ÍNDICE

1. OBJETIVO

El objetivo de esta política de seguridad de la información es orientar a los Proveedores de la Organización (ver DEFINICIONES Y PREMISAS) sobre las directrices de seguridad de la información a observar en sus actividades para la Organización, de forma que contribuyan con la protección de los activos de información bajo su custodia o acceso.DEFINICIONES Y PREMISAS

2. APLICACIÓN Y ÁREAS INVOLUCRADAS

Proveedores y socios de la Organización.

3. DEFINICIONES Y PREMISAS

Organización: Takoda y demás empresas del grupo según corresponda.

3.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Todos los Proveedores de la Organización deben estar comprometidos con el cumplimiento de la política de seguridad de la información de la Organización, no suministrando ni apropiándose indebidamente de recursos de información.

- Confidencialidad – El Proveedor debe contribuir al mantenimiento de la confidencialidad y restricción de acceso de las informaciones compartidas o accedidas en el ejercicio de sus actividades.
- Integridad – El Proveedor se compromete con el uso adecuado y autorizado de los activos de la Organización, incluyendo informaciones. No está permitida la alteración de informaciones o activos sin la debida autorización.
- Disponibilidad – El Proveedor vela por la preservación de los entornos y recursos tecnológicos de la Organización de su suministro o soporte, de modo de no comprometer la disponibilidad de los servicios.

Se considera incidente de seguridad de la información involucrando Proveedores, cualquier incumplimiento de los principios de seguridad de la información establecidos en esta política.

Los incidentes de seguridad originados por Proveedores pueden ocasionar investigaciones que resulten en sanciones, penalidades y responsabilizaciones legales y contractuales.

3.1.1. Código de Conducta

Es responsabilidad de todos los colaboradores, Proveedores y socios de la Organización, la conducta correcta y ética, obedeciendo los preceptos del Código de Conducta de la Organización.

Se espera de los Proveedores un comportamiento ético y de elevada moral, respeto y observancia de las leyes vigentes, así como de los reglamentos y estándares de la Organización, particularmente en lo que respecta a la seguridad de la información. Entre las conductas esperadas se destacan:

- Ejercer el trabajo profesional con responsabilidad, dedicación, honestidad y justicia, buscando siempre la mejor solución;
- Esforzarse por adquirir continuamente competencias técnicas y profesionales, manteniéndose siempre actualizado con los avances de la profesión y el área de actuación;
- Actuar dentro de los límites de su competencia profesional;
- Guardar confidencialidad profesional de las informaciones a las que tenga acceso en razón del ejercicio de sus actividades contratadas;
- Atender a las expectativas de confianza depositadas por la Organización, accediendo y utilizando recursos e informaciones solo en el límite de la necesidad de su actividad contratada;
- Orientar su relación con colegas en los principios de consideración, respeto y solidaridad, así como conducir las actividades profesionales, cuando sea aplicable, con dedicación y competencia;
- Cumplir los compromisos y plazos establecidos;
- No practicar actos deliberados que puedan comprometer la seguridad, la privacidad o que atenten contra la reducción o anulación de controles y protecciones de seguridad de la información.

3.1.2. Documentación Normativa de Seguridad de la Información de la Organización

Para respaldar el Sistema de Gestión de Seguridad de la Información de la Organización (SGSI), adherente a la norma ISO/IEC 27001, fueron establecidos documentos específicos disponibles en el sistema de documentación corporativa de la Organización, MOGIT.

El Proveedor debe mantenerse informado de los requisitos y normas de la Organización que regulan su actuación en la Organización, así como de las actualizaciones que puedan afectar sus actividades.

4. RESPONSABILIDAD

4.1. RESPONSABILIDADES GENERALES DEL PROVEEDOR DE LA ORGANIZACIÓN

Todos los Proveedores deben seguir las orientaciones generales de seguridad de la información y contribuir a la identificación de amenazas y riesgos a la seguridad de la información.

4.1.1. Identificación de Desviaciones / Riesgos

Todo impedimento de la prestación del servicio en la forma acordada deberá ser reportado a la Organización, para que su impacto sea analizado y las medidas pertinentes sean adoptadas.

4.1.2. Comunicación de incidentes de seguridad de la información

Los Proveedores son parte integrante del flujo de comunicación de eventos de seguridad que puedan interferir negativamente en su actuación contratada.

Todo comportamiento anormal de servicios de red y sistemas de información, percibido por el Proveedor, debe ser reportado a: soc@takodadatacenters.com o al canal oficial del CSIRT de la Organización.

5. DESCRIPCIÓN DE LA POLÍTICA

Los Proveedores deben seguir las orientaciones específicas de seguridad de la información, cuando aplique.

5.1. Gestión de activos

- Los Proveedores deben observar reglas para el uso de equipos computacionales autorizados por la Organización en entornos de trabajo, tales como: utilizar solo software licenciado, no instalar software no autorizado y no almacenar informaciones confidenciales en dispositivos no autorizados.
- El Proveedor que utilice equipos computacionales de propiedad de la Organización debe utilizarlos solo para los fines descritos en la contratación.
- La necesidad de guardar o transportar equipos computacionales por el Proveedor de la Organización debe ser expresamente autorizada por la Organización.
- Solo los soportes de guarda y transporte de activos de información expresamente autorizados por la Organización pueden ser utilizados por el Proveedor.
- No está permitida la guarda de activos de información de la Organización por el Proveedor después del cierre de la actividad contratada, salvo determinación contractual expresa.

5.2. Control de acceso físico y lógico

- Los Proveedores deben portar identificación clara y visible (credencial / etiqueta) u ofrecer documentación de identificación personal siempre que sea solicitado.
- Los Proveedores deben utilizar identificación y autenticación de usuarios de sistema concedidos formalmente por la Organización para la realización de sus actividades.
- Las credenciales de acceso a sistemas disponibilizadas para Proveedores son de uso intransferible.
- Los sistemas de información provistos por Proveedores de la Organización, para uso de colaboradores de la Organización, deben ofrecer autenticación segura, con soporte a autenticación multifactor siempre que sea técnicamente posible.

5.3. Delimitación de perímetro y protección de seguridad física

- Los Proveedores deben actuar y transitar solo en lugares expresamente autorizados y relacionados con su actuación contratada.

5.4. Uso aceptable de activos y recursos

- Los Proveedores deben utilizar activos de información solo para el propósito relacionado con su actuación contratada.
- Los Proveedores no pueden reconfigurar ni alterar capacidades y restricciones definidas en equipos y recursos tecnológicos de propiedad de la Organización sin autorización expresa.

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

- Los sistemas de información provistos por Proveedores, para uso de colaboradores de la Organización y/o sus clientes, deben ofrecer garantías de seguridad, incluyendo pruebas de penetración, evaluaciones de vulnerabilidades y cumplimiento de los estándares de seguridad de la Organización.

5.6. Recursos Humanos, Interacciones y Comunicaciones

- Los Proveedores deben utilizar solo recursos humanos (colaboradores) expresamente declarados y autorizados para la prestación de las actividades contratadas.

- Las interacciones entre el Proveedor y la Organización deben realizarse por los medios y soportes autorizados por la Organización.
- La comunicación y envío de informaciones debe ocurrir de forma segura, observando los protocolos y aplicativos de comunicación autorizados por la Organización.

5.7. Planes de Continuidad, Desastre o Situación de Emergencia

- Cuando sean activados en escenario de contingencia, activación de planes de continuidad y/o recuperación de desastres, los Proveedores responsables deben seguir las orientaciones de la Organización y contribuir con la restauración de los servicios en el menor tiempo posible.
- Si así está definido en contrato, los Proveedores que soportan áreas críticas de negocio deben ofrecer, regularmente, resultados de pruebas de ejecución de sus planes de continuidad.
- Todas las acciones de emergencia ejecutadas con la participación del Proveedor deben obedecer los principios de seguridad de la información establecidos en esta política.

5.8. Requisitos Legales y Regulatorios adicionales

- Todas las imposiciones de seguridad, adicionales a esta política, determinadas por requisitos Legales o Regulamentos Sectoriales a los que la Organización esté sujeta, deben ser igualmente observadas por el Proveedor.
- Si el Proveedor almacena datos de la Organización o de sus Clientes fuera del territorio nacional, deberá informar a la Organización el país de almacenamiento y garantizar el cumplimiento de la legislación de protección de datos aplicable, incluyendo la Ley 1581 de 2012.

5.9. Criptografía, Privacidad y Monitoreo

- El Proveedor que maneje datos personales en razón de su actividad contratada es responsable de garantizar que esos datos sean gestionados de conformidad con la Ley 1581 de 2012 y los estándares de privacidad de la Organización.
- Todas las informaciones confidenciales, con acceso concedido al Proveedor, deben obedecer los principios de seguridad y gestión de claves establecidos en la Política de Criptografía de la Organización.
- La Organización se reserva el derecho de monitorear y controlar acciones de credenciales provistas por la Organización y utilizadas por Proveedores, así como de auditar el cumplimiento de esta política.

5.10. Subcontratación

- El Proveedor que opte por la subcontratación de parte o todo el alcance de servicios, debe obtener anuencia previa de la Organización para ello.
- Si la subcontratación es aprobada por la Organización, es responsabilidad del Proveedor garantizar el conocimiento y cumplimiento de todas las directrices de seguridad de la información de la Organización por parte del subcontratado.

6. REFERENCIA A OTROS DOCUMENTOS

No aplica.