OBJETIVO

La política de seguridad para las relaciones con los proveedores tiene como objetivo establecer las directrices y los requisitos de seguridad de la información entre Gestión de Seguridad Electrónica S.A.– GSE y sus proveedores y/o terceros, de acuerdo con su clasificación, con el fin de salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información.

Adicionalmente, se buscar asegurar que toda relación con proveedores, y en particular con aquellos que tienen acceso a la información de GSE, se encuentre debidamente protegida con base a los acuerdos y contratos correspondientes, independientemente del servicio proporcionado o relación que lo vincule con GSE.

ALCANCE

El presente documento aplica a los proveedores y terceros que brinden servicios a Gestión de Seguridad Electrónica S.A. de acuerdo con su clasificación, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la seguridad de la información.

RESPONSABLES

Los usuarios de esta política son la alta dirección y las personas pertenecientes a:

- Equipo de Compras
- Supervisores de Contrato
- Equipo del SIGR

GENERALIDADES

Los requisitos de seguridad y privacidad de la información necesarios para la mitigación de los posibles riesgos asociados con el acceso de proveedores a los activos de información de la compañía deben ser acordados y documentados entre GSE y el proveedor de tal manera que se asegure la protección de los activos de la compañía.

SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES

Esta política se considera como un documento anexo al contrato, oferta u orden de compra que regula la relación contractual. En desarrollo de esta política, EL

PROVEEDOR deberá tener en cuenta todo lo establecido y en especial deberá cumplir con lo siguiente:

- Proteger la confidencialidad, integridad, disponibilidad y privacidad de la información propiedad de GSE, 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 relacione a GSE.
- Deben contar con políticas, normas y/o 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.
- La disponibilidad se rige por los acuerdos de niveles de servicio que se especifiquen en el marco del contrato, oferta u orden de compra 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 GSE esté disponible cuando GSE lo requiera.
- Hacer extensivo el acuerdo de confidencialidad y estas políticas a sus funcionarios y terceros involucrados en el desarrollo de la relación contractual.
- Los Proveedores y/o terceros que presten el servicio de desarrollo de software a GSE deben implementar normas o las mejores prácticas de la industria en el desarrollo de las aplicaciones y acogerse e implementar el manual de desarrollo seguro de GSE, para garantizar la seguridad de los sistemas.
- Los Proveedores y/o terceros que presten el servicio de desarrollo de software a GSE antes de enviar una aplicación a producción o ponerla a disposición de GSE, deberán 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, en todo caso, no deberán entregar aplicaciones con vulnerabilidades críticas, altas, ni medias. La no verificación de este procedimiento no exime a EL PROVEEDOR de su responsabilidad.
- Los Proveedores y/o terceros que presten el servicio de desarrollo de software deberán utilizar software legalmente adquirido, en cumplimiento de la Ley 603 de 2000 o las normas que la reemplacen, modifiquen o adicionen.
- Para la adquisición de software a la medida, el proveedor deberá realizar las pruebas pertinentes siguiendo los parámetros establecidos en política de desarrollo seguro GSE.
- Los proveedores y/o terceros que presten servicios a GSE deben cumplir con las regulaciones locales e internacionales de privacidad y seguridad de la información, así como la ley de protección de datos personales.

- EL PROVEEDOR evitará la revelación, modificación, destrucción o mal uso de la información relacionada con el servicio prestado a GSE.
- En caso de ser requerido por norma o Ley, o en aquellos casos que GSE considere pertinente, se ejecutaran auditorías de tercera parte a los proveedores.
- En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.
- Se establece llevar a cabo el seguimiento periódico de conformidad al procedimiento de evaluación de proveedores, considerando el tipo de proveedor, acuerdos de niveles de servicio y criticidad de la información que maneja.
- Cuando se considere pertinente, para proveedores clasificados de impacto crítico en seguridad de la información se evaluará el plan de continuidad del proveedor junto con las pruebas realizadas.
- Los empleados de Gestión de Seguridad Electrónica que funjan como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas, así mismo, deberán acogerse a las recomendaciones que se emitan como resultado de las auditorias que GSE o terceros realicen sobre los mismos.
- Los controles de acceso físico o lógicos con los cuales los proveedores de GSE deben cumplir, tendrán que estar documentados y aprobados, además de ser de conocimiento de ambas partes.
- Los proveedores, dependiendo de su clasificación, deberán reportar los incidentes de seguridad de la información al oficial de seguridad de la información.
- GSE podrá realizar o solicitar auditorias sobre los sistemas informáticos del proveedor, dependiendo de su clasificación para garantizar el cumplimiento de los parámetros establecidos en las políticas de desarrollo seguro.
- Toda información reservada o confidencial suministrada por parte GSE, deberá ser tratada de acuerdo con la política y procedimiento de transferencia de la información GSE y/o ley 1581 de 2012.

CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

- Para toda adquisición de software y hardware que GSE realiza, es responsabilidad del proceso de Tecnología, en conjunto con seguridad y privacidad de la información, definir los requisitos de seguridad de acuerdo con el procedimiento de compras.
- Los proveedores clasificados de impacto crítico que contratan externamente servicios de otras compañías, y que estén relacionados con el suministro de tecnología de información y comunicación que prestan a GSE, deben asegurar que los requisitos y buenas prácticas de seguridad implementadas por GSE sean extensivos a sus terceros que intervengan directamente con los servicios prestados a GSE.
- Cada proveedor que sea contratado por GSE debe diligenciar el Anexo de Seguridad de la Información.
- Se debe garantizar que la infraestructura y/o servicio suministrado tenga controles de seguridad que permita mitigar la perdida de la confidencialidad, integridad, disponibilidad y privacidad de la información.

PROHIBICIONES

- El uso de los recursos proporcionados por GSE para actividades no relacionadas con el servicio contratado.
- La conexión a la red de GSE de equipos y/o aplicaciones que no estén autorizados por el proceso de Seguridad de la Información.
- Introducir en los Sistemas de Información o la Red de GSE contenidos inadecuados, obscenos, amenazadores, inmorales u ofensivos, ilegales y sin licenciamiento ni derechos de autor.
- Introducir voluntariamente en la red de GSE 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 GSE tendrá la obligación de utilizar programas antivirus licenciados comercialmente, con su base de firmas actualizado.
- Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que GSE les haya asignado.
- Intentar distorsionar los registros “log” de los sistemas de Información de GSE

GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES

Cuando se presentan cambios GSE establece y notifica los cambios que se generaron o se estimen realizar con respecto a los acuerdos contractuales iniciales, de acuerdo con lo establecido en el Procedimiento de evaluación de proveedores.

DOCUMENTOS DE REFERENCIA

- Norma Técnica Colombiana NTC-ISO/IEC 27001 en la versión vigente.
- Guía Técnica Colombiana GTC- ISO/IEC 27002 en la versión vigente.
- Criterios Específicos de acreditación entidades de Certificación especial CEA- ONAC-3.0.07
- Procedimiento de Compras
- Procedimiento Gestión del Cambio

REVISIÓN DE LA POLÍTICA

Esta política se debe revisar a intervalos planificados de un año, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.

ALVARO DE BORJA CARRERAS AMOROS

Firmado digitalmente por ALVARO DE BORJA CARRERAS AMOROS
Fecha: 2024.05.20 17:44:12 -05'00'

Presidente
Gestión de Seguridad Electrónica S.A

CONTROL DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	CARGO	CAMBIO
4	19/10/2022	Oficial de Seguridad de la Información	Se ajusta la codificación del documento, por el cambio de subproceso a macroproceso para Seguridad de la Información
			Se ajusta el objetivo del documento.
			Se ajusta el alcance del documento
			Se agrega en responsables al equipo de Seguridad de la Información
			Se ajustan las generalidades del documento. Se elimina el párrafo de Controles de seguridad de la información con proveedores. Se agrega el titulo Prohibiciones con su contenido. Se ajusta la versión del CEA en el documento
5	25/04/2024	Oficial de Seguridad de la Información	Se incluyen conceptos de privacidad de la información (protección de datos personales), actualización de la ISO 27001, se ajusta formato y código.