| | |
|---|---|
| | Código: GCCON-AN-001 |
| | Versión: 07 |

**PROCESO**

**GESTIÓN CONTRACTUAL**

**NOMBRE DEL FORMATO**

**Formato Anexo De Verificación y Evaluación del Cumplimiento de Requisitos Legales SIGA**

**CLASIFICACIÓN DE LA INFORMACIÓN**

| | | | | | |
|---|---|---|---|---|---|
| **Pública** | X | **Publica Clasificada** | | **Publica Reservada** | |

| | |
|---|---|
| **CONTRATO No.:** | **NOMBRE DE PROVEEDOR:** |
| **VIGENCIA DEL CONTRATO:** | **NOMBRE DEL SUPERVISOR DE CONTRATO:** |

**OBJETO: PRESTACIÓN DE SERVICIOS PARA LA ELABORACIÓN E INSTALACIÓN DE UN AVISO CON LA IMAGEN CORPORATIVA DE LA AGENCIA PÚBLICA DE EMPLEO DEL SENA REGIONAL CASANARE, DE ACUERDO CON EL MANUAL CORPORATIVO DE MARCA, EN LAS INSTALACIONES DE LA OFICINA PRINCIPAL DE YOPAL**

| | |
|---|---|
| **ASPECTO(S) AMBIENTAL(ES) ENERGÉTICO (S)**<br>- Generación de residuos peligrosos y especiales<br>- Consumo de recursos (arena, grava, arcilla/ madera)<br>- Consumo de sustancias químicas<br>- Generación de emisiones<br>- Emergencia por potencial derrame<br>- Potencial de lesiones o afectaciones a la salud<br>- Consumo de Energía<br>- Consumo de Agua | **RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO:**<br>- Riesgos de Seguridad: Materialización de accidente de trabajo<br>- Riesgo: Eléctrico/Energías peligrosas/trabajo en alturas/espacios confinados/ accidentes de transito.<br>- Riesgo Físico<br>- Riesgo Químico<br>- Riesgo Psicosocial<br>- Riesgo Locativo<br>- Riesgo Biológico<br>- Riesgo Mecánico<br>- Riesgo Biomecánicos<br>- Riesgo Publico<br>- Riesgo Tecnológico: Incendio y explosión<br>- Riesgos por Fenómenos Naturales |

| DESCRIPCIÓN DEL CRITERIO | ETAPA | CUMPLIMIENTO | | | OBSERVACIONES |
|---|---|---|---|---|---|
| | | SI | NO | N/A | (Indique aquí el documento que soporta su respuesta o la razón de que no aplique la disposición) |
| **CUMPLIMIENTO DE REQUISITOS LEGALES SG-SST APLICABLES A TODOS LOS CONTRATOS DE BIENES Y SERVICIOS** | | | | | |
| **Opción 1:**<br>1. Certificado de implementación del SG-SST firmada por el Representante Legal y Responsable del SG-SST<br><br>2. Fotocopia de cédula, Certificado Vigente Curso de SG-SST de 50 Horas o su actualización y/o Curso de 20 Horas y licencia de seguridad y salud en el trabajo del profesional del Responsable del SG-SST.<br><br>3. Certificación de autoevaluación de estándares mínimos emitido por ARL. | Precontractual | X | | | |
| **Personas Independientes:** Certificación Firmada por el representante legal donde indique que es persona natural que no tiene trabajadores a cargo y no esta obligada a implementar el Sistema de gestión de la seguridad y salud en el trabajo.<br><br>**Nota: De acuerdo con la resolución 0312 de 2019 en el *Parágrafo 2* . No están obligados a implementar los Estándares Mínimos los trabajadores independientes con afiliación voluntaria al Sistema General de Riesgos Laborales de que trata la Sección 5 del Capítulo 2 del Título 4 de la Parte 2 del Libro 2 del Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo. | Precontractual | X | | | |

| **Normatividad Seguridad y Salud en el Trabajo** |
|---|
| Resolución 2400 de 1979 - Por la cual se establecen algunas disposiciones sobre vivienda, higiene y seguridad en los establecimientos de trabajo. Incluye las características que deben cumplir estos establecimientos y también normas generales sobre riesgos físicos, químicos y biológicos. |
| Ley 9 de 1979 - Por la cual se dictan medidas sanitarias. |
| Resolución 2013 de 1986 - Por la cual se reglamenta la organización y funcionamiento de los Comités de Medicina, Higiene y Seguridad Industrial en los lugares de trabajo |
| Resolución 1792 de 1990 - Por la cual se adoptan valores límites permisibles para la exposición ocupacional al ruido. |
| Decreto Ley 1295 de 1994 - Sistema General de Riesgos Profesionales. |
| Ley 1010 de 2006 - Por medio de la cual se adoptan medidas para prevenir, corregir y sancionar el acoso laboral y otros hostigamientos en el marco de las relaciones de trabajo |
| Resolución 1401 de 2007 - Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo. |
| Resolución 2346 de 2007 - Por la cual se regula la práctica de evaluaciones médicas ocupacionales y el manejo y contenido de las historias clínicas ocupacionales. |
| Resolución 2646 de 2008 - Por la cual se establecen disposiciones y se definen responsabilidades para la identificación, evaluación, prevención, intervención y monitoreo permanente de la exposición a factores de riesgo psicosocial en el trabajo y para la determinación del origen de estas. |
| Resolución 1956 de 2008 - Adopta medidas frente al consumo de cigarrillo y tabaco. Establece espacios libres de humo y sustancias psicoactivas en la empresa. |
| Circular 0038 de 2010 - Adopta medidas frente al consumo de cigarrillo y tabaco. Establece espacios libres de humo y sustancias psicoactivas en la empresa. |
| Resolución 0652 de 2012 - Por la cualquier se establece la conformación y funcionamiento del Comité de Convivencia Laboral en entidades públicas y empresas privadas y se di tan otras disposiciones. |
| Resolución 1356 de 2012 - Modifica parcialmente la resolución 652 de 2012 |
| Ley 1562 de 2012 - Por la cual se modifica el Sistema de Riesgos Laborales y se dictan otras disposiciones en materia de salud ocupacional |
| Resolución 4272 de 2021 - Por la cual se establecen los requisitos mínimos de seguridad para el desarrollo de trabajo en alturas. |
| Ley 1616 de 2013 Art 9 - Promoción de la salud mental y prevención del trastorno mental en el ámbito laboral. |
| Decreto 1477 de 2014 - Expide la Tabla de Enfermedades Laborales, que tendrá doble entrada: i) agentes de riesgo, para facilitar la prevención de enfermedades en las actividades laborales, y ii) grupos de enfermedades, para determinar el diagnóstico médico en los trabajadores afectados. |
| Resolución 3368 de 2014 - Modifica el reglamento para protección contra caídas de trabajo en alturas. |
| Decreto 1072 de 2015 - Decreto Único Reglamentario del Sector Trabajo |
| Decreto 472 de 2015 - Establece los criterios de graduación de las multas por infracción a las normas de Seguridad y Salud en el Trabajo y Riesgos Laborales |
| Decreto 052 de 2017 - Modifica el artículo 2.2.4.6.37. del Decreto 1072 de 2015 Decreto Único Reglamentario del Sector Trabajo, sobre la transición para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) |
| Decreto 1496 del 06 de agosto de 2018: Por la cual se adopta el sistema globalmente armonizado para clasificación y etiquetado de productos químicos en Colombia. |
| Resolución 0312 de 2019 - Por la cual se definen los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST |
| Resolución 2404 de 2019 - Se adopta la Batería de Instrumentos para la Evaluación de Factores de Riesgo Psicosocial, la Guía técnica para la promoción, prevención e intervención de los factores psicosociales y sus efectos en la población |
| Resolución 0491 de 2020 - Reglamento trabajo seguro en espacios confinados |
| Circular 063 de 2020 - Actualización curso 50 horas SGSST |
| Circular 0064 de 2020 - Gestión Psicosocial y prevención de salud mental |
| Resolución 773 de 2021 - Se definen las acciones que deben desarrollar los empleadores para la aplicación del Sistema Globalmente Armonizado (SGA) de Clasificación y Etiquetado de Productos Químicos en los lugares de trabajo y se dictan otras disposiciones en materia de seguridad química. |
| Resolución 754 de 2021 - Por la cual se establecen los requisitos y el procedimiento para la expedición y renovación de la Licencia de Seguridad y Salud en el Trabajo |
| Resolución 4272 de 2021 Por la cual se establecen los requisitos mínimos de seguridad para el desarrollo de trabajo en alturas. |
| Resolución 40595 de 2022 - Por la cual se adopta la metodología para el diseño, implementación y verificación de los Planes Estratégicos de Seguridad Vial y se dictan otras disposiciones. |

| | |
|---|---|
| | Código: GCCON-AN-001 |
| | Versión: 07 |

| PROCESO |
|---|
| GESTIÓN CONTRACTUAL |
| NOMBRE DEL FORMATO |
| Formato Anexo De Verificación y Evaluación del Cumplimiento de Requisitos Legales SIGA |

| CLASIFICACIÓN DE LA INFORMACIÓN | | | | | |
|---|---|---|---|---|---|
| **Pública** | X | **Pública Clasificada** | | **Pública Reservada** | |

| | |
|---|---|
| **CONTRATO No/PROCESO No.:** | **NOMBRE DE PROVEEDOR/OFERENTE:** |
| **VIGENCIA DEL CONTRATO/PROCESO:** | **NOMBRE DEL SUPERVISOR DE CONTRATO:** |
| **OBJETO:PRESTACIÓN DE SERVICIOS PARA LA ELABORACIÓN E INSTALACIÓN DE UN AVISO CON LA IMAGEN CORPORATIVA DE LA AGENCIA PÚBLICA DE EMPLEO DEL SENA REGIONAL CASANARE, DE ACUERDO CON EL MANUAL CORPORATIVO DE MARCA, EN LAS INSTALACIONES DE LA OFICINA PRINCIPAL DE YOPAL** | |
| **ASPECTO(S) AMBIENTAL(ES) ENERGÉTICO (S)**<br>- Generación de residuos no peligrosos<br>- Generación de vertimientos<br>- Consumo de energía / gas<br>- Consumo de agua<br>- Consumo de químicos<br>- Consumo de insumos<br>- Potencial de lesiones o afectaciones a la salud. | **RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO**<br>- Consumo de alimentos y bebidas<br>- Viabilidad de enfermedades trasmitidas por alimentos (ETA) e intoxicaciones alimentarias.<br>- Riesgos de Seguridad: Materialización de accidente de trabajo<br>- Riesgo: Eléctrico/Energías peligrosas/trabajo en alturas/espacios confinados/ accidentes de transito.<br>- Riesgo Físico<br>- Riesgo Químico<br>- Riesgo Psicosocial<br>- Riesgo Locativo: Caídas a mismo y a diferente nivel.<br>- Riesgo Biológico<br>- Riesgo Mecánico<br>- Riesgo Biomecánico<br>- Riesgo Publico<br>- Riesgo Tecnológico: Incendio y explosión<br>- Riesgos por Fenómenos Naturales |

| | | | | | | |
|---|---|---|---|---|---|---|
| Relación del personal que ingresa a las instalaciones con su respectivo pago de seguridad social, certificados de afiliación a EPS, AFP y ARL, de manera mensual los primeros 5 días del mes.<br><br>Nota: Aplicable únicamente cuando se requiere ingreso de personal externo a la entidad para el cumplimiento de contrato. | Contractual | Sistema de Gestión de Seguridad y salud en el trabajo | **X** | | | |
| Listado de trabajadores que desarrollen actividades de trabajo en alturas, con su respectivo Certificado vigente de trabajo en alturas avanzado y reentrenamiento acorde a requerimientos de la normatividad vigente. (SI APLICA) | Contractual | Sistema de Gestión de Seguridad y salud en el trabajo | **X** | | | |
| Listado de trabajadores que desarrollen actividades de trabajo en espacios confinados, con su respectivo Certificado vigente de Trabajador entrante en espacios confinados acorde a requerimientos de la normatividad vigente. (SI APLICA) | Contractual | Sistema de Gestión de Seguridad y salud en el trabajo | **X** | | | |

| | |
|---|---|
| | Código: GCCON-AN-001 |
| | Versión: 07 |

| PROCESO |
|---|
| GESTIÓN CONTRACTUAL |
| **NOMBRE DEL FORMATO** |
| **Formato Anexo De Verificación y Evaluación del Cumplimiento de Requisitos Legales SIGA** |

| CLASIFICACIÓN DE LA INFORMACIÓN | | | | | |
|---|---|---|---|---|---|
| **Pública** | x | **Pública Clasificada** | | **Pública Reservada** | |

| | |
|---|---|
| **CONTRATO No./PROCESO No.:** | **NOMBRE DE PROVEEDOR/OFERENTE:** |
| **VIGENCIA DEL CONTRATO/PROCESO:** | **NOMBRE DEL SUPERVISOR DE CONTRATO:** |

**OBJETO:** PRESTACIÓN DE SERVICIOS PARA LA ELABORACIÓN E INSTALACIÓN DE UN AVISO CON LA IMAGEN CORPORATIVA DE LA AGENCIA PÚBLICA DE EMPLEO DEL SENA REGIONAL CASANARE, DE ACUERDO CON EL MANUAL CORPORATIVO DE MARCA, EN LAS INSTALACIONES DE LA OFICINA PRINCIPAL DE YOPAL

| | |
|---|---|
| **ASPECTO(S) AMBIENTAL(ES) ENERGÉTICO (S)**<br>- Generación de residuos peligrosos y especiales<br>- Consumo de recursos (arena, grava, arcilla/ madera)<br>- Consumo de sustancias químicas<br>- Generación de emisiones<br>- Emergencia por potencial derrame<br>- Potencial de lesiones o afectaciones a la salud<br>- Consumo de Energía<br>- Consumo de Agua | **RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO**<br>- Consumo de alimentos y bebidas<br>- Viabilidad de enfermedades trasmitidas por alimentos (ETA) e intoxicaciones alimentarias.<br>- Riesgos de Seguridad: Materialización de accidente de trabajo, - Potencial de lesiones o afectaciones a la salud<br>- Riesgo: Eléctrico/Energías peligrosas/trabajo en alturas/espacios confinados/ accidentes de transito.<br>- Riesgo Físico<br>- Riesgo Químico<br>- Riesgo Psicosocial<br>- Riesgo Locativo: Caídas a mismo y a diferente nivel.<br>- Riesgo Biológico<br>- Riesgo Mecánico<br>- Riesgo Biomecánico<br>- Riesgo Publico<br>- Riesgo Tecnológico: Incendio y explosión<br>- Riesgos por Fenómenos Naturales |

| DESCRIPCIÓN DEL CRITERIO | ETAPA | APOYO TÉCNICO REQUERIDO | CUMPLIMIENTO | | | OBSERVACIONES |
|---|---|---|---|---|---|---|
| | | | SI | NO | N/A | (Indique aquí el documento que soporta su respuesta o la razón de que no aplique la disposición) |
| **Criterios para el prestador del servicio** | | | | | | |
| Plan anual de capacitación de SST incluyendo inducción y reinducción. | Contractual | Sistema de Gestión de Seguridad y Salud en el Trabajo | x | | | |
| Plan de Emergencias. | | Sistema de Gestión de Seguridad y Salud en el Trabajo | | | | |
| Programa de protección contra caídas y procedimiento de rescate (SI APLICA). | | Sistema de Gestión de Seguridad y Salud en el Trabajo | | | | |

| | |
|---|---|
| | Código: GCCON-AN-001 |
| | Versión: 07 |

| PROCESO |
|---|
| GESTIÓN CONTRACTUAL |
| **NOMBRE DEL FORMATO** |
| Formato Anexo De Verificación y Evaluación del Cumplimiento de Requisitos Legales SIGA |

| CLASIFICACIÓN DE LA INFORMACIÓN | | | | | |
|---|---|---|---|---|---|
| **Pública** | x | **Pública Clasificada** | | **Pública Reservada** | |

| | |
|---|---|
| **CONTRATO No/PROCESO No.:** | **NOMBRE DE PROVEEDOR/OFERENTE:** |
| **VIGENCIA DEL CONTRATO/PROCESO:** | **NOMBRE DEL SUPERVISOR DE CONTRATO:** |

**OBJETO:** PRESTACIÓN DE SERVICIOS PARA LA ELABORACIÓN E INSTALACIÓN DE UN AVISO CON LA IMAGEN CORPORATIVA DE LA AGENCIA PÚBLICA DE EMPLEO DEL SENA REGIONAL CASANARE, DE ACUERDO CON EL MANUAL CORPORATIVO DE MARCA, EN LAS INSTALACIONES DE LA OFICINA PRINCIPAL DE YOPAL.

| | |
|---|---|
| **PROPIEDADES DEL SGSPI**<br><br>- Confidencialidad<br>- Integridad<br>- Disponibilidad<br>- Privacidad<br><br>(Norma NTC/IEC ISO 27001:2022) | **RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**<br><br>- Pérdida de confidencialidad de los activos de información<br>- Pérdida de integridad de los activos de información<br>- Pérdida de disponibilidad de los activos de información<br><br>**Definición Activos de Información:** Todos aquellos que son necesarios para el desarrollo de las actividades, que de no existir impiden o dificultan el procesamiento o generación de información. Pueden ser fuentes de información, aplicativos, la misma información generada, entre otros. pueden ser: Información, bases de datos, sistemas de información, personas, áreas seguras, servicios, hardware, software, entre otros. |

| DESCRIPCIÓN DEL CRITERIO | ETAPA | APOYO TÉCNICO REQUERIDO | CUMPLIMIENTO | | | OBSERVACIONES |
|---|---|---|---|---|---|---|
| | | | SI | NO | N/A | (Indique aquí el documento que soporta su respuesta o la razón de que no aplique la disposición) |
| **Criterios para Contratar y Supervisar contratos donde se gestione cualquier tipo de activos de información del SENA** | | | | | | |
| **Políticas de Seguridad y Privacidad de la Información y Protección de Datos Personales**<br>Se debe incluir como una obligación la aceptación y cumplimiento de las políticas mencionadas y realizar la socialización de estas, así como validar su cumplimiento. | Precontractual y contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **Aceptación del proveedor de la politica de seguridad y privacidad de la información, proteccion de datos de personales, documento de socializacion al contratista de las politicas por parte de la entidad** |
| **Identificación Matriz de Riesgos**<br>En la matriz del riesgos del proceso se deben identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de los activos de información y los controles que debe implementar el SENA y el proveedor para mitigarlos. | Precontractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El supervisor debe hacer seguimiento a que los contratistas operen o visiten solo la zona donde se realizan los eventos, igualmente el contratista debe garantizar el tratamiento de los datos de los funcionarios, de acuerdo a las normas de la entidad. Se valida la matriz de riesgo** |
| **Protección de datos en la Nube**<br>adquirir productos de nube que durante su operación puedan resultar en tratamiento o transferencia de datos personales resulta fundamental planear dónde se almacenarán los datos, el tipo de almacenamiento y la región geográfica de ese almacenamiento. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **no aplica, porque no se adquirien productos en la nube** |
| **Seguimiento Matriz de Riesgos**<br>Se debe realizar seguimiento periódico a la matriz de riesgos identificada, validando que no se haya materializado algún riesgos, que los controles se ejecuten en la periodicidad y alcance establecidos, que no se requiera identificar algún otro riesgo, determinar posibles nuevas amenazas o vulnerabilidades en los productos o servicios contratados, los cuales como resultado deberán ser gestionados por el proveedor del servicio de acuerdo con los ANS establecidos en el contrato. | contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **aplica por riesgos de seguridad fisica y tratamiento de datos.** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Firma de acuerdos de confidencialidad**<br>Los acuerdos de confidencialidad deben reflejar los requisitos y controles de seguridad pertinentes en el SGSPI, asegurando la protección de la información institucional y de datos personales y el cumplimiento de las directrices de seguridad específicos. Esto requiere establecer cláusulas detalladas sobre la protección y manejo de la información, responsabilidades de las partes, mecanismos de control de acceso, y procedimientos de notificación y respuesta ante posibles brechas de seguridad. | contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | **x** | | | **Aunque es personal operativo, durante su tránsito por las sedes y subsedes, pueden tener acceso visual a proyectos de investigación, prototipos de aprendices, áreas administrativas o estar cerca a areas seguras. El contrato debe incluir una cláusula estándar de confidencialidad y no divulgación. Documento que soporta el cumplimiento: ISO 27001:2022 (Control A.5.20 - Seguridad de la información en las relaciones con los proveedores y A.5.8 - Acuerdos de confidencialidad). Se debe realizar antes de iniciar cualquier actividad que implique acceso a información técnica o administrativa.** |
| **Disponibilidad de los sistemas de información y/o plataformas**<br>Para asegurar la disponibilidad de los bienes y servicios contratados, el proveedor debe implementar medidas como la redundancia de sistemas, la planificación de capacidad, el monitoreo continuo de los sistemas y la realización de pruebas de disponibilidad periódicas. Es importante identificar y gestionar los riesgos que puedan afectar la disponibilidad de los sistemas, así como contar con procesos y procedimientos claros para responder a interrupciones de servicios y restaurar la funcionalidad de los sistemas, bienes y servicios contratados de manera rápida y eficiente. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | X | **es un contrato de prestacion de servicios, no sistemas de información o plataforma de TI** |
| **Clasificación de la Información**<br>De acuerdo con la clasificación de la información (Pública, Pública Clasificada y Pública Reservada), el supervisor del contrato debe informar y en conjunto con el proveedor establecer los controles que el proveedor debe implementar para garantizar la confidencialidad, integridad y disponibilidad según su clasificación. | contractual y postcontractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El supervisor informará al contratista sobre el manejo adecuado de la información intercambiada durante la ejecución del contrato. Esto incluye garantizar la confidencialidad de la información 'publica ''Pública Clasificada o Reservada' entregada por el SENA. El contratista debe clasificar la información que genere o gestione durante el contrato bajo las categorías de Pública, Pública Clasificada o Pública Reservada, según los lineamientos de transparencia del SENA.** |
| **Continuidad de los servicios**<br>El proveedor debe establecer un plan de continuidad del negocio que incluya medidas para garantizar la disponibilidad y el funcionamiento continuo de los servicios, incluso en situaciones de crisis o desastres. Esto implica identificar y mitigar los riesgos que puedan afectar la continuidad de los servicios. El objetivo es minimizar el impacto de interrupciones en los servicios y garantizar la prestación ininterrumpida de los mismos, protegiendo así la información y los activos críticos de la entidad. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **No aplica, no afecta la continuidad de los servicios de la entidad** |
| **Copias de respaldo**<br>El proveedor debe establecer una estrategia de copias de respaldo que aborde la identificación de los activos de información críticos, la frecuencia de las copias de respaldo, los procedimientos de almacenamiento seguro, la verificación periódica de la integridad de las copias y la capacidad de recuperación de la información. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **No aplica, no se tiene accesos a base de datos, por lo tanto no se requiere realizar copias de respaldo** |
| **Gestión de accesos**<br>El acceso a los sistema de información ofrecidos por el proveedor de contemplar la identificación y control de los usuarios, la asignación de privilegios y derechos de acceso, la revisión periódica de los privilegios, la gestión de contraseñas seguras, doble factor de autenticación, la autenticación de usuarios y la monitorización de los accesos. Gestionando en primera medida la integración con el directorio activo | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **Entendido como acceso lógico (usuarios, contraseñas, directorio activo, VPN). El personal del contratista no tendrá cuentas institucionales, ni acceso a los sistemas de la entidad.** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Accesos por parte de los proveedores**<br>El supervisor del contrato debe gestionar los accesos a los recursos y activos de información institucionales teniendo en cuenta el alcance del contrato, los privilegios, tiempos, personas, entre otros | contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El contratista debe tramitar ante el supervisor las autorizaciones necesarias para el acceso físico o digital a las instalaciones y sistemas, cumpliendo con las directrices de seguridad perimetral. Documento que soporta el cumplimiento: ISO 27001:2022 (Controles A.7.1 y A.7.2 - Perímetros de seguridad física y controles de entrada física) y Manual GOR-M-002 V01. solicitud de acceso a traves de correo electronico y bitacora de ingreso a la entidad.** |
| **Destrucción y/o eliminación de la información finalizado el contrato**<br>Se debe establecer procedimientos claros y seguros para la destrucción y eliminación de la información una vez finalizado el contrato, con el fin de garantizar la protección de los activos de información. Estos procedimientos deben incluir la identificación de los datos a ser eliminados, el uso de métodos seguros de destrucción como la trituración de documentos o el borrado seguro de medios electrónicos, así como el registro de la actividad | postcontractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El contratista debe certificar la destrucción segura o la devolución de la información y activos del SENA al finalizar el contrato, asegurando que no queden copias en equipos externos. Documento que soporta el cumplimiento: ISO 27001:2022 (Control 8.10 Eliminación de información y 8.3 - Retención de información), Manual de Políticas de Seguridad y Privacidad de la Información (GOR-M-002 V01).** |
| **Retorno de los activos de información**<br>El retorno de los activos de información debe ser gestionado de manera controlada y segura para garantizar la protección en especial de la información personal. Esto implica establecer procedimientos para la recepción y verificación de los activos de información, asegurando que se eliminen o se destruyan de manera segura los datos personales que ya no son necesarios, y registrando detalladamente todas las acciones realizadas durante el proceso. | postcontractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **A la terminación del contrato o cuando el personal del contratista sea desvinculado, el contratista deberá devolver al supervisor del SENA todos los activos suministrados para la ejecución de sus labores. Esto incluye estrictamente la devolución de credenciales de acceso físico (carnés, tarjetas, llaves) y la entrega de cualquier documentación técnica original prestada (planos). Documento que soporta el cumplimiento: ISO 27001:2022 (Control 5.11 - Devolución de activos), Manual de Políticas de Seguridad y Privacidad de la Información (GOR-M-002 V01).** |
| **Protección de datos personales**<br>Entre el proveedor y la entidad deben acordar medidas técnicas y organizativas para proteger la confidencialidad, integridad y disponibilidad de los datos personales. Esto incluye la autorización del tratamiento, la identificación y clasificación de los datos personales, el acceso restringido a los mismos, el cifrado de la información sensible, la gestión de los registros de procesamiento, la realización de evaluaciones de riesgos periódicas. | precontractual, contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El contratista acepta la politica de tratamiento de datos personales de la entidad y entregará al SENA datos personales de sus trabajadores (cédulas, planillas de seguridad social/ARL, certificados de trabajo en alturas). El contratista debe garantizar que cuenta con la autorización de sus empleados para compartir estos datos con el SENA, documento soportado en (Ley 1581 de 2012 y Manual GOR-M-003).** |
| **Certificación de la norma ISO 27001**<br>El proveedor al ser certificado ISO 27001 asegura poseer un sistema de gestión de seguridad de la información eficaz para protege los activos y datos entregados en custodia o tratamiento según la naturaleza del contrato. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **el proceso es un contrato que no amerita que el proveedor este certificado** |
| **Gestión de cambios**<br>El proveedor debe tener implementado un proceso gestión de cambio estructurado y controlado para planificar, evaluar, autorizar e implementar cambios en los activos de información en los bienes y servicio de acuerdo a lo contratado. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **el proveedor no va realizar cambios que afecten nuestros sistemas ni la continuidad de los servicios de la entidad** |
| **Análisis de vulnerabilidades**<br>El proveedor debe identificar y evaluar periódicamente (mínimo cada 6 meses) y gestionar las posibles debilidades y vulnerabilidades de los sistemas de información según aplique en la naturaleza del contrato. Este análisis permite detectar vulnerabilidades que podrían ser aprovechadas por amenazas y comprometer la seguridad de la información. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **no aplica, no hay sistemas de información o plataforma de TI, por lo tanto no aplica seguimiento de vulnerabilidades ciberneticas** |
| **Gestión de incidentes de seguridad**<br>En los requisitos contractuales de cualquier bien y servicio se debe incluir la obligación del reporte oportuno de cualquier evento o incidente de seguridad que ponga en riesgos la confidencialidad, integridad, disponibilidad y privacidad de la información. Aportando las evidencias y apoyando en su gestión en la medida de lo posible. | contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El contrato debe incluir la obligación del contratista de reportar de manera inmediata al supervisor del SENA cualquier evento o incidente físico que comprometa los activos del Centro. Esto incluye: pérdida o robo de credenciales de acceso físico (carnés, llaves, tarjetas), daños accidentales a la infraestructura tecnológica o de red durante las labores de entrega (que afecten la disponibilidad de los servicios), y el hallazgo o exposición indebida de documentación física confidencial o datos personales en la zona de entrega.Documento que soporta el cumplimiento: Manual de Políticas de Seguridad y Privacidad de la Información (GOR-M-002 V01), ISO 27001:2022 (Control 5.24 - Planificación y preparación para la gestión de incidentes de seguridad de la información y Control 6.8 - Notificación de eventos de seguridad).** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Acuerdos de Nivel de Servicios**<br>Se debe solicitar al proveedor el establecimiento de acuerdos de nivel de servicios ANS acordados con el SENA, para la atención de casos, requerimientos, incidentes, según la criticidad del servicio. Así mismo se deben solicitar la formalización de un documento de atención, donde se identifiquen claramente los canales y procesos para solicitudes, así como el personal designado por el proveedor. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **para el proceso contractual no aplica el establecimiento de ANS** |
| **Sensibilización sobre el SGSPI**<br>Se debe gestionar con los proveedores los espacios de sensibilización que se requieran para socializar las políticas y controles establecidos por el SENA para el aseguramiento de sus activos de información | contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **El contratista debe participar en las jornadas de capacitación, inducción y sensibilización sobre el SGSPI programadas por el Centro, garantizando que su personal conozca y aplique los protocolos institucionales. (con la suscripción del acta de inicio, se dará una transferencia al contratista sobre las políticas y controles establecidos por el SENA.)** |
| **Auditorías al proveedor**<br>Las auditorías a los proveedores son un procedimiento en la gestión de SGSPI para garantizar que en el desarrollo de un contrato con un proveedor se cumplan con los estándares de seguridad de la información requeridos por la entidad. Estas auditorías involucran la evaluación de los controles de seguridad implementados por el proveedor para proteger la confidencialidad, integridad y disponibilidad de los datos y activos de información. | | Sistemas de Gestión de Seguridad y Privacidad de la Información | | | x | **no aplica por el tipo de contrato** |
| **Seguimiento periódico**<br>Se debe solicitar al proveedor la generación de informes periódicos de los servicios o productos que evidencie el cumplimiento de los indicadores establecidos, así como contar con evidencias de reuniones periódicas de seguimiento acorde a lo establecido en las cláusulas, anexos técnicos y según requerimiento del supervisor del contrato. Y contar con los resultados de revisiones técnicas, administrativas o auditorias de cumplimiento en búsqueda de acciones de mejora o verificación del cumplimiento requerido | contractual | Sistemas de Gestión de Seguridad y Privacidad de la Información | x | | | **el proveedor debe generar informes de cumplimiento de actividades, en los cuales debe adjuntar cumplimiento de las politicas de seguridad y privacidad de la información de la entidad** |

| |
|---|
| Ley 1273 de 05 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. |
| Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. |
| Ley 1712 de 2014, Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. |
| Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". |
| Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa. |
| Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital. |
| Documento CONPES 3975 de 2019 - Política Nacional para la Transformación Digital e Inteligencia Artificial. |
| Documento CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital. |
| Norma Técnica Colombiana NTC/ISO 27001 versión 2022, Sistemas de Gestión de Seguridad de la Información (SGSPI). Requisitos. Anexo A Control 5.19 Seguridad de la información en la relaciones con los proveedores |
| Resolución 500 de 2021 por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. |
| |