REGISTRO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO - CRCRN

O Conselho Regional de Contabilidade do Rio Grande do Norte (CRCRN) tem primado pela adequação às diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD). Essa adequação se reflete na elaboração de Políticas relacionadas à segurança da informação e à privacidade dos dados dos titulares constantes em sua base.

A Resolução CRCRN nº 186/2023 instituiu a Política de Incidentes de Segurança da Informação em nosso Conselho, e na qual consta a definição de 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 de informação protegida, remoção ou limitação de uso de 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*.

Cabe observar que no presente ano, o CRCRN não registrou qualquer tipo de incidente dessa natureza no presente ano, até o momento de finalização desse documento em nenhum dos seus setores. Para ilustrar a informação segue o *check list* constantes na Política de Incidentes de Segurança da Informação do CRCRN com os incidentes e respectiva detecção:

Incidentes de Segurança da Informação		
	Tipo de incidente	**Resultado**
1.	Violação de Política de Controle de Ativos de TI;	Não detectado
2.	Violação de política de segurança;	Não detectado
3.	Realização de acesso indevido/não autorizado às instalações, equipamentos, sistemas e serviços, etc. do CRCRN;	Não detectado
4.	Realização de acesso indevido/não autorizado aos dados, informações e documentos do CRCRN;	Não detectado

5.	Uso de dispositivo de tecnologia contaminado com vírus à rede do CRCRN;	Não detectado
6.	Violação de norma de utilização ou configuração de dispositivo de tecnologia da informação;	Não detectado
7.	Vazamento de dados pessoais;	Não detectado
8.	Utilização indevida de credenciais de autenticação (senhas) por indivíduo não proprietário delas ou de outrem;	Não detectado
9.	Facilitação de fluxo de comunicação de rede (atividade maliciosa por detecção de padrão ou análise manual) ou envolvendo dispositivos identificados por grupos de segurança como fonte de atividades maliciosas;	Não detectado
10.	Omissão de 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 pelo CRCRN;	Não detectado
11.	Violação de direito autoral ou propriedade intelectual de qualquer natureza;	Não detectado
12.	– realizar tentativa de fraude (bem ou malsucedida) independentemente do dano causado;	Não detectado
13.	Demais eventos que constituam violação de requisito de segurança estabelecido pela ***Política de Segurança da Informação do CRCRN***, tenham eles origem no próprio CRCRN ou em grupos externos.	Não detectado