

MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE RELACIONES CON PROVEEDORES

Esta política tiene como finalidad garantizar la protección de los activos de información de STI que son accesibles por los proveedores de servicio, en la presente política se define los siguientes aspectos:

1. Política de seguridad de la información para las relaciones con los proveedores

- Todo proveedor de servicio que brinde servicios a STI, debe suscribir un acuerdo de confidencialidad, la misma que será parte del contrato de prestación de servicios como anexo.
- Los proveedores de servicio sólo podrán desarrollar para STI, aquellas actividades cubiertas bajo el correspondiente contrato u orden de prestación de servicios.
- El proveedor de servicio debe proporcionar los datos completos de la persona de contacto, quien se encarga de recibir todo tipo de información referente a seguridad de la información.
- El proveedor de servicio proporciona, mientras dure la vigencia del contrato, la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informa cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
- Todo proveedor de servicio debe velar que su personal que presta los servicios directamente a STI, cumpla con las políticas de seguridad de la información recogidas en el presente documento. En caso de incumplimiento, STI se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de STI de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.
- Cualquier tipo de intercambio de información que se produzca entre STI y el proveedor de servicio se debe entender que ha sido realizado dentro del marco establecido por el contrato u orden de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.
- Todo proveedor de servicio que tenga acceso a la información de STI en ejecución de un contrato u orden de prestación de servicios, debe considerar que dicha información, es confidencial y sujeto a la Ley de Protección de Datos Personales.
- Ningún proveedor de servicio puede utilizar la información de STI para beneficio propio o de terceros. La información a la que tenga acceso el proveedor únicamente puede ser utilizada para los fines específicamente indicados en el contrato u orden de prestación de servicios. Toda información proporcionada por STI, sigue siendo de propiedad de esta última.
- El proveedor de servicio y su personal únicamente puede utilizar la información y activos tecnológicos autorizados por STI para el desarrollo de los servicios contratados.
- La distribución de la información ya sea en formato digital o papel, se realiza mediante los recursos determinados en el contrato de prestación de servicios y para la finalidad exclusiva de facilitar las funciones asociados a dicho contrato.
- STI, se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre los recursos de difusión.
- Los recursos que STI que pone a disposición del proveedor de servicio, independientemente del tipo que sean, (informáticos, datos, software, redes, Sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. STI se reservan el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

2. Abordar la seguridad dentro de los acuerdos con proveedores

- En los contratos suscritos con proveedores o terceros que presten sus servicios a STI se deben establecer y acordar los requisitos de seguridad que debe cumplir el proveedor o tercero para poder tener acceso, procesar, almacenar, comunicar información de STI o para el suministro de componentes de infraestructura tecnológica a STI. En los acuerdos se deben incluir las medidas necesarias para el tratamiento de los riesgos de seguridad de la información derivados de las

actividades realizadas por el proveedor o tercero. Los acuerdos deben ser formalizados antes del inicio de las actividades con el proveedor o tercero.

- Al finalizar sus contratos los proveedores o terceros que presten sus servicios a STI deben efectuar la devolución de información o activos de información propiedad de STI que estuvieron bajo su responsabilidad y procurar la destrucción o borrado seguro de información confidencial conocida en razón de su actividad.
- Los proveedores y terceros que presten sus servicios a STI deben cumplir con la reglamentación en materia de derechos de autor y propiedad intelectual, incluido, pero no limitado al uso de información y software.
- Los proveedores y terceros que presten sus servicios a STI no están autorizados para utilizar los recursos de información y tecnológico de STI para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.
- No está autorizada la utilización de equipos informáticos dentro de las redes de comunicaciones de STI que no cumplan con los controles de seguridad especificados por el sistema de gestión de seguridad de la información de STI.
- Todo término de referencia o especificación técnica que elabore el área usuaria, y que éste contemple la gestión, transformación o transmisión de información de STI, debe incluir un acápite que mencione que el proveedor o tercero firmará un acuerdo de confidencialidad al inicio de la prestación del servicio.
- No está autorizada la modificación o desactivación de los controles de seguridad instalados en los componentes de información y tecnología de STI sin contar con autorización del responsable del área usuaria que utilizan el recurso informático.

3. Cadena de suministro de tecnología de información y comunicación

- Los terceros que reciban información de STI deben garantizar que aplicarán todas las medidas de seguridad razonables a su alcance, para evitar divulgación, fuga o uso no autorizado de información y deben aceptar que protegerán la información suministrada aplicando los controles que se especifiquen al momento de la entrega de la información.

4. Monitoreo y revisión de servicios de los proveedores

- Los trabajadores deben reportar al área de Logística, a través de sus responsables de área usuaria, el incumplimiento de las condiciones contractuales en la prestación de servicios contratados con proveedores o terceros.