1 – CONTROLE DE ALTERAÇÕES

Revisão	Data	Descrição	Autor
00	28.11.2023	Emissão do Documento	Gyanne G. Tavechio
01	23.01.2025	Alterado lay-out da documentação	Gyanne G. Tavechio

2 – OBJETIVO E CONSIDERAÇÕES

2.1 A Política de Incidentes de Segurança da Informação da ACRO tem por objetivos:

2.1.1 Diminuir os danos totais causados por incidentes que não puderam ser evitados, bem como a sua reincidência;

2.1.2 Promover a efetiva e eficaz Política da Segurança da Informação na ACRO; e

2.1.3 Diminuir o número total de incidentes de segurança da informação envolvendo a ACRO, por meio de prevenção sistemática dos eventos e eliminação de situações que permitem a ocorrência desses incidentes.

2.2 A Política de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação da ACRO e visa orientar o funcionamento do processo de gestão de incidentes de segurança digital e não digital da informação, de forma que estes sejam tratados adequadamente, reduzindo ao máximo os impactos para o negócio.

3 – DOCUMENTOS DE REFERÊNCIA

3.1 Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais

3.1.1 ABNT NBR ISO 27001:2022

4 – RESPONSABILIDADE E AUTORIDADES

4.1 Ao Comitê Gestor de Privacidade e Proteção de Dados compete:

4.1.1 Conduzir o processo de Gestão de Incidentes de Segurança da Informação;

4.1.2 Investigar incidentes, levantamento, cadeia de custódia e segurança das evidências;

4.1.3 Acompanhar os planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;

4.1.4 Comunicar aos gestores responsáveis;

4.1.5 Realizar as análises dos pós-incidentes (post mortem) para identificação e tratamento de causas raiz e aprimoramento de processos da ACRO e do próprio processo de gestão de incidentes de segurança da informação.

4.2 À Gestão de TI compete:

4.2.1 Executar os procedimentos de tratamento de incidentes de segurança da informação das informações digitais definidos nesta política, observado o que dispõe o Plano de Continuidade de TI da ACRO, no surgimento de qualquer denúncia e ou detecção automatizada e de registrar os incidentes tratados, conforme o modelo apresentado no Anexo I – Relatório de Incidentes;

4.2.2 Definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo a ACRO;

4.2.3 avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

4.2.4 Dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área; e

4.2.5 Elaborar, anualmente, relatório estatístico do número de incidentes para fins de acompanhamento pela ACRO.

4.3 À Coordenadora do Sistema de Gestão compete:

4.3.1 Executar os procedimentos de tratamento de incidentes de segurança da informação das informações não digitais definidos nesta política no surgimento de qualquer denúncia e/ou detecção automatizada e de registrar os incidentes tratados;

4.3.2 Definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo a ACRO;

4.3.3 avaliar periodicamente e analisar criticamente os registros de incidentes que resultem do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos; e

4.3.4 Dar suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

4.4 As responsabilidades dos gestores ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e pré-definidos pelo Comitê de Privacidade e Proteção de Dados.

4.5 As responsabilidades dos diretores, empregados e colaboradores são:

4.5.1 Os diretores, empregados e colaboradores devem estar em capacidade de identificar incidentes de segurança da informação quando for testemunhado;

4.5.2 Os diretores, empregados e colaboradores devem notificar qualquer evento de segurança ou fragilidade observada que possa causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de

informação nos sistemas, serviços ou redes da ACRO; e

4.5.3 Todos os empregados e colaboradores devem informar imediatamente à área de Gestão de TI todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento;

4.5.4 Na apuração dos incidentes de segurança da informação será considerada a vontade orientada à realização do incidente de segurança, ou seja, o elemento subjetivo que concretiza os requisitos de vulnerabilidade dos dados pessoais; e

4.5.5 Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos diretores, empregados e colaboradores, sob o risco de violar a política de segurança digital e não digital e da informação, bem como provocar danos aos sistemas, serviços ou recursos tecnológicos digitais ou não digitais.

5 - DESCRIÇÃO

5.1 O ACRO, no exercício de suas atribuições legais,

5.1.1 Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

5.1.2 Considerando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

5.1.3 Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta política em relação aos dados pessoais, mesmo após o seu término,

5.1 DA POLÍTICA E DEFINIÇÕES

5.1.1 Fica instituída a Política de Incidentes de Segurança da Informação da ACRO.

5.1.2 Para os efeitos desta Resolução, entende-se por:

5.1.2 Atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.

5.1.3 Atividade Crítica: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

5.1.4 Atividade Maliciosa: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema, serviço ou rede.

5.1.5 Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

5.1.6 Evento de Segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma

possível falha da política de segurança, falha das salvaguardas, ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança.

5.1.7 Fluxo de Trabalho de Incidentes: predefinição de etapas que devem ser tomadas para lidar com um tipo particular de Incidente.

5.1.8 Gerenciamento de Incidentes: processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um sistema, serviço ou rede seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado.

5.1.9 Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

Considera-se omissão a não observância das políticas de segurança definidas pela ACRO.

5.2 DA ABRANGÊNCIA

5.2.1 A Política de Incidentes de Segurança da Informação abrange todos os incidentes, confirmados ou sob suspeita, que envolvam o nome ou a propriedade da ACRO, bem como qualquer conselheiro, funcionário ou colaborador, no exercício da sua função ou relação com a ACRO.

5.2.2 A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

5.2.2.1 Violar da Política de Controle de Ativos de Tecnologia da Informação da ACRO;

5.2.2.2 Violar uma política de segurança, explícita ou implícita;

5.2.2.3 realizar acesso indevido ou não autorizado às instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pela ACRO que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

5.2.2.4 Realizar acesso indevido ou não autorizado aos dados, informações e documentos mantidos, tratados e controlados pela ACRO que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

5.2.2.5 Conectar dispositivo de tecnologia à rede da ACRO que esteja contaminado com vírus de computador detectado por mecanismo automatizado ou pessoal qualificado;

5.2.2.6 Violar norma de utilização ou configuração de dispositivo de tecnologia da informação, conectado ou não à rede da ACRO, detectada automática ou manualmente;

5.2.2.7 vazar dados pessoais;

5.2.2.8 utilizar credenciais de autenticação (senhas) por indivíduo não proprietário delas ou de outrem;

5.2.2.9 Facilitar fluxo de comunicação de rede caracterizado como atividade maliciosa por detecção de padrão ou análise manual, ou envolvendo dispositivos identificados por grupos de segurança como fonte de atividades

maliciosas;

5.2.2.10 Omitir a comunicação de fragilidade de segurança conhecida em processo, instalações, equipamentos, sistemas e serviços de informação e armazenamento de dados, informações e documentos mantidos, tratados e controlados pela ACRO;

5.2.2.11 violar direito autoral ou propriedade intelectual de qualquer natureza;

5.2.2.12 realizar tentativa de fraude, bem ou malsucedida, independentemente do dano causado; e

5.2.2.13 quaisquer outros eventos que constituam violação de requisito de segurança estabelecido pela Política de Segurança da Informação da ACRO, tenham eles origem no própria ACRO ou em grupos externos.

5.3 Violações e Sanções Aplicáveis

5.3.1 A violação a esta Política estará sujeita a medidas disciplinares e legais quando aplicáveis. As violações serão devidamente investigadas, de acordo com os procedimentos internos da ACRO, garantindo anonimato aos envolvidos.