POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

HISTORIA DE REVISIONES

Fecha	Versión	Descripción	Autor
09-agosto-2017	01	Creación del documento	Andres Corredor
09-agosto-2017	01	Revisión del documento	Leidy Viviana Rico
11-agosto-2017	01	Aprobación del documento	Jairo León

I. ALCANCE

El presente documento reúne las Políticas de Seguridad que deben cumplir los proveedores que tengan acceso a la información de PEOPLE PASS S.A. e intercambien, procesen, almacenen, modifiquen o creen nueva información confidencial propiedad de PEOPLE PASS S.A., o los que utilicen sus equipos de cómputo en la red de PEOPLE PASS S.A., esto con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por PEOPLE PASS S.A.

II. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política es un documento anexo al contrato u oferta que regula la relación contractual. El proveedor deberá cumplir lo siguiente:

1.
Todo proveedor y/o tercero que tenga acceso a los activos de información y preste servicios a PEOPLE PASS S.A. debe contar con políticas, normas y estándares de Seguridad de la Información al interior de su organización; las cuales deben desarrollarse y mantenerse actualizadas acorde con los riesgos a los que se ve enfrentada su organización.

2.
Proteger la confidencialidad, integridad y disponibilidad de la información propiedad de PEOPLE PASS S.A., así como la de sus clientes y terceros, cuando los servicios contratados así lo requieran; siempre que sea generada, almacenada o procesada como parte del desarrollo de la relación contractual que lo une a PEOPLE PASS S.A.

3.
Los proveedores sólo podrán desarrollar para PEOPLE PASS S.A. aquellas actividades cubiertas bajo el correspondiente contrato de prestación del servicio u otro equivalente.

4.
La disponibilidad se rige por los acuerdos de niveles de servicio que estén explícitos en el marco del contrato u oferta que se haya establecido; en caso de no existir un acuerdo de nivel de servicio explícito, EL PROVEEDOR deberá actuar con la máxima diligencia para que la información de PEOPLE PASS S.A. esté disponible cuando PEOPLE PASS S.A. lo requiera.

5.
Utilizar software legalmente adquirido, en cumplimiento de la Ley 603 de 2000 o las normas que la reemplacen, modifiquen o adicionen. Para el efecto mantendrá indemne a PEOPLE PASS S.A. de cualquier tipo de reclamación en tal sentido, y en caso de que PEOPLE PASS S.A. se vea obligada a pagar algún tipo de sanción por el incumplimiento de la citada disposición, EL PROVEEDOR se compromete a reembolsar a PEOPLE PASS S.A., la totalidad de los gastos en que haya incurrido.

6.
Todo Proveedor y/o tercero que preste el servicio de desarrollo de Software a PEOPLE PASS S.A. debe implementar normas o las mejores prácticas de la industria en el desarrollo de las aplicaciones para garantizar la seguridad de los sistemas.

7.
Todo Proveedor y/o tercero que preste el servicio de desarrollo de Software a PEOPLE PASS S.A. antes de enviar una aplicación a producción o ponerla a disposición de PEOPLE PASS S.A., debe realizar la revisión de los códigos fuente a través de un procedimiento manual o automático que permita identificar posibles vulnerabilidades en la codificación y su correspondiente solución. La no verificación de este procedimiento no exime a EL PROVEEDOR de su responsabilidad.

8.
Hacer extensivo el acuerdo de confidencialidad y estás políticas a los funcionarios y terceros involucrados en el desarrollo de la relación contractual.

9.
Informar a PEOPLE PASS S.A. los cambios o la instalación de nueva infraestructura tecnológica y/o física que haga parte del procesamiento de información de propiedad de PEOPLE PASS S.A., sus clientes y/o terceros.

10.
Colaborar y permitir a PEOPLE PASS S.A. realizar auditorías sobre la infraestructura tecnológica y/o física que soporta la prestación de los servicios que hacen parte de la relación contractual, auditorías que deberán ser avisadas a EL PROVEEDOR con tres (3) días calendario de antelación, indicando los nombres y documentos de identidad de las personas que las realizarán que podrán ser trabajadores o personal externo autorizado de PEOPLE PASS S.A. Para efectuar estas auditorías, las Partes tendrán en cuenta el cumplimiento del acuerdo de confidencialidad firmado entre ellas y con terceros. EL PROVEEDOR se compromete a poner a disposición de PEOPLE PASS S.A. a personal de EL PROVEEDOR que permita realizar las verificaciones correspondientes, así como documentación (física, digital) e infraestructura que facilite el desarrollo de la auditoría en buen término.

11.
EL PROVEEDOR se obliga a contratar personal con las capacidades profesionales o técnicas requeridas para la relación contractual con PEOPLE PASS S.A. , en consecuencia, en el

proceso de selección del personal que se requiera para el desarrollo de la relación contractual, EL PROVEEDOR debe hacer una verificación de datos de la hoja de vida, referencias y antecedentes de los candidatos involucrados en la relación contractual, además de lo estipulado en las políticas internas de contratación del personal de EL PROVEEDOR.

12.
Establecer con PEOPLE PASS S.A. el procedimiento adecuado para el borrado seguro de la información propiedad de PEOPLE PASS S.A., sus clientes y/o terceros. Este procedimiento deberá ser desarrollado antes o durante el transcurso de la relación contractual.

13.
Controlar la salida de información propiedad de PEOPLE PASS S.A. que se encuentre alojada bajo los dispositivos que administra y controla EL PROVEEDOR, estos controles deberán ser notificados a PEOPLE PASS S.A. durante el transcurso de la relación contractual.

14.
Informar a PEOPLE PASS S.A. cualquier fuga, pérdida o alteración de información de propiedad de PEOPLE PASS S.A., sus clientes y/o usuarios y la correspondiente medida de mitigación.

15.
Intercambiar la información confidencial de PEOPLE PASS S.A. de forma segura, cifrándola de acuerdo con los procedimientos de PEOPLE PASS S.A.

16.
EL PROVEEDOR evitará la revelación, modificación, destrucción o mal uso de la información relacionado con el servicio prestado a PEOPLE PASS S.A.

17.
Todo Proveedor y/o tercero que preste el servicio de alojamiento u otro servicio en la nube a PEOPLE PASS S.A. debe garantizar la segmentación de la red con el fin de restringir la entrada o salida de internet de los servidores o servicios prestados a PEOPLE PASS S.A. que no se encuentren en el segmento de la Zona Desmilitarizada DMZ.

18.
EL PROVEEDOR responde directamente por el acceso que sus empleados tengan a documentos confidenciales de PEOPLE PASS S.A. y deberá entenderse que este acceso es estrictamente temporal, sin otorgarle derecho alguno de titularidad o copia sobre dicha información. Así mismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación contractual entre EL PROVEEDOR y PEOPLE PASS S.A.

19.
Todo Proveedor y/o tercero que preste el servicio de alojamiento u otro servicio en la nube a PEOPLE PASS S.A. debe realizar análisis de vulnerabilidades internas y externas sobre los servidores y dispositivos de red internos y externos que le prestan el servicio a PEOPLE PASS S.A., este análisis de vulnerabilidades debe ser trimestral y después de implementar una actualización o modificación significativa, mediante métodos manuales o automáticos según los estándares de la industria. Cada vez que se lleve a cabo esta actividad, EL PROVEEDOR deberá presentar un informe con los resultados a PEOPLE PASS S.A.

20.
Todo Proveedor y/o tercero que preste el servicio de alojamiento u otro servicio en la nube a PEOPLE PASS S.A. deben realizar pruebas de penetración internas y externas sobre la infraestructura y aplicaciones que le prestan el servicio a PEOPLE PASS S.A. mínimo una vez al año y después de implementar una actualización o modificación en la infraestructura o aplicaciones, las cuales deberán efectuarse por personal calificado y según los estándares de la industria. Cada vez que se lleve a cabo esta actividad, EL PROVEEDOR deberá presentar un informe con los resultados a PEOPLE PASS S.A.

21.
TTodo Proveedor y/o tercero que preste el servicio de alojamiento u otro servicio en la nube a PEOPLE PASS S.A. debe contar con los sistemas actualizados y las remediaciones de las vulnerabilidades críticas y altas encontradas de los sistemas que le prestan el servicio a PEOPLE PASS S.A. En consecuencia, debe notificar a PEOPLE PASS S.A. los cambios que implementar,

solicitando a PEOPLE PASS S.A. autorización para establecer el día, fecha y hora en que sea posible efectuarla, con el objeto de no afectar la disponibilidad de los servicios de PEOPLE PASS S.A.

22.
Todo proveedor y/o tercero que esté relacionado con los procesos y activos críticos para el negocio de PEOPLE PASS S.A., debe contar con Controles para evitar ataques contra la seguridad de la información y Plan de Contingencia y Continuidad del Negocio para los servicios prestados a PEOPLE PASS S.A.

23. Se prohíbe expresamente:

El uso de los recursos proporcionados por PEOPLE PASS S.A. para actividades no relacionadas con el servicio contratado.

La conexión a la red de PEOPLE PASS S.A. de equipos y/o aplicaciones que no estén autorizados por el Ingeniero de Seguridad de la Información.

Introducir en los Sistemas de Información o la Red de PEOPLE PASS S.A. contenidos inadecuados, obscenos, amenazadores, inmorales u ofensivos.

Introducir voluntariamente en la red de PEOPLE PASS S.A. cualquier tipo de malware (programas, macros, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo el personal o sistema con acceso a la red de PEOPLE PASS S.A. tendrá la obligación de utilizar los programas antivirus licenciados con su base de firmas actualizado.

Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que PEOPLE PASS S.A. les haya asignado.

Intentar distorsionar o falsear los registros "log" de los Sistemas de Información de PEOPLE PASS S.A.

25.
Todo proveedor y/o tercero que preste servicios a PEOPLE PASS S.A. debe cumplir con las regulaciones locales e internacionales de privacidad y seguridad de la información.

26.

Para reportar un evento sospechoso o un incidente de seguridad asociado a las actividades desarrolladas por PEOPLE PASS S.A., sus clientes y/o sus terceros, por favor póngase en contacto con el Ingeniero de Riesgo y Seguridad de la Información de PEOPLE PASS S.A. a través de los siguientes canales de comunicación:

Teléfono *+57(1) 7434700*.
Extensión *229*.

III. DOCUMENTOS ANEXOS

EL PROVEEDOR acepta y reconoce los siguientes anexos a la presente Política:
a.Procedimiento de Borrado Seguro de la Información;
b.Procedimiento de Cifrado de la Información.
Las Partes suscriben el presente documento como aceptación de cumplimiento de las políticas de seguridad.

POR PEOPLE PASS S.A.

_____

Nombre Rep. Legal:
Cc:
PEOPLE PASS S.A.
Nit: 900296669-1

POR EL PROVEEDOR

_____

Nombre Rep. Legal:
Cc:

Nit:

peoplepass
La más efectiva forma de dar bonos