RESUMEN

1. INTRODUCCIÓN

El objetivo principal de esta Política de Seguridad de la Información para Socios es dirigir un programa efectivo para la protección de los activos de información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, siendo la base para el establecimiento de estándares y procedimientos de Seguridad de la Información en el Grupo WEG.

2. ALCANCE

Todos los Socios (cualquier persona que tenga una relación jurídica con el Grupo WEG como proveedor de productos, licencias o servicios) deben cumplir con los requisitos de Seguridad de la Información aquí definidos. El cumplimiento de las directrices establecidas es esencial para la efectiva relación de colaboración firmada y la consecución de niveles adecuados de protección de la información.
Las directrices y requisitos establecidos en este documento se aplican a todos los Socios que tienen acceso a los datos, información y sistemas del Grupo WEG. Los socios serán responsables de sí mismos y de sus empleados, proveedores y prestadores de servicios.

3. DEFINICIONES

- **DPIA:** es el acrónimo de Evaluación de Impacto de Protección de Datos, que significa Informe de Impacto de Protección de Datos Personales (RIPD) en la Ley General de Protección de Datos (LGPD) de Brasil.
  Este proceso identifica, evalúa y mitiga los riesgos de privacidad en los proyectos de datos antes de que se implementen. Es una responsabilidad legal y obligatoria cuando el tratamiento de datos puede poner en riesgo los derechos y libertades de los interesados.
- **Opt-in:** es un término en inglés que significa la autorización de un usuario para recibir información de una empresa.
- **Opt-out:** es un término que significa "elegir irse", es un movimiento en el que el individuo tiene la autonomía de dejar de ser parte de algo que está insertado.
- **Segregación de Funciones (SOD):** SOD es el acrónimo *de Segregación de Funciones*, es un principio de control interno que tiene como objetivo evitar riesgos, como fraudes, errores y ataques cibernéticos, en las organizaciones. La segregación de funciones se basa en la delegación de tareas entre diferentes personas o grupos, con el fin de evitar que una misma persona tenga control total sobre sistemas, procesos o actividades confidenciales.
- **Política de mínimos privilegios:** Se trata de un concepto de ciberseguridad que consiste en otorgar a los usuarios solo los mínimos privilegios necesarios para desempeñar sus funciones.
- **Runbooks**: guías detalladas que describen los procedimientos y procesos de una organización, con el objetivo de garantizar que las actividades se realicen de manera consistente, segura y eficiente.
- **Hardening:** proceso que tiene como objetivo fortalecer la seguridad de los sistemas, redes, software, hardware, firmware e infraestrutura de TI, haciéndolos más resistentes a los ciberataques.
- **Parches de seguridad:** actualizaciones correctivas que tienen como objetivo corregir vulnerabilidades, fallas y errores en software y plataformas. La palabra "parche" es un término en inglés que significa "parche" o "parche".

- **OWASP:** Open Worldwide Application Security Project (OWASP) es una organización internacional sin ánimo de lucro que trabaja para mejorar la seguridad de las aplicaciones web y móviles. OWASP es una de las principales iniciativas para combatir el cibercrimen.
- **Privacidad y Seguridad por Diseño:** conceptos que hacen referencia a la protección de datos y a la seguridad del sistema de forma proactiva, desde la concepción de un proyecto o servicio.
- **Phishing:** un tipo de ciberataque que tiene como objetivo robar información personal o acceder a cuentas en línea. Los estafadores utilizan mensajes fraudulentos que parecen legítimos para engañar a las víctimas y que revelen datos confidenciales.
- **Hacking ético:** El hacking ético o hacking ético, es una práctica de seguridad digital que consiste en simular un ciberataque para identificar y corregir vulnerabilidades en sistemas, redes o aplicaciones.
- **Pruebas de penetración:** Las pruebas de penetración (o pentesting) son un ataque simulado autorizado que las organizaciones realizan en sus propios sistemas informáticos o redes para evaluar su seguridad. El objetivo es descubrir vulnerabilidades utilizando las mismas herramientas, técnicas y procesos que utilizan los piratas informáticos. Al exponer las debilidades de la ciberseguridad, las pruebas de penetración ayudan a reducir los riesgos de ciberataques maliciosos.

4. RESPONSABILIDADES

4.1. Área de contratación de servicios de proveedores

- Durante el proceso de contratación de Socios (incluyendo empleados, proveedores y prestadores de servicios vinculados al Socio) que necesiten acceder a la red interna, sistemas, información o datos del Grupo WEG, el área contratante debe asegurarse de que todos los involucrados conozcan esta política de seguridad de la información.
- El área de contratación debe asegurarse de que los contratos con los Socios incluyan cláusulas específicas sobre seguridad de la información y protección de datos, incluso con referencia expresa a esta Política de Seguridad de la Información.

4.2. Socios

- Es responsabilidad de los Socios observar y seguir las pautas establecidas en esta Política de Seguridad de la Información; y
- Las actividades realizadas deberán cumplir con la legislación vigente y la normalización de organismos y entidades reguladoras en materia de Seguridad de la Información aplicables al objeto del contrato.

5. DIRECTRICES

5.1. General

Los socios, ya sean proveedores de productos, licencias o servicios, deben comprometerse a cumplir plenamente con lo siguiente:

- Proteger la información contra el acceso, la modificación, la destrucción o la divulgación no autorizados, manteniendo su confidencialidad;

- Asegurar que los recursos puestos a su disposición sean utilizados únicamente para los fines aprobados por el Grupo WEG;
- Asegurar que los sistemas y la información bajo su responsabilidad estén adecuadamente protegidos de acuerdo con los estándares del Grupo WEG;
- Garantizar la continuidad del procesamiento de la información crítica del negocio;
- Cumplir con las leyes y normas que regulan los aspectos de propiedad intelectual;
- Implementar y mantener controles de seguridad de la información, de acuerdo con las mejores prácticas del mercado y la normatividad aplicable;
- Informar inmediatamente al Grupo WEG cualquier incumplimiento de la Política de Seguridad de la Información para los Socios, por sí mismos o por otras personas, estén o no vinculadas al socio.
- Cumplir con las Condiciones Generales de Compra de Bienes, Materiales y/o Servicios ("CGC") del Grupo WEG – disponibles en: https://www.weg.net/ -> Se trata de WEG -> CONDICIONES GENERALES DE COMPRA PARA PROVEEDORES – y el Código de Ética para Proveedores del Grupo WEG ("Código de Ética") – disponible en: https://www.weg.net/ -> Este es WEG -> CÓDIGO DE ÉTICA PARA PROVEEDORES. El Partner deberá cumplir estrictamente con los parámetros que le sean aplicables en materia de protección de datos y privacidad establecidos en cualquier legislación aplicable, así como seguir las mejores prácticas del mercado en la materia.
- Los socios que realizan actividades críticas en nombre del Grupo WEG deben someterse a un proceso de evaluación de la Seguridad de la Información ("IS"). En el proceso de evaluación de SI, se llevará a cabo una autoevaluación de SI durante las fases de calificación del proveedor y negociación del contrato. Dependiendo del resultado de la Autoevaluación, el Grupo WEG podrá solicitar procedimientos adicionales para verificar la adecuación del socio a los parámetros de SI establecidos en esta Política de Seguridad de la Información para Socios.

6. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

6.1. CONDUCTA DE LOS SOCIOS EN EL ENTORNO DEL GRUPO WEG

6.1.1. Acceso lógico y uso aceptable

- Para los Socios que necesiten acceder al ambiente del Grupo WEG de forma remota, el gerente de WEG responsable del contrato debe proporcionar acceso a través de un usuario único e individual, en el que solo podrán tener acceso a los recursos y ambientes de trabajo necesarios para el desempeño de sus funciones;
- Las computadoras de los Socios no pueden ser conectadas a la red interna del Grupo WEG sin la aprobación previa del área responsable de la seguridad de la información, el software de los equipos de los Socios debe estar debidamente licenciado;
- Está prohibido acceder, descargar o distribuir cualquier contenido que viole los derechos de autor o la propiedad del Grupo WEG. Asimismo, no se permite el acceso o distribución de contenidos ilícitos, pornográficos de cualquier naturaleza o que infrinja el estatuto del niño y del adolescente;
- Las credenciales de acceso puestas a disposición del socio son solo para uso exclusivo y no pueden divulgarse ni compartirse con otros;
- El socio debe mantener seguras sus credenciales de acceso, y es su única y exclusiva responsabilidad por cualquier uso que se haga con sus credenciales de acceso, incluido cualquier uso indebido;

- Es responsabilidad del socio comunicar cualquier despido de sus empleados, proveedores o prestadores de servicios.

6.1.2. Notificación de incidentes de seguridad de la información

El Socio deberá, cuando descubra un incidente o sospeche razonablemente que está ocurriendo o ha ocurrido un incidente:

- Iniciar inmediatamente la gestión de incidentes para investigar, contener y proteger rápidamente los sistemas de TI y los datos de la empresa en riesgo, minimizar y mitigar el impacto del incidente en los sistemas de TI;
- Notifique inmediatamente al Grupo WEG por correo electrónico soc@weg.net.

El socio debe notificar el incidente incluyendo la siguiente información:

- La naturaleza y el presunto alcance del incidente;
- La fecha sospechosa en la que comenzó el incidente;
- La fecha y hora del descubrimiento del incidente;
- Acciones tomadas por el socio para garantizar la provisión continua de alcance y para proteger y recuperar los datos de la empresa, cuando corresponda; y
- Datos de contacto de un representante de un socio para responder a las solicitudes de información del Grupo WEG.

El Socio debe proporcionar al Grupo WEG la siguiente información a la brevedad posible:

- la(s) causa(s) presunta(s) del incidente y el/los actor(es) involucrado(s);
- El impacto estimado del incidente;
- Acciones correctivas propuestas y tiempo estimado para la recuperación completa del impacto del incidente; y
- Acciones correctivas propuestas, incluso para garantizar la provisión continua de alcance y para proteger y recuperar los datos de la empresa cuando corresponda.

El Socio deberá proporcionar al Grupo WEG actualizaciones periódicas de la información proporcionada de conformidad con los párrafos anteriores, junto con cualquier otra información que el Grupo WEG pueda solicitar razonablemente en relación con el incidente (incluidos los registros de todos los accesos a los sistemas informáticos relevantes en relación con el incidente y las pruebas que demuestren la protección y recuperación efectivas de los datos de la empresa).

El Socio proporcionará inmediatamente al Grupo WEG toda la asistencia que el Grupo WEG pueda necesitar para permitirle investigar, responder, mitigar el impacto y corregir incidentes (incluida la protección y recuperación de los datos de la empresa) y comunicarse y responder a las personas o autoridades públicas, incluidas las autoridades reguladoras pertinentes.

El Socio proporcionará al Grupo WEG un informe final del incidente, incluyendo un análisis de la causa raíz, tan pronto como esté disponible.

Sin perjuicio de cualquier disposición en contrario en el contrato, un incidente no se considerará un evento de fuerza mayor en la medida en que haya sido contribuido por cualquier incumplimiento de este anexo o negligencia de un miembro del socio.

6.1.3. Seguridad de los equipos

- Cada Socio es responsable de la protección de los dispositivos físicos que contienen información del Grupo WEG y que se encuentran bajo su custodia; y
- Los socios son conscientes de que el acceso a cualquier entorno del Grupo WEG o el uso de cualquier recurso de TI en el entorno del Grupo WEG, incluso en situaciones en las que el socio utiliza equipos de propiedad personal, están sujetos a supervisión e inspección, excepto en situaciones en las que la ley local aplicable prohíba expresamente dicha conducta.

6.1.4. Incumplimiento de conducta

Las siguientes situaciones se consideran violaciones de esta Política de Seguridad de la Información para Socios, sin limitarse a:

- Cualquier acción, omisión u otra situación que pueda exponer al Grupo WEG a pérdidas financieras o de imagen, directa o indirectamente, potenciales o reales, comprometiendo sus activos de información;
- Uso indebido o divulgación de cualquier información sin el permiso expreso del Grupo WEG, tales como: datos corporativos, secretos comerciales u otra información;
- El incumplimiento omiso u omiso de cualquier directriz, regla, parámetro u obligación establecida en la presente Política de Seguridad de la Información para Socios;
- Uso de datos, información, equipos, software, sistemas u otros recursos tecnológicos, con fines ilícitos, que pueden incluir la violación de leyes, regulaciones internas y externas, ética o requisitos de los organismos reguladores en el área de operación del Grupo WEG; y
- Falta de comunicación inmediata al Grupo WEG de cualquier incidente de Seguridad de la Información o incumplimiento de esta Política de Seguridad de la Información para Socios.

6.2. CONTROLES DE SEGURIDAD Y PRIVACIDAD EN EL ENTORNO DE SOCIOS

A solicitud del área de negocios del Grupo WEG, el Socio en cuestión será registrado por el equipo de Gobernanza de Seguridad de la Información en una herramienta de verificación de su cibersalud. Esta plataforma proporciona puntuaciones de puntuación.

La puntuación global del Partner debe alcanzar al menos el 80% o la puntuación media de su segmento de mercado proporcionada por la propia herramienta, la que sea mayor.

Los Socios que no alcancen el puntaje deseado recibirán un informe de adecuación y cumplimiento del Grupo WEG para que el socio pueda tomar medidas para alcanzar el puntaje deseado dentro de los 180 días.

Además del procedimiento de registro descrito anteriormente, el socio debe seguir las siguientes pautas de seguridad de la información, también previstas en el documento de Autoevaluación enviado y mantenido por el área de Seguridad de la Información.

6.2.1. Privacidad

- Presentar a través de documentación el flujo de datos WEG en el entorno del Partner, conteniendo todo su ciclo de vida (recopilación, procesamiento, almacenamiento, intercambio y eliminación).
- Informar al Grupo WEG qué información se recopila, con qué finalidad, cuál es la base legal para el tratamiento de los datos, dónde se almacenan y por cuánto tiempo, buscando siempre minimizar el período de almacenamiento y la cantidad de información recopilada.

- Contar con una evaluación de impacto relacionada con los datos personales del titular (EIPD), así como contar con un proceso que otorgue al Grupo WEG acceso irrestricto a su información procesada y almacenada, prevista en el alcance del contrato.
- Contar con un proceso *de inclusión* y *exclusión* para la expresión previa y libre del Grupo WEG y de los titulares de datos personales sobre el intercambio a través de una asociación. También cabe destacar que el valor predeterminado debe ser no compartir. Solo después de la aceptación de la parte interesada, el socio podrá compartir datos con los socios.

6.2.2. Control de acceso

- Contar con un proceso de gestión de acceso debidamente documentado;
- Permitir al Grupo WEG el acceso ilimitado a los datos e informaciones almacenados o a ser tratados, de acuerdo con los servicios específicos definidos, valorando la confidencialidad, integridad, disponibilidad y recuperabilidad de estos datos e información;
- Dar visibilidad al Grupo WEG de los procedimientos y controles utilizados para cumplir con el contrato, como se describe en el punto anterior, en particular, para la identificación y segregación de los datos de los clientes del Grupo WEG, a través de controles físicos o lógicos;
- No permitir el uso de cuentas compartidas o usuarios genéricos para sistemas críticos, así como mantener controles relacionados con el inicio de sesión, tales como (pero no limitado a): forzar cambios en el primer acceso, bloquear al usuario después de una serie de ciertos intentos no válidos, requerir patrones de contraseña complejos y otras prácticas de seguridad de la información de acuerdo con los mejores estándares del mercado;
- Contar con un proceso formalizado y documentado para otorgar, cambiar y revocar el acceso, especialmente aquellos con acciones privilegiadas;
- Disponer de un proceso de control de la ausencia de segregación de funciones (SOD);
- Adoptar una política de privilegios mínimos;
- Disponer de métodos para el control de acceso físico y lógico de los visitantes; y
- Disponer de controles de acceso remoto para empleados/proveedores de servicios durante *los periodos de* teletrabajo.

6.2.3. Supervisión de los servicios y gestión de la operación de seguridad de la información

- Asegurar que cuenta con el más alto nivel de capacidad en el suministro de información y recursos de gestión adecuados para el seguimiento de los servicios a prestar, así como asegurar el cumplimiento de la legislación y normativa vigente;
- Informar y dar acceso al Grupo WEG, cuando así lo solicite, sobre los recursos de gestión adecuados para el seguimiento de los servicios contratados;
- Disponer de recursos y herramientas para monitorear la capacidad y disponibilidad de sus activos, correlacionar alertas y generar tickets de incidentes de forma automatizada;
- Contar con un proceso estructurado de respuesta a incidentes, que incluya la categorización de incidentes y *runbooks* para controlar y resolver incidentes conocidos.
- Prevenir, detectar y reducir incidentes relacionados con el entorno cibernético, evidenciando procedimientos y controles que abarquen, al menos, autenticación, cifrado, prevención y detección de intrusiones, prevención de fugas de datos, pruebas y escaneos periódicos para detectar

vulnerabilidades, aplicación de *parches* de seguridad, aplicación de *hardening* en sus servidores y estaciones de trabajo, la protección contra software malicioso y el bloqueo de software no aprobado, el establecimiento de mecanismos de trazabilidad y segmentación de la red informática, el mantenimiento de copias de seguridad de datos e información;

- WEG se reserva el derecho de revocar inmediata y unilateralmente cualquier acceso en caso de un incidente de seguridad o comportamiento anormal/inapropiado en el entorno de WEG que involucre al Socio, ya sea confirmado, bajo sospecha o bajo investigación;
- Proporcionar, cuando se solicite, información relacionada con el número de incidentes ocurridos en los últimos 24 meses, clasificándolos por su relevancia. Todos los datos sobre incidentes de gravedad "media", "alta" o "muy alta" deben ser almacenados por el Socio durante al menos 5 años; y
- Mantener permanentemente informado al Grupo WEG de cualquier limitación que pueda afectar la prestación de servicios o el cumplimiento de la legislación y normativa vigente.

6.2.4. Gestión de amenazas

El Socio se asegurará de que las vulnerabilidades de los sistemas informáticos se parcheen o actualicen de manera oportuna. En cualquier caso, el socio deberá:

a) Dentro de las 24 horas siguientes al descubrimiento de cualquier vulnerabilidad crítica (CVSS o CVE 9.0 o superior) en los sistemas informáticos pertinentes del grupo contratante que no haya sido proporcionada por un tercero:

- Comenzar el proceso de desarrollo e implementación de una actualización o parche para corregir la vulnerabilidad;
- Notifique al Grupo WEG en soc@weg.net y proporcione detalles sobre la vulnerabilidad y la amenaza relacionada, y que medidas há implementado el socio para mitigar la amenaza o vulnerabilidad.
- Asegurarse de que todos los sistemas de TI relevantes de los socios tengan instalados e implementados los últimos parches proporcionados por terceros; y
- Instale e implemente actualizaciones o parches para las vulnerabilidades incluidas en el catálogo de vulnerabilidades explotadas conocidas de la Agencia de Seguridad Cibernética y de Infraestructura de EE. UU. *dentro de las 24 horas posteriores al lanzamiento de la actualización o parche.* Si alguna actualización o parche no puede ser aplicado por cualquier motivo dentro de las 24 horas, el socio debe notificar inmediatamente al Grupo WEG dentro de soc@weg.net.

b) El Socio deberá:

- Garantizar que los sistemas de TI pertinentes se supervisen continuamente para garantizar su seguridad, autenticidad, confidencialidad, integridad y disponibilidad; y
- Generar continuamente los registros relevantes del sistema de TI necesarios para: (A) permitir la respuesta a incidentes; (B) identificar la fuente de un incidente; y (C) recrear la secuencia de eventos que condujeron a un incidente. El socio debe mantener estos registros de forma segura durante al menos 180 días a partir de la fecha de generación para que solo los usuarios autorizados puedan acceder a estos registros.

6.2.5. Seguridad en el desarrollo de sistemas

- Adopte prácticas *de privacidad y seguridad por diseño* en sus procesos de desarrollo de software;

- Describir las características de seguridad y los datos a los que acceden las aplicaciones, que deben ser evaluados por el área de Seguridad de la Información durante la fase de aprobación (Ej: Especificación Técnica y/o Diagrama Funcional);
- Utilizar rutinas de validación de integridad para evitar errores, ya sean involuntarios o intencionados, utilizando datos ficticios o anonimizaciones en un entorno no productivo;
- Adoptar prácticas de análisis de seguridad en el código fuente;
- Adoptar prácticas de análisis de seguridad en sus aplicaciones (Pruebas de Hacking Ético y pruebas de penetración);
- Proporcionar validaciones de seguridad en el proceso de calidad y verificación del código. Como mínimo, se deben tener en cuenta aquellos que aparecen en el TOP 10 de OWASP.

6.2.6. Continuidad del negocio, gestión, retención y almacenamiento de datos.

- Definir un programa de continuidad de negocio para asegurar que los posibles incidentes no afecten los servicios prestados al Grupo WEG, especialmente contemplando el plan de recuperación de desastres, probando regularmente los controles de aseguramiento con el fin de verificar cuán preparada está la empresa para casos reales;
- Informar y dar acceso al Grupo WEG, cuando así lo solicite, sobre las medidas de seguridad para la transmisión y almacenamiento de datos e información, así como su disposición, utilizando procedimientos de exclusión seguros (digitales y/o físicos);
- Contar con un proceso de ejecución de respaldos que se realice periódicamente sobre los activos que almacenan información del Grupo WEG, con el fin de evitar o minimizar la pérdida de datos en caso de incidentes.

6.2.7. Formación y sensibilización

- Asegurar la existencia de un programa de formación y concienciación en Seguridad de la Información y Privacidad de Datos, con una periodicidad mínima anual, para todos sus empleados, proveedores y prestadores de servicios, debiendo contemplarse la formación con la aplicación obligatoria del Código de Conducta de Partners para los empleados, proveedores y prestadores de servicios de nueva contratación.
- Incluir en su programa de formación y concienciación sobre Seguridad de la Información y Privacidad de Datos campañas de prevención del *phishing* y orientación sobre ingeniería social, así como charlas, emisión de boletines informativos de SI y Privacidad de Datos, etc.
- Los empleados, proveedores o prestadores de servicios de los socios que tengan acceso o procesen datos personales y/o información confidencial deben conocer esta Política y lo que concierne a la formación en seguridad de la información.

6.2.8. Servicios y certificaciones

El Socio deberá:

- Notificar, previa y formalmente, la subcontratación de servicios pertinentes al objeto del contrato con el Grupo WEG;
- Contar con reconocimientos de seguridad de la información o continuidad del negocio, comprobados por informes de auditoría externa independientes;

- Informar y dar acceso al Grupo WEG, cuando así lo solicite, sobre las certificaciones necesarias para la prestación de servicios, así como los informes relacionados con los controles utilizados en la prestación de los servicios contratados, elaborados por una firma auditora independiente especializada; y
- Contar con mecanismos para comunicar anomalías o incidentes de seguridad al Grupo WEG, a las Personas involucradas y a la Autoridad Nacional de Protección de Datos.

7. EVALUACIONES PERIÓDICAS

El Grupo WEG podrá realizar, siempre que lo considere necesario, evaluaciones para dar fe de la efectividad de la implementación de los controles presentados en este documento, y para tal fin, deberá notificar al socio con 30 días de anticipación. Las evaluaciones también pueden ocurrir en caso de un incidente de seguridad o cambio en las condiciones del mercado aplicables al segmento del socio o del Grupo WEG.

8. SANCIONES

La violación de un control o el incumplimiento de la Política de Seguridad de la Información para Socios y sus definiciones se consideran faltas o violaciones graves, y se pueden aplicar penalidades o sanciones aplicables de acuerdo con las políticas internas del Grupo WEG y/o previstas en el contrato.
En caso de violación de cualquier obligación o disposición de esta Política por parte del socio, sus empleados, proveedores, prestadores de servicios y/o cualquier persona relacionada con el socio, el asociado se compromete a indemnizar, eximir de responsabilidad, defender y eximir de responsabilidad al Grupo WEG de cualquier pérdida o daño, sin perjuicio de otras penalidades, sanciones y/o penalizaciones previstas en el contrato o por la ley.
El Socio reconoce y acepta que la mera indemnización puede no ser la forma adecuada para remediar cualquier violación de esta Política, y el Grupo WEG puede utilizar cualquier forma y/o medio de ejecución específica de obligaciones que pueda ser aplicable en caso de amenaza o violación efectiva de esta Asociación.