Para el cumplimiento de los requerimientos de seguridad de la información y Ciberseguridad se tendrán en cuenta las siguientes definiciones:

1. **Seguridad de la Información:** Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene,reproduzca o procese en los sistemas informáticos de la entidad.

2. **Ciberseguridad:** Es el desarrollo de capacidades empresariales para defender y anticiparlas amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

3. **Evento de Ciberseguridad:** Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

4. **Incidente de Ciberseguridad:** Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

En consecuencia y de acuerdo con el objeto del presente contrato, EL CONTRATISTA/CONTRATANTE se compromete a cumplir con las siguientes:

CLÁUSULAS DE SEGURIDAD DE LA INFORMACIÓN

Sin perjuicio de cualesquiera otros términos y condiciones del Acuerdo, se exige al CONTRATISTA/CONTRATANTE aplicar los siguientes requisitos de seguridad de la información:

1. Control de acceso lógico.

Para garantizar el cumplimiento de los requisitos de S3 sobre el control de la seguridad para el acceso, el CONTRATISTA/CONTRATANTE deberá:

i. Proteger la confidencialidad de todas las contraseñas o claves de acceso asignadas al CONTRATISTA/CONTRATANTE por S3.
ii. Contar con una política de contraseñas en virtud de la cual su personal, incluidos los subcontratistas/contratantes, que puedan tener acceso a los sistemas del CONTRATISTA/CONTRATANTE o de S3, cambien las contraseñas inmediatamente después de recibirlas y posteriormente las cambien cada noventa (90) días o con mayor frecuencia, y eviten contraseñas triviales o evidentes.
iii. Oportunamente retirar los privilegios de acceso lógico al personal del CONTRATISTA/CONTRATANTE, incluidos los subcontratistas/contratantes que, ya sea por transferencia interna o cese de la relación con el CONTRATISTA/CONTRATANTE, o de ser el caso, dejan de estar involucrados en el procesamiento de la información y datos de S3.

2. Responsabilidades del personal.

Para garantizar el cumplimiento de los requisitos referentes a la responsabilidad de los

empleados, el CONTRATISTA/CONTRATANTE deberá: Certificar que todos los dispositivos utilizados por los empleados cumplan y sigan cumpliendo los siguientes requisitos:

i. Deben aplicarse y estar al día en las actualizaciones (*Service pack)* más recientes y todos los parches de seguridad aplicables a todos los sistemas operativos y software residentes en los dispositivos.
ii. Los dispositivos deben tener el software estándar de la industria contra programas maliciosos (*malware)* instalado, funcionando y actualizado con el último archivo de firma.
iii. El dispositivo debe tener instalado y activo un producto de seguridad tipo cortafuego (*firewall)* personal y estándar de la industria.
iv. Deben asegurar que los computadores utilizados para el procesamiento de datos suministrados por S3 no cuentan con accesos habilitados a puertos USB.
v. Garantizar que los datos de clientes suministrados por el s3 no serán tratados a través de dispositivos móviles, celulares, tabletas, etc.
vi. Abstenerse de realizar almacenamientos o tratamientos de datos suministrados por el S3 en la nube, para los casos en que la solución tecnológica se encuentre alojada en la Nube esta deberá cumplir con la circular externa 005 de 2019 de la Superintendencia Financiera de Colombia.

3. Seguridad de los servidores

Para asegurar la integridad, confidencialidad y disponibilidad de todos los servidores utilizados para procesar la información y datos de S3, y para mitigar la amenaza,riesgo e impacto del uso indebido y abusos externos o internos de las plataformas de servidores, el CONTRATISTA/CONTRATANTE deberá:

i. Proteger el acceso a todos los servidores, como mínimo, mediante una combinación de la identificación (ID) del usuario y la contraseña secreta;
ii. Cambiar todas las contraseñas de los servidores que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente cada noventa (90) días o más frecuentemente;
iii. Hay que asegurar que los servidores se encuentren ubicados en zonas físicamente seguras;
iv. Reforzar la seguridad de todos los servidores utilizados para procesar, almacenar o transmitir datos e información de S3, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores;
v. Implementar herramientas de análisis de la seguridad de los servidores para informar periódicamente sobre el estado de cada servidor y verificar que todas las configuraciones, parámetros y opciones estén conformes con el estado de reforzamiento acordado para ese dispositivo y para detectar cambios no autorizados a partir de la línea base de la configuración aprobada del servidor.
vi. Registrar toda la actividad de acceso del servidor y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de doce (12) meses.
vii. Revisar periódicamente (al menos una vez al año) todos los controles de seguridad del servidor definidos anteriormente para asegurarse de que todavía estén vigentes.

4. Seguridad de los archivos de datos y bases de datos

Para asegurar la integridad, confidencialidad y seguridad en general de todas las bases de datos y archivos de datos utilizados para almacenar información y datos de S3, el CONTRATISTA/CONTRATANTE deberá:

i. Almacenar la información "Confidencial" de S3 (por ejemplo, contraseñas, datos de los clientes, etc.) en un formato cifrado de conformidad con las mejores prácticas de la industria; y acorde al estándar de criptografía aprobado por S3.
ii. Ubicar todos los servidores de bases de datos, servidores de archivos y repositorios que contengan datos de S3 en un área físicamente segura.
iii. Restringir todo el acceso físico y lógico a las bases de datos, archivos de datos e información y datos almacenados en éstos, así como a cualquier sistema o componente de la red relacionado con el procesamiento de transacciones según un esquema basado solo en la "necesidad de conocer o usar" del negocio.
iv. Proteger todos los accesos a las bases de datos y archivos de datos utilizando, como mínimo, una combinación de la identificación del usuario y la contraseña secreta.
v. Cambiar todas las contraseñas de las bases de datos que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente cada noventa (90) días.
vi. Registrar toda la actividad de acceso a las bases de datos y archivos de datos, y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de doce (12) meses.
vii. Registrar toda la actividad de transacciones y almacenar los datos de dicha actividad de una manera apropiada durante al menos tres (3) años desde la fecha de cada transacción.
viii. Manejar todas las copias de respaldo de todos los registros de las bases de datos y archivos de datos de conformidad con medidas estrictas de seguridad y controles de acceso, ejerciendo controles idénticos o similares a los empleados para las bases de datos y los archivos de datos principales.
ix. Implementar herramientas de análisis de la seguridad de las bases de datos para revisar periódicamente las configuraciones de las bases de datos y garantizar el cumplimiento de las configuraciones de base esperadas.
x. Eliminar y destruir de una manera adecuada y segura todas las instancias de cualquier información o datos del S3 y material impreso conexo para asegurar que las transacciones y demás datos no puedan ser recuperados por personas no autorizadas.
xi. Revisar en forma periódica (al menos una vez al año) todos los controles de seguridad de la base de datos definidos anteriormente para asegurar que continúan vigentes.
xii. Los datos que el S3 suministre al CONTRATISTA/CONTRATANTE deben ser transmitidos de forma cifrada o encriptada y segura cumpliendo los protocolos para tal fin.

5. Seguridad de la red

Para mitigar la amenaza, riesgo e impacto de intrusiones, abuso o uso indebido del sistemao la red, el CONTRATISTA/CONTRATANTE deberá:

i. Instalar, configurar y activar un sistema integral de protección contra intrusiones (en la red y el host), de conformidad con las mejores prácticas de la industria, para que en forma continua evite, detecte e informe la ocurrencia de ataques no autorizados

a la red y en contra de sus sistemas, incluidos, entre otros, intentos de penetración, ataques por denegación de servicio y sondeos excesivos.

ii. Instalar cortafuegos (firewall) para redes basados en las mejores prácticas de la industria entre los servidores y las puertas de enlace (Gateway) a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet.

iii. Registrar toda la actividad de los cortafuegos y puertas de enlace y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de doce (12) meses.

iv. Proteger los datos contra la divulgación no autorizada durante su tránsito a través de redes públicas a S3, o sus agentes autorizados, o sus clientes, para garantizar la seguridad de los datos que sean propiedad de S3 o estén relacionados con S3.

v. Aplicar las técnicas criptográficas, "Transport Layer Security" (TLS) versión 1.2 o superior para la autenticación mutua de certificados (del cliente al servidor o de servidor a servidor), y una longitud mínima de clave de 256 bits o una norma equivalente basada en las mejores prácticas de la industria.

6. Protección contra programas maliciosos (malware)

Para mitigar la amenaza, riesgo e impacto de los virus informáticos, gusanos, troyanos y otros tipos de software malicioso, colectivamente llamado "*malware*", EL CONTRATISTA/CONTRATANTE:

i. Instalar, configurar, activar y mantener actualizado un software antivirus y anti-espías (antispyware) basado en las mejores prácticas de la industria, en todos los servidores, dispositivos, computadoras portátiles y estaciones de trabajo que procesen o almacenen las transacciones y cualquier otro dato de S3.

ii. Configurar dicho software antimalware para invocarlo automáticamente en el arranque y ejecutarlo interactivamente de forma continua, en todos los dispositivos donde esté instalado.

iii. Informar todos los incidentes relacionados con el malware a S3 en un plazo de 2 horas. Estos reportes deberán ser notificados al correo electrónico erika.reyes@s3.com.co

7. Vulnerabilidades de la seguridad e instalación de parches de seguridad

Para mitigar la amenaza, riesgo e impacto de las vulnerabilidades de la seguridad en el sistema o red, EL CONTRATISTA/CONTRATANTE deberá:

i. Desarrollar e implementar un proceso para investigar continuamente las fuentes fiables de advertencias sobre vulnerabilidades de la seguridad emergentes.

ii. Identificar vulnerabilidades específicas que puedan impactar los ambientes operativos o plataformas utilizados por EL CONTRATISTA/CONTRATANTE en nombre de S3.

iii. Evaluar la criticidad de una vulnerabilidad en relación con las operaciones generales del CONTRATISTA/CONTRATANTE y S3, a fin de determinar la conveniencia de instalar el correspondiente parche de seguridad.

iv. Probar e instalar oportunamente los parches de seguridad.

8. Alerta y escalamiento de problemas y gestión de incidentes de seguridad.

En el caso de pérdida, acceso no autorizado, o divulgación no autorizada de la Información Confidencial de S3, Información Personal de S3, u otros datos de S3 (cada uno de ellos una "Violación de Seguridad de la información"), el proveedor inmediatamente y tan pronto como sea posible, después de determinar que se ha producido una Violación de la Seguridad de la Información:

i. Implementar, mantener y cumplir procedimientos documentados de alerta y escalamiento de problemas, que el Proveedor y S3 podrán modificar ocasionalmente de mutuo acuerdo y actuando de forma razonable.

ii. Investigará la violación de seguridad de la información y proporcionar a S3 la información detallada sobre la violación de seguridad de la información.

9. Control de cambios

Para garantizar el cumplimiento de los requisitos de S3 y de las mejores prácticasde la industria para la gestión y el control de cambios, EL CONTRATISTA/CONTRATANTE deberá:

i. Desarrollar, probar y documentar cada cambio de conformidad con la gestión de cambios y las normas, procedimientos y procesos de control, preservando la integridad lógica continua de los datos, programas y rastros de auditoría.

10. Respaldo y recuperación

Para garantizar el cumplimiento de los requisitos de S3 y de las mejores prácticasde la industria para el respaldo y la recuperación, EL CONTRATISTA/CONTRATANTE deberá:

i. Implementar medidas de respaldo adecuadas, incluido el almacenamiento de los archivos de datos de respaldo en lugares seguros fuera del sitio de procesamiento, para permitir la recuperación eficiente del sistema;
ii. Facilitar la reanudación de las aplicaciones críticas y actividades de negocios de una manera oportuna después de una emergencia o desastre; y
iii. Mantener un plan de continuidad y de recuperación de desastres documentado para cada sistema crítico relacionado con S3 y para las aplicaciones de negocios, y probarlo anualmente.

11. Notificación.

En caso de pérdida, acceso no autorizado, o divulgación no autorizada de la Información Confidencial de S3, Información Personal de clientes o colaboradores de S3 u otros datos de S3 conocido como "Violación de Seguridad de los Datos", el proveedor de forma inmediata, después de determinar que ha ocurrido la Violación de la Seguridad de los Datos, deberá:

Notificar a S3 de las violaciones de seguridad de los datos a los siguientes correos electrónicos:

i. juridica@s3.com.co
ii. erika.reyes@s3.com.co

CLÁUSULAS DE SEGURIDAD Y SALUD EN EL TRABAJO Y MEDIO AMBIENTE.

Sin perjuicio de cualesquiera otros términos y condiciones del Acuerdo, se exige al CONTRATISTA/CONTRATANTE aplicar los siguientes requisitos de seguridad y salud en el trabajo:

i. Dar cumplimiento a las obligaciones con los Sistemas de Seguridad Social en salud, pensión, Sistema General de Riesgos Laborales y aportes parafiscales, cuando haya lugar a ello, y presentar los documentos respectivos que así lo acrediten, conforme lo establecido en el artículo 50 de la Ley 789 de 2002, en la Ley 828 de 2003, la Ley 1562 de 2012, decreto 1072 de 2015 y demás normas que regulen la materia.
ii. Dar aplicación a las políticas expedidas por S3 en materia seguridad y salud en el trabajo, gestión Ambiental y demás que adopte la organización y emplear los formatos que para tal fin apruebe S3 SIMPLE, SMART, SPEEDY.
iii. Proveer un ambiente de trabajo saludable y seguro, que proteja a su personal, al personal de S3 SIMPLE, SMART, SPEEDY y a terceros, de cualquier peligro asociado con la prestación de servicios. Hacen parte del ambiente de trabajo todas las instalaciones, equipos, herramientas y demás elementos utilizados por EL CONTRATISTA/CONTRATANTE en prestación de los servicios, así como prácticas de trabajo.
iv. Prevenir efectos dañinos para el medio ambiente, actuando siempre de conformidad con la legislación nacional y las normas de S3 SIMPLE SMART SPEEDY S.A.S. sobre la materia.
v. Emplear personal que posea las habilidades, conocimientos, licencias y certificados requeridos y necesarios para ejecutar los trabajos correspondientes en forma segura y de calidad, manteniendo a disposición de S3 SIMPLE SMART SPEEDY S.A.S. los registros y la documentación apropiada que confirme tales habilidades, conocimientos y aptitudes.
vi. EL CONTRATISTA/CONTRATANTE deberá dar estricto cumplimiento a la legislación vigente sobre Seguridad y Salud en el trabajo y medio Ambiente, así como a las disposiciones administrativas y reglamentarias de S3 SIMPLE SMART SPEEDY S.A.S. y a las instrucciones escritas o verbales que sobre la materia imparta el representante autorizado de S3 SIMPLE SMART SPEEDY S.A.S. durante la ejecución de la obra o servicio.
vii. En caso de producirse un accidente causado por las actividades inherentes a la ejecución del contrato que haya celebrado con S3 SIMPLE SMART SPEEDY S.A.S. si este accidente ha afectado al personal de dicho CONTRATISTA/CONTRATANTE, colaboradores de S3 o terceros, EL CONTRATISTA/CONTRATANTE notificará por escrito la ocurrencia de dicho accidente al administrador del Contrato respectivo, en un plazo máximo de dos días hábiles.

CLÁUSULAS RELATIVAS A SAGRILAFT

Las partes declaran bajo gravedad de juramento lo siguiente:

i. Que sus ingresos o bienes no provienen de ninguna actividad ilícita de las contempladas en el Código Penal Colombiano o en cualquier norma que lo sustituya, adicione o modifique. En consecuencia, declaran que sus ingresos o bienes

están ligados al desarrollo normal de actividades lícitas propias de su objeto social.

ii. Que no han efectuado transacciones u operaciones destinadas a la realización o financiamiento de actividades ilícitas contempladas en el Código Penal Colombiano o en cualquier norma que lo sustituya, adicione, o modifique, o a favor de personas relacionadas con dichas actividades.

iii. Que no han incurrido ni participado, ni incurrirán ni participarán, a ningún título y en ninguna calidad, en prácticas, actos, omisiones o delitos relacionados directa o indirectamente con corrupción pública o privada.

iv. Que en la ejecución del presente contrato, se abstendrán de tener vínculos con terceros que se conozca por cualquier medio estén vinculados a actividades de lavado de activos o financiación del terrorismo.

v. Que han tomado y tomarán en todo momento durante la vigencia del contrato, todas las medidas necesarias para evitar incurrir y para prevenir que cualquiera de sus empleados, contratistas, administradores, apoderados, mandatarios, representantes legales y cualquier otra persona sujeta a su control, haya incurrido o incurra en cualquiera de dichas conductas.

vi. Abstenerse de utilizar sus operaciones como instrumento para el ocultamiento, manejo, inversión o aprovechamiento, en cualquier forma, de dinero u otros bienes provenientes de actividades delictivas o para dar apariencia de legalidad a las transacciones y fondos vinculados con las mismas, o destinadas a la realización de actividades ilícitas.

vii. Cumplir a cabalidad con las normas sobre prevención y control al lavado de activos y financiación del terrorismo (LA/FT) que le resulten aplicables (de ser el caso), teniendo implementados las políticas, procedimientos y mecanismos de prevención y control al LA/FT que se derivan de dichas disposiciones legales.

CLÁUSULAS RELATIVAS A ETICA EMPRESARIAL

i. LAS PARTES declaran que conocen que, está prohibido dar, ofrecer o prometer a un servidor público, extranjero o nacional, directa o indirectamente, sumas de dinero, cualquier objeto de valor pecuniario u otro beneficio o utilidad, a cambio de que el servidor público extranjero o nacional, realice, omita, o retarde, cualquier acto relacionado con el ejercicio de sus funciones y en relación con un negocio o transacción internacional o nacional, de acuerdo a lo establecido en la Ley No. 1778 de 2016 o las normas que la sustituyan, modifiquen o adicionen. Así mismo se comprometen a no realizar estas conductas.

ii. Para los propósitos del presente contrato, se entenderá como "Servidor Público" para efectos nacionales o en el extranjero, toda persona que tenga un cargo legislativo, administrativo o judicial en un Estado, sus subdivisiones políticas o autoridades locales, o una jurisdicción extranjera o local, sin importar si el individuo hubiere sido nombrado o elegido.

iii. LAS PARTES reportarán inmediatamente cualquier irregularidad de la cual tengan conocimiento o tengan bases razonables para creer que haya ocurrido con respecto a EL CONTRATO, relacionada con esta cláusula o cualquier incumplimiento legal.

iv. LAS PARTES declaran que ni él ni ningún funcionario, empleado, agente, subcontratista, dependiente es un Servidor Público.

v. LAS PARTES se obligan a reportar a través de la línea ética de S3 cualquier conflicto de interés real o potencial, la cual cuenta con los siguientes canales:

a. Correo electrónico: lineaeticaS3@s3.com.co
b. Página web: s3.com.co

c. Teléfono: 6510051 extensión 2057

12. **INTEGRIDAD Y VINCULACIÓN DEL PRESENTE DOCUMENTO:** En virtud de lo consagrado en el presente instrumento, EL CONTRATISTA/CONTRATANTE declara que la suscripción del presente documento será vinculante y tendrá efectos para cualquier documento, acuerdo, contrato, alianza y/o cualquier otro tipo de relación contractual y/o comercial suscrita con la empresa S3 Simple Smart Speedy S.A.S.

PARÁGRAFO: Previo acuerdo entre las PARTES, EL PROVEEDOR/CONTRATISTA se compromete a permitir que LA ORGANIZACIÓN o quien ésta nombre, desarrolle auditorias sobre las actividades desarrolladas por EL PROVEEDOR/CONTRATISTA para el cumplimiento del objeto del contrato, orden de compra u orden de servicio y sus anexos, las cuales estarán sujetas al secreto profesional y al cumplimiento de las obligaciones de confidencialidad establecidas en el contrato, orden de compra u orden de servicio. En caso de delegarse la auditoría a un tercero LA ORGANIZACIÓN garantizará que no serán competidores directos de EL PROVEEDOR/CONTRATISTA.

Por medio del presente documento LA ORGANIZACIÓN se compromete a tomar todas las medidas del caso para que sus ejecutivos, funcionarios, empleados y consultores que realicen dichas auditorías, respeten la confidencialidad de la información conocida por dicha labor.

En el supuesto de que el informe de la auditoría muestre incumplimientos de EL PROVEEDOR/CONTRATISRA en la ejecución de sus prestaciones, este presentará un plan de acción a LA ORGANIZACIÓN.

_____
Firma
Nombre
CC
Nombre de la empresa
NIT
Indique si es contratista o cliente

13. CONTROL DE CAMBIOS

Versión	Sección modificada	Motivo de la modificación	Fecha de Modificación	Cargo de quien modifica
1	Todo el documento	Creación del documento	17/08/2022	Director de Seguridad de la Información, planeación y procesos
2	Encabezado	Se actualiza logo corporativo	04/09/2023	Líder Planeación y Procesos