ÍNDICE

1. OBJETIVO

El objetivo de esta política de seguridad de la información es guiar a los Proveedores de la Organización (ver Definiciones y Premisas) 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 la Organización 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 la Organización, así como el uso adecuado de los recursos tecnológicos, entornos y dependencias a los que acceden los Proveedores 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 la Organización.

3. DEFINICIONES Y PREMISAS

Organización: TIVIT, Takoda y demás compañías de acuerdo con la aplicabilidad

3.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACION

Todos los Proveedores se comprometerán a observar la política de seguridad de la información de la Organización 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 la Organización, 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 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 debe clasificarse como confidencial y pertenecer a la Organización.
- Integridad – El Proveedor se compromete con el uso adecuado y autorizado de los activos de la Organización, 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 valora la preservación de los entornos de la Organización 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, 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 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 negocios de la Organización, la conducta correcta y ética, obedeciendo los preceptos de respeto a las personas y la preservación de la imagen de la Organización y su compromiso con la seguridad de la información.

Se espera que los Proveedores se comporten éticamente y con alta moral, respeto y cumplimiento de las leyes vigentes, así como de las regulaciones de la Organización, 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 la Organización, 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 la Organización.

3.1.2. Documentación normativa de seguridad de la información de la Organización

Para dar soporte al Sistema de Gestión de Seguridad de la Información (SGSI) de la Organización, adhiriendo a la norma nacional (Brasil) ABNT NBR ISO/IEC 27001 o (demás países) ISO/IEC 27001 para implementar, monitorear y mejorar los controles e indicadores de eficiencia y eficacia del proceso que garantiza la seguridad de la información en la Organización, varios documentos, procedimientos e instrucciones se publican y actualizan constantemente. Es responsabilidad del Proveedor cumplir con estas regulaciones, incluso si no están explícitamente contenidas en esta política específica. A tal orden, el Proveedor buscará, siempre que no encuentre suficiente orientación en este documento, instrucciones específicas de la Organización y complementará la comprensión de los requisitos de seguridad de la información cuando sea necesario.

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

4. RESPONSABILIDAD

4.1. RESPONSABILIDADES GENERALES DEL PROVEEDOR

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

4.1.1. Identificación de Desviaciones / Riesgos

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

4.1.2. Informe de incidentes de seguridad de la información

Los Proveedores 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 la Organización y manejados apropiadamente para asegurar la integridad y calidad de la infraestructura de TI de la Organización.

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

5. DESCRIÇÃO DA POLÍTICA

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

5.1. Gestión de activos

- Los Proveedores deben observar las reglas para el uso de equipos informáticos autorizados por la Organización 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 la Organización deben ser declarados.
- El Proveedor que utiliza equipos informáticos propiedad de la Organización 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 la Organización.
- La necesidad de almacenamiento o transporte de equipos informáticos por parte del Proveedor debe ser expresamente autorizada por la Organización. El Proveedor sólo podrá utilizar los lugares de almacenamiento y tránsito de este equipo especificados en la autorización concedida.
- El Proveedor sólo podrá utilizar los soportes para el almacenamiento y transporte de activos de información expresamente autorizados por la Organización.
- La custodia de los activos de información de la Organización por parte del Proveedor 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 deben llevar una identificación clara y visible (carnet / insignia / etiqueta) o proporcionar documentación de identificación personal cuando se solicite.
- Los Proveedores deben utilizar la identificación y autenticación de los usuarios del sistema otorgados formalmente por la Organización 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 la Organización no son transferibles.
- Los sistemas de información proporcionados por los Proveedores para el uso de los empleados de la Organización 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 de la Organización 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 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 deben utilizar activos de información solo para el propósito relacionado con su desempeño contratado.
- Los Proveedores no pueden reconfigurar o cambiar las capacidades y restricciones definidas en los equipos y recursos tecnológicos de propiedad de la Organización. Los equipos y recursos tecnológicos de posesión o propiedad del Proveedor, utilizados en su desempeño contratado, no deben ofrecer riesgos y vulnerabilidades. El uso de dichos equipos puede ser objeto de inspección y evaluación por la Organización 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 para el uso de los empleados de la Organización 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, la Organización 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 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 la Organización).
- Las interacciones entre el Proveedor y la Organización deben ser llevadas por las formas y medios autorizados por la Organización.
- La comunicación y el envío de información deben realizarse de forma segura, observando los protocolos y aplicaciones de comunicación autorizados por la Organización.

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 responsables de acciones de emergencia deben priorizar las acciones de acuerdo con el nivel de prioridad clasificado por la Organización, respetando los Acuerdos de Nivel de Servicio (ANS) definidos en el contrato.
- Si se define en el contrato, los Proveedores 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 la Organización.
- Todas las acciones de emergencia ejecutadas con la participación del Proveedor deben cumplir con los principios de seguridad de la información establecidos por la Organización.

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 la Organización está sujeta, generan obligaciones de cumplimiento solidario del Proveedor, limitadas a su cumplimiento contratado.
- Si el Proveedor almacena datos de la Organización o sus Clientes fuera del territorio nacional, debe informar a la Organización del país de almacenamiento. El cambio de almacenamiento a cualquier país que no sea el inicialmente informado debe ser consultado previamente y autorizado por la Organización.

5.9. Cifrado, Privacidad y Monitoreo

- El Proveedor 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, debe cumplir con los principios de seguridad y gestión de claves establecidos por la Organización. El Proveedor no está autorizado a cambiar los permisos ni interferir con la gestión del acceso a la información propiedad de la Organización.
- La Organización se reserva el derecho de supervisar y controlar las acciones de credenciales próvidas por la Organización y utilizadas por los Proveedores, así como de inspeccionar el contenido de los mensajes y comunicaciones realizados a través del uso de la red informática bajo la responsabilidad de la Organización.

5.10. Contratación subcontratista

- El Proveedor que opte por subcontratar parte o todo el alcance de los servicios, debe obtener el consentimiento previo de la Organización para hacerlo.
- Si el subcontrato es aprobado por la Organización, es responsabilidad del Proveedor 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.