NORMA DE GESTÃO DE INCIDENTES: DADOS PESSOAIS

SUMÁRIO

1 INTRODUÇÃO

A presente norma é parte integrante do Programa de Privacidade e Proteção de Dados do **HOSPITAL NOSSA SENHORA DA CONCEIÇÃO S.A.** que por sua matriz e filiais compõem o **GRUPO HOSPITALAR CONCEIÇÃO** ("**GHC**"). O **GHC** procura aplicar de forma efetiva todos os seus valores, especialmente o comprometimento e a transparência no que diz respeito à proteção e tratamento dos dados pessoais que tenhamos acesso, direta ou indiretamente e elaborou a presente norma de gestão de incidentes contendo dados pessoais, determinando diretrizes, competências e responsabilidades, objetivando a garantia da melhor forma de resposta em caso de qualquer Incidente de Segurança ("Incidente") que venha a envolver Dados Pessoais, incluindo os meios de comunicação interna, as atribuições de cada setor e o reconhecimento das fragilidades e eventos que podem causar danos ao **GHC**, seus agentes públicos, fornecedores, titulares etc.

Outrossim, por meio desta norma, também serão determinados os meios de controle, registro e reporte de Incidentes e seus riscos, garantindo, por meio de rápida resposta, a minimização de eventuais vulnerabilidades surgidas em decorrência do Incidente. Ainda, este documento objetiva mitigar riscos ou danos que possam ocorrer aos titulares de dados pessoais - sejam eles usuários, parceiros ou agentes públicos do **GHC** - e seus dados, não se restringindo àqueles relativos aos dados sensíveis, (referentes à saúde ou à vida sexual, dados genéticos ou biométricos), e sim quaisquer dados que, quando tratados de forma combinada com outras informações, permitam inferir informações dessa natureza.

2 ABRANGÊNCIA

A presente norma é aplicada para qualquer caso de Incidente que envolva dados pessoais, estando amplamente em consonância com as demais políticas do **GHC** e documentos correlatos, principalmente com o Plano de Gestão de Incidentes (disponível no Repositório de Documentos). Ainda, este documento foi elaborado observando as legislações pertinentes de proteção e segurança de dados e leis correlatas.

Dessa forma, a aplicação deste documento se destina a todos os agentes públicos do **GHC** independentemente de seu grau hierárquico ou cargo. Assim como a todas as partes relacionadas e, em especial, a prestadores de serviços e órgãos públicos que

possuam relação com o **GHC** e que possam ter acesso a qualquer fonte de informação,dados pessoais ou outros dados do **GHC** ou de qualquer outro titular que o **GHC** venha a, eventualmente, tratar.

3 TERMOS E DEFINIÇÕES RELATIVAS AO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

Inicialmente, cabe destacar que um Incidente envolvendo dados pessoais é toda e qualquer violação de segurança que, de forma acidental ou dolosa, enseje ou seja capaz de dar ensejo à destruição, perda, alteração, divulgação, uso ou acesso não autorizados a dados pessoais tratados pelo **GHC**.

Incidentes podem se configurar por diversos modos, como é possível analisar:

Vazamento de dados pessoais	**Configura-se por ser o Incidente no qual os dados pessoais são expostos e disponibilizados, *indevidamente,* por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país.**
Acesso não autorizado	Configura-se por ser o Incidente no qual o acesso (lógico ou físico) a um sistema que possua dados pessoais é tentado ou obtido, *sem que se tenha a devida autorização para tal acesso*. Portanto, o acesso não autorizado é aquele cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida.
Negação de serviço	Configura-se por ser o Incidente no qual o *acesso (lógico ou físico) a um sistema que armazene* dados pessoais *é prejudicado ou impossibilitado,* de forma que a integridade dos dados pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada à indisponibilidade do acesso.
Uso inapropriado	Configura-se por ser o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas do **GHC**, incluindo a Política de Segurança da Informação, e demais gestões internas utilizadas para garantir a Privacidade e Proteção de Dados.

É por meio dessa gestão de Incidentes que se garante a implementação da gestão da confiabilidade, composta de três aspectos basilares, quais sejam:

Confiabilidade	Garantir que a informação, quando necessária, esteja acessível apenas aos agentes públicos autorizados e/ou processos, e seja devidamente protegida do conhecimento alheio.
Integridade	Garantir que a informação esteja correta, verdadeira e não esteja adulterada, espelhando a realidade.
Disponibilidade	Garantir que os sistemas, aplicativos e dados estejam disponíveis e acessíveis para usuários autorizados quando eles precisarem.

Desse modo, salienta-se que um Incidente não se caracteriza unicamente pelo vazamento de informações, pela invasão de criminosos virtuais, como hackers, ou pela infecção de sistemas por arquivos maliciosos, podendo, por exemplo, se apresentar por meio do uso inapropriado ou acesso indevido a dados de forma que possa danificar os sistemas e dados internos do **GHC**.

Destaca-se que as situações listadas no presente documento são meramente exemplificativas, uma vez que não é possível precisar todos os Incidentes que possam vir a ocorrer. Dessa forma, em caso de suspeita ou efetiva ocorrência de um Incidente, é necessário que os agentes públicos do GHC notifiquem à Gerência de Informática ou ao Encarregado de Dados Pessoais, conforme dispuser o Plano de Gestão de Incidentes ou a presente norma, reportando o maior número possível de informações sobre o fato.

4 RESPONSABILIDADES E OBRIGAÇÕES DAS GERÊNCIAS

Cada uma das gerências do **GHC**, diretamente envolvidas na governança ou não, tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme descrito a seguir:

4.1 Compete a todas as gerências:

- Prezar pela comunicação imediata sobre a ocorrência ou a mera suspeita de um Incidente ou de um risco, mediante o preenchimento do formulário constante no **Anexo I**;
- Cumprir rigorosamente as Políticas e gestões vigentes que possam contribuir para a segurança das informações e gestão de incidentes do **GHC**, contribuindo para a mitigação de riscos;
- Participar ativamente de treinamentos e programas de conscientização para mitigação de Incidentes;
- Realizar a gestão do monitoramento, comunicação e tratamento de riscos e Incidentes que afetem sua área;
- Fiscalizar agentes públicos, terceiros, fornecedores e quaisquer partes relacionadas com a sua Gerência em relação ao cumprimento de regras de segurança, voltadas à prevenção de riscos e Incidentes, prestando orientação e aplicando as sanções, quando for o caso.

4.2 Compete à Gerência de Informática:

- Observar o Plano de Resposta à Incidentes do **GHC**, específico da Gerência de Informática;
- Auxiliar as gerências no preenchimento do formulário constante no **Anexo I**;
- Elaborar testes de segurança, realizar avaliações preventivas e reativas e produzir relatórios sobre os indicadores referentes à segurança da rede de computadores do **GHC**;
- Implementar e receber do Comitê de Proteção de Dados Pessoais medidas que visem mitigar os riscos e realizar o monitoramento acerca dos resultados em Relatório de Incidentes;
- Mapear, tratar, diagnosticar e monitorar os arquivos, programas maliciosos (tais como malwares, ransomwares, spywares) ou eventuais ações de usuários com potencial de gerar Incidentes e riscos ao sistema do GHC;
- Receber, registrar, classificar e monitorar, em conjunto com o gerente ou agente público competente, os comunicados de riscos ou Incidentes, visando implementar medidas necessárias para neutralização, reestabelecimento de sistemas, recuperação de ativos, a fim de garantir que o risco e incidentes aconteçam;

- Avaliar junto ao Encarregado de Dados todos os riscos atinentes a dados pessoais, devendo considerar, dentre outros aspectos:
    - O contexto da atividade de tratamento de dados;
    - As categorias e quantidades de titulares afetados;
    - Os tipos e quantidade de dados violados;
    - Os potenciais danos materiais, morais, reputacionais causados aos titulares;
    - Se os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares;
    - As medidas de mitigação adotadas pelo controlador após o incidente.
- Produzir, em conjunto com o Encarregado de Dados, um Relatório de Tratamento do Incidente, no qual constarão todos os detalhes do evento, tais como avaliação, possíveis motivos, evidências, classificação quanto à criticidade, ativos comprometidos, extensão dos danos e demais detalhes úteis ao tratamento e registro do Incidente;
- Extrair o conteúdo didático de Incidentes ocorridos no GHC, utilizando o documento em treinamentos a fim de elaborar materiais para conscientização dos usuários sobre como prevenir e reagir aos Incidentes que prejudiquem a segurança da informação e os dados tratados pelo GHC e seus agentes públicos no desempenho de suas atividades;
- Divulgar formulário destinado a instruir o processo de comunicação de riscos e Incidentes pelos usuários, constante no **Anexo I**;
- Informar aos comunicantes dos riscos ou Incidentes sobre o resultado do tratamento;

Produzir e atualizar os materiais didáticos, realizar treinamentos e eventos voltados à segurança da informação e proteção de dados, tendo por base as informações extraídas dos tratamentos, resguardada a anonimização e sigilo de informações.

4.3 Compete ao Encarregado de Proteção de Dados:

- Apoiar a Gerência de Informática no desempenho de suas atribuições, bem como apoiar o setor afetado pelo Incidente no que for possível;
- Oferecer orientações aos demais agentes públicos, terceiros, fornecedores e usuários do **GHC**, referentes à prevenção de incidentes;

- Comunicar ao **GHC** e ao titular a respeito da ocorrência de Incidentes que possam acarretar riscos ou danos relevantes aos titulares. O comunicado aos titulares deve fazer uso de linguagem clara e conter:
    - A descrição da natureza dos dados pessoais afetados;
    - O resumo e data da ocorrência do incidente;
    - As informações sobre os titulares envolvidos;
    - A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
    - Os riscos relacionados ao incidente;
    - Os motivos da demora, no caso de a comunicação não ter sido imediata; (devendo sempre respeitar o prazo de 02 (dois) dias úteis – ou outro estabelecido pela Autoridade Nacional) - para seu reporte, e;
    - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
    - Dados de contato do Encarregado de Proteção de Dados do GHC.
    - Receber e atender as comunicações da **Autoridade Nacional de Proteção de Dados - ANPD** referentes a Incidentes, desenvolvendo, quando for o caso, em conjunto com o Comitê, planos para publicação do Incidente e medidas para reverter ou mitigar seus efeitos.

4.4 Compete aos Agentes Públicos, usuários e todos aqueles que possuam alguma vinculação ao GHC:

- Observar e realizar efetivamente as medidas de segurança previstas, mas não limitadas, nas Políticas e Normas referentes à segurança da informação e proteção de dados pessoais do **GHC**;
- Comunicar imediatamente à Gerência de Informática e ao Encarregado de Dados possíveis e quaisquer indícios de risco ou Incidente que afetem a segurança da informação e/ou os dados pessoais do **GHC**;
- Registrar via documentos e comunicar à Gerência de Informática e ao Encarregado de Dados sobre pontos vulneráveis de segurança com potencial de acarretar Incidentes, bem como sugerir melhorias.

As gerências e os responsáveis listados acima, quando da constatação de um Incidente ou sua mera suspeita, deverão atuar em conjunto com o Time de Resposta à Incidentes (TRI), conforme disposições tratadas no Plano de Gestão de Incidentes.

Ainda, toda medida que vier a ser adotada para a contenção do Incidente deverá ter sido cuidadosamente analisada e aprovada pelo TRI junto à Gerência de Informática, que deverão atuar para mitigação de eventuais danos decorrentes do Incidente, bem como para adotar medidas que diminuam o risco de sua ocorrência.

Por fim, a presente norma deverá ser observada junto ao Plano de Gestão de Incidentes para que seja adotado o procedimento correto para mitigação total do Incidente e de possíveis riscos constatados durante as operações do **GHC**.

5 REGRAS GERAIS PARA TRATAMENTO DE INCIDENTES

O tratamento de ameaças e Incidentes do **GHC** ocorrerá de acordo com o seguinte cronograma:

5.1 Comunicação:

Uma vez identificado o risco ou o Incidente, a pessoa que o constatar, deverá, no prazo máximo de 24 (vinte e quatro) horas, comunicar a Gerência de Informática pelo fone 32551689 (ramal 1689) ou pelo e-mail dpo@ghc.com.br, sendo tais informações posteriormente comunicadas ao Encarregado de Dados. A fim de cumprir com os requisitos elencados pela lei, a comunicação obrigatoriamente deverá conter:

- A data e hora em que a suspeita do Incidente ou o risco foi descoberto;
- O(s) tipo(s) de informações envolvidas;
- A(s) causa(s) do possível Incidente ou de um efetivo Incidente;
- O contexto em que ocorreu;
- Informações adicionais que sirvam para facilitar o entendimento do evento, suas causas e consequências.

ATENÇÃO: A comunicação sobre riscos ou até mesmo a suspeita de um Incidente é necessária para que seja devidamente registrada junto das medidas realizadas para

mitigar o possível Incidente. Assim, caso o comunicante constate tal suspeita e não o comunique, sanções disciplinares podem ser aplicadas.

5.2 Análise

Após a comunicação, se seguirá a imediata análise do risco ou Incidente pela Gerência de Informática, que deverá:

- Arquivar a comunicação, caso identifique que não se trata de risco ou Incidente relativo à segurança da informação;
- Produzir o Relatório de Tratamento de Incidente, classificando-o de acordo com seu nível de criticidade, nos termos das tabelas abaixo.

IMPACTO						
	Muito Alto	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

Criticidade	Descrição	Peso
Muito baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	**1**
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	**5**
Alta	**Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	**8**
Muito Alta	**Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	**10**

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
0 – 9,99	10 – 39,99	40 – 79,99	80 - 100

5.3 Escalação

Classificado o risco ou Incidente, caso envolva dados pessoais, a Gerência de Informática solicitará apoio por e-mail ao Encarregado de Dados e/ou ao gerente e agentes públicos da gerência afetada, cujo apoio julgue necessário.

A depender da criticidade, complexidade, extensão dos danos e ativos afetados (conforme analisados pelas tabelas supracitadas), a Gerência de Informática deve envolver o Comitê de Proteção de Dados Pessoais na gestão do Incidente.

5.4 Tratamento

Após a escalação, a Gerência de Informática com apoio do Encarregado de Dados e demais gestores e usuários, respeitada a ordem de prioridade de acordo com a classificação de criticidade:

- Alimentará o Relatório de Tratamento de Incidente, documentando o impacto e quais ativos e gerências foram ou serão afetados;

- Implementará ações necessárias para estancar os danos gerados pelo Incidente, isolando ambientes, diretórios e sistemas comprometidos;
- Identificará possíveis eventos que podem ter gerado o Incidente, coletando e documentando evidências;
- Avaliará possíveis soluções com base em seu conhecimento, normas técnicas, apoio de demais áreas ou empresas terceirizadas, aplicando as ações necessárias para neutralização do Incidente, reestabelecimento de sistemas, recuperação de ativos, garantindo que o risco de recorrência foi eliminado ou mitigado, se não for possível sua eliminação;
- Quando assim definido pelo Comitê de Proteção de Dados Pessoais, o Encarregado comunicará aos titulares afetados e à Autoridade Nacional de Proteção de Dados sobre a ocorrência de incidentes envolvendo dados pessoais, seguindo as determinações do Comitê e em prazo não superior a 02 (dois) dias úteis, conforme disposição regulada pela Autoridade Nacional, por meio de preenchimento de formulário e demais orientações constantes no link:
    - https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis.
- Se certificará de que inexistem outros incidentes ou riscos relacionados, abrindo chamados adicionais se for o caso;
- Encerrado o tratamento, devolverá o caso ao Comitê de Proteção de Dados Pessoais para validação.

5.5 Validação

Finalizado o tratamento, a Gerência de Informática reportará por meio do Relatório de Tratamento de Incidentes ao Comitê de Proteção de Dados Pessoais, que validará se o tratamento aplicado foi suficiente para a completa resolução do Incidente, bem como se há a necessidade de coleta de demais dados e evidências para fins didáticos e de auditoria.

5.6 Encerramento

Validado o tratamento, a Gerência de Informática encerrará o chamado, inserindo todos os dados necessários no Relatório de Tratamento de Incidente e informará ao comunicante sobre o resultado do tratamento.

6 ASPECTO DIDÁTICO

A fim de reduzir riscos e fortalecer a segurança da informação:

- O Comitê deverá produzir um relatório anual com informações relacionadas a Incidentes, do qual constará um resumo dos Relatórios de Tratamento de Incidente do período, indicadores sobre Incidentes, análise da efetividade de tratamentos, recomendações para neutralização ou redução de ameaças, riscos e Incidentes. O relatório será apresentado à Diretoria para debate e planejamento de medidas;
- Os incidentes supracitados relacionados à segurança da informação serão tratados pela Gerência de Informática e os relacionados à proteção de dados serão tratados pelo DPO;

O relatório semestral guiará a formulação de um inventário para monitoramento e avaliação dos riscos, o qual deverá ser debatido junto ao Comitê.

7 REVISÃO

A presente norma foi aprovada em 30/03/2023 e será revisada pelo Comitê de Proteção de Dados Pessoais sempre que se fizer necessário, com a subsequente aprovação da Diretoria-Executiva.

A presente Norma entra em vigor nesta data, em função da sua aprovação pela Diretoria-Executiva do Grupo Hospitalar Conceição.

Porto Alegre, 30 de março de 2023.

Cláudio da Silva Oliveira
Diretor-Presidente

Moises Renato Gonçalves Prevedello
Diretor Administrativo e Financeiro

Francisco Antônio Zancan Paz
Diretor Técnico

8 ANEXO I – RELATÓRIO DE TRATAMENTO DE INCIDENTE

Área comunicante: _____

Dados do comunicante:

Nome:

E-mail:

Telefone:

Incidente de segurança:

☐ Acesso não autorizado
☐ Uso inapropriado
☐ Outro (especificar no campo abaixo):
☐ Negação de serviço
☐ Vazamento de dados pessoais

_____

1. Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu:

2. Quando o incidente ocorreu? [Data e hora]

☐ Não tenho conhecimento. Justifique:

☐ Não tenho certeza. Justifique:

3. Qual a natureza dos dados afetados?

☐ Origem racial ou étnica.

☐ Convicção religiosa.

☐ Opinião política.

☐ Filiação a sindicato.

☐ Filiação a organização de caráter religioso, filosófico ou político.

☐ Dado referente à saúde.

☐ Dado referente à vida sexual.

☐ Dado genético ou biométrico.

☐ Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).

☐ Dado financeiro.

☐ Nomes de usuário ou senhas de sistemas de informação.

☐ Dado de geolocalização.

Outros: _____

4. Possíveis causas e evidências do Incidente:

5. Ativos comprometidos e extensão dos danos:

6. Criticidade:

☐ Muito alto ☐ Alto

☐ Médio ☐ Baixo

7. Ações de mitigação:

Porto Alegre, xx de xxxxxx de 20xx.

_____	_____
[ENCARREGADO DE DADOS]	**[GERENTE DA ÁREA – IDENTIFICAÇÃO DO INCIDENTE]**

_____

GERENTE DE INFORMÁTICA