Este procedimento pertence a **OceanPact** / Geociências

Política de Segurança da Informação

CORP-POL-0003	**Política**	Rev.05 01/09/2020

Nº da revisão	Item	Descrição	Data
03		Mudança de layout e revisão ortográfica geral	28/10/2018
04		Adequação de PSI para toda empresa.	03/06/2020
05		Alteração do nome do arquivo	01/09/2020

Este procedimento pertence a **OceanPact** / Geociências

Política de Segurança da Informação

CORP-POL-0003	**Política**	Rev.05 01/09/2020

1. PROPÓSITOS E PRINCÍPIOS DA PSI

Implementar as melhores práticas de segurança da informação, tendo por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades e promover uma cultura educativa organizacional de proteção aos dados e à informação da **OCEANPACT**, de clientes, fornecedores e de parceiros.

Estabelecer as diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações a fim de preservar as informações quanto aos seguintes princípios:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, exata e completa;
- **Confidencialidade:** garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A **OCEANPACT** considera em suas políticas de segurança da informação o processo contínuo no qual os riscos são identificados, analisados, avaliados, tratados e reduzidos a um nível aceitável.

2. REFERÊNCIAS

- NBR ISO IEC 27001: 2013
- NBR ISO IEC 27002: 2013
- CIS CONTROLS V7.1

3. PROCEDIMENTOS E PLANOS PARA IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Procedimento de Backup para os dados digitais

4. RESPONSABILIDADES

Visa definir e atribuir todas as responsabilidades pela segurança da informação.

Colaborador

- É da responsabilidade de cada colaborador o prejuízo ou dano que vier a sofrer ou causar à OCEANPACT ou a terceiros em decorrência da não obediência às diretrizes desta política.
- Notificar via e-mail comite.si@oceanpact.com os incidentes, fragilidades ou ainda suspeitas de fragilidades de segurança da informação observadas na **OCEANPACT**.

Política de Segurança da Informação

Gestor

- Incentivar e monitorar o cumprimento da política de segurança da informação pelos colaboradores sob sua gestão.
- Garantir a adaptação dos processos, procedimentos e sistemas sob sua responsabilidade para atender à política de segurança da informação.
- Definir os níveis de acesso dos colaboradores sob sua gestão.
- Solicitar os acessos e os recursos para os colaboradores sob sua gestão.
- Realizar análise crítica periódica das permissões de acesso aos ativos de segurança da informação.
- Definir os níveis de segurança para as informações pertinentes ao seu processo e promover a rotulagem conforme política de classificação e tratamento da Informação.
- Identificar os riscos associados aos ativos da informação pertinentes ao seu processo e realizar a análise crítica periódica dos riscos associados aos ativos da informação.

Comitê de Segurança da Informação

- O Comitê de Segurança da Informação é multidisciplinar, composto por representantes dos Departamentos Jurídico, Recursos Humanos, Tecnologia da Informação, Qualidade e Compliance.
- O Comitê constitui um grupo de trabalho para tratar de questões, propor soluções, metodologias e processos específicos de segurança da informação. Nesse contexto, é responsável por analisar criticamente a política de segurança da informação.
- É responsável pela análise das infrações cometidas pelos colaboradores frente a essa política, com consequência de incidente grave, devendo examinar a gravidade e riscos sob o enfoque técnico e legal de cada infração cometida, resultando na recomendação de processo disciplinar para apuração dos fatos e aplicação das ações disciplinares cabíveis, para eventual encaminhamento às autoridades policiais ou judiciais, quando necessário.
- Todos os membros devem participar de um programa de conscientização de segurança, elaborado pela OCEANPACT a fim de que possam compreender e exibir os comportamentos e habilidades necessários para ajudar a garantir a segurança da organização.
- Este Comitê poderá ser acionado a qualquer momento pelos colaboradores para esclarecer dúvidas, obter orientações, expressar opiniões, reportar situações de violação a esta política ou outros eventos de segurança da informação, por meio da conta corporativa de e-mail comite.si@oceanpact.com.

Recursos Humanos

- Atribuir aos colaboradores, na fase de formalização dos contratos individuais de trabalho a responsabilidade pelo cumprimento da política de segurança da informação.

- Após o processo de contratação do colaborador, independentemente do regime de contrato, realizar conscientização sobre segurança da informação e solicitar a assinatura do Acordo de Responsabilidade e de Confidencialidade da Informação.
- Comunicar e divulgar esta política aos colaboradores, devendo recomendar as medidas que entender cabíveis, incluindo treinamentos periódicos e eventos de conscientização.
- Aplicar sanções previstas nesta política quando for o caso.
- Assegurar que os funcionários e partes externas estejam conscientes e cumpram as suas responsabilidades pela segurança da informação.
- Proteger os interesses da organização como parte do processo de mudança, informando imediatamente à área de Tecnologia da Informação o encerramento da contratação.

Tecnologia da Informação

- Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e reduzir o número de colaboradores que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Monitorar e auditar o ambiente tecnológico, implantação de sistemas de monitoramento de servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança da informação estabelecidos nesta política.

5. POLÍTICA DE CONTROLE DE ACESSO

Visa limitar o acesso à informação e aos recursos de processamento da informação.

A **OCEANPACT** deve manter um inventário de cada um dos sistemas de autenticação da organização.

- Os dispositivos de identificação e senhas devem proteger a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante a OCEANPACT ou terceiros.
- São de responsabilidade do colaborador quaisquer acessos realizados com o identificador/login, pois o mesmo é único, pessoal e intransferível.
- Todos os dispositivos de identificação utilizados na OCEANPACT, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm que estar associados a uma pessoa física e atrelados aos seus documentos oficiais reconhecidos pela legislação brasileira.
- O colaborador, vinculado a tais dispositivos identificadores, é responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

- Devem ser identificados os visitantes e prestadores de serviço terceirizados, distintamente dos funcionários.
- Deverá constar em todos os contratos da OCEANPACT com colaboradores e terceiros, o Acordo de Responsabilidade e Confidencialidade da Informação, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela OCEANPACT.
- O acesso à informação e às funções dos sistemas de aplicação devem ser restringidos por meio de controle dos direitos de acesso dos colaboradores, de forma a limitar quais dados ou funções dos sistemas de aplicação poderão ser acessados por determinado colaborador e qual o nível de permissão.
- Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.
- Deve ser considerada a autenticação de múltiplos fatores e canais criptografados, principalmente para contas com privilégios administrativos. Quando esse tipo de autenticação não for suportada (como por exemplo administrador local ou contas de serviço), as contas deverão ter senhas exclusivas. Entende-se como múltiplos fatores, combinações entre:
  - ✓ O que você sabe. Ex: Senha
  - ✓ O que você tem. Ex: Token
  - ✓ O que você é. Ex: Biometria

6. POLÍTICA DE SENHA

Visa orientar os usuários a seguir boas práticas quanto ao uso e criação de senhas.

- Ao realizar o primeiro acesso ao ambiente de rede local, o colaborador deverá trocar imediatamente a sua senha conforme as orientações da equipe de suporte, seguindo o número mínimo de caracteres e a complexidade exigida pelo sistema.
- A senha de acesso à rede local expirará automaticamente em 6 meses, sendo o colaborador notificado pelo sistema a partir de 5 dias antes do prazo máximo para sua alteração.
- Quando da renovação da senha, não serão aceitas as últimas 6 senhas já registradas.
- Em caso de digitação errônea por 3 vezes consecutivas da senha de acesso, a conta será bloqueada.
- A alteração da senha de acesso à rede também poderá ser feita a qualquer tempo pelo próprio colaborador.
- As senhas não devem ser expostas, compartilhadas ou reveladas a outras pessoas.
- O colaborador não deve transcrever a senha em papel ou outros meios.

- Em caso de descoberta da senha por terceiros, esquecimento da senha ou bloqueio de conta, a equipe de suporte deverá ser acionada por meio de abertura de chamado no Service Desk para troca de senha ou desbloqueio da conta.

7. POLÍTICA DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Visa assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

- A definição do grau de sensibilidade para a informação deve possibilitar:
  - ✓ A determinação das salvaguardas mínimas para proteger tais informações;
  - ✓ A garantia da continuidade operacional de processamento das informações.
- A classificação da informação é de responsabilidade do gestor do processo no qual a informação teve origem.
- Classificação da informação quanto ao sigilo:

Classificação	PÚBLICA	CONFIDENCIAL
Impacto quanto à perda de Confidencialidade	Inexistente	Alta
Definição	Toda informação que tenha sido recebida através de domínio público. O conhecimento desta informação pelo público não expõe a OceanPact a prejuízo financeiro ou constrangimento, tampouco compromete a segurança dos ativos.	Toda informação, incluindo comunicações orais ou escritas transmitidas ou divulgadas pela **OCEANPACT**, seus clientes ou fornecedores

8. POLÍTICA PARA SEGURANÇA FÍSICA E DO AMBIENTE

Visa prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

Controles de acesso ao Datacenter

- A OCEANPACT controla todos os acessos ao seu Datacenter, possuindo câmeras de segurança, monitoradas por Sistema de Monitoramento por CFTV - Circuito Fechado de Televisão.

- O controle de acesso é restrito a pessoas autorizadas, por sistemas baseados em cartão de acesso/biometria. Uma trilha de auditoria eletrônica é mantida e monitorada quanto aos acessos físicos.
- Todos os direitos de acesso são revistos e atualizados periodicamente.

9. POLÍTICA PARA USO DOS ATIVOS

Visa identificar os ativos da organização e definir as responsabilidades apropriadas para sua proteção.

- A **OCEANPACT** utiliza uma ferramenta de descoberta ativa para identificar dispositivos conectados à rede da organização e atualizar o inventário de ativos de hardware.
- A **OCEANPACT** disponibiliza para seus colaboradores equipamentos exclusivamente para o desempenho de suas atividades profissionais; portanto o uso inadequado desses equipamentos para fins não delineados pela **OCEANPACT** é proibido.
- O colaborador deve zelar pelo bom uso dos recursos de informática a ele disponibilizados, não removendo, alterando ou acrescentando qualquer tipo de componente interno de *hardware* ou *software*.
- Todos os dispositivos de armazenamento de dados portáteis (DVD`s, CD`s, pendrives), especialmente os de origem externa, devem ser submetidos a uma rotina de verificação quanto à existência de vírus antes de serem utilizados no ambiente da **OCEANPACT**.
- É vedado o armazenamento, na rede da **OCEANPACT** ou em quaisquer equipamentos de propriedade da **OCEANPACT**, de material obsceno, ilegal ou não ético, fato que ensejará a apuração de responsabilidade.
- Arquivos particulares ou não pertinentes ao negócio da **OCEANPACT** não devem ser copiados/movidos para a rede da **OCEANPACT**, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem aviso prévio.
- Informações relacionadas a concorrentes, propostas comerciais, protótipos e projetos da concorrência não devem ser armazenadas na rede da **OCEANPACT** ou em quaisquer equipamentos de propriedade da **OCEANPACT**.
- Documentos necessários para as atividades da **OCEANPACT** devem ser salvos na rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador.
- O colaborador não deve executar nenhum tipo de comando ou programa que venha a sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e autorização da Diretoria.

- O colaborador não deve consumir alimentos e bebidas próximo aos recursos tecnológicos e aos documentos físicos corporativos, podendo ser responsabilizado por danos causados em decorrência deste ato.
- O colaborador deve manter a configuração do equipamento disponibilizado pela equipe de suporte, o qual possui os controles de segurança definidos pela **OCEANPACT**.
- A conexão de quaisquer equipamentos que não sejam de propriedade da **OCEANPACT** deve ser realizada em rede específica.
- É vedada a conexão de quaisquer equipamentos que não sejam de propriedade da **OCEANPACT** ou homologados pela **OCEANPACT** em sua rede corporativa, especialmente os *notebooks* e *smartphones* particulares, já que comprometem a segurança da informação e também a qualidade dos serviços.
- Na utilização de equipamentos de propriedade da **OCEANPACT**, o colaborador deverá tomar os seguintes cuidados:
    - ✓ Desligar o equipamento ao final do expediente;
    - ✓ Sempre que tiver dúvidas ou problemas relacionados aos equipamentos, o colaborador deverá se comunicar com a equipe de suporte por meio de abertura de chamado no Service Desk;
    - ✓ O uso das impressoras deve ser feito, exclusivamente, para impressão de documentos ou de outras informações que sejam de interesse da **OCEANPACT**;
    - ✓ O colaborador deve retirar imediatamente da impressora os documentos para ela enviados caso contenham informações sensíveis.
- A **OCEANPACT** tem propriedade legal sobre todos os arquivos produzidos em seus computadores, reservando-se o direito de manter, a seu critério, histórico de acessos e transações realizadas com uso da Internet ou Intranet, quando considerado necessário por motivos de segurança ou para fins de auditoria.
- A forma da informação impõe restrições às medidas necessárias para sua proteção, porém não importa a forma que a informação toma ou os meios pelos quais é compartilhada: ela deve sempre ser apropriadamente protegida. A informação eletrônica, física ou verbal, deve ser tratada conforme a política de classificação e tratamento da informação.

10. POLÍTICA PARA MESA E TELA LIMPAS

Visa dotar uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

- As mesas de trabalho devem estar limpas de papéis e mídias de armazenamento removíveis que contenham informações sensíveis.
- Os papéis e mídias contendo informações sensíveis devem ser guardados em mobília segura, imediatamente após o uso.

- As áreas de trabalho dos computadores devem estar limpas de arquivos que contenham informações sensíveis. Estes arquivos devem estar armazenados apropriadamente na rede.
- Sempre que não for utilizar o computador ou tiver que se ausentar da sala, o colaborador deverá efetuar procedimento de desconexão: logoff ou o bloqueio do computador.
- O sistema operacional deve fazer o bloqueio automático de tela a partir de 10 minutos de inatividade.

11. POLÍTICA PARA TRANSFERÊNCIA DE INFORMAÇÕES

Visa manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

- Os requisitos para confidencialidade da informação estão descritos no Acordo de Responsabilidade e Confidencialidade da Informação.
- Os colaboradores devem ser extremamente cautelosos na utilização de quaisquer meios de comunicação, ficando proibida qualquer troca de informações com o meio exterior sobre informações com mais alto grau de sensibilidade sem autorização, justificativa e criptografia.
- Entende-se por disseminação de informações com mais alto grau de sensibilidade específicas da **OCEANPACT** toda e qualquer troca de mensagens com o meio exterior, que contenha qualquer referência a:
  - ✓ Documentos sobre clientes, faturamento e dados financeiros da **OCEANPACT**;
  - ✓ Documentação dos sistemas (código fonte, diagramas, documentação de tabelas, etc.);
  - ✓ Diagramas, propostas, *checklists* operacionais, projetos, *papers* técnicos ou da empresa;
  - ✓ Decisões sobre aquisições, fusões e incorporações;
  - ✓ Patentes, pesquisas, desenvolvimento de *software* e de soluções.

E-mail

- O correio eletrônico corporativo fornecido pela **OCEANPACT** deve ser utilizado em função das atividades da **OCEANPACT**.
- É expressamente proibido:
  - ✓ O envio de material obsceno, ilegal ou não ético, propagandas, mensagem do tipo "corrente", de entretenimento, discriminatórias, preconceituosas ou ofensivas no que se refere a nacionalidade, raça, orientação sexual, religião ou opinião política;
  - ✓ O envio simultâneo de mensagens para todos os usuários da rede da **OCEANPACT**, salvo para comunicações administrativas e previamente autorizadas que devam ser dirigidas a todos os funcionários;

- ✓ A inserção ou disseminação de arquivos que contenham vírus ou qualquer espécie de programas nocivos;
- ✓ O envio de grande quantidade de mensagens de *e-mail* que prejudique a capacidade técnica da rede;
- ✓ Divulgar conteúdo que viole quaisquer direitos autorais, patentes, marcas registradas, marcas de serviço, nomes comerciais, segredos comerciais ou outros direitos de propriedade intelectual da **OCEANPACT** ou de terceiros;
- ✓ Participar de listas de discussão que possam abordar assuntos alheios às áreas fins da empresa e de suas gerências;
- ✓ Anunciar quaisquer produtos ou serviços, bem como promover qualquer marca, setor, empresa ou outras formas de autopromoção;
- ✓ Forjar quaisquer das informações do cabeçalho do remetente;
- ✓ Expor contas de *e-mail* em provedores de acesso à internet para coletar respostas e mensagens enviadas, quando tais mensagens violem esta política.

- As mensagens de correio eletrônico sempre devem incluir assinatura com as seguintes informações:
  - ✓ Nome Completo
  - ✓ Área/Setor
  - ✓ Cargo
  - ✓ Telefone
  - ✓ Logo da empresa
- Todas as mensagens trafegadas no domínio da **OCEANPACT** permitem rastreabilidade.

12. POLÍTICA PARA USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Visa garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

- É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela **OCEANPACT**, notificar imediatamente a equipe de suporte e procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência.
- O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo ele o responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à **OCEANPACT** ou a terceiros.
- O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da **OCEANPACT** deverá submeter previamente tais equipamentos ao processo de homologação da equipe de suporte.

- O trabalho remoto à rede da **OCEANPACT** somente é permitido por meio do acesso via VPN – Virtual Private Network.
- A concessão do acesso remoto via VPN será de exclusivo critério da **OCEANPACT** e mediante solicitação por meio de abertura de chamado no Service Desk, que optará para qual rede o colaborador terá permissão de acesso. A referida concessão será feita de forma individual, sendo os colaboradores responsáveis por seus acessos via VPN bem como por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os colaboradores deverão adotar medidas de cautela, para que terceiros não tenham acesso, sem autorização, à sua conexão de VPN.
- As sessões de videoconferência devem ser feitas por meio de software homologado pela equipe de TI e sempre com controle de acesso às salas virtuais.
- Durante as sessões de videoconferência deve-se optar por locais reservados atentando sempre para o vazamento de informações, tanto pela exposição a câmera quanto à propagação do áudio.
- Proteja o acesso a salas de videoconferência com senha. Não envie o convite a terceiros, exceto se devidamente autorizado pelo gestor;
- Atente para as informações expostas pela câmera e não grave, tire prints ou "selfies" que exponham a sessão em andamento;
- Não divulgue informações de "reuniões virtuais", exceto se devidamente autorizado pelo gestor.

13. POLÍTICA PARA USO E INSTALAÇÃO DE SOFTWARE

Visa definir e implementar critérios para a instalação de software pelos usuários.

- A OCEANPACT estabelece padrões de configuração de segurança para todos os sistemas operacionais e softwares autorizados.
- O uso de software pirata pode acarretar os seguintes prejuízos à **OCEANPACT**:
  - ✓ Infringência à lei nº. 7.646, de 18 de dezembro de 1987 que proíbe a reprodução, comercialização, importação e utilização de cópias de programas de computador feitas sem a devida autorização do titular dos direitos autorais;
  - ✓ Exposição negativa da imagem da **OCEANPACT** perante a sociedade pelo descumprimento à lei;
  - ✓ Incidência de multas, pagamento de indenizações e outras penalidades previstas em lei;
  - ✓ Risco de incidência de vírus de computador, em função do desconhecimento da procedência;
  - ✓ Poderá causar lentidão ou parada de funcionamento dos computadores.
- É proibida a instalação de software sem que esteja devidamente identificado, licenciado e homologado pela **OCEANPACT**.

- Softwares do tipo "jogos eletrônicos" não podem ser instalados, armazenados ou usados em qualquer computador da **OCEANPACT**.
- Não é permitido o download de software, programas ou executáveis da Internet ou de quaisquer outros meios para os computadores da **OCEANPACT** sem prévia autorização da área de Tecnologia da Informação, evitando assim qualquer contaminação por vírus que possa comprometer os sistemas e informações da **OCEANPACT** ou gerem problemas com a legislação de direitos autorais.
- A aquisição de software não constante da relação dos homologados deverá ser solicitada por meio de abertura de chamado no Service Desk.
- A **OCEANPACT** deve possuir um catálogo de todos os softwares autorizados necessários na empresa para qualquer finalidade do negócio em qualquer sistema.
- Os softwares fornecidos por entidades externas, sem ônus para a **OCEANPACT** e acompanhados da autorização do detentor legal dos direitos autorais, deverão ser submetidos à equipe de suporte para homologação, quando serão realizados testes e verificações de sua integridade e compatibilidade com os recursos já existentes na rede da **OCEANPACT**.

14. POLÍTICA DE BACKUP

Visa proteger contra a perda de dados.

- A OCEANPACT deve adotar as soluções de Backup e Disaster Recovery para proteger os seus dados contra perdas descritas no Procedimento de Backup para os dados digitais.
- As necessidades especiais de backup devem ser solicitadas à equipe de suporte por meio de abertura de chamado no Service Desk.
- O colaborador da área deve solicitar à equipe de suporte a restauração da cópia de segurança por meio de abertura de chamado no Service Desk em caso de perda ou danos na informação.

15. POLÍTICA PARA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Visa implementar controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos (malwares).

- A **OCEANPACT** adota soluções de proteção contra malware (códigos maliciosos) gerenciadas centralmente, com medidas de detecção e de prevenção para monitorar e defender continuamente cada uma das estações de trabalho e servidores da organização.
- Todos os servidores e estações de trabalho da **OCEANPACT** devem ter software antivírus instalado, ativado e atualizado sistematicamente.

- Todos os colaboradores são responsáveis pela prevenção de contaminação da rede e, em caso de identificação ou suspeita de vírus, devem solicitar análise pela equipe de suporte por meio de abertura de chamado no Service Desk.
- Os colaboradores também são responsáveis pela não interrupção da verificação periódica dos sistemas de proteção contra vírus em suas estações de trabalho.
- Em quaisquer situações, qualquer software ou arquivo proveniente de redes ou usuários externos deverão ser verificados por sistemas de proteção contra vírus.

16. REGISTROS E MONITORAMENTO

Visa registrar eventos e gerar evidências.

- A **OCEANPACT** registra eventos (log) das atividades dos usuários, exceções, falhas e eventos de segurança da informação produzidos, mantidos e analisados criticamente, a intervalos regulares.
- Assegura que os logs apropriados estejam sendo agregados a um sistema central de gerenciamento de logs para análise e revisão.
- Os registros de eventos (log) são protegidos contra acesso não autorizado e adulteração.

17. POLÍTICA PARA GESTÃO DE VULNERABILIDADES TÉCNICAS

Visa evitar a exploração de vulnerabilidades técnicas.

- As vulnerabilidades técnicas devem ser identificadas por meio de um scanner de vulnerabilidades, específico para este fim, e são registradas e tratadas chamados abertos no sistema de Service Desk.
- A OCEANPACT deve analisar sistemas de informação criticamente, através de testes de invasão externos e internos regulares para identificar vulnerabilidades e vetores de ataque que possam ser usados.

18. POLÍTICA PARA SEGURANÇA EM REDES

Visa proteger as informações em redes e dos recursos de processamento da informação que os apoiam.

- O acesso à rede de visitantes da **OCEANPACT** será liberado somente para fins de acesso à internet, por meio de abertura de chamado no Service Desk para a equipe de suporte.
- Os acessos originados na rede interna com destino a qualquer rede externa só pode ser realizados com equipamentos da **OCEANPACT** ou homologados pela **OCEANPACT**.

- A navegação em sites não relacionados à atividade funcional do colaborador não é proibida, porém seu uso deve ser feito de maneira responsável, antes do início do expediente ou no horário de almoço, de modo que abusos possam ser notificados aos gestores e punidos.
- A navegação em sites de categoria restringida pela **OCEANPACT** é expressamente proibida conforme abaixo:
  - ✓ Propaganda político-partidária;
  - ✓ Violação de direito autoral;
  - ✓ Conteúdo ofensivo, difamatório, ilegal, discriminatório e similares;
  - ✓ Pornográfico;
  - ✓ Crackers(quebra de um sistema de segurança de forma ilegal ou sem ética);
  - ✓ Ferramentas de proxy (acesso a Internet de forma oculta ou disfarçada);
  - ✓ Violência e agressividade;
  - ✓ Acesso externo com a finalidade de divulgação de dados sensíveis;
  - ✓ Terrorismo e disseminação de violência a partir de crença ou posição política;
  - ✓ Práticas de comercialização, divulgação ou posicionamento sobre drogas;
  - ✓ Pedofilia.

19. POLÍTICA PARA RELACIONAMENTO COM FORNECEDORES

Visa garantir a proteção dos ativos da organização acessíveis pelos fornecedores.

- Os requisitos de segurança da informação devem ser acordados com o(s) fornecedor(es), e documentados no Acordo de Responsabilidade e Confidencialidade da Informação, a fim de mitigar os riscos associados com o acesso a ativos da OCEANPACT.
- O Acordo de Responsabilidade e Confidencialidade da Informação firmado com o(s) fornecedor(es) deve contemplar todas as diretrizes desta política aplicáveis ao prestador de serviço.

20. PROCESSO DISCIPLINAR

Visa orientar os colaboradores quanto as possíveis ações para os que cometerem violações de segurança da informação.

- O colaborador tem por obrigação cumprir esta política. Desta forma, o não cumprimento será considerado uma infração.
- Diante da constatação de um incidente, reportado e constatado pelo Comitê de Segurança da Informação, sanções serão aplicadas de acordo com o **CORP-PRO-0006 - Procedimento de Consequências.**

- Com relação aos colaboradores terceirizados será solicitado à empresa prestadora da respectiva mão de obra o afastamento temporário ou definitivo do funcionário conforme a falta cometida, podendo, em último caso, a OCEANPACT solicitar a rescisão do respectivo contrato de prestação de serviço.