ÍNDICE

1. OBJETIVO

El objetivo de esta política de seguridad de la información es guiar a los Proveedores de TIVIT en las directrices de seguridad de la información vigentes, así como describir su participación y responsabilidad en el cumplimiento de los objetivos y estrategias de excelencia establecidos por TIVIT como proveedor de productos y servicios de tecnología de la información. Las instrucciones y reglas descritas en el presente documento deben seguirse para garantizar, de manera coherente y eficiente, la protección de la información proporcionada por TIVIT, así como el uso adecuado de los recursos tecnológicos, entornos y dependencias a los que acceden los Proveedores de TIVIT debido a la prestación de servicios, garantizando la custodia correcta y evitando amenazas deliberadas o accidentales.

2. APLICACIÓN Y ÁREAS INVOLUCRADAS

Proveedores y socios comerciales de TIVIT.

3. DEFINICIONES Y PREMISAS

3.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACION

Todos los Proveedores de TIVIT se comprometerán a observar la política de seguridad de la información de TIVIT y no proporcionar o apropiarse indebidamente de los recursos de información, utilizando sistemas y recursos tecnológicos únicamente de acuerdo con las autorizaciones e instrucciones especificadas por TIVIT, mediante el seguimiento y la preservación de los activos. También deben estar impregnados de mantener y preservar los principios básicos de la seguridad de la información:

- Confidencialidad – El Proveedor TIVIT debe contribuir al mantenimiento de la confidencialidad y restricción del acceso a la información compartida o a la que se puede acceder debido al ejercicio de su función y servicio contratado. Toda la información compartida o accesible para el Proveedor TIVIT debe clasificarse como confidencial y pertenecer a TIVIT.
- Integridad – El Proveedor TIVIT se compromete con el uso adecuado y autorizado de los activos de TIVIT, incluida la información. No se permite el manejo o edición de activos de información fuera de su ámbito de trabajo o limitaciones impuestas por procedimientos o controles de acceso a los sistemas de información.
- Disponibilidad – El Proveedor TIVIT valora la preservación de los entornos tivit y los recursos tecnológicos de su suministro o soporte, con el fin de favorecer la continuidad y la oferta ininterrumpida de servicios.

Se considera un incidente de seguridad de la información que involucra a los Proveedores de TIVIT, cualquier violación de los principios de seguridad de la información y, en particular, la

violación de datos: caracterizada por una violación de seguridad que conduce a la destrucción accidental o ilegal, pérdida o divulgación no autorizada, acceso a datos protegidos transmitidos o almacenados, y procesamiento o procesamiento no permitido.

Los incidentes de seguridad derivados de los Proveedores de TIVIT pueden dar lugar a investigaciones que resulten en sanciones y responsabilidad legal, así como cancelaciones de contratos y el deber de indemnizar.

3.1.1. Código de Conducta

Es responsabilidad de todos los empleados, proveedores y socios de negócios de TIVIT, la conducta correcta y ética, obedeciendo los preceptos de respeto a las personas y la preservación de la imagen de TIVIT y su compromiso con la seguridad de la información.

Se espera que los Proveedores TIVIT se comporten éticamente y con alta moral, respeto y cumplimiento de las leyes vigentes, así como de las regulaciones TIVIT, incluyendo:

- Realizar trabajo profesional con responsabilidad, dedicación, honestidad y justicia, siempre buscando la mejor solución;
- Esforzarse por adquirir continuamente habilidades técnicas y profesionales, mantenerse siempre al día con los avances en la profesión y las especialidades;
- Actuar dentro de los límites de su competencia profesional;
- Mantener el secreto profesional de la información a la que tiene acceso debido al ejercicio de sus actividades contratadas;
- Cumplir con las expectativas de confianza depositadas por TIVIT, accediendo y utilizando recursos y información sólo en el límite de la necesidad de realizar su trabajo y autorización otorgada;
- Guiar su relación con los colegas sobre los principios de consideración, respeto y solidaridad, así como llevar a cabo actividades profesionales, que impliquen interacción o contribución en grupos, sin discriminación de ningún tipo, sea de color, sexo, nacionalidad, edad, religión, estado civil o cualquier otra condición humana;
- Cumplir con compromisos y plazos;
- No realice actos deliberados que puedan comprometer la seguridad, privacidad o que sirvan para disminuir o cancelar los controles y protecciones de seguridad establecidos por TIVIT.

3.1.2. Documentación normativa de seguridad de la información TIVIT

Para dar soporte al TIVIT Information Security Management System (ISMS), adhiriendo a la norma nacional (Brasil) ABNT NBR ISO/IEC 27001:2013 o (demás países) ISO/IEC

27001:2013 para implementar, monitorear y mejorar los controles e indicadores de eficiencia y eficacia del proceso que garantiza la seguridad de la información en TIVIT, varios documentos, procedimientos e instrucciones se publican y actualizan constantemente. Es responsabilidad del Proveedor TIVIT cumplir con estas regulaciones, incluso si no están explícitamente contenidas en esta política específica. A tal orden, el Proveedor TIVIT buscará, siempre que no encuentre suficiente orientación en este documento, instrucciones específicas de TIVIT y complementará la comprensión de los requisitos de seguridad de la información cuando sea necesario.

El Proveedor TIVIT debe mantenerse informado de los requisitos y estándares de TIVIT que rigen su desempeño con TIVIT, así como de las actualizaciones de estas documentaciones.

4. RESPONSABILIDAD

4.1. RESPONSABILIDADES GENERALES DEL PROVEEDOR DE TIVIT

Todos los Proveedores de TIVIT deben seguir las pautas generales de seguridad de la información y contribuir a la identificación de amenazas y riesgos para la operación TIVIT.

4.1.1. Identificación de Desviaciones / Riesgos

Todo y cualquier impedimento a la prestación del servicio de la manera acordada debe ser reportado a TIVIT, de modo que su impacto sea analizado y comunicado, internamente, minimizando los impactos en la reputación e imagen de TIVIT y/o su desempeño específico contratado.

4.1.2. Informe de incidentes de seguridad de la información

Los Proveedores de TIVIT son una parte integral del flujo de comunicación de eventos de seguridad que pueden interferir negativamente con su rendimiento contratado o indicar un comportamiento anormal de los recursos de TI en uso. Tales eventos pueden ser clasificados como incidentes de seguridad de la información por TIVIT y manejados apropiadamente para asegurar la integridad y calidad de la infraestructura de TI de TIVIT.

Todo comportamiento anormal de los servicios de red y los sistemas de información, percibido según el Proveedor TIVIT, debe ser reportado a: soc.hotline@tivit.com

5. DESCRIÇÃO DA POLÍTICA

Los proveedores de TIVIT deben seguir pautas específicas de seguridad de la información cuando corresponda.

5.1. Gestión de activos

- Los Proveedores TIVIT deben observar las reglas para el uso de equipos informáticos autorizados por TIVIT en entornos de trabajo como dispositivos móviles, tabletas digitales, computadoras personales y dispositivos portátiles. Todos los equipos informáticos llevados al entorno de trabajo en las instalaciones de TIVIT deben ser declarados.
- El Proveedor TIVIT que utiliza equipos informáticos propiedad de TIVIT debe utilizarlo únicamente para los propósitos descritos en el contrato específico, siendo responsable de mantener el estado de conservación del equipo y su retorno inmediato al sector responsable, una vez terminado o rescindido su contratación con TIVIT.
- La necesidad de almacenamiento o transporte de equipos informáticos por parte del Proveedor TIVIT debe ser expresamente autorizada por TIVIT. El Proveedor TIVIT sólo podrá utilizar los lugares de almacenamiento y tránsito de este equipo especificados en la autorización concedida.
- El Proveedor TIVIT sólo podrá utilizar los soportes para el almacenamiento y transporte de activos de información expresamente autorizados por TIVIT.
- La custodia de los activos de información TIVIT por parte del Proveedor TIVIT no está permitida después de la terminación de la actividad contratada, a menos que se indique lo contrario en el contrato.

5.2. Control de acceso físico y lógico

- Los Proveedores de TIVIT deben llevar una identificación clara y visible (carnet / insignia / etiqueta) o proporcionar documentación de identificación personal cuando se solicite.
- Los Proveedores TIVIT deben utilizar la identificación y autenticación de los usuarios del sistema otorgados formalmente por TIVIT para llevar a cabo sus actividades, informando de errores o accesos que no correspondan o excedan el alcance de su cumplimiento contratado.
- Las credenciales de acceso al sistema disponibles para los proveedores de TIVIT no son transferibles.
- Los sistemas de información proporcionados por los Proveedores TIVIT, para el uso de los empleados de TIVIT, deben ofrecer una autenticación segura y proporcionar medios de trazabilidad de las acciones realizadas. La disponibilidad o integración de estos sistemas debe utilizar preferiblemente varios factores (autenticación fuerte) y conectarse mínimamente a los controladores TIVIT por medio de la autenticación moderna de Azure AD para la autenticación de usuario.

5.3. Delimitación del perímetro y protección de la seguridad física

- Los Proveedores de TIVIT deben actuar y transitar únicamente en lugares expresamente autorizados y relacionados con su desempeño contratado.

5.4. Uso aceptable de activos y recursos

- Los Proveedores de TIVIT deben utilizar activos de información solo para el propósito relacionado con su desempeño contratado.
- Los Proveedores de TIVIT no pueden reconfigurar o cambiar las capacidades y restricciones definidas en los equipos y recursos tecnológicos de propiedad de TIVIT. Los equipos y recursos tecnológicos de posesión o propiedad del Proveedor TIVIT, utilizados en su desempeño contratado, no deben ofrecer riesgos y vulnerabilidades. El uso de dichos equipos puede ser objeto de inspección y evaluación por TIVIT en cualquier momento e incluyendo la prohibición de uso.

5.5. Análisis y garantías de seguridad en los sistemas de información

- Los sistemas de información proporcionados por los Proveedores TIVIT, para el uso de los empleados de TIVIT y/o sus clientes, deben ofrecer garantías de seguridad de la información aplicada. Los certificados de análisis de seguridad en vigor, realizados por terceros competentes y entidades independientes, deberán presentarse siempre que se solicite. Además, TIVIT se reserva el derecho de realizar análisis de seguridad (análisis de vulnerabilidades, pruebas de penetración o de otro tipo) para mantener esta garantía de seguridad de la información en estos sistemas.

5.6. Recursos Humanos, Interacciones y Comunicaciones

- Los Proveedores TIVIT deben utilizar únicamente recursos humanos (empleados) expresamente declarados y autorizados para la prestación de actividades contratadas (incluso en actividades realizadas fuera de las instalaciones de TIVIT).
- Las interacciones entre el Proveedor de TIVIT y TIVIT deben ser llevadas por las formas y medios autorizados por TIVIT.
- La comunicación y el envío de información deben realizarse de forma segura, observando los protocolos y aplicaciones de comunicación autorizados por TIVIT.

5.7. Planes de Continuidad, Desastre o Situación de Emergencia

- Cuando se activan en una situación de contingencia, activación de planes de continuidad y/o recuperación ante desastres, los Proveedores TIVIT responsables de acciones de emergencia deben priorizar las acciones de acuerdo con el nivel de prioridad clasificado por TIVIT, respetando los Acuerdos de Nivel de Servicio (ANS) definidos en el contrato.
- Si se define en el contrato, los Proveedores TIVIT que apoyan áreas de negocio críticas, ofrecerán regularmente resultados de pruebas para la ejecución de planes de continuidad y/o recuperación ante desastres relacionados con el alcance de los productos y servicios del contrato, con el fin de demostrar el cumplimiento del proceso, entregas y tiempos acordados con TIVIT.
- Todas las acciones de emergencia ejecutadas con la participación del Proveedor TIVIT deben cumplir con los principios de seguridad de la información establecidos por TIVIT.

5.8. Requisitos legales y reglamentarios adicionales

- Todos los cargos de seguridad, además de esta política, determinados por los requisitos legales o la Regulación Sectorial a la que TIVIT está sujeta, generan obligaciones de cumplimiento solidario del Proveedor TIVIT, limitadas a su cumplimiento contratado.
- Si el Proveedor TIVIT almacena datos de TIVIT o sus Clientes fuera del territorio nacional, debe informar a TIVIT del país de almacenamiento. El cambio de almacenamiento a cualquier país que no sea el inicialmente informado debe ser consultado previamente y autorizado por TIVIT.

5.9. Cifrado, Privacidad y Monitoreo

- El Proveedor TIVIT que maneja los datos personales en detrimento de su actividad contratada es responsable de garantizar que dichos datos se gestionen de acuerdo con todas las normas de Privacidad y Protección de Datos Personales aplicables.
- Toda la información confidencial, con acceso otorgado al Proveedor TIVIT, debe cumplir con los principios de seguridad y gestión de claves establecidos por TIVIT. El Proveedor TIVIT no está autorizado a cambiar los permisos ni interferir con la gestión del acceso a la información propiedad de TIVIT.
- TIVIT se reserva el derecho de supervisar y controlar las acciones de credenciales utilizadas por los Proveedores de TIVIT, así como de inspeccionar el contenido de los mensajes y comunicaciones realizados a través del uso de la red informática bajo la responsabilidad de TIVIT.

5.10. Contratación subcontratista

- El Proveedor TIVIT que opte por subcontratar parte o todo el alcance de los servicios, debe obtener el consentimiento previo de TIVIT para hacerlo.
- Si el subcontrato es aprobado por TIVIT, es responsabilidad del Proveedor TIVIT garantizar el conocimiento y el cumplimiento de todas las directrices proporcionadas en el presente documento por los subcontratistas.

6. REFERENCIA A OTROS DOCUMENTOS

No aplica.