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

XXV. **Gestão de continuidade:** processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e seu valor agregado. É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos

componentes (processos, pessoas softwares, hardware, infraestrutura etc.) por ele utilizados;

XXVI. **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, à Tecnologia da Informação e Comunicações (TIC);

XXVII. **Gestão de Riscos em Segurança da Informação e Comunicações**: 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;

XXVIII. **Gestor de Segurança da Informação e Comunicações:** responsável pelas ações de segurança da informação e comunicações no âmbito do CHC-UFPR/Ebserh;

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

XXX. **Inventário e Mapeamento de Ativos de Informação**: processo interativo e evolutivo, composto por três etapas:

1. A identificação e classificação de ativos de informação;
2. Identificação de potenciais ameaças e vulnerabilidades; e
3. Avaliação de riscos.

XXXI. **Política de Segurança da Informação e Comunicações**: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e

indireta, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

XXXII. **Recurso Criptográfico**: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXXIII. **Segurança da Informação e Comunicações (SIC)**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXIV. **Termo de Responsabilidade (TR)**: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XXXV. **Termo de Confidencialidade (TC)**: documento formal, a ser assinado por prestadores de serviço da administração central do Ministério da Defesa, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;

XXXVI. **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXXVII. **Trilhas de Auditoria**: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados; e

XXXVIII. **Usuários**: servidores, empregados públicos, terceirizados, consultores, auditores, estagiários, estudantes, professores, médicos e residentes que obtiveram autorização do

responsável pela área interessada para acesso aos Ativos de Informação do CHC-UFPR/Ebserh, formalizada por meio da assinatura do Termo de Responsabilidade.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 9º A POSIC do CHC-UFPR/Ebserh orienta-se pelos seguintes princípios:

I. **Disponibilidade**: garante que a informação estará acessível e utilizável por pessoa física, sistema, órgão ou entidade, quando requisitada;
II. **Integridade**: garante que a informação não será modificada, gravada ou excluída sem autorização ou acidentalmente;
III. **Confidencialidade**: garante que a informação será acessada apenas por pessoa física, sistema, órgão ou entidade autorizada e credenciada; e
IV. **Autenticidade**: garante a identificação de pessoa física, sistema, órgão ou entidade que produziu, expediu, modificou ou excluiu a informação.

Art. 10 As ações da POSIC, no âmbito do CHC-UFPR/EBSERH, são norteadas pelos seguintes princípios:

I. **Criticidade**: define a importância da informação para a continuidade do negócio da organização;
II. **Celeridade**: garante respostas rápidas a incidentes e falhas de segurança;
III. **Clareza**: as regras e a documentação sobre segurança da informação e comunicações devem ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;
IV. **Ética**: preserva o direito do servidor, militar, colaborador, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação e comunicações;

V. **Legalidade**: devem ser levadas em consideração as leis as normas e as políticas organizacionais administrativas, técnicas e operacionais vigentes; e

VI. **Responsabilidade**: os usuários são responsáveis pelo cumprimento desta POSIC e devem respeitar a legislação e normas pertinentes à Segurança da Informação e Comunicações vigentes.

Art. 11 São observados, ainda, sem prejuízo dos demais, os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 12 Esta POSIC tem como principal diretriz a preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação do CHC-UFPR/Ebserh.

Art. 13 Pressupostos básicos

I. O sucesso das ações nos assuntos de segurança da informação e comunicações está diretamente associado à capacitação dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

II. A informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.

III. A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade,

disponibilidade, conformidade e confidencialidade.

IV. Todos os usuários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional e sejam usuários dos ativos sigilosos, devem assinar o Termo de Responsabilidade quanto ao sigilo dos dados, informações e conhecimentos do CHC-UFPR/Ebserh.

Art. 14 Para cada uma das diretrizes constantes das Seções deste Capítulo devem ser elaboradas normas técnicas específicas, manuais e procedimentos.

Art. 15 Tratamento da Informação

I. Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas

II. atividades, é considerada bem e propriedade do CHC-UFPR/Ebserh e deve ser protegida segundo as diretrizes descritas nesta POSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do órgão e preservar sua imagem.

III. É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo CHC-UFPR/Ebserh.

IV. Os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos de negócio do CHC-UFPR/Ebserh.

V. As informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e legislação específica em vigor.

VI. Todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

VII. As informações produzidas ou custodiadas pelo CHC-UFPR/Ebserh devem ser descartadas

conforme o seu nível de classificação.

VIII. Deve ser adotada uma solução de Gestão Eletrônica de Documentos com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa.

IX. A manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor.

X. A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento.

XI. O tratamento de dados pessoais sensíveis somente poderá ocorrer com consentimento do titular ou seu responsável legal, de forma destacada e para finalidades específicas, sendo que, sempre que possível, anonimizados.

Art. 16 Tratamento de Incidentes de Rede. A Equipe de Tratamento de Incidentes de Rede (ETIR), definida pela Ebserh Sede, tem a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Art. 17 Gestão de Risco.

I. Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação e comunicações.

II. Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito do CHC-UFPR/EBSERH.

III. Os usuários serão subsidiados com informações e, quando aplicável, treinamentos e capacitações para tal. A responsabilidade destas ações é do Comitê de Segurança da Informação, Setor de Tecnologia da Informação e Saúde Digital e Unidade de Comunicação Regional e, subsidiariamente, de todas as unidades funcionais.

IV. O processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade, conforme procedimentos definidos em norma específica sobre o tema.

Art. 18 Gestão de Continuidade

I. O CHC-UFPR/Ebserh deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

II. As informações de propriedade ou custodiadas pelo CHC-UFPR/Ebserh, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança atualizada e guardada em local remoto, de forma a garantir a continuidade das atividades do órgão.

III. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Art. 19 Auditoria e Conformidade

I. O CHC-UFPR/Ebserh deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos sistemas corporativos e a sua rede interna.

II. Deve ser realizada periodicamente verificação de conformidade das práticas de SIC aplicadas no CHC-UFPR/Ebserh com esta POSIC, bem como com a legislação específica em vigor.

III. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o CHC-UFPR/Ebserh.

IV. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

V. Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade.

VI. Os procedimentos e as metodologias utilizados na auditoria e conformidade no âmbito do CHC-UFPR/Ebserh serão definidos em norma específica, em conformidade com as diretrizes desta POSIC e demais legislações em vigor.

Art. 20 Controle de Acesso. O controle de acesso aos sistemas corporativos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico e serão definidos em norma específica, em conformidade com as diretrizes desta POSIC.

Art. 21 Uso de e-mail (correio eletrônico). O correio eletrônico é um recurso de comunicação institucional do CHC-UFPR/Ebserh e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta POSIC e das normas específicas, além das demais diretrizes do Governo Federal.

Art. 22 Acesso à Internet.

I. O acesso à rede mundial de computadores (Internet) deve ser definido em norma específica, em conformidade com as diretrizes desta POSIC, orientações governamentais e

legislações específicas em vigor.

II. Uso das Redes Sociais. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações do CHC-UFPR/Ebserh, deve ser regida por normas internas especificas e deve estar em consonância tanto com a POSIC quanto com os objetivos estratégicos da instituição.

Art. 23 Inventário e Mapeamento de Ativos de Informação

I. Nos aspectos relacionados à SIC, o processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios para a Gestão de SIC, Gestão de Riscos de SIC, Gestão de Continuidade de Negócios, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de geração da base de dados sobre os ativos de informação.

II. O processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

Art. 24 Dispositivos Móveis. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito do CHC-UFPR/Ebserh deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário e ser definido em norma específica, em conformidade com as diretrizes desta POSIC.

Art. 25 Computação em Nuvem. A implementação ou contratação de computação em nuvem no âmbito da administração central do CHC-UFPR/Ebserh deve observar norma específica, em

conformidade com as diretrizes desta POSIC e com as demais legislações vigentes sobre o tema.

Art. 26 Criptografia

I. A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico, conforme procedimentos definidos em norma e legislações específicas em vigor.

II. Qualquer sistema utilizado no CHC-UFPR/Ebserh e que contenham tabelas com senhas, deverão ter estas tabelas armazenadas criptografadas.

Art. 27 Contratação de Serviços.

I. Nos editais de licitação e nos contratos de empresas prestadoras de serviços com o CHC-UFPR/Ebserh deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta POSIC, bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade e do Termo de Confidencialidade.

II. A empresa contratada também deverá demonstrar que possui mecanismos que assegurem a segurança das informações do CHC-UFPR/Ebserh por ela acessadas direta ou indiretamente (acesso aos ativos que contêm informações) e cumprir o disposto nesta POSIC quando aplicável.

III. O apoio técnico aos processos de planejamento e avaliação da qualidade das soluções de tecnologia da informação e comunicações poderá ser objeto de contratação, desde que sob supervisão de servidores ou empregados do CHC-UFPR/Ebserh.

CAPÍTULO VIII

DAS COMPETÊNCIAS

Art. 28 Ao Comitê de Segurança da Informação (CSI) compete:

I. Atualizar a POSIC;

II. Propor, analisar e aprovar normas complementares relativas à segurança da informação e comunicações, em conformidade com as legislações vigentes sobre o tema;

III. Tratar dos assuntos de Segurança da Informação no âmbito do CHC-UFPR/Ebserh e assessorar diretamente o chefe do SETISD e a alta gestão.

Art. 29 Ao SETISD compete:

I. Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC em conformidade com as diretrizes desta POSIC;

II. Elaborar, implementar e atualizar normas internas específicas em conformidade com esta POSIC e demais diretrizes do Governo;

III. Manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais do CHC-UFPR/Ebserh.

Art. 30 À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais compete:

I. Coordenar as atividades de tratamento e resposta a incidentes de segurança.

II. Promover a recuperação de sistemas.

III. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de rede por meio de verificações de conformidade.

IV. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação

de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis.

V. Receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores do CHC-UFPR/Ebserh;

VI. Executar as ações necessárias para tratar quebras de segurança.

VII. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes; e

VIII. Cooperar com outras equipes de Tratamento e Resposta a Incidentes.

Art. 31 Divisão de Gestão de Pessoas (DivGP):

I. Comunicar mensalmente ao SETISD, por meio de documento do Sistema Eletrônico de Informações (SEI), o ingresso, a alteração de lotação ou localização, bem como o desligamento de pessoal, inclusive postos terceirizados, no âmbito do CHC-UFPR/Ebserh.

II. Definir, nas descrições de cargos e funções, as responsabilidades pela manutenção das ações de SIC, bem como colher a assinatura do Termo de Responsabilidade e do Termo de Confidencialidade que envolvam o manuseio dos ativos de informação.

CAPÍTULO VIX

DAS ATRIBUIÇÕES

Art. 32 O Gestor de Segurança da Informação e Comunicações possui as seguintes atribuições:

I. 7.1.1. Planejar e coordenar a execução das ações de SIC.

II. 7.1.2. Definir estratégias para a implementação desta POSIC e suas normas complementares.

III. 7.1.3. Supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de SIC.

IV. 7.1.4. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas.

V. 7.1.5. Encaminhar os fatos apurados, decorrentes de quebras de segurança, para a aplicação das penalidades previstas.

VI. 7.1.6. Gerenciar a análise de risco.

VII. 7.1.7. Verificar se os procedimentos de SIC estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativos internos específicos; e

VIII. Providenciar a divulgação interna e permanente desta POSIC e de suas normas complementares.

CAPÍTULO X

RESPONSABILIDADES

Art. 33 Do Usuário

I. Acessar a rede de dados do CHC-UFPR/Ebserh somente após tomar ciência das normas de SIC e assinar o Termo de Responsabilidade.

II. Tratar a informação digital como patrimônio do CHC-UFPR/Ebserh e como recurso que deva ter seu sigilo preservado.

III. Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do CHC-UFPR/Ebserh exclusivamente para o interesse do serviço.

IV. Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las.

V. Não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua lotação ou cujo teor não tenha autorização ou necessidade de conhecer.

VI. Não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros.

VII. No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso.

VIII. Não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional do CHC-UFPR/Ebserh por terceiros.

IX. Responder perante o CHC-UFPR/Ebserh pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil.

X. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente.

XI. Não transferir qualquer tipo de arquivo que pertença ao CHC-UFPR/Ebserh outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente.

XII. Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não são permitidos na rede computacional do CHC-UFPR/Ebserh.

XIII. Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional do CHC-UFPR/Ebserh pode ser auditada.

XIV. Estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional do CHC-UFPR/Ebserh deve obedecer a esse preceito.

XV. Utilizar unicamente e-mail institucional aprovado na realização de suas atribuições.

XVI. Ao assinar o Termo de Responsabilidade, o usuário declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta POSIC.

Art. 34 Do Custodiante da Informação

I. Cumprir e zelar pela observância integral das diretrizes desta POSIC e demais normas e procedimentos decorrentes.

II. Zelar pela disponibilidade, integridade, confidencialidade e autenticidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta POSIC e demais normas e procedimentos decorrentes, mediante assinatura do Termo de Responsabilidade.

III. Participar de capacitação e treinamento em segurança da informação e comunicações, quando convocado.

IV. Utilizar os recursos que lhe foram concedidos somente para o fim a que se destinam.

V. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada.

VI. Preservar a classificação do grau de sigilo a documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções; e

VII. Comunicar prontamente ao seu Chefe imediato e ao Gestor de Segurança da Informação e Comunicações qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

CAPÍTULO XI

DIVULGAÇÃO

Art. 35 A POSIC e suas atualizações, após publicação, deverão ser divulgadas amplamente aos usuários do CHC-UFPR/Ebserh e disponibilizadas na intranet para eventuais consultas.

CAPÍTULO XII

ATUALIZAÇÃO

Art. 36 A atualização desta POSIC deve ser realizada sempre que se fizer necessário, não excedendo o período máximo de três anos.

CAPÍTULO XII

PENALIDADES

Art. 37 O usuário responderá pelo prejuízo que vier a ocasionar ao CHC-UFPR/Ebserh em decorrência do descumprimento de uma ou mais regras previstas nesta POSIC.

Art. 38 A desobediência às regras estabelecidas implicará ao infrator as penalidades previstas em lei, nos âmbitos administrativo, civil e penal.

CAPÍTULO XIII

EMBASAMENTO LEGAL

Art. 39 Esta POSIC foi elaborada com base nas seguintes referências legais e normativas:

- Lei nº 7.232, de 29 de outubro de 1984.
- Lei nº 9.983, de 14 de julho de 2000.
- Lei nº 12.527, de 18 de novembro de 2011.
- Lei nº 12.737, de 30 de novembro de 2012.
- Lei nº 12.965, de 23 de abril de 2014.
- Lei nº 13.709, de 14 de agosto de 2018.
- Decreto nº 9.637, de 26 de dezembro de 2018.
- Decreto nº 11.529, de 16 de maio de 2023.
- Decreto nº 7.724, de 16 de maio de 2012.

- Decreto nº 7.845, de 14 de novembro de 2012.
- Instrução Normativa GSI nº 1, de 27 de maio de 2020.
- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.
- Norma ABNT NBR/ISO/IEC 27001/2022.
- Norma ABNT NBR/ISO/IEC 27002/2022.
- Código Penal Brasileiro (Decreto-Lei nº 2.848, de 7 de dezembro de 1940).
- Política de Segurança da Informação da rede Ebserh Versão 2.0.
- Política de proteção de dados pessoais da Ebserh Versão 1; e
- Política de classificação de informação, sigilo e temporalidade da Ebserh.

Tipo de documento:	**POLÍTICA**	**PO.SUP.CSI.001**	
Título do documento:	**Política de Segurança da Informação e Comunicação (POSIC)**	Emissão: 16/04/2024 Versão: 1ª	Próxima revisão: 16/04/2028
Lotação:	SUP/ Comitê de Segurança da Informação (CSI)		
Responsável pela execução do procedimento:	Comitê de Segurança da Informação		

HISTÓRICO DE REVISÃO

VERSÃO	DATA	DESCRIÇÃO DA ALTERAÇÃO E RESPONSÁVEL

Elaboração: Felipe Veiga Ramos, André Luiz de Souza Paula, Daniel Reblo Brun, Renato Augusto Peret de Almeida, Flávio André dos Santos, Rafael Henrique Gusso Rosado, Luana de Assis, Ana Cristina Matheus Medeiros, Gisely Dib do Vale, Carolina Montegute Feckinghaus, Roberto Sebastião Marques, Luis Carlos Ceres Vieira, Pablo Cordeiro da Silva, Irene Tomoko Nakano, Ida Eveline Rockel, Felipe Alves Angêlo, Leonardo Borsa, Cristine Heloisa de Miranda, Dafne Wandressa Salvador, Clarisse Oliveira de Carvalho, Valério Filomena de Oliveira, Denise Jorge Munhoz da Rocha e Jonathas da Silva Vieira	Data: 16/04/2024
Revisão:	Data:
Revisão (UGQ): Reginaldo Witiuk	Data: 11/07/2024
Aprovação (COLEX): Claudete Reggiani, Luiz Renato Carazzai, Jorge Vinícius Cestari Felix e Railson Henneberg	Data: 11/07/2024
Aprovação (Presidente do Comitê CSI): Felipe Veiga Ramos	Data: 31/07/2024
Validação (UGQ): Ana Cristina Matheus Medeiros	Data: 31/07/2024

Documento aprovado e validado conforme Processo SEI nº 23759.004695/2024-17

Documento aprovado pelo Colegiado Executivo sob processo SEI nº 23759.008885/2024-11

ANEXO I

COMPLEXO HOSPITAL DE CLÍNICAS – UFPR/EBSERH

SETOR DE TECNOLOGIA DA INFORMAÇÃO E SAÚDE DIGITAL

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu, _____, Matrícula nº _____, CPF nº, _____, Carteira de Identidade nº_____, expedida pelo _____ em _____ lotado(a) _____ _____, na qualidade de USUÁRIO(A) da rede de computadores ou CUSTODIANTE de informações do COMPLEXO DO HOSPITAL DE CLÍNICAS – UFPR/Ebserh, declaro ter conhecimento da Política de Segurança da Informação e Comunicações, segundo a qual, sem restar qualquer dúvida de minha parte, devo cumprir todas as suas diretrizes e orientações.

Estou ciente de meu compromisso no COMPLEXO DO HOSPITAL DE CLÍNICAS – UFPR/Ebserh e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto na POSIC e na legislação vigente.

Curitiba - PR, ____ de _____ de _____

Assinatura

(Usuário)

ANEXO II

COMPLEXO HOSPITAL DE CLÍNICAS – UFPR/EBSERH

SETOR DE TECNOLOGIA DA INFORMAÇÃO E SAÚDE DIGITAL

TERMO DE CONFIDENCIALIDADE

A _____, inscrita no CNPJ sob o nº _____, sediada _____, por intermédio de seu representante legal, o Sr.(a.)_____, portador(a) da cédula de identidade nº _____, expedida pelo (a)_____ e CPF nº _____, declara que, para fins da execução do contrato nº _____, comprometemo-nos a manter em sigilo, ou seja, não revelar ou divulgar as informações confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços nas instalações do COMPLEXO DO HOSPITAL DE CLÍNICAS – UFPR/Ebserh, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a eles se referem e ainda respeitar as normas de segurança vigentes.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o COMPLEXO DO HOSPITAL DE CLÍNICAS – UFPR/Ebserh de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, danos, perdas, custas e despesas que porventura venha a sofrer como resultado da violação do disposto neste instrumento.

_____

Local e Data

_____

Nome, Cargo e Assinatura (Representante da Licitante)