

SUMÁRIO EXECUTIVO DE GOVERNANÇA DE T.I

REUNIÃO DOS COMITÊS 08/09/2026



COMPANHIA DOCAS DO
RIO GRANDE DO NORTE -
CODERN

MEMBROS DOS COMITÊS



COMITÊ DE SEGURANÇA DA INFORMAÇÃO

DIRETOR PRESIDENTE:

PAULO HENRIQUE DE MACEDO CARLOS

MEMBROS:

JOÃO BATISTA DANTAS BEZERRA JÚNIOR

SÉRGIO KLEBER MATIAS DE LIMA

ALEXANDRE CIRINO ALVES

JORGE MAGNUS ANTUNINO



COMITÊ DE GOVERNANÇA DIGITAL

DIRETOR PRESIDENTE:

PAULO HENRIQUE DE MACEDO CARLOS

MEMBROS:

JOÃO BATISTA DANTAS BEZERRA JÚNIOR

SÉRGIO KLEBER MATIAS DE LIMA

MONALISSAN SAUNDERS B. L. DA SILVA

ALEXANDRE CIRINO ALVES

JORGE MAGNUS ANTUNINO



EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS –ETIR

DIRETOR PRESIDENTE:

PAULO HENRIQUE DE MACEDO CARLOS

MEMBROS:

JOÃO BATISTA DANTAS BEZERRA JÚNIOR

SÉRGIO KLEBER MATIAS DE LIMA

FRANCIWANDER DE SOUZA PEREIRA

ALEXANDRE CIRINO ALVES

JORGE MAGNUS ANTUNINO

COMO ATUAM?



COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Responsável por estabelecer diretrizes, acompanhar a implementação e promover ações voltadas à proteção das informações da Companhia, assegurando a confidencialidade, integridade, disponibilidade e conformidade dos ativos de informação.



COMITÊ DE GOVERNANÇA DIGITAL

Responsável por orientar, deliberar e acompanhar as iniciativas de governança digital, assegurando o alinhamento estratégico das ações e projetos com o Plano de Transformação Digital (PTD) e o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).



EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS –ETIR

Equipe técnica responsável por prevenir, detectar, analisar, responder e apoiar a recuperação de incidentes de segurança cibernética, atuando na mitigação de riscos e na preservação da continuidade e da segurança dos serviços e ativos tecnológicos da Companhia.

NOSSOS OBJETIVOS



COMITÊ DE SEGURANÇA DA INFORMAÇÃO



Proteger as informações e reduzir os riscos de segurança da Companhia.

COMITÊ DE GOVERNANÇA DIGITAL



Alinhar a tecnologia aos objetivos estratégicos e à transformação digital da Companhia.

EQUIPE DE PREVENÇÃO, TRATAMENTO E
RESPOSTA A INCIDENTES CIBERNÉTICOS –ETIR



Prevenir, responder e mitigar incidentes de segurança cibernética, garantindo a continuidade dos serviços.



COMITÊ DE SEGURANÇA DA INFORMAÇÃO

DIRETRIZES DE CONTROLE DE ACESSO E
GOVERNANÇA NA NOVA INTRANET E
INTEGRAÇÕES INSTITUCIONAIS



COMITÊ DE SEGURANÇA DA INFORMAÇÃO



DIAGNÓSTICO E AÇÕES

Estabelecer uma matriz de responsabilidades e protocolos padronizados de segurança para o acesso aos dados corporativos. O foco é garantir a integridade e a confidencialidade das informações durante a expansão dos sistemas internos (Fase 2 da Intranet) e na troca de dados com entidades externas parceiras.

AUTENTICAÇÃO MULTIFATOR (MFA):

DEFINIÇÃO DO ESCOPO E CRONOGRAMA DE OBRIGATORIEDADE DO MFA PARA O ACESSO À NOVA INTRANET E VPN.

DISCUTIR QUAIS MÉTODOS SERÃO HOMOLOGADOS INTERNAMENTE (APLICATIVO AUTENTICADOR, TOKEN, SMS, ETC.)

E A PRIORIZAÇÃO IMEDIATA PARA PERFIS DE ALTA CRITICIDADE, COMO ADMINISTRADORES DE TI, GESTORES E ACESSOS EXTERNOS (**MATRIZ DE PERFIS DE ACESSO**).

RASTREABILIDADE E RESPOSTA A INCIDENTES:

IMPLEMENTAÇÃO E RETENÇÃO DE LOGS DE AUDITORIA.

DISCUTIR COMO A INFRAESTRUTURA ATUAL PODE MONITORAR E ALERTAR SOBRE ACESSOS ATÍPICOS, EXPORTAÇÕES EM MASSA DE DADOS ESTRATÉGICOS OU FALHAS REPETIDAS NAS TENTATIVAS DE MFA



COMITÊ DE GOVERNANÇA DIGITAL

MODERNIZAÇÃO DO SIGAP 2.0,
INTEROPERABILIDADE COM RECEITA FEDERAL E
GOVERNANÇA DE DADOS



COMITÊ DE GOVERNANÇA DIGITAL



DIAGNÓSTICO E AÇÕES

Apresentar o status estratégico da atualização arquitetural do SIGAP 2.0. O foco é validar o sucesso das entregas recentes (faturamento e contratos do dashboard) e alinhar o avanço do cronograma de interoperabilidade com sistemas federais, controle de acesso e a nossa Intranet institucional.

GOVERNANÇA DE DADOS E BI PARA APOIO À DECISÃO: APRESENTAÇÃO DOS RESULTADOS DA FASE DE TESTES DOS NOVOS DASHBOARDS. O MÓDULO DE BUSINESS INTELLIGENCE, NESTE PRIMEIRO MOMENTO, CONSOLIDA OS DADOS PROVENIENTES DO SIGAP. EM SUA SEGUNDA FASE, ESTÁ PREVISTA A INTEGRAÇÃO DOS DADOS ORIUNDOS DO SISTEMA FORTES, AMPLIANDO A CAPACIDADE DE GERAÇÃO DE INDICADORES E SUBSIDIANDO A ANÁLISE E A TOMADA DE DECISÕES ESTRATÉGICAS.

INTEROPERABILIDADE ADUANEIRA (SISCOMEX E API RECINTOS): ALINHAMENTO TÉCNICO SOBRE A NOVA ARQUITETURA QUE PERMITIRÁ AO SIGAP 2.0 O ENVIO DIRETO DE DADOS PARA OS SISTEMAS DA RECEITA FEDERAL. O OBJETIVO É GARANTIR CONFORMIDADE, SEGURANÇA E FLUIDEZ NAS OPERAÇÕES PORTUÁRIAS.

GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS: A CENTRALIZAÇÃO DO CREDENCIAMENTO DE ACESSO DE PESSOAS (FÍSICAS E JURÍDICAS) ÀS INSTALAÇÕES DO PORTO PASSARÁ A SER FEITA DIRETAMENTE PELO SIGAP 2.0.

SINERGIA DE ECOSISTEMA (SIGAP X INTRANET): DISCUSSÃO SOBRE COMO A ARQUITETURA DO SIGAP 2.0 FORNECERÁ UMA BASE DE DADOS CENTRALIZADA E CONFIÁVEL PARA ALIMENTAR OS FLUXOS DE TRABALHO E CONSULTAS DENTRO DA NOVA INTRANET.



EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS –ETIR

**APERFEIÇOAR A ATUAÇÃO DA ETIR, POR MEIO DE
CAPACITAÇÕES E PROVIMENTO DE MECANISMOS
DE SEGURANÇA, COM O OBJETIVO DE PREVENIR,
CORRELACIONAR, GERENCIAR E RESPONDER A
EVENTOS DE SEGURANÇA DA INFORMAÇÃO NA
ORGANIZAÇÃO.**



ETIR



DIAGNÓSTICO E AÇÕES

Aperfeiçoar a atuação da ETIR multidisciplinar por meio de capacitação contínua, padronização de procedimentos e implementação progressiva de mecanismos de segurança. O foco é fortalecer a capacidade institucional de prevenir, detectar, analisar, gerenciar e responder a incidentes cibernéticos, garantindo o atendimento às recomendações da CGU, às metas do PPSI e a transparência das ações por meio de sumários digitais.

INFORMAMOS QUE A CODERN MANTÉM UMA EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) ESTRUTURADA COM O OBJETIVO DE PROMOVER UMA ATUAÇÃO INTEGRADA E MULTIDISCIPLINAR NA ORGANIZAÇÃO. ATUALMENTE, A EQUIPE É COMPOSTA PELA TOTALIDADE DOS COLABORADORES DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO, CONTANDO TAMBÉM COM A PARTICIPAÇÃO ESTRATÉGICA DE INTEGRANTE DA COORDENAÇÃO DE RISCOS E DE REPRESENTANTE DA GUARDA PORTUÁRIA, PROPORCIONANDO UMA ABORDAGEM ABRANGENTE DOS ASPECTOS RELACIONADOS À SEGURANÇA LÓGICA E À INTEGRIDADE FÍSICA DOS ATIVOS PORTUÁRIOS.

RESSALTA-SE, AINDA, QUE, DIANTE DA IDENTIFICAÇÃO DE EVENTUAL INCIDENTE CIBERNÉTICO, DEVERÃO SER OBSERVADOS OS PROCEDIMENTOS DE COMUNICAÇÃO AOS ÓRGÃOS COMPETENTES, INCLUINDO O CISC E O CTIR GOV. ADICIONALMENTE, NO ÂMBITO DA SEGURANÇA PORTUÁRIA, A GUARDA PORTUÁRIA DEVERÁ OBSERVAR OS PROCEDIMENTOS PRÓPRIOS DE COMUNICAÇÃO, MEDIANTE EMISSÃO DE ROIP À CESPORTOS E À CONPORTOS, CONFORME APLICÁVEL.

NESSE CONTEXTO, SEGUE O DESPACHO Nº 159 – RECOMENDAÇÃO 8 – PLANO DE AÇÃO (11724332), QUE DETALHA AS AÇÕES, PRAZOS E MEDIDAS ESTABELECIDAS PELA COMPANHIA PARA O ATENDIMENTO DA RECOMENDAÇÃO.

CISC SIGNIFICA CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO.

CTIR GOV SIGNIFICA CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

ETIR



PLANO DE AÇÃO – APERFEIÇOAMENTO DA ETIR

3. Cronograma e Plano de Ação

Prazo	Ação	Responsável	Resultado Esperado
Contínuo (Bimestral)	Realizar reuniões de alinhamento da equipe e publicar o Sumário Digital no site institucional da CODERN.	ETIR / TI	Acompanhamento periódico das ações e transparência das atividades da equipe.
3º Trim/2026	Consolidar a composição, atribuições e responsabilidades da ETIR.	GEDADOS / ETIR	ETIR formalizada e organizada.
4º Trim/2026	Realizar o curso <i>CIS Controls 1 a 6</i> para a equipe.	ETIR	Capacitação técnica da equipe.

4º Trim/2026	Elaborar procedimentos básicos de prevenção e resposta a incidentes.	ETIR	Padronização da atuação.
Semestral/2027	Realizar Exercício Simulado de incidente cibernético (Tabletop Exercise).	ETIR / Riscos	Avaliação prática da capacidade de resposta.
2027/2028	Viabilizar a contratação de empresa especializada para realização de Teste de Intrusão (Pentest) estruturado na infraestrutura crítica da Companhia, condicionada à disponibilidade de dotação orçamentária, com posterior execução do teste após a formalização da contratação.	TI / Terceirizada	Identificação e correção de vulnerabilidades.

ETIR



PLANO DE AÇÃO – APERFEIÇOAMENTO DA ETIR

2. Ações Já Realizadas

A CODERN já possui a ETIR estruturada e com caráter multidisciplinar, composta por colaboradores de Tecnologia da Informação (TI), com participação de representantes da área de riscos e da Guarda Portuária, garantindo uma visão holística na resposta a incidentes.

Em atendimento às metas do Programa de Privacidade e Segurança da Informação (PPSI) e às recomendações da CGU, a GEDADOS executou as seguintes ações:

- **Capacitação das Lideranças:** Realização do curso *Segurança da Informação para Todos* (ENAP - <https://www.escolavirtual.gov.br/curso/1256>). Os certificados constam como evidência no Processo SEI nº [50902.000476/2026-01](#).
- **Inclusão em Plano de Capacitação:** Previsão da realização do curso *Segurança Cibernética: Controles 1 a 6 do CIS Controls* (ENAP) é 25/09/2026 conforme despacho [11726270](#), sendo este curso presente no Plano de Capacitação 2026/2027 (Planilha GEDADOS nº [11462238](#), Processo SEI nº [50902.001003/2026-12](#)).



OBRIGADO!

O SUCESSO É FRUTO DO
TRABALHO EM EQUIPE.



INFORMATICA@CODERN.COM.BR



84 40055326



WWW.CODERN.COM.BR