ITAIPU BINACIONAL	POLÍTICA SECTORIAL	POLÍTICA SETORIAL
	Asunto POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EM TIC - PSITIC	Assunto POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM TIC - PSITIC

1. **FINALIDAD**

Establecer las directrices para protección de la información generada, procesada y guardada por cualquier activo de TIC (Tecnología de la Información, Tecnología de Automatización y Telecomunicaciones) de diversos tipos de amenazas, fraude, fuga o desvío, garantizando su confidencialidad, disponibilidad, autenticidad e integridad.

2. **ÁMBITO DE APLICACIÓN**

Esta política se aplica a todos los ambientes, aplicaciones de negocio, personas y procesos pertinentes a TIC, debiendo ser difundida para toda ITAIPU.

3. **PREMISAS**

Esta política está alineada al Plan Estratégico, a las normas internas de ITAIPU, a los marcos legales vigentes en el Paraguay y Brasil y a las mejores prácticas mundiales aplicables al tema.

4. **DIRECTRICES**

4.1. **Alegato de desconocimiento:** Aclarar a todos los usuarios de los recursos de los Ambientes de TIC, que las normativas que rigen la Seguridad de Información en TIC en ITAIPU son consideradas de conocimiento público, no siendo aceptable cualquier argumento que justifique desconocimiento de esta política.

4.2. **Ambientes de TIC:** Asegurar la confidencialidad, disponibilidad e integridad de los ambientes de TIC de ITAIPU.

4.3. **Análisis de los Procesos y Recursos de TIC:** Asegurar la periodicidad de análisis de los procesos y recursos de TIC para detectar vulnerabilidades y amenazas de seguridad.

4.4. **Autenticidad:** Asegurar la origen de la información, con vistas a garantir evidencias no repudiables de su autoría.

4.5. **Capacitación y Concientización:** Promover la capacitación y la concientización de todos los usuarios de los Ambientes de TIC sobre las amenazas a la seguridad de los activos de TIC.

1. FINALIDADE

Estabelecer as diretrizes para proteção da informação gerada, processada e guardada por qualquer ativo de TIC (Tecnologia da Informação, Tecnologia de Automação e Telecomunicação) de diversos tipos de ameaça, fraude, vazamento ou desvio, garantindo a sua confidencialidade, disponibilidade, autenticidade e integridade.

2. ÂMBITO DE APLICAÇÃO

Esta política se aplica a todos os ambientes, aplicações de negócio, pessoas e processos pertinentes à TIC, devendo ser difundida para toda ITAIPU.

3. PREMISSAS

Esta política está alinhada ao Plano Estratégico, às normas internas da ITAIPU, aos marcos legais vigentes no Brasil e no Paraguai e às melhores práticas mundiais aplicáveis ao tema.

4. DIRETRIZES

4.1. **Alegação de Desconhecimento:** Esclarecer a todos os usuários dos recursos dos Ambientes de TIC, que as normativas que regem a Segurança da Informação em TIC em ITAIPU são consideradas de conhecimento público, não sendo aceitável qualquer argumento que justifique desconhecimento desta política.

4.2. **Ambientes de TIC:** Assegurar a confidencialidade, disponibilidade e integridade dos ambientes de TIC da ITAIPU.

4.3. **Análise dos Processos e Recursos de TIC:** Assegurar a periodicidade da análise dos processos e recursos de TIC para detectar vulnerabilidades e ameaças de segurança.

4.4. **Autenticidade:** Assegurar a identificação da informação, com vistas a garantir evidências não repudiáveis de sua autoria.

4.5. **Capacitação e Conscientização:** Promover a capacitação e a conscientização de todos os usuários dos Ambientes de TIC sobre as ameaças à segurança dos ativos de TIC.

4.6. **Ciclo de vida de la Información:** Proveer medios que permitan al usuario de TIC aplicar las mejores prácticas de seguridad, en conformidad legal, en el ciclo de vida de la información, desde su creación, registro, acceso, uso, reproducción, transmisión, guarda y descarte.

4.7. **Comunicación de Incidentes:** Proveer medios de comunicación con las áreas de TIC para atender y orientar en los casos de incidentes de seguridad con los Activos de TIC de ITAIPU.

4.8. **Confidencialidad:** Garantizar que la información sea accesible solamente a usuarios y/o sistemas autorizados.

4.9. **Conformidad:** Garantizar que todos los requisitos de seguridad aplicables a ITAIPU estén siendo cumplidos.

4.10. **Continuidad de los Servicios:** Asegurar la continuidad de las operaciones de ITAIPU basadas en los recursos disponibles de los Ambientes de TIC, de forma a reducir cualquier eventual interrupción causada por desastres o fallas de seguridad, a través de la combinación de acciones de prevención y recuperación.

4.11. **Control de Acceso:** Asegurar que todos los recursos de los Ambientes de TIC de ITAIPU solamente sean accedidos por usuario y/o sistema debidamente autorizado por las áreas competentes, respetando el Manual de Organización de ITAIPU.

4.12. **Custodia de la Información Clasificada:** Garantizar medios y soporte para custodia de las informaciones clasificadas en cuanto a confidencialidad, integridad y disponibilidad.

4.13. **Desarrollo de Aplicaciones de Negocio:** Asegurar que el desarrollo interno y/o externo de aplicaciones de negocio, así como los productos adquiridos en el mercado y adaptados, incorporen los requisitos de seguridad.

4.14. **Disponibilidad:** Garantizar que la información y/o recurso esté accesible siempre que sea necesario y mediante la debida autorización para su acceso y/o uso.

4.6. **Ciclo de vida da Informação**: Prover meios que permitam ao usuário de TIC aplicar as melhores práticas de segurança, em conformidade legal, no ciclo de vida da informação, desde a sua criação, registro, acesso, uso, reprodução, transmissão, guarda e descarte.

4.7. **Comunicação de Incidentes:** Prover meios de comunicação com as áreas de TIC para atender e orientar nos casos de incidentes de segurança com os ativos de TIC da ITAIPU.

4.8. **Confidencialidade:** Garantir que a informação esteja acessível somente a usuários e/ou sistemas autorizados.

4.9. **Conformidade:** Garantir que todos os requisitos de segurança aplicáveis a ITAIPU estejam sendo cumpridos.

4.10. **Continuidade dos Serviços:** Assegurar a continuidade das operações da ITAIPU baseadas nos recursos disponíveis nos Ambientes de TIC, de forma a reduzir qualquer eventual interrupção causada por desastres ou falhas de segurança, através da combinação de ações de prevenção e recuperação.

4.11. **Controle de Acesso:** Assegurar que todos os recursos dos Ambientes de TIC da ITAIPU somente sejam acessados por usuário e/ou sistema devidamente autorizado pelas áreas competentes, respeitando o Manual de Organização da ITAIPU.

4.12. **Custodia da Informação Classificada:** Garantir meios e suporte para custodia das informações classificadas quanto à confidencialidade, integridade e disponibilidade.

4.13. **Desenvolvimento de Aplicações de Negócio:** Assegurar que o desenvolvimento interno e/ou externo de aplicações de negócio, assim como os produtos adquiridos no mercado e customizados, incorporem requisitos de segurança.

4.14. **Disponibilidade:** Garantir que a informação e/ou recurso esteja acessível sempre que necessário e mediante a devida autorização para seu acesso e/ou uso.

4.15. **Documentación:** Asegurar que las aplicaciones de negocio y procesos de TIC de ITAIPU estén adecuadamente documentadas, de modo a garantizar su entendimiento y recuperación.

4.16. **Gestión de los Recursos de TIC:** Asegurar la gestión de los recursos de TIC, de forma que estén debidamente inventariados y con sus responsables identificados.

4.17. **Integridad:** Garantizar que la información se mantenga fidedigna, sin perder sus características originales.

4.18. **Monitoreo:** Monitorear el tráfico de eventos críticos, dando amplia divulgación de esa actividad y evidenciando posibles incidentes.

4.19. **Prestación de Servicios por Terceros:** Identificar y evaluar los riesgos de la prestación de servicios de TIC por terceros, a fin de garantizar la seguridad de la información en TIC.

4.20. **Prevención y Respuesta a Incidentes:** Asegurar que sean tomadas acciones preventivas con el objetivo de disminuir el riesgo de ocurrencia de incidentes de seguridad y aplicar las medidas necesarias para la solución de los incidentes.

4.21. **Privacidad:** Asegurar, de forma ecuánime, la privacidad de datos e informaciones relacionadas a los usuarios, en conformidad con los marcos legales paraguayos y brasileños, reglamentos y normas que rigen las actividades de ITAIPU.

4.22. **Propiedad:** Asegurar que todas las informaciones generadas por los usuarios de TIC en el ejercicio de sus actividades en ITAIPU, así como los activos de TIC disponibilizados, sean de propiedad y/o derecho de uso exclusivo de ITAIPU.

4.23. **Protección:** Todos los usuarios de los Ambientes de TIC de ITAIPU deben proteger los recursos a él asignados contra modificación, uso indebido, destrucción, desvío, acceso o divulgación no autorizada e informar eventuales incidentes.

4.24. **Publicidad:** Asegurar que el marco normativo que regula la Seguridad de la

4.15. **Documentação:** Assegurar que as aplicações de negócio e processos de TIC da ITAIPU estejam adequadamente documentadas, de modo a garantir seu entendimento e recuperação.

4.16. **Gestão dos Recursos de TIC:** Assegurar a gestão dos recursos de TIC, de forma que estejam devidamente inventariados e com seus responsáveis identificados.

4.17. **Integridade:** Garantir que a informação se mantenha fidedigna, sem perder suas características originais.

4.18. **Monitoramento:** Monitorar o tráfego de eventos críticos, dando ampla divulgação dessa atividade e evidenciando possíveis incidentes.

4.19. **Prestação de Serviços por Terceiros:** Identificar e avaliar os riscos da prestação de serviços de TIC por terceiros, a fim de garantir a segurança da informação em TIC.

4.20. **Prevenção e Resposta a Incidentes:** Assegurar que sejam tomadas ações preventivas com o objetivo de diminuir o risco de ocorrência de incidentes de segurança e aplicar as medidas necessárias para solução dos incidentes.

4.21. **Privacidade:** Assegurar, de forma equânime, a privacidade de dados e informações relacionadas aos usuários, em conformidade com os marcos legais brasileiros e paraguaios, regulamentos e normas que regem as atividades da ITAIPU.

4.22. **Propriedade:** Assegurar que todas as informações geradas pelos usuários de TIC no exercício de suas atividades na ITAIPU, bem como os ativos de TIC disponibilizados, sejam de propriedade e/ou direito de uso exclusivo da ITAIPU.

4.23. **Proteção:** Todos os usuários dos Ambientes de TIC da ITAIPU devem proteger os recursos a ele disponibilizados contra modificação, uso indevido, destruição, desvio, acesso ou divulgação não autorizada, e informar eventuais incidentes.

4.24. **Publicidade:** Assegurar que o marco normativo que regula a Segurança da

Información en TIC de ITAIPU sea ampliamente divulgado para los usuarios de los recursos y de los ambientes de TIC de ITAIPU.

4.25. **Responsabilidad:** Establecer las responsabilidades de todos los usuarios y gestores de los recursos de los Ambientes de TIC de ITAIPU.

4.26. **Seguridad del Perímetro:** Asegurar que el acceso físico a las instalaciones restrictas de TIC de ITAIPU, sea realizado por personas y equipos debidamente autorizados.

4.27. **Sigilo Profesional:** Asegurar que los usuarios de TIC estén sujetos a las reglas referentes al secreto profesional, debiendo garantizar adecuada protección, considerando cláusulas contractuales, Términos de Confidencialidad y Sigilo, Reglamento de Personal y otros documentos normativos de ITAIPU.

4.28. **Temporalidad:** Garantizar que la información sea preservada en la forma y por el plazo mínimo prescrito en el reglamento competente.

4.29. **Utilización de los Recursos:** Los recursos de los Ambientes de TIC de ITAIPU colocados a disposición de usuarios deben ser utilizados solamente para los fines lícitos, éticos y administrativamente aprobados por ITAIPU.

4.30. **Violaciones:** Asegurar que las tentativas de violaciones y las violaciones de seguridad de TIC sean registradas y encaminadas a las instancias pertinentes para determinar las circunstancias y el respectivo tratamiento técnico, administrativo y jurídico.

Informação em TIC da ITAIPU seja amplamente divulgado para usuários dos recursos e dos ambientes de TIC da ITAIPU.

4.25. **Responsabilidade:** Estabelecer as responsabilidades de todos os usuários e gestores dos recursos dos Ambientes de TIC da ITAIPU.

4.26. **Segurança de Perímetro:** Assegurar que o acesso físico às instalações restritas de TIC da ITAIPU seja realizado por pessoas e equipamentos devidamente autorizados.

4.27. **Sigilo Profissional:** Assegurar que os usuários de TIC estejam sujeitos às regras referentes ao sigilo profissional, devendo garantir adequada proteção, considerando cláusulas contratuais, Termos de Confidencialidade e Sigilo, Regulamento de Pessoal e outros documentos normativos da ITAIPU.

4.28. **Temporalidade:** Garantir que a informação seja preservada na forma e pelo prazo mínimo prescrito na regulamentação competente.

4.29. **Utilização dos Recursos:** Os recursos dos Ambientes de TIC da ITAIPU colocados à disposição dos usuários devem ser utilizados apenas para as finalidades lícitas, éticas e administrativamente aprovadas pela ITAIPU.

4.30. **Violações:** Assegurar que as tentativas de violações e as violações de segurança de TIC sejam registradas e encaminhadas às instâncias pertinentes para determinar as circunstâncias e o respectivo tratamento técnico, administrativo e jurídico.