

Entidade: AR ODLEVATI, vinculada à AC SINCOR RFB
Processo nº: 00100.00043/2014-71

Nos termos do Parecer CGAF/DAFN/ITI - 33/2014 e consoante Parecer ICP 33/2014 -PFE/ITI/PGF/AGU, DEFIRO o pedido de credenciamento da AR ODLEVATI, vinculada à AC SINCOR RFB, com instalação técnica situada na Rua José Soares de Azevedo, nº 172, sala 01, bairro Vila Santa Luzia, Taboão da Serra-SP, para as Políticas de Certificados já credenciadas.

Entidade: AR CERTIFID, vinculada à AC SOLUTI MÚLTIPLA
Processo nº: 00100.000112/2014-46

Nos termos do Parecer CGAF/DAFN/ITI - 43/2014 e consoante Parecer ICP 72/2014 -PFE/ITI/PGF/AGU, DEFIRO o pedido de credenciamento da AR CERTIFID, vinculada à AC SOLUTI MÚLTIPLA, com instalação técnica situada na Avenida Castelo Branco, nº 4721, Quadra 29, Lote 01/08/09, Setor Rodoviário, Goiânia-GO, para as Políticas de Certificados já credenciadas.

Entidades: AC VALID BRASIL, vinculada à AC VALID e AC VALID RFB, vinculada à AC RFB

Processos nºs: 00100.000297/2012-27 e 00100.000298/2012-71
Acolhe-se os Pareceres CGAF/ITI nº 009/2014 e 010/2014 e Notas nºs 422/2014/DSB/PFE-ITI/PGF/AGU e 437/2014/PRCC/PFE-ITI/PGF/AGU que aprovam a versão 2.1 das DPC, PC A1 e PC A3 da AC VALID BRASIL, vinculada à AC VALID, a versão 2.1 da DPC e PC A1 e versão 2.2 da AC VALID RFB, vinculada à AC RFB. Os arquivos contendo os documentos aprovados possuem os hashes SHA1 informados no Parecer e devem ser publicados pela AC em seu repositório no prazo máximo de 30 dias, a contar da data desta publicação.

RENATO DA SILVEIRA MARTINI

CONTROLADORIA-GERAL DA UNIÃO SECRETARIA EXECUTIVA

PORTARIA Nº 1.213, DE 3 DE JUNHO DE 2014

Institui a Política de Segurança Corporativa na Controladoria-Geral da União.

O SECRETÁRIO EXECUTIVO DA CONTROLADORIA-GERAL DA UNIÃO, no uso da competência que lhe foi atribuída pelo art. 24 do Anexo ao Decreto nº 8.109, de 17 de setembro de 2013, e tendo em vista o disposto no Decreto nº 3.505, de 15 de junho de 2000, no Decreto nº 7.845, de 14 de novembro de 2012, na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e na Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, resolve:

PRESIDÊNCIA DA REPÚBLICA CASA CIVIL IMPRESA NACIONAL

DILMA VANA ROUSSEFF
Presidenta da República

ALOIZIO MERCADANTE OLIVA
Ministro de Estado Chefe da Casa Civil

FERNANDO TOLENTINO DE SOUSA VIEIRA
Diretor-Geral da Imprensa Nacional

DIÁRIO OFICIAL DA UNIÃO

SEÇÃO 1
Publicação de atos normativos

SEÇÃO 2
Publicação de atos relativos a pessoal da Administração Pública Federal

SEÇÃO 3
Publicação de contratos, editais, avisos e ineditais

JORGE LUIZ ALENCAR GUERRA
Coordenador-Geral de Publicação e Comunicação

ALEXANDRE MIRANDA MACHADO
Coordenador de Editoração e Divulgação Eletrônica dos Jornais Oficiais

FRANCISCO DAS CHAGAS PINTO
Coordenador de Produção

A Imprensa Nacional não possui representantes autorizados para a comercialização de assinaturas impressas e eletrônicas

http://www.in.gov.br ouvidoria@in.gov.br
SIG, Quadra 6, Lote 800, CEP 70610-460, Brasília - DF
CNPJ: 04196645/0001-00
Fone: 0800 725 6787

Art. 1º Instituir a Política de Segurança Corporativa e apresentar as diretrizes de segurança adotadas pela Controladoria-Geral da União - CGU.

Art. 2º Norteiam esta Política de Segurança Corporativa os princípios da disponibilidade, da integridade, da autenticidade, além dos princípios que regem a Administração Pública.

CAPÍTULO I CONSIDERAÇÕES INICIAIS

Seção I Da Abrangência

Art. 3º As diretrizes da Política de Segurança Corporativa da CGU, constantes nesta Portaria e em sua regulamentação, devem ser observadas por todos os agentes públicos, colaboradores e, no que couber, pelos visitantes que tenham acesso às instalações da CGU, em todas as suas unidades, e aplicadas a todos os sistemas de informação e processos corporativos do órgão, para a garantia da disponibilidade, da integridade e da autenticidade das informações.

Seção II Dos Conceitos e Definições

Art. 4º Para os efeitos desta Portaria são estabelecidos os seguintes conceitos e definições:

I - Agente Público: todo aquele que exerce, ainda que transitoriamente, com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na CGU;

II - Ativos de Informação: é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos do órgão, seus meios de armazenamento, transmissão e processamento, os equipamentos necessários e os sistemas utilizados para tal, os locais onde se encontram esses meios, e também aqueles que a eles têm acesso;

III - Ativos físicos: quaisquer equipamentos ou instalações;

IV - Autenticidade: qualidade da informação que foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

V - Código fonte: é a sequência de instruções que formam um software;

VI - Colaboradores: fornecedores, estagiários e terceirizados alocados no órgão;

VII - Dado: constitui a matéria-prima da informação;

VIII - Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

IX - Dispositivos móveis: equipamentos portáteis dotados de capacidade computacional;

X - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, que comprometa a segurança da informação;

XI - Informação: dados com significado, relevância e propósito;

XII - Integridade: qualidade da informação que não foi modificada ou destruída de maneira não autorizada ou acidental;

XIII - Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

XIV - Gestão de Risco: conjunto de processos que permitem 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;

XV - Métodos criptográficos: técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário;

XVI - Perímetro de segurança física: barreiras físicas para impedir o acesso não autorizado;

XVII - Recursos Computacionais: qualquer equipamento capaz de armazenar, transmitir, capturar, processar ou imprimir dados, bem como todos os sistemas ou serviços disponibilizados pela rede de dados da CGU;

XVIII - Software Proprietário: é aquele cuja cópia, redistribuição ou modificação é, em alguma medida, proibida pelo seu criador ou distribuidor;

XIX - Tratamento da Informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo; e

XX - Usuário: qualquer agente público ou colaborador que possua autorização para a utilização de recursos computacionais da CGU.

CAPÍTULO II GESTÃO DA POLÍTICA DE SEGURANÇA CORPORATIVA

Seção I Do Sistema de Gestão

Art. 5º O Sistema de Gestão de Segurança Corporativa da CGU é composto por:

I - Comitê Permanente de Segurança Corporativa - COPESEG, órgão instituído por portaria da Secretaria Executiva da CGU, com caráter permanente, para o qual devem convergir as informações relativas à implementação e ao cumprimento da Política de Segurança Corporativa;

II - Núcleo Técnico de Segurança Corporativa - NUTASEG, constituído por servidores designados pelo COPESEG;

III - Dirigente da Unidade Administrativa: dirigentes das unidades organizacionais da CGU, conforme definidos no Regimento Interno da CGU; e

IV - Outros gestores que possam vir a ser nomeados em situações específicas.

Art. 6º Compete ao COPESEG:

I - formular propostas de criação e de adequação da política e das normas atinentes à Segurança Corporativa da CGU;

II - propor medidas para acompanhar e avaliar a implementação da Política de Segurança Corporativa junto às unidades da CGU;

III - propor a adoção de ações de conscientização e capacitação de pessoal visando difundir os conhecimentos e dar efetividade à Política de Segurança Corporativa;

IV - receber das unidades da CGU informações sobre dificuldades relativas à implementação e ao cumprimento da Política de Segurança Corporativa;

V - propor a adoção de medidas corretivas e as adequações normativas e procedimentais necessárias para prevenir situações de vulnerabilidade à Segurança Corporativa; e

VI - compartilhar informações sobre novas tecnologias, produtos, ameaças, vulnerabilidades, gerenciamento de risco, políticas de segurança e outras atividades relativas à Segurança Corporativa com outros órgãos e empresas, públicas ou privadas, de modo a prover a CGU do conhecimento das práticas mais modernas e adequadas para proteção de suas informações.

Art. 7º Compete ao NUTASEG auxiliar o COPESEG na execução de suas competências, e notadamente:

I - produzir estudos técnicos;

II - avaliar e verificar o cumprimento da Política de Segurança Corporativa, das normas e dos procedimentos de segurança corporativa, por meio de pesquisas, auditorias ou outros métodos que julgar adequados;

III - negociar com os responsáveis pelas diversas áreas organizacionais os requisitos de segurança a serem atendidos e os controles a serem implementados; e

IV - avaliar a eficácia dos procedimentos de segurança e sua conformidade com os requisitos legais, com as normas e diretrizes internas e com os requisitos técnicos de segurança corporativa.

Art. 8º Compete ao Dirigente da Unidade Administrativa garantir o cumprimento da Política de Segurança Corporativa em sua unidade organizacional.

CAPÍTULO III DIRETRIZES

Seção I Da Classificação da Informação

Art. 9º O COPESEG deverá orientar as unidades sobre os critérios para classificação da informação e os procedimentos adequados à sua proteção visando assegurar que os ativos da informação recebam um nível adequado de proteção.



Art. 10. Toda informação deve ser protegida de acordo com seu valor, sensibilidade e criticidade.

Art. 11. Na classificação da informação deverá ser utilizado o critério menos restritivo possível.

Seção II Do Tratamento da Informação

Art. 12. O COPESEG deverá propor diretrizes de segurança da informação e comunicações para a instituição do processo de tratamento da informação em todo o seu ciclo de vida, conforme inciso V do art. 4º da Lei 12.527, de 2011.

Seção III Do Controle dos Ativos de Informação

Art. 13. O COPESEG poderá estabelecer procedimentos para a realização dos inventários dos ativos informacionais, formas de classificação da informação e responsabilidades pela manutenção dos controles necessários para protegê-la.

Art. 14. Todo ativo de informação deve ser avaliado para indicar a necessidade, a prioridade, o nível esperado de proteção e, ainda, possuir um proprietário responsável.

Seção IV Do Tratamento de Incidentes de Segurança

Art. 15. Poderão ser estabelecidos pelo COPESEG procedimentos formais para prevenção, investigação, detecção, notificação e tratamento de incidentes de segurança.

§ 1º Os incidentes de segurança devem ser registrados e analisados periodicamente, servindo de subsídio para melhorias nos procedimentos de segurança e para verificar falhas dos controles de segurança vigentes.

§ 2º O COPESEG deve ser informado por meio de relatórios gerenciais sobre incidentes de segurança.

Art. 16. O COPESEG poderá adotar medidas para conscientização dos agentes públicos e colaboradores sobre os procedimentos definidos no artigo anterior, afetos à sua atuação.

Seção V Da Gestão de Risco

Art. 17. Poderão ser estabelecidos pelo COPESEG diretrizes e procedimentos para o processo de Gestão de Riscos de Segurança da Informação e Comunicações, incluindo-se a implementação de um Plano de Tratamento de Riscos, considerados os objetivos estratégicos, os processos, os requisitos legais e a estrutura da CGU.

Seção VI Da Gestão de Continuidade

Art. 18. Serão estabelecidos pelos Dirigentes das Unidades Administrativas, sob orientação do COPESEG, procedimentos e normas de modo a minimizar, em nível aceitável, os impactos sobre o órgão na ocorrência de falhas ou desastres significativos por meio da combinação de ações de prevenção e recuperação.

Art. 19. Os procedimentos e as normas para continuidade dos serviços devem prever testes e atualizações regulares, de forma a assegurar sua permanente atualização e efetividade.

Seção VII Da Auditoria e Conformidade

Art. 20. Serão estabelecidos pelos Dirigentes das Unidades Administrativas, sob orientação do COPESEG, procedimentos e normas para a implantação do processo de Avaliação de Conformidade em Segurança, a se realizar periodicamente.

Art. 21. O processo de Avaliação de Conformidade em Segurança compreende o exame sistemático do grau de atendimento dos requisitos relativos à Segurança Corporativa com as legislações específicas.

Seção VIII Da Gestão de Pessoal

Art. 22. Serão tomadas medidas para conscientizar os servidores públicos e colaboradores sobre os procedimentos de segurança instituídos pela CGU, afetos à sua atuação, as ameaças e preocupações relativas à segurança corporativa e as suas responsabilidades e obrigações visando reduzir riscos de erro humano, furto, fraude e uso não apropriado da informação.

Art. 23. O Comitê Permanente de Segurança Corporativa proporá a inclusão no Plano Anual de Capacitação de atividades de divulgação e disseminação das orientações previstas nesta Política de Segurança Corporativa, bem como treinamento e capacitação dos servidores públicos e demais colaboradores.

Art. 24. O ingresso e o desligamento dos servidores públicos e colaboradores, bem como o encerramento de contratos, devem ser realizados de modo controlado, garantindo:

- I - a devolução de todos os ativos físicos;
- II - o cancelamento de autorizações de acesso às informações classificadas; e
- III - a entrega de compromisso assinado de não divulgação de informações sigilosas.

Seção IX Da Segurança Física e do Ambiente

Art. 25. Será assegurada a salvaguarda dos locais e dos ativos físicos onde são elaborados, tratados, custodiados, manuseados ou guardados dados e informações críticas ou sensíveis, independentemente do meio onde estão armazenados, abrangendo:

- I - perímetro de segurança física;
- II - segurança de salas e instalações;
- III - proteção contra ameaças externas e ao meio ambiente;
- IV - trabalho em áreas seguras;
- V - acesso do público, áreas de entrega e carregamento;
- VI - instalação, manutenção e proteção de ativos físicos; e
- VII - reutilização e alienação de ativos físicos.

Seção X Da Segurança Lógica

Art. 26. Cabe ao COPESEG zelar pela segurança dos recursos computacionais, assegurando a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e dos serviços, abrangendo:

- I - cópias de segurança;
- II - monitoramento da estrutura de TI;
- III - gestão de softwares homologados; e
- IV - gestão de mudanças.

Art. 27. Todo acesso e toda informação veiculada eletronicamente são passíveis de monitoramento de acordo com normativo específico.

Seção XI Do Controle de Acesso

Art. 28. Cabe ao COPESEG estabelecer procedimentos de controles de acesso físico e lógico, respectivamente, às instalações e aos sistemas e recursos de informática, assegurando a concessão e atualização dos perfis de acesso conforme as atividades executadas.

Art. 29. O COPESEG deverá zelar pela publicação de procedimentos para concessão de uso de serviços ou recursos disponíveis e os respectivos responsáveis por essa concessão.

Seção XII Da Segurança das Comunicações

Art. 30. Cabe ao COPESEG estabelecer procedimentos e normas para utilização dos meios de comunicação, inclusive uso de dispositivos móveis, correio eletrônico e acesso à internet, bem como as responsabilidades dos usuários no tocante às informações em trânsito.

Seção XVII Das Responsabilidades

Art. 31. É responsabilidade dos agentes públicos, colaboradores e visitantes zelar pela estrita observância do disposto nesta Portaria, e comunicar formalmente ao COPESEG qualquer irregularidade ou ameaça à segurança da informação na CGU.

Art. 32. A violação da Política de Segurança Corporativa ou a quebra de segurança por agentes públicos, colaboradores e visitantes será comunicada pelo COPESEG às autoridades competentes para a apuração.

CAPÍTULO IV DISPOSIÇÕES GERAIS

Art. 33. A CGU deverá zelar para que sejam implementados pelos membros do SISEG procedimentos apropriados visando a garantia da conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários.

Art. 34. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela CGU devem observar o contido nesta Política e nos seus dispositivos complementares.

Art. 35. A Política de Segurança Corporativa da CGU e as normas geradas a partir dela serão revisadas, no mínimo a cada 3 (três) anos, ou sempre que houver alteração dos procedimentos vigentes.

Art. 36. Os casos omissos e as dúvidas surgidas na aplicação desta Política serão dirimidos pelo COPESEG.

Art. 37. Revoga-se a Portaria nº 913, de 2 de maio de 2010.

Art. 38. Esta Portaria entra em vigor na data de sua publicação.

CARLOS HIGINO RIBEIRO DE ALENCAR

SECRETARIA DE PORTOS AGÊNCIA NACIONAL DE TRANSPORTES AQUAVIÁRIOS

RESOLUÇÃO Nº 3.412, DE 29 DE MAIO DE 2014

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE TRANSPORTES AQUAVIÁRIOS - ANTAQ, no uso da competência que lhe é conferida pelo art. 54, inciso IV, do Regimento Interno, considerando o que consta do processo nº 50300.002251/2013-45 e tendo em vista o que foi deliberado na 363ª Reunião Ordinária da Diretoria, realizada em 26 de maio de 2014, resolve:

Art. 1º Reconhecer a possibilidade de celebração de Contrato de Adesão entre a Secretaria de Portos da Presidência da República - SEP/PR, na condição de Poder Concedente, e a empresa Companhia Norte de Navegação e Portos S/A - CIANPORT, CNPJ nº 14.789.807/0001-60, visando à construção e exploração de instalação portuária, na modalidade de Terminal de Uso Privado - TUP, no município de Santana - AP, eis que atendidas as exigências do Instrumento Convocatório nº 40/2013, nos termos do art. 8º e seguintes da Lei nº 12.815, de 2013, e art. 26 e seguintes do Decreto nº 8.033/2013.

Art. 2º Esta Resolução entra em vigor na data de sua publicação no Diário Oficial da União.

MÁRIO POVIA

RESOLUÇÃO Nº 3.414, DE 29 DE MAIO DE 2014

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE TRANSPORTES AQUAVIÁRIOS - ANTAQ, no uso da competência que lhe é conferida pelo art. 54, inciso IV, do Regimento Interno, considerando o que consta do processo nº 50300.000428/2014-51 e tendo em vista o que foi deliberado na 363ª Reunião Ordinária da Diretoria, realizada em 26 de maio de 2014, resolve:

Art. 1º Revogar a Resolução nº 3068-ANTAQ, de 19 de setembro de 2013, publicada no DOU de 20 de setembro de 2013.

Art. 2º Declarar extinto o Contrato de Arrendamento PRES 002.91, de 25 de janeiro de 1991, celebrado entre a Companhia Docas do Estado de São Paulo - CODESP e a empresa Fisher S.A. Agroindústria.

Art. 3º Autorizar a Companhia Docas do Estado de São Paulo - CODESP a celebrar Contrato de Transição, em caráter excepcional, pelo prazo máximo de 180 (cento e oitenta) dias, com cláusula resolutiva, junto à empresa Fisher S.A. Agroindústria, inscrita no CNPJ/MF sob nº 52.311.529/0002-00, nos termos do § 1º do art. 35 da Norma aprovada pela Resolução nº 2.240-ANTAQ, com a redação dada pela Resolução nº 2.826-ANTAQ c/c o Despacho Ministerial GM/SEP/PR-2014, de 30 de abril de 2014, visando a continuidade da exploração da área de 14.440m² (quatorze mil, quatrocentos e quarenta metros quadrados), localizada no porto organizado de Santos, até que se conclua o procedimento licitatório.

Art. 4º Estabelecer que, uma vez expirado o prazo contratual sem que o procedimento licitatório da área em questão tenha sido concluído pela autoridade competente, desde que mantidas as mesmas condições de exploração e operacionalidade, a Autoridade Portuária ficará autorizada a celebrar novo instrumento contratual, nos mesmos moldes, devendo encaminhá-lo por cópia à ANTAQ em até 30 (trinta) dias após a sua assinatura.

Art. 5º Determinar à Superintendência de Portos - SPO, que se certifique de que a área em comento efetivamente esteja contemplada no Bloco 1 do Programa de Licitação de Arrendamentos Portuários, até a correspondente adjudicação.

Art. 6º Determinar a instauração de Processo Administrativo Contencioso - PAC, caso ainda não o tenha ocorrido, com a finalidade de apurar eventual conduta omissiva por parte da Autoridade Portuária, relativamente à deflagração do devido procedimento licitatório pertinente à área objeto do Contrato PRES 002.91, cujo prazo de vigência se expirou em 24 de setembro de 2012.

Art. 7º Esta Resolução entra em vigor na data de sua publicação no Diário Oficial da União.

MÁRIO POVIA