



REQUISITOS DE CITI PARA PROVEEDORES

RESPONSABLES:

Jefe de Abastecimiento Global de Citi

FECHA DE EMISIÓN

Enero de 2015

REVISADO:

Marzo 2022

VERSIÓN:

6.0

ÍNDICE

1	RESUMEN GENERAL.....	3
2	IGUALDAD DE OPORTUNIDADES EN EL EMPLEO / ACCIÓN AFIRMATIVA	5
3	ANTI SOBORNOS	6
4	REGALO Y ENTRETENIMIENTO	7
5	DIVERSIDAD DE PROVEEDORES Y PRINCIPIOS DE PROVEEDORES.....	8
6	PROHIBICIÓN CONTRA LA ESCLAVITUD MODERNA	9
7	PERSONAL DEL PROVEEDOR.....	11
8	GESTIÓN DE FRAUDE	12
9	INTERACCIÓN CON LOS MEDIOS Y APARICIONES PÚBLICAS	13
10	COMUNICACIONES ELECTRÓNICAS ESCRITAS	14
11	ACTIVIDADES POLÍTICAS Y CONTRIBUCIONES	14
12	ANTI-LAVADO DE DINERO (“AML”).....	15
13	GESTIÓN DE REGISTROS	16
14	SERVICIOS DE CARA AL CLIENTE	17
15	CONTINUIDAD DEL NEGOCIO	21
16	NORMAS DE INVESTIGACIÓN DE ANTECEDENTES GLOBALES.....	26
17	GASTOS	28
18	SEGURIDAD DE LA INFORMACIÓN (IS).....	29
19	PAUTAS PARA UN LUGAR DE TRABAJO SEGURO	55
20	INTELIGENCIA ARTIFICIAL/APRENDIZAJE AUTOMÁTICO	56
	APÉNDICE - DEFINICIONES	57

1 RESUMEN GENERAL

1.1 Requisitos

Estos Requisitos de Citi para Proveedores ("**Requisitos**") detallan algunas de las obligaciones que los Proveedores deben cumplir en el curso de sus negocios con Citi. Ciertos Requisitos son aplicables a todos los Proveedores, mientras que la aplicabilidad de otros Requisitos a un Proveedor en particular depende de los tipos de productos y servicios que el Proveedor proporciona a Citi (estos últimos se resumen en la Sección 1.2 a continuación y se indican en el comienzo de cada disposición enumerada en el mismo). Los términos en mayúscula tendrán los significados que se les atribuyen en el presente, incluido el Apéndice adjunto, a menos que no se indique tal significado en el presente, en cuyo caso tendrá el significado que se les atribuye en el Contrato, según se define a continuación.

Estos Requisitos son obligaciones contractuales en virtud de los acuerdos del Proveedor con Citi (incluidos, entre otros, documentos transaccionales, por ejemplo, órdenes de trabajo, cronogramas de licencias) (cada uno un "**Contrato**"), y se suman a cualquier obligación especificada en cualquier Acuerdo, cualquier obligaciones en virtud de la Ley aplicable (según se define ese término a continuación), cualquier aviso al Proveedor de Citi que informe al Proveedor de sus obligaciones en virtud del mismo (cada uno un "**Aviso**"), o cualquier requisito adicional más específico implementado por los negocios o funciones de Citi. Las obligaciones y los requisitos más restrictivos se aplicarán en la medida de cualquier conflicto entre cualquiera de los requisitos anteriores y las Restricciones. Los proveedores deben asumir un papel proactivo y consultar con su principal contacto comercial de Citi (o su designado) con respecto a cualquier pregunta que tengan sobre estos Requisitos, incluidos los cambios en los mismos, cualquier exención solicitada de los mismos o cualquier conflicto percibido en estos o con la Ley aplicable.

El incumplimiento de estos Requisitos, o cualquier requisito adicional especificado por una empresa de Citi con la que el Proveedor hace negocios, puede resultar en la rescisión del Contrato del Proveedor con Citi. Además, las violaciones de los Requisitos también pueden ser violaciones de la ley aplicable y pueden dar lugar a daños civiles adeudados a Citi (o a terceros) o sanciones penales para el Proveedor. Los proveedores no pueden utilizar el cumplimiento de sus propias políticas como sustituto de su obligación de cumplir con cualquier disposición de estos Requisitos sin el consentimiento por escrito de Citi.

1.2 Requisitos Aplicables a Proveedores Selectivos

El siguiente cuadro enumera ciertos Requisitos que se aplican a ciertos Proveedores que cumplen con los criterios de aplicabilidad designados en el mismo. Las secciones no mencionadas a continuación son aplicables a TODOS los proveedores.

Número de la Sección	Título de la sección	Aplicabilidad
12	ANTI LAVADO DE DINERO	Aplicable a los Proveedores que realizan ciertos servicios relacionados con el cliente (es decir, incorporación, verificación de cuentas y transacciones de clientes) o la entrega de datos/métricas relacionadas con las actividades anteriores; <u>Y/O</u> Proveedores que actúan como intermediarios con respecto a efectivo o instrumentos financieros (p. ej., captura remota de depósitos, servicio de mensajería, servicios de vehículos armados o de cajas fuertes).
13	GESTIÓN DE REGISTROS	Aplicable a Proveedores que acceden a, procesan o almacenan información de Citi
14	SERVICIOS DE CARA AL CLIENTE	Aplicable al Proveedor que interactúa con cualquier individuo en su calidad de cliente pasado, actual o potencial de Citi o de una parte relacionada (como un empleado o un representante) de dicho cliente (cada uno de estos tipos de individuos, se denomina un "Cliente").
15	CONTINUIDAD DEL NEGOCIO	Aplicable a Proveedores que están incluidos en el Plan de Recuperación para la unidad de Negocios de Citi o si el proveedor aloja una aplicación con capacidades de recuperación (es decir, Capacidad de Tiempo de Recuperación de Tecnología numérica (TRTC)), que es utilizada por Citi. El Responsable de la Actividad Comercial de Citi (BAO, por su nombre en inglés) es responsable de comunicar la aplicabilidad y requisitos COB al Proveedor.
16	NORMAS DE INVESTIGACIÓN DE ANTECEDENTES GLOBALES	Aplicable a Proveedores cuyo personal tiene acceso a los sistemas/redes de Citi; <u>Y/O</u> acceso sin escolta a las instalaciones de Citi (Dicho personal deberá tener un GEID, y estar registrado en el Sistema de Gestión de No Empleados de Citi); <u>Y/O</u> Proveedores que acceden a, procesan, almacenan o administran Información Confidencial o Superior de Citi
17	GASTOS	Aplicable a Proveedores que son elegibles contractualmente para reclamar gastos comerciales reembolsables
18	SEGURIDAD DE LA INFORMACIÓN (IS)	Aplicable a Proveedores que acceden a, procesan, gestionan, almacenan Información de Citi; <u>Y/O</u> Proveedores responsables como los albergues de aplicaciones orientadas a Internet de la marca Citi; <u>Y/O</u> Proveedores con conectividad a los recursos de red de Citi; <u>Y/O</u> Proveedores que requieren acceso sin escolta a las instalaciones de Citi.
19	PAUTAS PARA UN LUGAR DE TRABAJO SEGURO	
20	INTELIGENCIA ARTIFICIAL/APRENDIZAJE AUTOMÁTICO	Aplicable a Proveedores que utilizan Inteligencia Artificial/Aprendizaje Automático (AI/ML), según lo definido por Citi en cualquier parte del producto o servicio que están brindando.

2 IGUALDAD DE OPORTUNIDADES EN EL EMPLEO / ACCIÓN AFIRMATIVA

Como parte de nuestros esfuerzos para cumplir con los requisitos reglamentarios federales de no discriminación y acción afirmativa, Citi ha desarrollado un programa y políticas de igualdad de oportunidades de empleo y acción afirmativa que están diseñados para garantizar la igualdad de oportunidades de empleo para todas las personas calificadas sin distinción de raza, color, religión, sexo, orientación sexual, identidad de género, origen nacional, edad, estado civil, información genética, discapacidad, condición de veterano protegido o cualquier otro motivo prohibido por la ley.

Esto incluye, entre otras cosas, lo siguiente:

- i.** Contratación, colocación, transferencia, descenso o promoción
- ii.** Reclutamiento, publicidad o solicitud de empleo.
- iii.** Tratamiento durante el empleo
- iv.** Tasas de pago u otras formas de compensación
- v.** Selección para la formación, incluido el aprendizaje
- vi.** Despido o terminación del empleo

Los Proveedores cumplirán, y harán que su Personal cumpla, con los requisitos de todas las leyes y reglamentaciones aplicables de no discriminación y acción afirmativa, incluidas, entre otras, las leyes o reglamentaciones que Citi notifique al Proveedor por escrito con las que debe cumplir.

Consulte la Declaración de política de acción afirmativa e igualdad de oportunidades de empleo de Citi en los EE.UU. para obtener más información, que se puede encontrar en [https://www.ecfr.gov/current/title-41/subtitle-B/chapter-60/part-60-300#p-60-300.44\(f\)\(1\)\(ii\)](https://www.ecfr.gov/current/title-41/subtitle-B/chapter-60/part-60-300#p-60-300.44(f)(1)(ii)).

3 ANTI SOBORNOS

Citi cuenta con políticas, procedimientos y controles internos para cumplir con las leyes antisoborno y prohíbe estrictamente el soborno o los pagos de facilitación en cualquier forma. Los proveedores o cualquier persona que actúe en nombre de Citi llevará, a cabo sus actividades de acuerdo con los más altos estándares de conducta comercial, lo que incluye el cumplimiento de todas las leyes que prohíben el soborno, la corrupción, el fraude y las declaraciones falsas, incluida la Ley de Prácticas Corruptas en el Extranjero de los EE. UU. ("FCPA"), la Ley contra el Soborno del Reino Unido, cada una de sus enmiendas o cualquier ley, norma o regulación aplicable contra el soborno, la corrupción, el fraude o el soborno (colectivamente, "Leyes contra el soborno").

Ningún Proveedor, ni ningún integrante de su personal, que opere en nombre de Citi, (i) habrá realizado, conferido u ofrecido ningún pago, beneficio o ventaja a ninguna Persona; (ii) realizará, conferirá u ofrecerá pagos, beneficios o ventajas a cualquier Persona; o (iii) ha recibido o aceptado o recibirá o aceptará cualquier pago, beneficio u otra ventaja de cualquier Persona, en cada caso de violación de Anti-Soborno. El Proveedor llevará a cabo sus negocios en nombre de Citi de conformidad con estos Requisitos, incluida esta Sección, según corresponda. Los proveedores también deberán mantener políticas y procedimientos apropiados para garantizar el cumplimiento con todas las leyes antisoborno.

Para obtener una descripción general del Programa Antisoborno de Citi, visite [Relaciones con Inversores de Citigroup](#) (en Políticas de Citi, seleccione Programa antisoborno).

4 REGALO Y ENTRETENIMIENTO

Los proveedores no pueden proporcionar regalos ni otorgar nada de valor (incluido el entretenimiento) a los empleados de Citi, donde hacerlo crearía un conflicto de intereses real o aparente, comprometería la integridad o el juicio del empleado o influiría de manera inadecuada en la toma de decisiones del empleado o provocaría que el empleado actúe en contra de sus deberes. Sin limitar lo anterior, los regalos en efectivo o su equivalente, incluidas las tarjetas de regalo, los certificados de regalo, los sobres rojos y los cupones, no están permitidos bajo ninguna circunstancia y los Proveedores no deben proporcionar regalos de negocios distintos al efectivo que excedan, en total, US \$ 100 por persona por año calendario a un empleado de Citi. La aceptación por parte de cualquier empleado de Citi de regalos de negocios está sujeta a la aprobación previa según el estándar de regalos y entretenimientos de Citi, y puede estar sujeto a límites adicionales según las políticas específicas de negocios, regionales y/o de entidades jurídicas de Citi.

Cuando un Proveedor ofrece entretenimiento de negocios (por ejemplo, invitaciones a comer, o bien, para eventos sociales, deportivos, culturales o similares) a un empleado de Citi, el Proveedor debe asistir al evento, y el entretenimiento debe ser adecuado, convencional y razonable, no debe ser lujoso ni excesivamente frecuente y no debe perseguir el claro objetivo de influir en los negocios de Citi. Si el Proveedor no asiste al evento, el entretenimiento se considerará un regalo de negocios.

El Proveedor no podrá, en nombre de Citi o supuestamente en nombre de Citi, dar regalos, entretenimiento ni ninguna cosa de valor a persona alguna fuera de Citi.

5 DIVERSIDAD DE PROVEEDORES Y PRINCIPIOS DE PROVEEDORES

Citi ha implementado un Programa de Diversidad de Proveedores que, entre otras iniciativas, fomenta el uso de empresas certificadas como propiedad de minorías, mujeres, personas discapacitadas o veteranos como proveedores y subcontratistas ("Proveedores Diversos") en la mayor medida posible para ayudar a los Proveedores Diversos en su crecimiento y desarrollo a largo plazo. Para ayudar a Citi a cumplir con estos objetivos, el Proveedor, de conformidad con sus otras obligaciones en virtud del presente y en la medida en que utilice Subcontratistas o compre bienes o servicios en relación con el desempeño del Proveedor de sus obligaciones en virtud de este Contrato, hará esfuerzos de buena fe para asignar no menos del quince por ciento (15%) de la cantidad que el Proveedor gasta con respecto a sus Subcontratistas en bienes y servicios obtenidos de Diversos Proveedores. El Proveedor proporcionará a Citi información relacionada con los gastos del Proveedor, ya sean directos o indirectos, mediante la compleción del "Formulario de Nivel 2 de Perfil de Diversidad" (que Citi puede proporcionar trimestralmente) por parte de los Proveedores Diversos y el envío del formulario completado a Citi dentro de un plazo de catorce (14) días calendario siguientes al último de:

- i. el cierre del trimestre durante el cual Citi presenta un Formulario de Nivel 2 de Perfil de Diversidad al Proveedor, o
- ii. la fecha en que el Proveedor recibe un Formulario de Nivel 2 de Perfil de Diversidad de Citi.

Citi conservará y tratará todos los Formularios de Nivel 2 del Perfil de Diversidad de acuerdo con las obligaciones de confidencialidad de Citi según se establece en el Apéndice E. El Proveedor enviará todos los Formularios de Nivel 2 del Perfil de Diversidad a la atención del Programa de Diversidad de Proveedores de Citigroup, 388 Greenwich Street, 19th Floor, New York, NY 10013, con atención al Director del Programa de Diversidad de Proveedores.

Hay información adicional disponible en el sitio [Haciendo negocios con Citi](#), que describe las expectativas adicionales de Citi para los Proveedores que se pueden encontrar en:

[Declaración de Principios de Proveedores de Citi](#)

[Estrategia de progreso sostenible de Citi](#)

[Marco de Política Ambiental y Social](#)

[Declaración de derechos humanos de Citi](#)

6 PROHIBICIÓN CONTRA LA ESCLAVITUD MODERNA

Citi se compromete a implementar sistemas y controles destinados a identificar y abordar el riesgo de que la esclavitud moderna y la trata de personas puedan tener lugar dentro de su organización o en cualquiera de sus cadenas de suministro. Todos los Proveedores de Citi deberán cumplir con los Requisitos establecidos a continuación y desarrollar políticas y procedimientos efectivos en toda la empresa para identificar y abordar el riesgo de la esclavitud moderna y la trata de personas dentro de sus propias operaciones y cadenas de suministro. Los proveedores deben completar el Cuestionario de Responsabilidad Corporativa de Citi a pedido de Citi para permitir que Citi evalúe la exposición al riesgo y los posibles pasos de mitigación, particularmente para Proveedores en sectores y geografías de mayor riesgo.

6.1 Prevención del Trabajo Infantil. El proveedor no empleará mano de obra infantil. El término “niño” se refiere a cualquier persona menor de 15 años (o 14 cuando la ley del país lo permita), o menor de la edad para completar la educación obligatoria, o menor de la edad mínima para trabajar en el país, cualquiera que sea menor. Sujeto a la prohibición de anulación respecto de la contratación de fuerza laboral infantil, si se emplea a trabajadores menores de 18 años, se debe considerar particularmente qué tareas llevarán a cabo y las condiciones en las que se requiere que trabajen para garantizar que no sufran daños físicos, mentales ni de otro tipo como resultado directo o indirecto del trabajo o las condiciones laborales.

6.2 Empleo de Libre Elección. El proveedor se asegurará de que los trabajadores NO sean forzados, coaccionados mental o físicamente, en condiciones de servidumbre, contratados o sometidos a trabajo penitenciario involuntario o tráfico de esclavos o sometidos a trabajo obligatorio en cualquier forma, incluidas las horas extraordinarias forzadas. Todo trabajo debe llevarse a cabo de forma voluntaria. Las obligaciones del proveedor en virtud del presente incluyen, entre otras, garantizar lo siguiente:

- i. **Contratos, Salarios y Jornada Laboral:** Los trabajadores deben contar con un documento escrito en el cual se detallen sus términos de empleo o contratación, que les resulte fácil de comprender, y que establezca con claridad sus derechos y obligaciones. Este documento escrito debe incluir, entre otras cosas, términos transparentes con respecto al salario, el pago de horas extras, los períodos de pago, las horas laborales y los derechos relacionados con los descansos y las vacaciones. Dichos términos por escrito se proporcionarán al trabajador antes de que comience a trabajar, deberán ser respetados por el empleador y deberán cumplir con los estándares de la industria y los requisitos mínimos de las leyes aplicables y los convenios colectivos donde se lleva a cabo el trabajo.
- ii. **Derecho a Cesar Librementemente el Trabajo:** Los trabajadores deben tener el derecho de rescindir la relación laboral con libertad, según corresponda tras un período razonable de aviso, de acuerdo con las leyes y los acuerdos colectivos aplicables, sin que se les impongan sanciones inadecuadas.
- iii. **Tratamiento inhumano:** Los trabajadores, sus familiares o aquellas personas estrechamente relacionadas con ellos no deben estar sujetos a tratamiento severo o inhumano, incluidos, entre otros, castigos físicos; violencia física, psicológica o sexual; o coacción, abuso verbal, acoso o intimidación. Los trabajadores inmigrantes, sus familiares o las personas estrechamente relacionadas con ellos no deben estar sujetos a discriminación en sus términos y condiciones laborales debido a su nacionalidad.

- iv. **Salarios, beneficios y horario laboral:** La remuneración debe cumplir con todas las leyes salariales aplicables, incluidas aquellas relacionadas con el salario mínimo, las horas extras y los beneficios obligatorios. Los empleados deben tener la posibilidad de ganar salarios justos, según lo determinado por las leyes locales aplicables. La semana laboral no debe exceder el máximo establecido por las leyes locales.
- v. **No confiscación de documentos de identidad:** No se debe confiscar ni retener los documentos de identidad ni los permisos de viaje, pasaportes u otros documentos oficiales o elementos de valor de los trabajadores como condición de empleo. La retención de propiedad no debe usarse, de forma directa o indirecta, para restringir la libertad de los trabajadores ni para generar esclavitud en el lugar de trabajo.
- vi. **Sin Cargos de Contratación ni Servidumbre por Deudas:** No deben cobrarse a los trabajadores los cargos o costos asociados al reclutamiento de trabajadores (incluidos, entre otras cosas, los cargos relacionados con visas de trabajo, costos de viaje y costos de procesamiento de documentos), ya sea de forma directa o indirecta. De la misma manera, no se debe obligar a los trabajadores a realizar pagos con la intención o consecuencia de generar esclavitud en el lugar de trabajo, incluidos pagos del Seguro Social, ni a liquidar deudas a cambio de su trabajo. Si se determina que se han cobrado honorarios o costos a los trabajadores en relación con el proceso de contratación o se incurre durante el transcurso del empleo, el Proveedor debe buscar que se le reembolsen dichos costos. Cuando sea necesario contratar trabajadores contratados a través de un tercero, como una agencia de empleo, solo se contratarán agencias de empleo acreditadas. Cuando los trabajadores sean contratados para ser empleados directamente, solo se contratarán agencias de contratación acreditadas.
- vii. **Libertad de Movimiento:** Los trabajadores tendrán libertad de movimiento sin restricciones irrazonables y no estarán confinados físicamente al lugar de trabajo u otros lugares controlados por el empleador (por ejemplo, bloques de alojamiento). A los trabajadores no se les debe imponer el requisito de ocupar instalaciones controladas por el empleador, excepto en caso de que esto resulte necesario debido a la ubicación o la naturaleza del trabajo que desempeñan.
- viii. **Reclamos sin represalias:** Los trabajadores tendrán la libertad de presentar quejas a sus empleadores sobre el trato que les da el empleador y los trabajadores no sufrirán perjuicios, represalias o victimización por haber presentado una queja.

7 PERSONAL DEL PROVEEDOR

7.1 Formación, Asignación, Reasignación y Gestión del Personal del Proveedor. El Proveedor utilizará una cantidad adecuada de personas con la capacitación, la educación, la experiencia y las habilidades adecuadas para prestar los Servicios de la manera más efectiva de acuerdo con cualquier Contrato y corroborará las calificaciones de dichas personas a solicitud. Una vez que el Personal haya sido asignado a un Proyecto, el Proveedor no reasignará ni utilizará a ningún Personal para otros asuntos que reduzcan su disponibilidad para trabajar en el Proyecto sin el consentimiento previo por escrito de Citi y, en general, asignará Personal a los Proyectos de una manera que minimice interrupciones por necesidad de reorientación. El Proveedor se asegurará de que su Personal no se presente como empleado o agente de Citi, ni busque ser tratado como empleado de Citi por ningún motivo, incluidas las reclamaciones de derecho a beneficios complementarios proporcionados por Citi, o para ingresos por discapacidad, impuestos de seguridad social o beneficios, impuestos federales de desempleo, beneficios estatales de seguro de desempleo o retención de impuestos federales sobre la renta. El Proveedor es el único responsable de todas las responsabilidades relacionadas con el empleador con respecto a su Personal, incluidas, entre otras, el mantenimiento de todas las coberturas de seguro requeridas, la presentación de todas las declaraciones de impuestos aplicables y la realización de todos los pagos y depósitos de impuestos requeridos de manera consistente con el estado del Proveedor como un contratista independiente.

7.2 Reposición de Personal del Proveedor. El Proveedor eliminará y reemplazará a cualquier Personal asignado por el Proveedor a un Proyecto si Citi notifica al Proveedor que él o ella no es aceptable para Citi por cualquier otro motivo no discriminatorio. El Proveedor también acuerda remover y reemplazar a cualquier Personal asignado a un Proyecto y prohibirle que brinde Servicios a Citi (o cualquier responsabilidad con respecto a la entrega o supervisión de los Servicios) inmediatamente cuando no tenga la capacidad o la disposición de brindar los Servicios de manera oportuna y profesional.

7.3 Políticas de Personal del Proveedor. El Proveedor declara, garantiza y acuerda que mantiene y administra de manera efectiva políticas y procedimientos integrales para calificar a su Personal que son personas naturales y están asignadas para brindar Servicios en el sitio a Citi, y que esas políticas y procedimientos incluyen verificación de autorización de trabajo, verificaciones de antecedentes de historial laboral y condenas penales, como se establece más adelante en este documento, y pruebas de drogas previas al empleo, todo en la medida permitida por la Ley aplicable y cualquier acuerdo de negociación colectiva aplicable. Sin limitar la generalidad de lo anterior, el Proveedor declara, garantiza y acuerda que cuenta con controles y procedimientos para garantizar el pleno cumplimiento por parte del Proveedor de todas las Leyes aplicables relacionadas con la inmigración, incluida la validación de que todo el Personal del Proveedor asignado a Citi esté autorizado para trabajar durante la asignación en pleno cumplimiento de todas las Leyes Aplicables relacionadas con la inmigración. Previa solicitud, el Proveedor proporcionará de inmediato a Citi evidencia escrita de la autorización de trabajo para cualquiera o todo el Personal del Proveedor asignado a Citi y su cumplimiento con la Ley aplicable relacionada con la inmigración y reemplazará a cualquier Personal que no tenga autorización de trabajo de acuerdo con la Ley aplicable con personal reemplazos adecuadamente calificados, incluida la provisión de toda la capacitación y orientación necesarias para garantizar la prestación oportuna y efectiva de los Servicios, en cada caso, sin costo adicional.

8 GESTIÓN DE FRAUDE

8.1 En relación con los esfuerzos de Citi para identificar y mitigar el riesgo de fraude (“Gestión de Fraude”). **Todos los Proveedores deberán:**

- i. Cooperar con cualquier investigación de Citi de presunto o posible robo, fraude u otra posible actividad delictiva o mala conducta, y cualquier enjuiciamiento de conducta fraudulenta o delictiva según las medidas permitidas por la ley;
- ii. Garantizar la notificación y la derivación oportunas de cualquier posible evento de fraude a Citi. Esto incluye, entre otros, intento, sospecha, robo real o presunto, fraude (p. ej., presentación deliberada de datos falsos, inexactos o tergiversados sobre el Proveedor, esquemas de facturación, desaparición de fondos o valores, etc.), actividad delictiva o irregularidades que involucren a Citi, a un empleado de Citi, a un Proveedor o agente de Citi o una persona que no sea un empleado de Citi (por ejemplo, empleados temporales y contratistas);
- iii. Permitir el monitoreo y la supervisión por parte de Citi y sus representantes y apoyar a Citi
– y las fuerzas del orden – a llevar a cabo investigaciones sobre posibles actividades fraudulentas que involucraban a ese Proveedor;
- iv. Informar, de manera oportuna, cualquier conflicto de intereses (incluidos los conflictos de intereses entre Proveedores/Empleados de Proveedores y/o Empleados de Citi) del que tengan conocimiento los Proveedores; y
- v. Apoyar los procesos de prevención de fraude de Citi durante la configuración o actualización de la cuenta bancaria de un Proveedor en el sistema de pago de Proveedores de Citi.

8.2 Además de esto, los Proveedores que brindan servicios que están inherentemente más expuestos al riesgo de fraude **deben:**

- i. Documentar y seguir el Programa de Gestión de Riesgos de Fraude que identifica los riesgos de fraude significativos relevantes a los servicios que prestan a Citi y los controles y procedimientos que se aplican para mitigar dichos riesgos;
- ii. Completar la capacitación de concientización sobre fraude (dentro de los 90 días calendario posteriores a la contratación y anualmente a partir de entonces) y capacitar al personal sobre los elementos específicos del riesgo de fraude que se relacionan con los servicios específicos brindados a Citi; y
- iii. Monitorear instancias de intentos de fraude y mantener controles efectivos para mitigar el riesgo de fraude en los servicios que prestan a Citi, documentar procedimientos para los controles y probar la efectividad de los controles de forma constante, generando reportes de cualquier deficiencia encontrada al Responsable de la Actividad Comercial (Business Activity Owner, BAO).

8.3 Los Proveedores con mayor riesgo inherente de fraude incluyen, entre otros, aquellos que:

- i. tienen acceso a datos clasificados como Confidenciales o superiores (cuando no están bajo el control o la supervisión directos de Citi) que pueden usarse para permitir fraudes como el acceso a cuentas internas, transacciones financieras, transacciones en efectivo.
- ii. tienen conectividad a las redes o sistemas de Citi; y

- iii. proporcionan, respaldan o tienen acceso a servicios y capacidades que podrían ser objetivos para cometer o permitir fraudes, inclusive:
- a. Identificación, incorporación o procesamiento de solicitudes de nuevos clientes;
 - b. Actividades de pago/transferencia de fondos de Citi o Clientes, y/o la autenticación del acceso de clientes de Citi a estos servicios;
 - c. Realización, verificación o compleción de cambios a datos de Citi o clientes de Citi (p. ej., grupos demográficos);
 - d. Provisión, servicio o autorización de instrumentos transaccionales (p.ej., tarjetas de débito/crédito, billeteras electrónicas (eWallets), chequeras, etc.);
 - e. Provisión o respaldo de actividades de gestión de fraudes operacionales a Citi, relacionadas con la prevención, detección o respuesta a eventos de fraude;
 - f. Provisión de acceso físico a dinero en efectivo, instrumentos financieros y activos / bienes físicos;
 - g. Acceso sin escolta o fuera de horario a las instalaciones de Citi;
 - h. Estados financieros: actividades contables, como contabilización de entradas en el libro mayor / libro auxiliar;
 - i. Obtención y gasto de recompensas por actividades incentivadas.

9 INTERACCIÓN CON LOS MEDIOS Y APARICIONES PÚBLICAS

Asuntos Públicos Globales de Citi es el único departamento autorizado para emitir comunicados de prensa o declaraciones públicas en nombre de Citi. Los proveedores no pueden emitir comunicados de prensa que identifiquen directa o indirectamente a Citi, ningún contrato o acuerdo entre un proveedor y Citi ni ningún producto o servicio que Citi adquiera de un proveedor. Los Proveedores no pueden dar su consentimiento ni participar en ninguna actividad de relaciones públicas relacionada con Citi con Clientes, empleados de Citi, otros Proveedores de Citi, otros clientes de Proveedores o cualquier otro tercero sin la aprobación previa por escrito de su principal contacto comercial de Citi.

Los proveedores no pueden publicar ni postear ningún material en formato escrito o electrónico (incluidos libros, artículos, podcasts, webcasts, blogs, publicaciones en sitios web, fotos, videos, redes sociales u otros medios), realizar o dar discursos, dar entrevistas o hacer apariciones públicas que mencionen a Citi, las operaciones, los Clientes, los productos o los servicios de Citi, sin la aprobación previa por escrito de su contacto comercial principal de Citi y el funcionario de asuntos públicos sénior del país o la región.

Ya sea en relación con la prestación de servicios o productos a Citi o no, los Proveedores no pueden usar los signos, marcas registradas, marcas de servicio, nombres comerciales, logotipos, símbolos o nombres de marca de propiedad de Citi, sin, en cada caso, obtener el consentimiento previo por escrito de Citi. Los proveedores no pueden usar el nombre, el logotipo o las marcas comerciales, las instalaciones o las relaciones de Citi para beneficio o para trabajar fuera de Citi (incluso en membretes o sitios web personales, blogs u otros sitios de redes sociales). Además, los Proveedores no podrán hacer uso del nombre, las instalaciones o relaciones de Citi para fines de beneficencia o gratuitamente.

10 COMUNICACIONES ELECTRÓNICAS ESCRITAS

Al interactuar con el personal de Citi, o en el desempeño de sus obligaciones para o en nombre de Citi, los Proveedores pueden usar solo aquellos Equipos, Sistemas y Servicios de Comunicaciones Electrónicas que son proporcionados, sancionados o aprobados por Citi. Los Canales de eComm de Citi nuevos, ampliados o modificados, ya sea como una herramienta independiente o integrada en una plataforma más amplia, proporcionada por Citi o por un tercero, deben aprobarse de acuerdo con los Requisitos de Citi aplicables contenidos en el presente, o de los cuales el Proveedor haya sido notificado en escrito por su BAO. Queda prohibido comunicarse con el personal de Citi sobre el negocio de Citi a través de plataformas de mensajería no aprobadas por Citi, como WhatsApp, WeChat y cualquier otra plataforma electrónica interactiva.

Además, los Proveedores no deben tener expectativas de privacidad con respecto a las Comunicaciones Electrónicas escritas creadas, descubiertas, utilizadas, accedidas, descargadas, almacenadas, transmitidas, recibidas o eliminadas a través de los Equipos, Sistemas y Servicios de Comunicaciones suministrados por Citi. Citi puede monitorear los Equipos, Sistemas y Servicios de Comunicaciones Electrónicas así como las Comunicaciones Electrónicas. Dichas Comunicaciones Electrónicas son propiedad de Citi y pueden retenerse de conformidad con los requisitos aplicables para la retención de registros (sujeto a las leyes y regulaciones locales).

11 ACTIVIDADES POLÍTICAS Y CONTRIBUCIONES

Una variedad de leyes, como financiamiento de campañas, regalos y entretenimiento, cabildeo legislativo y regulatorio, adquisiciones, pago por juego y valores, regulan las actividades políticas, incluidos los requisitos de divulgación, de Citi y sus Proveedores. Se prohíbe cualquier actividad política por parte de los Proveedores que no cumpla con las políticas, normas o leyes relevantes de Citi.

La actividad política incluye pero no se limita a:

- i. hacer contribuciones políticas corporativas o personales, solicitar contribuciones políticas, usar fondos o recursos de la empresa (como instalaciones, equipos, software o personal) u ofrecer servicios personales voluntarios durante el tiempo de la empresa en nombre de un candidato que hace campaña para un cargo público, un comité de partido político o un comité político;
- ii. cabildeo o participación en cualquier acercamiento a funcionarios públicos, ya sea directamente o a través de terceros, incluidos los intentos de influir en la legislación y, según la jurisdicción, puede incluir intentos de influir en la elaboración de normas de la agencia o la adjudicación de contratos gubernamentales; o
- iii. buscar, aceptar u ocupar cualquier cargo político asociado con un gobierno, incluida cualquier junta, comisión u otra organización similar del gobierno.

Ningún Proveedor puede emprender o realizar ninguna actividad política en nombre de (o supuestamente en nombre de) Citi sin la autorización previa por escrito del Control de Operaciones Globales de Asuntos Gubernamentales Globales de Citi (ggacontrol@citi.com). Aunque Citi puede pagar un cargo

y/o reembolsar los gastos de bolsillo por servicios de actividad política permitidos y contratados proporcionados por el Proveedor, como cabildeo, Citi nunca reembolsará a un Proveedor ni a ninguno de sus empleados por contribuciones políticas personales o corporativas de ningún tipo.

12 ANTI-LAVADO DE DINERO (“AML”)

Aplicable a los Proveedores que realizan ciertos servicios relacionados con clientes (es decir, incorporación, verificación de cuentas y transacciones de clientes) o la entrega de datos/métricas relacionadas con las actividades anteriores; Y/O actuar como intermediario con respecto a efectivo o instrumentos financieros (p. ej., captura remota de depósitos, servicios de mensajería, vehículos blindados o cajas de seguridad).

12.1 Obligaciones Relacionadas con AML:

- i. Mantener y cumplir con los procesos y procedimientos de Citi diseñados para abordar los requisitos de las leyes aplicables, incluida (i) la Ley Gramm-Leach-Bliley y las reglamentaciones promulgadas en virtud de la misma; (ii) la Ley USA PATRIOT y los reglamentos promulgados en virtud de la misma; (iii) cualquier ley o reglamento que aborde el lavado de dinero; y (iv) cualquier ley o reglamento relacionado con sanciones económicas. Dichas políticas y procedimientos abordarán las funciones y responsabilidades contra el lavado de dinero, incluidos los requisitos para informar de inmediato cualquier actividad observada que parezca inusual o potencialmente inusual relacionada con la entrada de efectivo; y
- ii. Asegurarse de que las personas de su Personal que brinden Servicios a Citi reciban capacitación anual con respecto a las funciones y responsabilidades contra el lavado de dinero, incluidos los requisitos para informar de inmediato cualquier actividad observada que parezca inusual o potencialmente inusual relacionada con la entrada de efectivo. La capacitación puede incluir componentes tales como:
 - a. Generación de informes y escalamiento de actividades sospechosas
 - b. Un programa de “Conozca a Su Cliente”, incluido un Programa de Identificación de Clientes, verificación de sanciones y nombres, diligencia debida para clientes y diligencia debida mejorada.
 - c. Monitoreo de transacciones
 - d. Generación periódica de informes/métricas, incluidos informes sobre cambios regulatorios o jurídicos y cambios significativos de los programas de AML
 - e. Pruebas y controles de la efectividad del programa de AML, incluidas visitas presenciales
- iii. Cumplir con cualquier disposición del Contrato que defina cualquier programa AML que deba ser instituido por el Proveedor.
- iv. Informar inmediatamente a Citi por escrito de cualquier sospecha de incumplimiento de la ley, incluida cualquier actividad observada que parezca inusual o potencialmente inusual relacionada con la entrada de efectivo relacionada con Citi o sus clientes.
- v. Cumplir con todas las leyes y regulaciones fiscales aplicables en los países donde operan. Bajo ninguna circunstancia los proveedores deben participar en una evasión fiscal deliberada ilegal o facilitar dicha evasión en nombre de otros, lo que puede incluir participar en actividades que ayuden a evadir el pago de los impuestos adeudados y pagaderos u ocultar información de las autoridades fiscales. Como tal,

los Proveedores adoptarán procedimientos de prevención razonables relacionados con la evasión de impuestos e informarán de inmediato a Citi por escrito sobre cualquier infracción o sospecha de infracción que se relacione con Citi.

- 12.2** Los proveedores deberán mantener políticas y procedimientos internos apropiados para cumplir con todas las leyes y reglamentaciones AML actualmente existentes o que entren en vigor en el futuro.

13 GESTIÓN DE REGISTROS

Aplicable a Proveedores que acceden a, procesan o almacenan Información de Citi.

Citi requiere que todos los Proveedores con la custodia de la Información de Citi trabajen con su Responsable de la actividad comercial ("**BAO**") o el contacto comercial principal de Citi para (i) identificar y clasificar la Información como Registros o Transitoria para los fines de administración de registros de Citi, (ii) clasificar los Registros de acuerdo con el Catálogo de Registros Maestros de Citi ("**MRC**"), (iii) conservar la Información en función de los requisitos de retención y (iv) en ausencia de Retenciones de Registros, disponer adecuadamente de la Información al final del Ciclo de Vida de la Información.

El proveedor debe trabajar con su contacto comercial principal de Citi o BAO para garantizar que el Inventario de registros identifique y clasifique los registros de acuerdo con los códigos de registro de Citi en el MRC y se actualice al menos una vez al año. El Proveedor tiene la obligación de respetar los requisitos de gestión de Registros comunicados por el BAO. Los registros y la información que hayan cumplido con la obligación de retención enumerada en el MRC y que no estén sujetos a retención de registros, deben desecharse dentro de un año de ser elegible para disposición. Los registros sujetos al Reglamento general de protección de datos (GDPR) deben eliminarse dentro de los 6 meses posteriores a la elegibilidad para su eliminación, a menos que estén sujetos a Retención de registros. El Proveedor debe suspender la destrucción o alteración de la Información de Citi cuando se le notifique una Retención de registros. La información transitoria debe destruirse no más de dos años después de su último uso, a menos que esté sujeta a Retención. El proveedor consultará con su principal contacto comercial de Citi o con el BAO en caso de duda.

Los proveedores que mantienen documentos en nombre de Citi son responsables de preservar ("mantener"), recopilar y producir toda la información que se considere relevante para un procedimiento legal o de otro tipo dentro del tiempo requerido según lo solicite el BAO.

Los proveedores no deben deshacerse de ninguna Información de Citi, independientemente de su clasificación (p. ej., Confidencial, No confidencial) sin su contacto comercial principal de Citi o la aprobación del BAO, que debe incluir la confirmación de que no se aplican Retenciones de registros activas a la Información que debe eliminarse. Los requisitos de gestión y retención de registros y todos los demás requisitos de manejo de información seguirán vigentes después de la terminación o vencimiento del contrato, a menos que se acuerde explícitamente lo contrario.

Los proveedores deberán mantener una lista de documentación de todo el personal del proveedor responsable de supervisar la gestión de la información de Citi bajo la custodia del proveedor y celebrar reuniones periódicas con su contacto comercial principal de Citi o el oficial de gestión de registros para revisar y actualizar los nombres de los contactos, los detalles de los procedimientos, las funciones y responsabilidades y el inventario de registros del proveedor.

14 SERVICIOS DE CARA AL CLIENTE

Aplicable al Proveedor que interactúa con cualquier individuo en calidad de cliente pasado, actual o potencial de Citi o de una parte relacionada (como un empleado o un representante) de dicho cliente (cada individuo, un "Cliente").

14.1 Horas Laborales. El Proveedor deberá instruir y hacer esfuerzos razonables para garantizar que aquellas personas de su Personal que trabajen en las instalaciones de Citi no intenten acceder a las instalaciones de Citi fuera del horario laboral normal (o en un feriado programado) para esas instalaciones y para cooperar con, y cumplir con las instrucciones relacionadas con la seguridad del Personal de Citi.

14.2 Políticas y Procedimientos. Con respecto a los Servicios orientados al cliente únicamente: El Proveedor reconoce y acepta que su compromiso en virtud de cualquier Contrato de que su Personal que trabaja en las instalaciones de Citi cumpla con las políticas y procedimientos del lugar de trabajo de Citi incluye el cumplimiento de los procedimientos de seguridad física y otras medidas de seguridad de Citi y sus Filiales. Citi hará todos los esfuerzos razonables para mantener al Proveedor informado sobre todos los procedimientos de seguridad física y otras medidas de seguridad. Citi tendrá la discreción de emitir, activar, confiscar y desactivar tarjetas de identificación, llaves u otros dispositivos de seguridad para o del Personal del Proveedor que trabaje en las instalaciones de Citi; siempre que no se considere que la realización de estas acciones por parte de Citi implique una relación laboral entre Citi y dicho Personal.

14.3 Plan de Recuperación Ante Desastres. El Proveedor mantendrá un plan de contingencia (un "Plan de Recuperación Ante Desastres") para la continuación del negocio (y proporcionará evidencia de sus pruebas actuales y periódicas si Citi lo solicita) para que, a pesar de cualquier interrupción en la capacidad del Proveedor para proporcionar los Servicios o realizar su otras obligaciones en virtud del presente desde cualquier lugar en particular o mediante los esfuerzos de cualquier individuo en particular, el Proveedor podrá proporcionar los Servicios y cumplir con sus obligaciones de inmediato desde un lugar alternativo o con Personal de reemplazo. Se debe proporcionar a Citi una copia del Plan de Recuperación Ante Desastres dentro de los diez (10) días calendario posteriores a la Fecha de entrada en vigencia de cada Orden de trabajo celebrada entre Citi y el Proveedor para los Servicios orientados al cliente, y anualmente a partir de entonces mientras cada Orden de trabajo esté en efecto. El Proveedor proporcionará a Citi cualquier instrucción u otra información necesaria para que Citi continúe recibiendo los Servicios del Proveedor en circunstancias en las que el Proveedor haya tenido que invocar su Plan de Recuperación Ante Desastres. El proveedor declara, garantiza y acuerda que su Plan de Recuperación Ante Desastres incluirá, como mínimo:

- i. el mantenimiento por parte del Proveedor de un sitio de recuperación de desastres secundario separado de las ubicaciones del Servicio, el almacenamiento de medios de respaldo en una ubicación separada de las ubicaciones del Servicio, el uso de líneas de comunicación y servidores redundantes, etc.
- ii. procedimientos para el respaldo/restauración del funcionamiento y la aplicación de los Servicios, incluido un plan detallado y documentado para responder a una interrupción prolongada en los Servicios causada por fallas en el suministro eléctrico, fallas en el sistema, desastres naturales u otras circunstancias imprevistas que incluyen procesos y procedimientos para reanudar las operaciones dentro de un período de tiempo acordado mutuamente;
- iii. procedimientos para la protección de todo el Contenido;

- iv. procedimientos y acuerdos con terceros para equipos de reemplazo (p. ej., equipos informáticos), y
- v. procedimientos para cualquier instalación de producción fuera del sitio. Además, el plan de Recuperación Ante Desastres del Proveedor estipulará que:
 - a. El Proveedor notificará a Citi por escrito dentro de un plazo de dos (2) horas de cualquier desastre que pueda afectar negativamente a los Servicios;
 - b. El Proveedor proporcionará a Citi, dentro de las 24 horas posteriores a dicha notificación, un plan para continuar brindando los Servicios en una instalación de procesamiento alternativa, y
 - c. los Servicios deben estar completamente operativos dentro de las 48 horas posteriores al aviso inicial. El Proveedor acepta, previa solicitud, divulgar la información necesaria para permitir que Citi desarrolle un plan de recuperación ante desastres y un plan de continuidad del negocio, que funcionarán en conjunto con el plan de recuperación ante desastres y el plan de continuidad del negocio del Proveedor. El Proveedor acepta probar anualmente su plan de recuperación ante desastres y, previa solicitud, proporcionar un informe escrito de los resultados de la prueba de recuperación ante desastres a Citi. En el caso de que partes de las instalaciones del Proveedor no funcionen, el Proveedor tratará a Citi de manera no menos favorable que el Proveedor trata a sus otros clientes comerciales. El Proveedor se asegurará de que cualquier Subcontratista del Proveedor mantenga un Plan de Recuperación Ante Desastres y procesos y controles relacionados que sean totalmente consistentes con las disposiciones y requisitos de esta Sección.

14.4 Certificado de Diligencia. El Proveedor reconoce que Citi y sus Afiliadas están obligadas a llevar a cabo una diligencia regular de aquellos de sus proveedores que brindan Servicios orientados al Cliente a través de un cuestionario/certificado anual (el “Certificado de Diligencia”) que aborda:

- i. Licencias comerciales del proveedor (incluidos artículos de incorporación, certificados de buena reputación, cualquier licencia requerida aplicable),
- ii. Cumplimiento del Proveedor con la Legislación Aplicable,
- iii. Cobertura del seguro,
- iv. Habilidades, calificaciones y experiencia
- v. La capacidad del proveedor (incluidos los niveles de dotación de personal y el equilibrio de la carga de trabajo),
- vi. Procesos comerciales relevantes,
- vii. Prácticas de compensación,
- viii. Viabilidad financiera y riesgo de contraparte,
- ix. Riesgo a la reputación (reclamaciones / litigios pendientes),
- x. Políticas y prácticas de cara al cliente,
- xi. Referencias del Proveedor,
- xii. relación de beneficiarios principales,
- xiii. dependencia de subcontratistas, contratistas o terceros proveedores,
- xiv. revisión del programa de formación,
- xv. plan de negocios continuo,
- xvi. resultados de auditoría de calidad y cumplimiento de cualquier compromiso de nivel de servicio aplicable, y
- xvii. gestión y almacenamiento de documentos.

El Proveedor, de vez en cuando, proporcionará a Citi cualquier otra información o documentos que Citi pueda solicitar para garantizar el cumplimiento de (i) cualquier Contrato, (ii) las políticas corporativas de Citi y (iii) los requisitos reglamentarios aplicables a Citi y al Proveedor.

14.5 Seguridad. Si alguna Información Confidencial se mantiene o se almacena de alguna manera en un sitio web o en un sistema accesible a través de la web, el Proveedor se lo comunicará a Citi, y dicha divulgación se podrá incluir en la descripción de los Servicios. Si el Proveedor mantiene o almacena Información Confidencial de Citi como se contempla anteriormente, entonces el Proveedor;

- i. hará que se realice una auditoría SSAE 16 (o cualquier guía autorizada sucesora para informar sobre organizaciones de servicios) una vez al año durante la vigencia de este Acuerdo, y (b) proporcionará a Citi, no más de una vez al año, una copia de los informes que reciba el Proveedor relacionados con el cumplimiento de SSAE 16 (o cualquier guía autorizada sucesora para informar sobre organizaciones de servicios);
- ii. cumplirá con los estándares de gestión de seguridad de la información ISO/IEC 207002 (o los estándares de gestión de seguridad de la información sucesores que establecen estándares y protocolos más altos); y (iii) se atenderá a las disposiciones de seguridad informática.

14.6 Quejas de Clientes. El Proveedor notificará por escrito a su contacto comercial principal de Citi (o persona designada) dentro de las veinticuatro (24) horas de cualquier presentación escrita u oral de insatisfacción o inquietud (cada una, una "Reclamación") recibida por el Proveedor de cualquier Cliente o de cualquier Regulador relacionado con los Servicios provistos por el Proveedor en nombre de Citi o de otra forma relacionado con Citi, incluida cualquier Queja en referencia a la posesión o uso de Datos del Cliente o a los derechos a la privacidad del Cliente. A menos que Citi ponga dicho sistema a disposición del Proveedor, el Proveedor también desarrollará, implementará y mantendrá un sistema ("Sistema de Seguimiento") razonablemente satisfactorio para Citi para realizar un seguimiento de las Quejas y proporcionar a Citi, a su discreción, una copia de los informes o acceso a los sistemas. El Sistema de Seguimiento:

- i. categorizará las Quejas por tipo, fecha de recepción y fecha de notificación de la Queja a Citi,
- ii. dará seguimiento al curso del manejo de la Queja hasta su conclusión/resolución, y
- iii. dispondrá sobre todos los demás asuntos que Citi pueda solicitar razonablemente. El Sistema de seguimiento debe estar diseñado para permitir que el Proveedor determine si recibe una cantidad excesiva de Quejas con respecto a un asunto en particular para que el Proveedor (en consulta con Citi) pueda determinar si existe un problema sistémico relacionado con el negocio del Proveedor o su provisión de Servicios y corrija los problemas de forma inmediata.

14.7 Seguridad de Redes y Comunicaciones. Implemente múltiples capas de defensa, incluso en los sistemas del proveedor, pero sin limitarse a firewalls, detección de intrusos en la red y sistemas de detección de intrusos basados en host. Todos los sistemas de monitoreo de seguridad, incluidos, entre otros, firewalls y sistemas de detección de intrusos, deben monitorearse las 24 horas del día, los 365 días calendario del año. Configure firewalls, enrutadores de red, conmutadores, balanceadores de carga, servidores de nombres, servidores de correo y otros componentes de red de acuerdo con estándares comerciales razonables de la industria. A pedido de Citi, con base en la información recibida por Citi sobre vulnerabilidades y amenazas, restrinja el acceso a cualquier componente específico de Citi de las redes, sistemas y aplicaciones utilizadas para brindar servicios bajo cualquier Contrato.

- 14.8 Plataformas de Infraestructura, Servicios y Seguridad de las Operaciones.** Configure todas las plataformas y servicios de infraestructura (sistemas operativos, servidores web, servidores de bases de datos, firewalls, enrutadores, etc.) utilizados para prestar servicios bajo cualquier Contrato y mecanismos de autenticación de acuerdo con las mejores prácticas de la industria. Asegúrese de que todo el acceso administrativo remoto a los sistemas de producción se realice a través de conexiones cifradas (es decir, SSH, SCP, interfaces de administración web habilitadas para SSL y soluciones VPN).
- 14.9 Seguridad de la Aplicación.** Permita que solo los usuarios autenticados y autorizados vean, creen, modifiquen o eliminen información administrada por aplicaciones utilizadas en relación con la prestación de servicios en virtud de cualquier Contrato. Asegúrese de que las cookies del navegador web que almacenan datos confidenciales estén cifradas mediante un algoritmo de cifrado público y ampliamente aceptado. Este cifrado debe realizarse independientemente de cualquier cifrado de transporte, como Secure Sockets Layer. Todas las demás cookies deben ser opacas. "Pause" y finalice las sesiones de comunicación del sistema después de un período de inactividad del usuario acordado mutuamente. Finalice cualquier sesión activa interrumpida por fallas en el suministro eléctrico, "caída del sistema", problema de red u otra anomalía, o cuando el usuario interrumpa la conexión. Valide todas las entradas y salidas antes de su uso para evitar ataques basados en datos como "secuencias de comandos entre sitios" e "inyección de SQL".
- 14.10 Seguridad de Datos.** Transmita toda la información altamente confidencial de Citi a través de algún mecanismo que no sea un navegador web, utilizando un algoritmo de cifrado aprobado por Citi. Cuando se requiera el almacenamiento de una base de datos, almacene toda la información de Citi clasificada como "Confidencial" o superior en una base de datos separada (es decir, una base de datos que no sea compartida con otros clientes del Proveedor ni accesible para ellos).
- 14.11 Seguridad Física.** Mantenga todas las estaciones de trabajo, servidores y equipos de red utilizados para prestar servicios en virtud de cualquier Contrato en instalaciones seguras de propiedad, operadas o contratadas por el Proveedor. Limite el acceso a estas instalaciones seguras a los miembros autorizados del personal del Proveedor con necesidades relacionadas con el trabajo. Supervise el acceso a estas instalaciones seguras mediante el uso de guardias de seguridad, cámaras de vigilancia, sistemas de entrada autorizados o métodos similares capaces de registrar la información de entrada y salida. Mantenga todos los medios de respaldo y archivos que contengan información de Citi u otra información utilizada para prestar servicios en virtud de cualquier Contrato, en áreas de almacenamiento seguras y con control ambiental que sean propiedad del Proveedor, que sean operadas o contratadas por este. Limite el acceso a las áreas de almacenamiento de respaldo y medios de archivo y a su contenido a los miembros autorizados del personal del proveedor con necesidades relacionadas con el trabajo.
- 14.12 Código Malicioso y Protección Antivirus.** Utilice los últimos productos de protección y detección de virus y códigos maliciosos disponibles en el mercado en todas las estaciones de trabajo y servidores utilizados para prestar servicios en virtud de cualquier Contrato. Informe a Citi sobre todos los casos de virus y códigos maliciosos, que no se manejen mediante las medidas de protección y detección implementadas, en cualquier estación de trabajo o servidor utilizado para brindar servicios en virtud de cualquier Contrato, dentro de las 24 horas posteriores al descubrimiento.
- 14.13 Continuidad de Negocio y Recuperación.** Realice respaldo de todos los sistemas, aplicaciones y datos utilizados para prestar servicios en virtud de cualquier Contrato de manera consistente con la reanudación del negocio especificada en cualquier otra parte de cualquier Contrato.

14.14 Estándares Regionales de Nivel de Servicio. Cada región es responsable de resolver y responder a las quejas e inquietudes de manera oportuna. Consulte los estándares/procedimientos regionales que incluyen la implementación y la definición de estándares de nivel de servicio. Las empresas cubiertas calcularán la puntualidad con las siguientes fechas de inicio:

- i. Para las interacciones telefónicas y personales, el Estándar de Nivel de Servicio comienza en la fecha en que la organización recibió la queja/inquietud.
- ii. Para las comunicaciones escritas y electrónicas y las redes sociales, el Estándar de Nivel de Servicio comienza en la fecha en que se detectó la insatisfacción.

14.15 Grabación de Llamadas y Retención de Llamadas. Los proveedores deben implementar un proceso para grabar y almacenar todas las llamadas relacionadas con Quejas/Inquietudes que son atendidas en los Centros de Llamadas por los empleados y sus gerentes directos, cuya función principal es hablar con los consumidores durante al menos 12 meses a partir de la fecha de la llamada, a menos que los requisitos reglamentarios locales indiquen lo contrario. Transfiera periódicamente los medios de respaldo a una instalación de almacenamiento segura fuera del sitio.

15 CONTINUIDAD DEL NEGOCIO

Aplicable a Proveedores que están incluidos en el Plan de Recuperación para la unidad de Negocios de Citi o si el proveedor aloja una aplicación con capacidades de recuperación (es decir, Capacidad de Tiempo de Recuperación de Tecnología numérica (TRTC)), que es utilizada por Citi. Citi Business (BAO) es responsable de comunicar la aplicabilidad y los requisitos COB al Proveedor.

15.1 Recursos de Recuperación. El Plan de Recuperación Ante Desastres de los Proveedores debe proporcionar recursos alternativos capaces de entregar todos los productos y servicios a Citi en caso de que las ubicaciones principales del Proveedor queden inhabilitadas. Los recursos de recuperación deben estar ubicados en ubicaciones separadas geográficamente de las ubicaciones principales con suficiente separación para minimizar o eliminar la amenaza de que el mismo evento de desastre pueda afectar tanto a las ubicaciones principales como a las de recuperación (en el caso de proveedores de aplicaciones SaaS alojadas en proveedores de servicios en la nube (CSP), dicha separación geográfica requiere Regiones CSP distintas para los entornos primario y CoB). Los recursos de recuperación no se limitan a sistemas de información, sino que incluyen todos los recursos necesarios para el suministro ininterrumpido de productos y servicios a Citi, y pueden incluir personal, edificios, equipos comerciales, centros de datos, redes de voz y datos, y servicios de transporte.

15.2 Niveles de Servicio de Recuperación. La continuidad comercial del proveedor debe cumplir con los niveles de servicio establecidos para que sea eficaz para Citi. Un Proveedor que aloja las Aplicaciones críticas de franquicia (FCA) de Citi utilizadas para el procesamiento de transacciones críticas, debe tener una medida de "brecha de aire" para respaldar los datos críticos necesarios para la recuperación, de modo que los datos de respaldo sean inmutables y/o almacenados fuera de línea (desconectados de la red), y la restauración de datos se puede lograr dentro de la capacidad de tiempo de recuperación de tecnología (TRTC) requerida. Como mínimo, el Plan de Recuperación Ante Desastres del Proveedor deberá establecer valores específicos para:

- i. El Tiempo de Recuperación Objetivo;
- ii. El Punto de Recuperación Objetivo;
- iii. La Capacidad de Recuperación; y

iv. La Duración de la Recuperación.

15.3 Plan de Recuperación Ante Desastres. La Política de Continuidad de Negocios de Citi requiere que los Proveedores que están incluidos en un Plan de Recuperación de Negocios de Citi tengan un Plan de Recuperación Ante Desastres para ayudar a garantizar que Citi continúe recibiendo los servicios de ubicaciones alternativas o con Personal de reemplazo a más tardar en el Tiempo de Recuperación Objetivo aplicable. Los Proveedores deben consultar con el principal contacto comercial de Citi correspondiente para comprender si es necesario que cuenten con un Plan de recuperación en caso de desastre y cuáles de los requisitos de Citi son aplicables a dicho plan, incluso aquellos con respecto a los RTO, los cuales, si no se define otra cosa en el contrato aplicable, son 4 horas o menos para aquellos procesos calificados por Citi como con una calificación de criticidad de “1”, 24 horas o menos para aquellos procesos calificados por Citi como con una calificación de criticidad de “2” y 72 horas o menos para aquellos procesos calificados por Citi como con una calificación de criticidad de “3”. El Proveedor proporcionará una copia en inglés del Plan de Recuperación Ante Desastres a Citi dentro de un plazo de diez (10) días calendario a partir de la fecha de entrada en vigencia del acuerdo en virtud del cual surge la obligación del Proveedor de cumplir con los requisitos de esta Sección 14, y anualmente a partir de entonces, junto con evidencia de sus pruebas actuales y periódicas (si Citi lo solicita).

15.4 Invocación del Plan de Recuperación Ante Desastres y Notificación de Crisis. El Proveedor notificará de inmediato al contacto comercial principal de Citi:

- i. cuando el Proveedor invoque su Plan de Recuperación Ante Desastres y;
- ii. en relación con cualquier crisis, amenaza, advertencia o evento cibernético contra el Proveedor o sus subcontratistas que sea razonablemente probable que tenga un impacto adverso en los servicios o productos proporcionados a Citi.

15.5 Pruebas. Todos los recursos y planes de recuperación del Proveedor deben probarse anualmente como mínimo. Las pruebas deberán demostrar la capacidad del Proveedor para cumplir con los niveles de servicio de recuperación para todos los productos y servicios entregados a Citi. Estas pruebas deben ser integrales e incluir el alcance completo de los Servicios proporcionados a Citi. Además, las pruebas deben incluir en su alcance eventos tanto naturales como provocados por el hombre, junto con ataques cibernéticos que incluyen, entre otros, ataques de denegación de servicio, ataques de denegación de servicio distribuido, ataques de malware y ransomware. Los proveedores deben notificar a Citi con al menos 30 días calendario de anticipación sobre las pruebas de recuperación de los servicios prestados a Citi. Citi puede participar u observar las pruebas de recuperación del Proveedor. Si Citi desea participar, el Proveedor le proporcionará a Citi los objetivos de la prueba, el plan de prueba y los procedimientos para conectarse al sitio de prueba antes de realizar la prueba. El Proveedor proporcionará a Citi dentro de un plazo de diez (10) días hábiles después de completar cada prueba, un resumen de los objetivos de la prueba, y el plan y los resultados de la prueba, incluidos los plazos necesarios para recuperar las funciones comerciales críticas y la evidencia de los resultados de la prueba (p. ej., capturas de pantalla).

15.6 Los proveedores deben probar los siguientes escenarios de interrupción:

- i. Negación de Acceso (Denial of Access, DOA)
- ii. Negación de Servicio (Denial of Service, DOS)

15.7 Participación de Citi / Revisión de Pruebas de Proveedores. Para cualquier prueba (incluida una nueva prueba) por parte del Proveedor de su Plan de Recuperación Ante Desastres, Citi participará en una actividad acorde con la Criticidad del Proceso/RTO.

15.8 Para pruebas de Denegación de Acceso (DOA):

- i. Procesos más críticos para la franquicia Citi. Citi participará en, u observará, las actividades de pruebas del Proveedor para todos los procesos que haya definido como “Críticos para la franquicia”. Para tales procesos, el Proveedor permite a Citi revisar los planes de recuperación que abarcan negocio y/o tecnología (según corresponda), guiones de las pruebas, resultados de las pruebas y evidencias.
- ii. Procesos con un RTO $\leq$ 24 horas. A menos que Citi solicite lo contrario, Citi no tiene que participar/observar las actividades de prueba del Proveedor; sin embargo, revisará los planes de recuperación que abarcan negocio y/o tecnología (según corresponda), guiones de las pruebas, resultados de las pruebas y evidencias.
- iii. Procesos con un RTO $>$ 24. A menos que Citi solicite lo contrario, Citi requerirá confirmación del Proveedor respecto a la planificación de recuperación que abarca negocio y/o tecnología (según corresponda), guiones de las pruebas, resultados de las pruebas y evidencias.

15.9 Para pruebas de Denegación de Servicio (DOS):

- i. Procesos con un RTO $\leq$ 72 horas. Citi participará en, u observará, las actividades de pruebas del Proveedor para todas las aplicaciones. El Proveedor permite a Citi revisar los planes de recuperación que abarcan tecnología, guiones de las pruebas, resultados de las pruebas y evidencias.
- ii. Procesos con un RTO $>$ 72 horas. A menos que Citi solicite lo contrario, Citi requerirá la certificación del Proveedor para la planificación de recuperación que cubra negocios y /o tecnología (según corresponda), guiones de prueba y resultados de prueba.

15.10 Abordar los Resultados de las Pruebas. Si los resultados de una prueba del Proveedor muestran deficiencias en el cumplimiento de los objetivos de la prueba o cualquier RTO aplicable, el Proveedor tendrá la responsabilidad de realizar un análisis de causa raíz y corregir rápidamente todas las deficiencias identificadas. Luego de la implementación de dicha medida correctiva, el Proveedor deberá realizar una nueva prueba a más tardar ciento veinte (120) días calendario posteriores a la falla de la prueba inicial (o el período de tiempo especificado en la Orden de trabajo correspondiente).

15.11 Pruebas de Volumen. Un Proveedor que aloja Aplicaciones Críticas de Franquicias (FCA) de Citi utilizadas para el procesamiento de transacciones críticas debe demostrar que los volúmenes de Producción se pueden procesar en su entorno CoB/recuperación de desastres. Citi y el Proveedor deben acordar la metodología a usar para la validación.

15.12 Gestión de Crisis. Junto con su plan de continuidad de negocios, el Proveedor debe mantener un plan de manejo de crisis para dirigir y controlar las operaciones de recuperación. Como mínimo, el plan de manejo de crisis del Proveedor debe identificar a personas específicas con la autoridad suficiente para poner en marcha una operación de recuperación, definir los protocolos de comunicación y derivación para reunir y difundir la información de crisis e incluir protocolos de notificación y escalamiento para comunicarse con Citi en el caso de una crisis.

15.13 Evaluaciones. Los Proveedores están sujetos al proceso de evaluación de CoB de terceros de Citi para evaluar las capacidades de continuidad del negocio acorde con la Importancia del Proceso / RTO:

- i. Los Proveedores que respaldan procesos con RTO menor o igual a 24 horas deben evaluarse en forma anual
- ii. Las evaluaciones para los proveedores que respaldan los procesos críticos de franquicia deben realizarse en el sitio del proveedor
- iii. Los Proveedores que respaldan procesos con RTO mayor a 24 horas y menor o igual a 72 horas no requieren que se lleve a cabo una evaluación, pero deben acreditar anualmente sus capacidades de recuperación
- iv. La evaluación consistirá en cuestionarios de recuperación comercial que requerirán respuestas del Proveedor con evidencia. Si los resultados de una evaluación de CoB identifican o indican problemas o inquietudes, Citi dejará constancia de los resultados en un aviso al Proveedor y trabajará con este en la identificación de medios para corregir los problemas.

15.14 Cambios al Plan de Recuperación Ante Desastres. El proveedor puede cambiar su Plan de Recuperación Ante Desastres siempre que los cambios no degraden el Plan de Recuperación Ante Desastres de una manera que probablemente afecte negativamente a los servicios (p. ej., prolongando sus RTO). El Proveedor comunicará de inmediato cualquier cambio en su Plan de Recuperación Ante Desastres a Citi y, a pedido de Citi, explicará los cambios para que Citi los comprenda completamente y pueda responder a los cambios.

15.15 Plan de Recuperación Ante Desastres de Subcontratistas. El Proveedor se asegurará de que cualquier Subcontratista del Proveedor mantenga un Plan de Recuperación Ante Desastres que sea totalmente consistente con los Requisitos de Citi para Proveedores.

15.16 Uso de los Sistemas de Citi para Prestar Servicios. Si Citi o las Filiales de Citi lo solicitan, los Proveedores que utilicen los Sistemas de Citi participarán, sin costo ni cargo para Citi, en los ejercicios de recuperación ante desastres de Citi.

15.17 Requisitos del Plan de Recuperación Ante Desastres aplicables a los servicios alojados. En la medida en que el Proveedor administre y proporcione un Servicio alojado a Citi, también se aplicarán las disposiciones que siguen. El Plan de Recuperación Ante Desastres incluirá, como mínimo:

- i. procedimientos para la respaldo/restauración del funcionamiento y la aplicación de los Servicios Alojados, incluido un plan detallado y documentado para responder a una interrupción prolongada de los servicios causada por un corte de energía, una falla del sistema, un desastre natural u otras circunstancias imprevistas que incluya procesos y procedimientos para reanudar las operaciones dentro de un período de tiempo acordado mutuamente;
- ii. procedimientos para la protección de todo el Contenido;
- iii. procedimientos y acuerdos con terceros para equipos de reemplazo (p. ej., equipos informáticos), y
- iv. procedimientos para cualquier instalación de producción fuera del sitio.
- v. Además, el Plan de Recuperación Ante Desastres del Proveedor estipulará que: (a) el Proveedor notificará a Citi por escrito en un plazo de dos (2) horas de cualquier desastre que pueda afectar negativamente a los Servicios alojados; (b) El Proveedor proporcionará a Citi, dentro de un plazo de 24 horas a partir de

dicho aviso, un plan para continuar brindando los Servicios alojados en una instalación de procesamiento alternativa, y (c) los Servicios alojados deben estar completamente operativos dentro de las 48 horas posteriores al aviso inicial.

- vi. El Proveedor acepta, previa solicitud, divulgar la información necesaria para permitir que Citi desarrolle un plan de recuperación ante desastres y un plan de continuidad del negocio, que funcionarán en conjunto con el plan de recuperación ante desastres y el plan de continuidad del negocio del Proveedor.
- vii. En el caso de que partes de las instalaciones del Proveedor no funcionen, el Proveedor tratará a Citi de manera no menos favorable que el Proveedor trata a sus otros clientes comerciales.

15.18 Resiliencia Operativa. El Proveedor se asegurará de que cualquier interrupción en la entrega de elementos de los Servicios que equivalgan a servicios comerciales importantes/críticos o respalden la provisión de servicios comerciales importantes/críticos por parte de Citi, según lo especifique Citi ocasionalmente ("Servicios Importantes/Críticos a Negocios") no exceda la duración establecida por Citi ni infrinja de otro modo ninguna métrica relevante establecida por Citi ("Tolerancias de impacto") según lo notificado al Proveedor ocasionalmente.

- i. Las Tolerancias de impacto se expresarán como una métrica clara, incluida una duración máxima tolerable o un tiempo de inactividad máximo tolerable durante el cual se puede interrumpir la prestación del Servicio comercial importante/crítico. Citi y el Proveedor revisarán las Tolerancias de impacto anualmente como parte de los procesos de gobierno de contratos en curso. Cuando Citi deba establecer dos Tolerancias de Impacto para un Servicio Comercial Importante/Crítico individual debido a los requisitos de más de un Organismo Regulador, entonces Citi puede especificar Tolerancias de Impacto separadas para dicho Servicio Comercial Importante/Crítico. El proveedor deberá:
- ii. Notificar a Citi tan pronto como se dé cuenta de que ha fallado (o es razonablemente probable que falle) en la entrega de cualquier Servicio Comercial Importante/Crítico dentro de las Tolerancias de Impacto correspondientes establecidas por Citi junto con una explicación de las razones de cualquier fallo posible o real y las medidas que se están tomando para mitigar el impacto de dicho fallo;
- iii. Cuando se le solicite, brindar asistencia razonable a Citi para permitirle identificar las personas, los procesos, la tecnología, las instalaciones y la información que son necesarios para que el Proveedor brinde cualquier Servicio Comercial Importante/Crítico;
- iv. Asistencia razonable a Citi con el fin de permitirle a Citi realizar:
 - a. cualquier prueba de escenario interno de la capacidad del Proveedor para permanecer dentro de la(s) Tolerancia(s) de Impacto para cada Servicio Comercial Importante/Crítico en el caso de una interrupción grave pero plausible en sus operaciones o las del Proveedor; y
 - b. cualquier lección aprendida ejercida después de una prueba de escenario para permitir que Citi identifique las debilidades y cualquier acción necesaria para mejorar la capacidad del Proveedor para responder y recuperarse de futuras interrupciones.
- v. Cuando cualquier prueba de escenario interna realizada por Citi identifique vulnerabilidades o limitaciones en la capacidad del Proveedor para brindar Servicios Comerciales Importantes/Críticos dentro de las Tolerancias de Impacto correspondientes establecidas por Citi y luego de que el Proveedor no entregue cualquier Servicio Comercial Importante/Crítico dentro de las

Tolerancias de impacto correspondientes establecidas por Citi, las partes acordarán un plan (incluido un cronograma para implementar el plan), para garantizar que el Proveedor tome las medidas necesarias para resolver o mitigar tales vulnerabilidades o limitaciones o corregir la causa de la falta de permanecer dentro de la(s) tolerancia(s) de impacto (según corresponda) tan pronto como sea razonablemente posible.

16 NORMAS DE INVESTIGACIÓN DE ANTECEDENTES GLOBALES

Aplicable a Proveedores cuyo personal tiene acceso a los sistemas o redes de Citi Y/O acceso sin escolta a las instalaciones de Citi. (Dicho personal deberá tener un GEID y estar registrado en el Sistema de Gestión de No Empleados de Citi)

- 16.1 Descripción General: Investigación de Antecedentes.** La investigación de antecedentes debe realizarse de acuerdo con todas las leyes y regulaciones locales aplicables. Toda la información y las autodivulgaciones descritas en este documento deben ser proporcionadas por el personal del Proveedor, según corresponda. La falsificación u omisión de información en un currículum vitae, durante la entrevista, en un formulario de incorporación o durante el proceso de incorporación, sin importar cuándo se descubra, podrá ser motivo para la negación o finalización de la asignación en Citi de acuerdo con las leyes locales. Los resultados negativos de cualquier investigación realizada, sin importar cuándo se descubran, también podrán ser motivo para la negación o finalización de la asignación en Citi de acuerdo con las leyes locales.

Información adicional sobre el tiempo de finalización de la investigación de antecedentes, requisitos específicos del país y excepciones para estas normas pueden ser encontrados en https://www.citigroup.com/citi/suppliers/data/country_background_screening_requirements_tables.pdf.

- 16.2 Recolección de Información Básica y Verificación de Identidad.** Antes de que el personal del Proveedor comience una asignación de Citi, los Proveedores deben recopilar el nombre y apellido de las personas, la dirección postal y la dirección permanente (si es diferente), el número de teléfono y la dirección de correo electrónico (si corresponde). El Personal del Proveedor también debe proporcionar documentación que valide su identidad. Esto puede incluir el suministro de información y/o documentación de un número de identificación nacional, una tarjeta de identificación con foto emitida por el gobierno o un pasaporte.
- 16.3 Evaluación de Sanciones.** Todo el personal del Proveedor debe ser examinado, con la lista de la Oficina de Control de Activos Extranjeros ("OFAC") del Departamento del Tesoro de los Estados Unidos, la lista de Nacionales Especialmente Designados y Personas Bloqueadas ("SDN") y la lista de regiones y jurisdicciones sujetas a sanciones impuestas por los Estados Unidos ("Sanciones de EE. UU."). La evaluación debe aplicarse a los nombres, las direcciones, los alias y la fecha de nacimiento proporcionados por el proceso de verificación, antes de su primer día de asignación (excepto donde la ley local no lo permita). Se debe prohibir que el Personal del Proveedor que, efectivamente, figuren en una lista de sanciones trabaje en la asignación de Citi. Cualquier indicación o tergiversación puede resultar en la inhabilitación o el cierre de la cesión.

Las listas OFAC están disponibles públicamente en este sitio web:

<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

- 16.4 Cumplimiento de Inmigración.** El Proveedor debe demostrar que cuenta con protocolos a fin de verificar que su Personal está autorizado para trabajar en los países donde se los asigne y que ha cumplido con todas las leyes y reglamentaciones aplicables para verificar la elegibilidad laboral. El Proveedor, además, debe demostrar que cuenta con protocolos para garantizar que su Personal cumpla con todas las leyes y reglamentaciones migratorias aplicables, y que su Personal tenga la clasificación de visa correspondiente para las asignaciones y actividades en las que participará.
- 16.5 Historial de Empleo.** Los proveedores deben validar el historial de empleo de su personal durante los últimos siete (7) años, o 10 años, si así lo requiere la regulación. El historial laboral de la persona debe validarse para garantizar que los empleadores, los puestos, las fechas y las funciones se hayan representado con precisión. El personal del proveedor también debe revelar cualquier empleo o asignación anterior como consultor o trabajador temporal con Citi o cualquiera de sus empresas predecesoras (lo que incluye, entre otros: Citibank, Citicorp, Travelers, Salomon Brothers y/o Smith Barney). También deben declarar si Citi o cualquiera de sus compañías antecesoras los despidieron, les pidieron que renunciaran o si se les negó el empleo o asignación luego de recibir una oferta de Citi o cualquiera de sus compañías antecesoras.
- 16.6 Historial Educativo.** Los proveedores deben validar el más alto nivel de educación de su personal. La información validada debe incluir las fechas de asistencia, nombre(s) de la institución, dirección(es) y grado(s) alcanzado(s).
- 16.7 Antecedentes criminales.** Cuando esté legalmente permitido, el personal de los Proveedores y los subcontratistas deben informar a Citi si están sujetos a un arresto, citación, comparecencia, acusación, convicción o condena por cualquier delito penal, incluida una declaración de culpabilidad o una declaración de no impugnación y cualquier participación en una desviación previa al juicio o programa similar. La revisión administrativa de los antecedentes penales y/o las comprobaciones de huellas dactilares deben completarse antes de la fecha de inicio de la asignación donde esté legalmente permitido y disponible. Las condenas penales por delitos relacionados con el robo, el fraude, la deshonestidad o el abuso de confianza, salvo que la ley lo prohíba, pueden dar lugar a la denegación y/o inelegibilidad para la asignación a Citi. Otras condenas pueden resultar en la negación y/o la inelegibilidad para la asignación de acuerdo con las leyes y regulaciones locales aplicables.
- 16.8 Prueba de Detección de Drogas.** Cuando esté legalmente permitido, los Proveedores deben asegurarse de que su personal complete una prueba de detección de drogas antes de comenzar la asignación con Citi. Como mínimo, el examen de drogas debe ser una prueba de "5 paneles", que evalúa la presencia de anfetaminas, cannabinoides (THC), cocaína, opiáceos y fenciclidina (PCP). Los resultados positivos deben adjudicarse y son suficientes para denegar la asignación, ya sea que los resultados se reciban antes o después del comienzo del trabajo, excepto cuando la ley local no lo permita. A determinados miembros del Personal del Proveedor se les podrá pedir que se sometan a una prueba de detección de drogas durante su asignación debido a los requisitos del puesto (por ejemplo, conductores, pilotos) o por otros motivos, de acuerdo con las leyes y reglamentaciones locales.

16.9 Reevaluación. El Personal del Proveedor cuya asignación termine debe volver a ser evaluado en caso de que sea reasignado a Citi. Para obtener información adicional sobre los requisitos de revisión, consulte los requisitos y excepciones específicos de cada país que se encuentran en https://citigroup.com/citi/suppliers/data/country_background_screening_requirements_tables.pdf.

16.10 Transferencias Internacionales. Todos los exámenes deben completarse de acuerdo con las regulaciones del país donde se encuentra la asignación. Si el personal del Proveedor se transfiere a un nuevo país y hay una interrupción en el servicio con Citi, la persona debe ser examinada según los requisitos del nuevo país.

17 GASTOS

Proveedores que son elegibles contractualmente para reclamar gastos comerciales reembolsables.

17.1 Generalidades. Citi solo reembolsará los gastos razonables relacionados con el negocio que hayan sido aprobados previamente por escrito por Citi y en los que haya incurrido el Proveedor en relación con la provisión de productos y servicios a Citi, que sean conformes con los términos del Contrato aplicable o con la Política de Gestión de Gastos de Citi, en su caso, y que estén adecuadamente justificados mediante recibos, facturas, itinerarios u otras formas de documentación que Citi considere aceptables.

17.2 Reembolsos. Estos gastos deben documentarse adecuadamente y facturarse a Citi de acuerdo con los requisitos de facturación de Citi. Un empleado de Citi no debe incurrir en gastos de un Proveedor en nombre de dicho Proveedor. Todo gasto presentado a Citi para el reembolso de partidas de gastos válidas y aprobadas debe incluir (además de todos los demás requisitos de facturación):

- i. el propósito comercial del gasto;
- ii. el importe y la descripción del gasto;
- iii. el lugar y la fecha del gasto;
- iv. el nombre/descripción del proyecto para el cual el Proveedor está prestando servicios;
- v. los nombres y la relación comercial del representante de Citi que solicitó los servicios por los que se incurrió en gastos; y
- vi. el número de la orden de compra, cuando corresponda.

Para obtener información sobre los gastos comerciales reintegrables permitidos, comuníquese con su principal contacto comercial en Citi. Los recibos, facturas, itinerarios u otras formas de documentación de respaldo que Citi considere aceptables deben presentarse con la reclamación de reembolso. Las reclamaciones de reembolso deben cumplir con las disposiciones en el Contrato pertinente o con la Política de Gestión de Gastos de Citi, cuando corresponda, y estar aprobados por el negocio patrocinador correspondiente y/o por el principal contacto comercial de Citi. Las solicitudes que no cumplan con los requisitos no recibirán reembolso.

18 SEGURIDAD DE LA INFORMACIÓN (IS)

Aplicable a los Proveedores que acceden a, procesan o almacenan/gestionan toda la Información de Citi como se clasifica y define en el Apéndice Y/O Alojamiento de aplicaciones de Internet de la marca Citi Y/O tienen conectividad a los recursos de red de Citi Y/O requieren acceso sin escolta a las instalaciones de Citi.

18.1 Generalidades. Esta Sección proporciona requisitos mínimos para los Proveedores de Citi, que almacenan, procesan, administran o acceden a la Información de Citi y/o alojan aplicaciones de Citi, con respecto a los controles de protección de información que Citi espera para garantizar que la información esté protegida de acuerdo con los requisitos legales y reglamentarios aplicables y los más altos estándares de la industria (por ejemplo, ISO/IEC 27002) en los lugares donde Citi y sus proveedores hacen negocios. Si las leyes, regulaciones o estándares relevantes de la industria establecen estándares más altos que los provistos aquí, los Proveedores deben cumplir con dichas leyes, regulaciones o estándares. Además, los Proveedores pueden tener la obligación de incorporar prácticas y procedimientos adicionales de seguridad de la información como parte de su cumplimiento con otras políticas de Citi, y con los términos y las condiciones de un Contrato. Si un Proveedor decide implementar prácticas de seguridad adicionales o procedimientos detallados para seguridad de la información, debe asegurar que dichas prácticas y procedimientos no entren en conflicto con los controles mínimos establecidos en esta Sección.

18.2 Política y Gobernanza de la Seguridad de la Información. Los Proveedores deben tener políticas y estándares documentados en materia de Seguridad de la información. El gobierno corporativo de la política debe incluir roles y responsabilidades claramente definidos, revisión anual y actualización de políticas y estándares, que sean coherentes con el estado de la tecnología, los estándares de la industria, los requisitos legales y reglamentarios.

18.3 Segregación de Funciones. El proveedor debe tener procesos establecidos que garanticen que ninguna persona individual pueda realizar dos funciones comerciales o dos de las funciones de TI, o dos funciones del Sistema de información controlada con acceso persistente para la misma actividad, cambio, Sistema de información o transacción sin autorización o detección a menos que existan controles compensatorios adecuados para mitigar el riesgo.

18.4 Excepciones.

- i. Un usuario puede iniciar o aprobar una transacción real y participar a su vez en la evaluación de nuevos requisitos para el mismo Sistema de información de Citi en un entorno no productivo.
- ii. Un Usuario con la función Desarrollar puede proporcionar soporte de producción, pero el acceso persistente al Sistema de Información de Citi solo se puede otorgar si el acceso está limitado a solo lectura o visualización y no incluye acceso a información Confidencial o superior.
- iii. La persona con la función Desarrollar o Certificar que necesita proporcionar soporte de interrupción/repación utilizando la función Implementar debe usar acceso privilegiado temporal al Sistema de Información Controlada.
- iv. Una persona que necesite actualizar los datos de producción fuera de los controles de aplicación debe usar un acceso privilegiado temporal.
- v. Una persona que necesite ver datos que contengan PII confidencial o información PII confidencial fuera de los controles de la aplicación debe usar un acceso privilegiado temporal.

- vi. Las personas que realizan la función de Desarrollar o Certificar no deben modificar ni instalar el sistema operativo o el software de infraestructura de base de datos en los Sistemas de información controlados.

18.5 Compromiso de la Dirección con la Seguridad de la Información. Los proveedores, que albergarán una aplicación orientada a Internet con la marca Citi y/o tendrán acceso a información de Citi con clasificación de Confidencial o superior, están sujetos al Proceso de Evaluación de Seguridad de la Información de Terceros (TPISA, por sus siglas en inglés) de Citi para la evaluación de las políticas, procedimientos y controles del Proveedor con respecto al cumplimiento de los Requisitos de Citi y cualquier requisito legal y/o reglamentario (aplicable a Citi o al Proveedor) relacionado con la seguridad de la información.

La evaluación consistirá en cuestionarios de seguridad que requerirán respuestas del Proveedor con evidencia de respaldo y visitas a lugares donde la Información Confidencial o superior de Citi puede ser almacenada, procesada, administrada o accedida por terceros para satisfacer las necesidades comerciales de Citi y sus clientes. Si los resultados de TPISA revelan o indican problemas o inquietudes de seguridad, Citi dejará constancia de los resultados en un aviso al Proveedor y trabajará con este en la identificación de medios para corregir los problemas. Los proveedores deben realizar rápidamente las correcciones necesarias o agregar los controles de compensación necesarios para abordar las inquietudes de Citi a satisfacción; y en todo caso en el plazo de 180 días naturales para las emisiones de Alto Riesgo, de 240 días calendario para las emisiones de Medio Riesgo y antes de la siguiente evaluación para las emisiones de Bajo Riesgo.

- i. El proveedor debe realizar periódicamente evaluaciones de sus operaciones comerciales y controles relacionados con sus estándares, políticas y procedimientos de seguridad de la información. Las evaluaciones periódicas deben incluir, como mínimo, lo siguiente:
 - a. Evaluación de los procesos que utiliza el Proveedor para garantizar el cumplimiento de la política y los estándares de SI;
 - b. Evaluación de los recursos de apoyo, como las aplicaciones y la infraestructura utilizadas por el Proveedor y los procesos de la SI utilizados por los subcontratistas del Proveedor (si corresponde) que respaldan sus operaciones comerciales o permiten a Citi realizar dichas evaluaciones. Se requiere el cumplimiento en el caso de que un tercero firme un nuevo contrato o renueve uno existente con un subcontratista que acceda, procese, gestione o deseche Información de Citi clasificada como Confidencial o superior.
- ii. Los problemas que se identificaron como resultado de cualquier evaluación de riesgos de seguridad de la información deben documentarse y rastrearse hasta el cierre con evidencia de la medida correctiva proporcionada a Citi.
- iii. Si la función de gestión de Seguridad de la Información del Proveedor se reubica más allá de las fronteras del país, el Proveedor debe obtener la aprobación documentada de Citi antes de dicha reubicación.
- iv. Si el Proveedor adquiere una nueva entidad, el Proveedor debe completar una evaluación de la entidad adquirida para el cumplimiento de estos Estándares.
- v. El proveedor no debe subcontratar las funciones de gestión de la seguridad, incluidas, entre otras, la gestión del firewall, la gestión de la configuración de la seguridad, la gestión de parches o las funciones de la Administración de seguridad de la información (ISA), para sistemas utilizados para almacenar, procesar y/o

- transmitir Información de Citi a menos que Citi lo apruebe por escrito con anticipación.
- vi. Si el Proveedor aloja un software o sitio web que contiene Información de Citi o tiene la marca Citi, se deben realizar evaluaciones de vulnerabilidad periódicas de acuerdo con el Estándar de Pruebas de seguridad del sistema (SST) de Citi y cualquier problema importante identificado durante la evaluación se debe corregir dentro de los plazos especificados por el Estándar Citi SST. Además, el Proveedor cumplirá con los estándares de gestión de seguridad de la información ISO/IEC 207000 relevantes (o estándares de gestión de seguridad de la información sucesores que establecen estándares y protocolos mayores) y cumplirá con las disposiciones de seguridad informática contenidas en esta Sección 18.
 - vii. Si se requiere conectividad a servidores y/o a Sistemas de información de la red interna de Citi, el Proveedor deberá notificarlo a su principal contacto comercial de Citi para poder seguir el proceso actual de conectividad.
 - viii. El Proveedor debe notificar rápidamente al contacto de Citi que corresponda sobre cualquier acceso o adquisición, pérdida, daño o eliminación no autorizados de Información de Citi, o cualquier otro riesgo para los Sistemas de información usados para almacenar, procesar y/o transmitir Información de Citi.
 - ix. El Proveedor debe asegurarse de que todas las actividades de alto riesgo y los cambios en los datos confidenciales tengan rastros de auditoría que permitan especificar qué persona realizó qué actividad o qué datos cambió.
 - x. El Proveedor debe asegurarse de que todos los datos confidenciales estén enmascarados en la pantalla y en papel (incluidos, por ejemplo, los informes de seguimiento, de excepción, reglamentarios y de otro tipo).
 - xi. El Proveedor debe restringir la impresión, grabación o copia de datos confidenciales, incluso por 'dispositivos propios'. El proveedor debe realizar todos los esfuerzos razonables para devolver o destruir toda la información de Citi en un momento acordado durante o al final del acuerdo.
 - xii. El Proveedor debe asegurarse de que todo su personal (empleados fijos y temporales, contratistas, subcontratistas) con acceso a la información de Citi firme un convenio de no revelación o confidencialidad (NDA).
 - xiii. Los empleados del Proveedor deben recibir un manual del empleado, o documento similar, que contenga el proceso disciplinario por incumplimiento con violaciones del código de conducta del Proveedor y políticas de Recursos Humanos que deben reconocerse como parte de su proceso de incorporación.
 - xiv. El Proveedor cuenta con un proceso para recuperar todos los activos cuando un empleado o no empleado es despedido o renuncia.

18.6 Riesgo de Seguridad de la Información del Subcontratista. El Proveedor debe exigir que los subcontratistas con acceso a los datos de su cliente requieran evaluaciones de seguridad de la información (IS) precontractuales y poscontractuales periódicas llevadas a cabo por personal calificado de Seguridad de la Información que incluyan que:

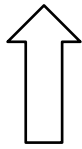
- i. Se ha implementado un proceso de evaluación de la seguridad de la información de los subcontratistas aprobado por la gerencia que cubre todos los pasos, desde el inicio de la evaluación hasta la gestión de problemas.
- ii. Los proveedores se aseguran de que se realicen evaluaciones de riesgo de la SI en sus subcontratistas que tienen acceso a Citi Confidencial y datos superiores mediante un cuestionario de evaluación de SI o una herramienta equivalente que cubre dominios de SI que se alinean con los cubiertos en el Cuestionario de evaluación de SI de terceros (TPAQ) de Citi e

- incluye un método lógico para calcular el riesgo de seguridad de la información en relación con los subcontratistas.
- iii. Los proveedores se aseguran de evaluar los controles de SI de los subcontratistas con acceso a la información de Citi, realizar un seguimiento de las finalizaciones de la evaluación y gestionar los problemas observados y los planes de acción correctiva (CAP) hasta el cierre.

18.7 Responsabilidad de los Bienes:

- i. El Proveedor debe asegurarse de mantener un Inventario de todas las aplicaciones y hardware bajo su control que se utilizan para almacenar, procesar y/o transmitir Información de Citi.
- ii. El Proveedor debe asegurarse de mantener un Inventario de los activos de Información de Citi bajo su control conforme a un proceso usado para mantener apropiadamente la precisión y la integridad de dicho inventario.
- iii. El Proveedor debe ser responsable de proteger toda la Información de Citi bajo su control.
- iv. El proveedor debe garantizar la responsabilidad de la actividad de sus usuarios de manera coherente con las prácticas de la industria.
- v. El acceso de usuarios a cuentas de correo electrónico en Internet externas y personales debe restringirse desde la red global del Proveedor donde resida Información de Citi.

18.8 Clasificación y Manejo de la Información. Citi clasifica la información conforme a las siguientes categorías: Consulte el Apéndice para obtener definiciones y ejemplos de cada clasificación que se enumera a continuación.

RESTRINGIDA	Más Sensible
PII SENSIBLE	
PII CONFIDENCIAL	
CONFIDENCIAL	
PII INTERNA	
INTERNA	
PÚBLICA	Menos Sensible

- i. Según la clasificación de la Información de Citi, Citi debe trabajar con el Proveedor para especificar el nivel de seguridad requerido para proteger dicha información y el Proveedor debe garantizar que existan controles suficientes, junto con los niveles elevados o modificados que Citi pueda requerir.
- ii. La información confidencial o superior debe almacenarse en dispositivos administrados por terceros que estén sujetos a un contrato entre el tercero y Citi que contenga disposiciones de confidencialidad consistentes con las políticas y estándares de Citi.
- iii. Si el Proveedor permite el uso de dispositivos que no pertenecen a la empresa para almacenar datos de Citi (es decir, dispositivos administrados por un tercero), el Proveedor debe tener una política vigente que requiera la aprobación específica de la administración y tener pautas establecidas y procedimientos de monitoreo para el uso y disposición de la información de Citi.
- iv. Solo la información clasificada por Citi como Pública puede almacenarse en dispositivos propiedad del personal del Proveedor (por ejemplo, computadoras en el hogar, asistentes digitales personales y aplicaciones de correo electrónico e Internet móvil).

- v. El Proveedor siempre debe proteger la Información de Citi del acceso, la modificación o la eliminación no autorizados.
- vi. La información de Citi colocada en medios electrónicos transportables (ETM) debe transferirse de manera segura y debe confirmarse la entrega. El proveedor debe confirmar que el destinatario previsto recibió el ETM en la fecha prevista de entrega y continuar el seguimiento con el destinatario previsto hasta el momento en que se confirme la entrega. Si no se recibe la confirmación de recibo para la fecha prevista de entrega, el Proveedor debe notificar a Citi.

18.9 Configuración segura.

- i. El Proveedor debe mantener una norma documentada sobre configuración segura para todos los recursos de información con el potencial para almacenar, procesar, transmitir o tener acceso a la información de Citi.
- ii. El proveedor debe incorporar procedimientos de seguridad de la información en sus procesos y procedimientos para la selección, desarrollo e implementación de aplicaciones, productos y servicios.
- iii. El Proveedor debe tener un procedimiento seguro de creación para todos los sistemas donde se almacene, procese y/o transmita Información de Citi.
- iv. El Proveedor debe mantener una imagen o plantilla segura de todos los sistemas.
- v. Todas las cuentas de usuario y contraseñas predeterminadas se eliminan y/o cambian de los sistemas, dispositivos de red y aplicaciones admitidos por el proveedor.
- vi. Las implementaciones de nuevos sistemas o los sistemas que se han visto comprometidos se configuran mediante el uso de una imagen o plantilla aprobada.
- vii. Cualquier cambio que deba aplicarse a una configuración segura es aprobado por la gerencia a través de un proceso de gestión de cambios.
- viii. Cuando ocurren cambios en la configuración segura, existe un proceso de notificación que incluye seguimiento y correcciones.
- ix. El procedimiento seguro de creación debe incluir herramientas para admitir la comprobaciones automatizadas de configuración para los ajustes estándares y de seguridad de creación al momento de la implementación en producción.

18.10 Requisitos de cifrado. Cuando un Tercero transmite y almacena información de Citi clasificada como confidencial o superior, se deben seguir los requisitos de cifrado. Los datos transmitidos entre Citi y el tercero de Citi deben cifrarse de extremo a extremo con herramientas o soluciones aprobadas por Citi. Los protocolos aprobados y los respectivos números de versión durante la transmisión de datos son los siguientes:

- i. Al intercambiar información de autenticación y autorización: SAML v2.0, OAuth v2.0 (solo autorización),
- ii. Para proteger los canales de comunicación y el intercambio de claves asociado: TLS v1.2 o TLS v1.3. Los conjuntos de cifrado TLS deben estar calificados como "fuertes", "recomendados" o equivalentes por SSL Labs o una organización similar con Perfect Forward Secrecy (PFS) habilitado Y/O DTLS v1.2 e IPSEC/IKE v2.

18.11 Los datos almacenados de forma persistente en el entorno de terceros de Citi o cuando se intercambian deben cifrarse por completo mediante herramientas o soluciones aprobadas por Citi. Los algoritmos aprobados y las longitudes de clave para cifrar datos son los siguientes:

- i. **Estándar de Cifrado Avanzado (AES):** Longitudes de clave aprobadas: 128 o 256 bits. No se permite AES con una longitud de clave de 192 bits. Modos restringidos: El modo Electronic Codebook (ECB) está prohibido excepto cuando la cantidad de texto sin formato es menor o igual que la longitud del bloque. Cifrado de la unidad de disco: Se recomienda AES con clave de 256 bits.
- ii. **ChaCha20 (un cifrado de flujo para casos de uso asociados):** Longitudes de clave aprobadas: 128 o 256 bits, con nonce de 96 bits y recuento de bloques de 32 bits o nonce de 64 bits y recuento de bloques de 64 bits. Tamaño máximo de datos: 16 petabytes.

18.12 Los criptosistemas de clave pública aprobados, el intercambio de claves, los mecanismos de acuerdo, el resumen de mensajes y las funciones de derivación de claves son los siguientes:

- i. **Criptosistemas de Clave Pública y Tamaños Mínimos de Longitud de Clave:** Rivest-Shamir-Adleman (RSA), algoritmo de firma digital (DSA): 2048. DSA no debe usarse para proteger los datos de Citi procesados o almacenados fuera del algoritmo de firma digital de curva elíptica de Citi (ECDSA): 256.
- ii. **Mecanismos de Intercambio y Acuerdo de Claves y Tamaños Mínimos de Longitud de Clave:** Diffie-Hellman (DH) / Ephemeral Diffie-Hellman (DHE): 2048. Curva elíptica Diffie-Hellman (ECDH) / Curva elíptica efímera Diffie-Hellman (ECDHE): 256.
- iii. **Funciones de Resumen de Mensajes:** Está prohibido crear una clave de cifrado de una longitud superior al número de bits aleatorios en el material utilizado para generar el hash. MD-5: Aceptable para aplicaciones de firma no digital. Prohibido para la generación y verificación de firmas digitales. SHA-1: Aceptable para aplicaciones de firmas no digitales y verificación de firmas digitales heredadas. Prohibido para generación de firma digital. Familia SHA-2, familia SHA-3 y POLY-1305: Aceptable para todas las aplicaciones criptográficas de función hash.
- iv. **Funciones de Derivación de Clave basadas en contraseña y requisitos mínimos:** PBKDF2: Recuento mínimo de iteraciones de 10000 con una sal de al menos 16 bytes. HKDF: Debe estar salado y debe incluirse el valor de entrada de información. ESCRITURA: Número mínimo de rondas/factor de costo de 10. Está prohibido el uso de NIST SP800-108 KDF para Stream Encryption. Bcrypt (para almacenamiento local de hash de contraseña): Número mínimo de rondas/factor de costo de al menos 10.

18.13 Correo Electrónico Externo: El requisito de cifrado para los correos electrónicos individuales que contengan Información de Citi con una Clasificación de Información de Citi Confidencial o superior, cuando el Proveedor no esté autorizado a utilizar el software o las herramientas de cifrado de extremo a extremo aprobadas por Citi según la normativa y/o la política del Proveedor, puede cumplirse en su totalidad a través del cifrado de transporte (por ejemplo, cifrado de puerta de enlace a puerta de enlace a través de Transport Layer Security, TLS). Los protocolos de correo electrónico seguro aprobados son:

- i. **El Cifrado Basado en la Identificación (IBE)** presenta correo electrónico cifrado y debe usarse únicamente dentro de las soluciones orientadas al cliente de Citigroup y los sistemas seguros de correo electrónico y entrega electrónica.
- ii. **Mutual TLS (MTLS)** cuenta con cifrado de sesión (no cifra la carga útil del correo electrónico) y es para uso con proveedores, socios y clientes que tienen acuerdos prenegociados para su uso.
- iii. **Domain Keys Identified Mail (DKIM)** incluye autenticación y gestión de claves y se utiliza con proveedores, socios y clientes.

18.14 Para el intercambio de información de autenticación y autorización, el protocolo de seguridad aprobado es SAML v2.0. Todas las implementaciones nuevas de SAML deben estar en la revisión 2.0.

18.15 Redes privadas: Las redes privadas que están reguladas de forma independiente por una autoridad reconocida y que cumplen con los estándares de la industria de servicios financieros para realizar transacciones comerciales entre contrapartes autorizadas o acreditadas (por ejemplo, SWIFT o un banco central) pueden considerarse exentas del requisito de cifrado de PII confidencial en tránsito hasta que esas redes proporcionen infraestructura necesaria para soportar completamente las transmisiones cifradas.

18.16 Voz y Fax: La información con una clasificación de Información de Citi de Confidencial o superior enviada por fax o discutida en llamadas de voz (incluida Voz sobre IP [VOIP]) puede enviarse sin cifrar. Cuando sea necesario, el Proveedor debe desarrollar procedimientos y guías específicos para proteger la información Confidencial o superior enviada a través de estos canales.

18.17 Gestión de Claves.

- i. Los algoritmos criptográficos estándar de la industria y las longitudes de clave mínimas deben implementarse para el cifrado.
- ii. El tercero de Citi debe tener un proceso formal documentado del ciclo de vida de la administración de claves con controles implementados para proteger las claves del uso o exposición no autorizados.
- iii. Las claves deben tener un propósito único y no deben usarse para ningún otro propósito, como cifrar datos de otra empresa o para el uso interno de terceros.
- iv. Las claves criptográficas simétricas y privadas no deben mostrarse en texto sin cifrar en ningún momento y deben almacenarse o transmitirse en forma cifrada solo mediante una clave de cifrado de clave (KEK).
- v. La clave de cifrado de clave (KEK) debe dividirse en dos o más componentes clave y someterse a XOR antes de la distribución y para la entrada/carga manual de la clave.
- vi. El acceso a los almacenes de claves que contengan claves privadas o simétricas debe segregarse adecuadamente con controles que limiten el acceso únicamente a personal o sistemas autorizados.
- vii. Cada solicitud para acceder a los almacenes de claves que contienen claves privadas o simétricas debe registrarse y documentarse con detalles como quién, cuándo y el propósito del acceso para fines de auditoría.
- viii. No se deben utilizar certificados autofirmados y comodín.
- ix. Las claves deben tener un período de tiempo criptográfico definido como se sugiere en NIST.SP.800.-57pt1r5: El cambio de clave no necesita coincidir con el vencimiento de la clave indicado. Las claves deben actualizarse o rotarse antes de su vencimiento para adaptarse a períodos de cambio, conflictos de programación y bloqueos del sistema.
- x. Las redes inalámbricas deben cifrarse con algoritmos de cifrado estándares de la industria.
- xi. Los Proveedores que utilicen cualquier forma de mecanismo criptográfico deben usar herramientas y técnicas estándares de la industria para la administración de claves.

18.18 Responsabilidad de Control de Acceso. A fin de proteger todos los Sistemas de Información Controlada utilizados para almacenar, acceder, gestionar, procesar o transmitir la Información confidencial o de nivel superior de Citi contra el acceso no autorizado, el proveedor debe gestionar el suministro de acceso lógico a todos los sistemas y aplicaciones; los controles deben estar totalmente documentados, ser auditables y otorgar el mínimo privilegio.

- i. El proveedor es responsable de los derechos de acceso de todos los usuarios de su organización.
- ii. El proveedor debe implementar controles de acceso que aseguren que a los usuarios se les otorguen solo los privilegios y derechos necesarios para realizar su función.
- iii. El Proveedor debe implementar un proceso para asegurar que todas las capacidades de acceso predeterminadas se eliminen, inhabiliten o protejan para evitar su uso no autorizado.

18.19 Gestión de Acceso de Usuarios. El proveedor debe gestionar el suministro de acceso lógico a los sistemas y aplicaciones que procesan, almacenan y/o transmiten la información confidencial o de nivel superior de Citi. Esto incluye:

- i. Identificación e inventario de sistemas de autenticación aprobados.
- ii. Todo acceso a los datos de Citi requiere la aprobación de un gerente o designado de un gerente así como del responsable del sistema.
- iii. Es posible que no se proporcionen combinaciones de privilegios/funciones a un usuario individual porque presentan conflictos de intereses o una violación de las reglas del verificador.
- iv. Un proceso de monitoreo para supervisar y gestionar los derechos de acceso otorgados/revocados para cada usuario en el sistema. Los proveedores de bajo riesgo quedan exentos de este requisito.

18.20 Identificación y Autenticación de Usuario. Todos los Sistemas de información controlados por el Proveedor deben autenticar la identidad de los usuarios o sistemas que acceden a estas plataformas antes de iniciar una sesión o transacción en la que se pueda acceder a la Información de Citi. Todos los usuarios deben:

- i. Ser identificados o asignados de manera única a la plataforma de tecnología mediante una identificación de usuario.
- ii. Ser autenticados en la plataforma de tecnología utilizando un método de autenticación - el Proveedor debe comunicarse con su contacto comercial principal para conocer los métodos aprobados actuales.
- iii. Todo uso de infraestructura de autenticación compartida (por ejemplo, inicio de sesión único, inicio de sesión reducido y otros servicios de autenticación compartida) deben guardar conformidad con los requisitos de autenticación. El Proveedor debe comunicarse con su contacto comercial principal para conocer los métodos aprobados.
- iv. Autenticación de usuarios para conexiones externas (Ver 18.8.9 Acceso Remoto).

18.21 Acceso Privilegiado Temporal. El proveedor debe mantener un inventario de todas las cuentas privilegiadas y administrativas. El acceso directo a una identificación funcional privilegiada debe otorgarse a través de un proceso de acceso privilegiado temporal. El acceso privilegiado a los Sistemas de información controlados debe seguir un proceso de Gestión de acceso privilegiado temporal que incluye procedimientos documentados de liberación de contraseñas/cuentas que:

- i. Requiere que el solicitante esté en una lista de usuarios autorizados previamente aprobados o que tenga una aprobación en el momento del uso.
- ii. Requiere justificación documentada en un ticket de cambio/problema antes de otorgar acceso.
- iii. Incluya una revisión independiente de la actividad realizada con el acceso.
- iv. Incluya un proceso para revocar o quitar el acceso después de un período predefinido de no más de 24 horas.

- v. Permite que la producción y el acceso de estabilización posterior a la implementación, como después de una actualización importante o una resolución de interrupción/reparación, se extiendan hasta siete (7) días calendario.

18.22 Acceso Privilegiado Persistente. Se puede otorgar acceso privilegiado persistente a un usuario en un Sistema de Información Controlado utilizado para almacenar, procesar, administrar y/o transmitir Información de Citi solo cuando se cumplan todas las condiciones siguientes:

- i. La justificación del acceso persistente se documenta como parte del proceso de aprobación.
- ii. El gerente del usuario y el dueño o delegado de la información del Sistema de información controlada aprueban el acceso.
- iii. Al iniciar sesión con una ID privilegiada, los administradores tienen prohibido acceder al correo electrónico, navegar por la Web o realizar cualquier función que no sea la aprobada para el uso privilegiado.

18.23 La Revisión de los Derechos de Acceso del Usuario debe incluir lo siguiente:

- i. El Proveedor debe implementar un proceso documentado para revisar, verificar y eliminar los derechos innecesarios del usuario a los Sistemas de Información Controlada utilizados para almacenar, procesar, administrar y/o transmitir Información de Citi.
- ii. El Proveedor debe revisar todos los derechos de usuarios al menos cada seis meses y eliminar los accesos innecesarios.
- iii. Los usuarios no deben revisar o aprobar sus propios derechos o los de una persona que les haya delegado responsabilidad de revisión.
- iv. El dueño o delegado de las identificaciones debe revisar una vez al año los derechos de todas las identificaciones funcionales privilegiadas no fijas de Sistemas de información de Producción y Continuidad de Negocio.
- v. La lista de usuario autorizado para ID Funcionales privilegiadas en los Sistemas de Información de Producción/CoB debe ser revisada trimestralmente por parte del/de los responsable(s) o delegado(s) de las identificaciones.
- vi. Luego de un cambio de función por parte de un empleado, el proveedor tiene 21 días calendario para realizar una revisión de acceso y derecho y eliminar el acceso a los datos de Citi si ya no los necesita para su nueva función.

18.24 Procedimientos de Inicio de Sesión Seguro.

- i. Las ID de inicio de sesión asociadas con una contraseña estática deben bloquearse después de un máximo de seis (6) intentos de inicio de sesión fallidos consecutivos.
- ii. Las identificaciones de inicio de sesión bloqueadas deben volver a habilitarse a través de un servicio de restablecimiento estándar de la industria u otra función autorizada. Se debe mostrar un texto en todos los puntos de entrada a la red en los que un usuario inicia sesión por primera vez o en donde sea autenticado, siempre que así lo permita el sistema operativo.

18.25 Sistema de Gestión de Contraseñas.

- i. Las contraseñas estáticas de usuarios nunca deben mostrarse en pantalla con texto visible.
- ii. Las contraseñas de identificaciones funcionales privilegiadas interactivas no deben ser preprogramadas en texto visible.
- iii. Las contraseñas deben contener un mínimo de ocho (8) caracteres, que deben contener letras y números, y deben ser sensibles a mayúsculas y minúsculas.

- iv. Los PIN pueden usarse como único método de autenticación para acceder a Sistemas de información solo si son necesarios para satisfacer límites físicos del dispositivo (por ejemplo, teclado, teléfono, tarjeta inteligente).
- v. Todas las contraseñas estáticas deben cambiarse, como mínimo, cada 90 días calendario. También tenga en cuenta lo siguiente:
- vi. Todos los sistemas de autenticación deben imponer un control de inactividad/no uso de inicio de sesión que no debe exceder los 100 días si es técnicamente factible. Los inicios de sesión deshabilitados pueden ser rehabilitados por el usuario u otra función autorizada.
- vii. El proceso de autenticación debe garantizar que no se use la misma contraseña dentro de al menos los últimos seis (6) cambios.

18.26 Uso de las Utilidades del Sistema. El Proveedor debe asegurarse de que el uso de Programas de Utilidades que puedan anular los controles del sistema y de la aplicación (p. ej., arrancar desde dispositivos periféricos) esté restringido y controlado.

18.27 Cierre de Sesión por Inactividad

- i. Para todos los usuarios de un Sistema de información controlada usado para almacenar, procesar y/o transmitir Información de Citi, se debe requerir la reautenticación o el reinicio de sesión.
- ii. La reautenticación de usuarios se debe exigir luego de un período de inactividad no superior a los 30 minutos. La actividad incluye cualquier entrada desde un extremo (mouse, teclado, pantalla táctil, etc.). Cuando este requisito se cumpla con un protector de pantalla protegido con contraseña, no se requiere su cumplimiento mediante inicio de sesión único o aplicación.

18.28 Validación de Datos de Entrada.

- i. Los Proveedores deben tener controles para la protección contra amenazas a la seguridad en línea (por ejemplo, secuencia de comandos entre sitios, inyección SQL, etc.).
- ii. La validación de entradas se debe implementar para todas las aplicaciones de Internet e Intranet.

18.29 Terminación del Acceso del Usuario.

- i. Tras la rescisión o renuncia, el acceso del usuario o los derechos que podrían permitir el acceso a los datos confidenciales o superiores de Citi (inicio de sesión de usuario en Desktop/Active Directory, inicio de sesión único (SSO), correo electrónico, tokens de contraseña de un solo uso (OTP) y acceso remoto) deben eliminarse al final del siguiente día hábil.
- ii. Si un empleado tiene acceso a los sistemas que pertenecen a, y son administrados por, Citi, Citi recibe una notificación de inmediato tras el cambio de función o el cese de empleo de tal persona.
- iii. El Proveedor ha implementado un proceso para recuperar todos los recursos de información cuando un empleado o no empleado es desvinculado laboralmente o renuncia.

18.30 Acceso Remoto. El Proveedor debe contar con controles de acceso remoto para proteger el acceso a las redes que pueden almacenar, procesar o transmitir datos de Citi confidenciales o de nivel superior, entre ellos:

- i. El acceso remoto a los sistemas de información utilizados para almacenar, procesar, administrar y/o transmitir información de Citi debe protegerse contra el uso no autorizado.
- ii. Todas las computadoras portátiles administradas por el Proveedor y todas las máquinas de escritorio utilizadas para almacenar, procesar y/o transmitir Información de Citi, utilizando acceso remoto donde hay almacenamiento/procesamiento local de información con una clasificación de Información de Citi de estado

confidencial o superior, debe cifrarse con una herramienta de cifrado que cumpla con los estándares de la industria.

- iii. Solo deben establecerse conexiones remotas a través de soluciones de acceso remoto que empleen autenticación de factores múltiples.
- iv. Los equipos administrados por el Proveedor deben tener un firewall personal activo cuando se conecten directamente (es decir, no a través de un firewall o proxy administrado por el proveedor) a Internet.
- v. Los dispositivos administrados por el Proveedor deben estar conectados regularmente a su red para recibir e instalar actualizaciones periódicas de software / antivirus como requisito para el acceso total a la red. Es posible que se permita acceso limitado con el propósito expreso de actualizar el dispositivo.
- vi. Si se utilizan dispositivos no pertenecientes a la compañía o no administrados por ella para tener acceso a la información confidencial o de nivel superior de Citi, deben usar una solución autorizada que no permita descargas a la máquina local. Deberán implementarse los siguientes controles:
 - a. Se impide que los datos de Citi se descarguen en el dispositivo personal fuera de una solución administrada por la compañía.
 - b. El Proveedor debe asegurarse de que dicho acceso esté protegido mediante autenticación basada en token o basada en certificados utilizando tecnologías estándar de acceso remoto (es decir, VPN, Horizon, etc.).
 - c. Las soluciones de acceso remoto como Terminal Services, VMware Horizon deben configurarse para deshabilitar el uso compartido del portapapeles y Drive Mapping sobre los protocolos Blast, PCoIP y RDP.
- vii. Todo el Personal del Proveedor, incluyendo, entre otros, empleados permanentes o temporales, contratistas y subcontratistas, que requieran acceso especial, privilegiado y/o de nivel administrativo a sistemas, depósitos de datos, aplicaciones y/o infraestructura, incluidos, entre otros, administradores de sistemas, administradores de bases de datos, administradores de control de acceso, administradores de firewall, administradores de sitios web, etc., que estén relacionados directa o indirectamente con los Servicios prestados para Citi deberán utilizar la autenticación multifactor y dicho acceso será registrado y supervisado de forma independiente por el Proveedor para actividad sospechosa y/o acceso no autorizado de acuerdo con los Requisitos de Citi para Proveedores, como se indica anteriormente.

18.31 Política de Escritorio Limpio y Pantalla Limpia. El personal del Proveedor debe proteger la Información de Citi en todas sus formas, incluida la información física usada o almacenada en su espacio de trabajo. Los proveedores deben comunicar este requisito a todo su personal al menos una vez al año a través de la concientización en SI.

18.32 Seguridad Contra Incendios.

- i. El Proveedor debe cumplir con los correspondientes requisitos legales y reglamentarios que rigen la seguridad física y la creación de un entorno de trabajo seguro, incluidos los códigos locales de prevención de incendios.
- ii. El proveedor debe utilizar uno o más sistemas de detección, alarma y supresión de incendios. Estos sistemas deben ser inspeccionados y probados una vez al año.

18.33 Seguridad Física.

- i. La Información de Citi debe ser almacenada en áreas seguras con controles que restrinjan el acceso solo a Personal autorizado.

- ii. El Proveedor debe contar con un sistema de acceso físico documentado y auditable.
- iii. El Proveedor debe usar una combinación de sistemas de detección de intromisiones y de alarma de seguridad que incluyan una alarma de seguridad monitoreada por un tercero, guardias de seguridad y videovigilancia, según corresponda para el entorno y los servicios suministrados.
- iv. El Proveedor debe tener una política de visitas documentada que incluya el requisito que todos los visitantes muestren una identificación verificable al llegar, y al registrar la entrada y la salida.

18.34 Procedimientos de Seguridad Operacional y Responsabilidad.

- i. El Proveedor debe implementar un Ciclo de vida de desarrollo de sistemas protegido (Secure System Development Life Cycle, S-SDLC), de conformidad con los estándares mínimos de Citi, si presta servicios de desarrollo de software a Citi.
- ii. El proveedor debe tener un proceso documentado de gestión de cambios.
- iii. El proveedor debe tener un proceso documentado de gestión de capacidad que cumpla con los estándares relevantes de la industria.
- iv. Cuando corresponda, el Proveedor debe asegurarse de que todos los entornos de desarrollo, prueba y producción estén separados de manera física y/o lógica entre sí.

18.35 Controles Contra Malware. El Proveedor debe asegurarse de que se toman las precauciones necesarias para prevenir y detectar la introducción de cualquier código malicioso (por ejemplo, virus, gusanos, troyanos, adware, spyware, ransomware u otros ataques cibernéticos similares en los que se pueden perder datos) y debe implementar controles preventivos, de detección y de recuperación para protegerse contra tales amenazas. El Proveedor debe:

- i. Implementar, actualizar y mantener tecnología antivirus y antispyware en todas las computadoras personales y tecnología en todos los servidores de red de área local (LAN), servidores de correo y otros dispositivos que almacenan, procesan y/o transmiten información de Citi.
- ii. Tener configuraciones de seguridad para evitar que los usuarios finales desactiven el antivirus/antimalware y los análisis programados.
- iii. Disponer de procedimientos automatizados y gestionados de forma centralizada para configurar y actualizar el software antivirus y antimalware
- iv. Se implementan procesos para identificar y abordar las computadoras que incumplen con las reglas donde las firmas del antivirus o los escáneres están desactualizados.

18.36 Controles Contra Código Móvil. Los proveedores deben asegurarse de tomar las precauciones necesarias para controlar el uso del Código Móvil. Cuando se autoriza el uso del Código móvil, la configuración debe, como mínimo, cumplir con todos los estándares de la industria y las obligaciones contractuales con Citi, garantizar que el Código móvil autorizado funcione de acuerdo con una política de seguridad claramente definida y documentada y evitar que se ejecute un Código móvil no autorizado.

En el caso de un Código Móvil que pueda afectar el sistema operativo o plataforma subyacente (es decir, fuera de la “zona protegida”), el Proveedor debe asegurar lo siguiente: un Código Móvil publicado por el Proveedor debe estar firmado por una Autoridad de certificación aprobada por Citi y el Proveedor debe administrar el ciclo de vida del certificado para abordar el vencimiento o la rotación del certificado. El Código Móvil firmado con certificados vencidos debe ser retirado de producción.

18.37 Registro de Auditoría. El proveedor debe asegurarse de que todos los sistemas de información controlada utilizados para acceder, almacenar, procesar, administrar y/o transmitir información de Citi utilizan registros de auditoría a nivel de infraestructura o aplicación para registrar los siguientes elementos:

- i. Acciones relevantes de seguridad de infraestructura para la plataforma asociada
- ii. Todas las alarmas del sistema asociadas con un firewall o evento de seguridad generado por IDS/IPS
- iii. Todos los intentos de violación de la seguridad del sistema (por ejemplo, intentos fallidos de inicio de sesión de usuario)
- iv. Todos los eventos significativos relacionados con transacciones financieras e información de Citi que incluyen específicamente los siguientes elementos:
 - a. actualizaciones en transacciones financieras;
 - b. actualizaciones en datos de PII Confidenciales;
 - c. actualizaciones en datos Restringidos;
 - d. actualizaciones en datos de Autenticación.
- v. Los artefactos de sesión (dirección IP como mínimo u otra información pertinente), como la identificación única del dispositivo, deben capturarse, cuando sea técnicamente factible, y registrarse para las aplicaciones de Citi (sitios web y aplicaciones móviles) para respaldar las investigaciones de fraude. Estos artefactos se deben capturar en transacciones de Citi y actividades de apertura de cuentas de Citi. Se debe capturar la información para que el artefacto de la sesión se pueda vincular con la transacción o la apertura de la cuenta.
- vi. Se deben registrar los eventos significativos de ISA, en especial, lo siguiente:
 - a. creación de usuarios;
 - b. modificación de derechos de acceso de usuarios
 - c. eliminación, creación, y modificación de perfiles en el Sistema de Información Controlado.
 - d. restablecimiento de contraseña;
 - e. cambios en la configuración de seguridad del sistema.
 - f. Se debe registrar toda la actividad interactiva de identificaciones funcionales privilegiadas.
 - g. Los registros de seguridad deben contener, al menos, la siguiente información, independientemente del sistema que genere el registro, a menos que no sea técnicamente posible:
 - 1. fecha y hora del evento (hora en formato UTC);
 - 2. identificación de usuario de la persona que realiza la acción;
 - 3. tipo de evento;
 - 4. activo o nombre de recurso afectado;
 - 5. tipo de acceso (eliminar, modificar, etc.);
 - 6. éxito o fracaso del evento
 - vii. origen (terminal, puerto, ubicación, IP, nombre de host, etc.)

18.38 Protección de la Información de Registro. El proveedor debe asegurarse de que los controles de acceso estén presentes para preservar la integridad de los registros de auditoría durante el inicio, el cierre, el almacenamiento y la transmisión.

- i. Para evitar modificaciones no autorizadas en los registros de auditoría, el proveedor debe asegurar que estos no sean sobrescritos ni modificados por los usuarios del sistema cuya actividad se está registrando.
- ii. El proveedor debe definir, mantener y cumplir con el período de retención de los datos de registro que cumplan con la Política de administración de registros de Citi y todos los requisitos legales y reglamentarios aplicables.
- iii. Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad deben sincronizarse con una fuente de tiempo precisa.

18.39 Uso del Sistema de Monitoreo. Los siguientes eventos deben ser capturados, registrados y revisados directamente o mediante un proceso de revisión automatizado:

- i. Todas las alarmas del sistema asociadas con un firewall o evento de seguridad generado por IDS/IPS
- ii. Todas las actualizaciones de recursos críticos, tal como se identifica en el procedimiento de creación estándar seguro.
- iii. Toda actividad interactiva realizada por identificaciones funcionales privilegiadas o identificaciones temporales.
- iv. **Excepciones:**
 - a. Eliminación de derechos de usuario, rol o perfil. ii. Donde la actividad de Administración de Seguridad de la Información es ejecutada por un flujo de trabajo automatizado / sistema de cumplimiento que tiene controles de integridad de extremo a extremo.

18.40 Correlación y Revisión de Registros.

- i. Cuando un evento registrado activa una alerta, se revisa dicho evento y se toman medidas de seguimiento e investigación si indica que es posible que haya ocurrido un incidente potencialmente perjudicial relacionado con la seguridad de la información.
- ii. El Proveedor debe asegurarse de que los registros de auditoría se agreguen a un sistema central de gestión de registros, como un sistema de Gestión de Eventos e Información de Seguridad (Security Information and Event Management, SIEM) o una herramienta analítica de registros para el análisis y revisión de la correlación de registros. Esta puede ser una función de su sistema central de gestión de registros o una herramienta por separado. Los proveedores de bajo riesgo quedan exentos de este requisito.
- iii. Los proveedores de alto riesgo deben revisar y ajustar periódicamente la configuración de su SIEM o herramienta de análisis de registros para mejorar la identificación de eventos procesables.

18.41 Control de Software Operacional.

- i. El proveedor debe asegurarse de que solo se utilicen los sistemas operativos y el software que actualmente son compatibles con un proveedor comercial aceptado por la industria o que tienen una versión activa y adecuada de parches y actualizaciones de configuración disponibles para abordar los problemas de seguridad.
- ii. El proveedor debe asegurarse de que se implemente un proceso documentado que especifique los períodos de tiempo dentro de los cuales se aplican todas las configuraciones y parches de seguridad aprobados.
- iii. Independientemente de cualquier acuerdo de mantenimiento por separado entre el Proveedor y Citi, el Proveedor debe asegurarse de que el software desarrollado para Citi y regido por un acuerdo de licencia no requiera el uso de versiones de software no compatible con vulnerabilidades conocidas Y SEA actualizado y parcheado según sea necesario de manera oportuna.
- iv. El software de aplicación de código abierto empleado para procesar la información de Citi debe adquirirse a través de proveedores establecidos y ser compatible.

18.42 Desarrollo de Software Seguridad.

- i. El proveedor de software debe tener un ciclo de vida de desarrollo de software (SDLC) aprobado por la administración, documentado y actualizado.
- ii. La seguridad debe revisarse en cada etapa del SDLC.
- iii. Se deben hacer cumplir las prácticas de codificación segura.

18.43 Gestión de Vulnerabilidades y Amenazas. Si el Proveedor mantiene o almacena Información Confidencial de Citi en un sitio web o sistema accesible por Internet, entonces, para protegerse contra una vulnerabilidad o amenaza que involucre productos o servicios que afecten a Citi (cada una, una "Vulnerabilidad"), el Proveedor debe cumplir con los siguientes Requisitos. En general, el Proveedor debe:

- i. Designar a un empleado del Proveedor, con conocimientos sobre asuntos de seguridad informática, para responder a las consultas de Citi sobre seguridad informática.
- ii. Hacer esfuerzos comercialmente razonables para monitorear, de manera regular, fuentes acreditadas de información sobre vulnerabilidades de seguridad informática, como FIRST, CERT/CC y listas de correo de proveedores, y tomar las medidas apropiadas para obtener, probar minuciosamente, aplicar y proporcionar a Citi paquetes de servicio relevantes, parches, actualizaciones y soluciones alternativas.
- iii. Probar, al menos trimestralmente, la implementación de sus medidas de seguridad de la información utilizando herramientas de escaneo de vulnerabilidades de redes, sistemas y aplicaciones y/o pruebas de penetración.
- iv. Permitir que Citi realice, a expensas de Citi y en tiempos razonables, Vulnerabilidad, piratería ética u otras evaluaciones de seguridad, para verificar el cumplimiento del Proveedor con sus obligaciones en virtud de cualquier Contrato y estos Requisitos, que incluyen, entre otros, la revisión de políticas, procesos y procedimientos, evaluación in situ de los arreglos de seguridad física, exploración de vulnerabilidades de redes, sistemas y aplicaciones, y pruebas de penetración, utilizando herramientas disponibles comercialmente y/o prácticas estándar de la industria para realizar estas inspecciones.

- v. Mantener, durante un período de al menos 180 días (o el período más largo que exija la ley o el contrato) archivos de registro detallados sobre todas las actividades en los sistemas del Proveedor, incluyendo, entre otros:
 - a. Todas las sesiones establecidas
 - b. Información relacionada con la recepción de información específica de un usuario u otro sistema
 - c. Intentos fallidos de autenticación de usuario
 - d. Intentos no autorizados de acceder a los recursos (software, datos, procesos, etc.)
 - e. Acciones del administrador
 - f. Eventos generados (p. ej., comandos emitidos) para realizar cambios en los perfiles de seguridad, niveles de permisos, configuraciones de seguridad de aplicaciones y/o recursos del sistema.
- vi. Todos los archivos de registro deben protegerse contra el acceso, la modificación o la eliminación no autorizados. Además, mantener registros relacionados con la privacidad u otras evaluaciones de riesgos de la información de seguridad, así como registros relacionados con acciones e investigaciones de seguridad de rutina, si corresponde, de acuerdo con la Política de administración de registros de Citi, incluido el período de retención requerido de Citi para dichos registros.
- vii. Cuando el Proveedor utilice contratistas o subcontratistas para prestar los Servicios, el Proveedor deberá, a sus expensas, garantizar que las evaluaciones de Vulnerabilidad requeridas en virtud de estos Requisitos se completen de la misma manera oportuna que si el Proveedor estuviera prestando dichos Servicios directamente y deberá garantizar que el requisito de que cualquier contratista o subcontratista facilite dichas evaluaciones se memorice en el acuerdo entre el Proveedor y el contratista/subcontratista correspondiente al Servicio, incluyendo el lenguaje que autoriza a Citi a realizar dichas evaluaciones.
- viii. Si el Proveedor es adquirido o adquiere otra entidad en una fusión o adquisición o transacción similar, y dicha transacción probablemente afectará los Servicios, el Proveedor debe notificar de inmediato a Citi por escrito y el Proveedor debe realizar una evaluación de seguridad de la información en la entidad resultante de conformidad con estos Requisitos para asegurarse de que dicho cambio no afecte el cumplimiento del mismo.
- ix. **Implementación de Procesos.** El Proveedor debe implementar un proceso de gestión de vulnerabilidades y amenazas que aborde y/o incluya de manera integral todo lo siguiente: (a) Descubrimiento y gestión de Vulnerabilidades en todos los activos que pueden usarse para procesar, almacenar, acceder o transmitir datos confidenciales o superiores de Citi; (b) El requisito de realizar exploraciones al menos mensuales utilizando una herramienta que descubra instancias de ocurrencia de Vulnerabilidades actualmente conocidas; (c) Clasificación de Vulnerabilidades de acuerdo con el “Common Vulnerability Scoring System (CVSS) v3.0” (ver <https://www.first.org/cvss>), con cronogramas de corrección basados en la gravedad; (d) El requisito de probar correcciones de Vulnerabilidad antes de la implementación de producción completa; (e) Un proceso de emergencia para corregir Vulnerabilidades críticas; (f) Si el proveedor aloja datos confidenciales o superiores de Citi en aplicaciones e infraestructura basadas en Internet,

debe haber una evaluación de vulnerabilidad anual "Pen Test" completada por el proveedor o una parte externa que se especialice en este tipo de evaluaciones; y (g) El proveedor debe hacer seguimiento a los activos que se acercan o han alcanzado un estado de Fin de vida útil (EOL) o Fin de soporte del proveedor (EOVS) y tiene procesos implementados para actualizar o reemplazar dichos activos.

- x. **Notificación.** Cuando el Proveedor identifique una Vulnerabilidad que involucre un producto o servicio que afecte a Citi, el Proveedor notificará a Citi por escrito dentro de las 48 horas posteriores a la identificación e incluirá una descripción de las acciones correctivas que está tomando el Proveedor. Cuando el Proveedor tenga conocimiento de una Vulnerabilidad que involucre un producto o servicio que afecte a Citi luego de la divulgación pública responsable de los canales de proceso (publicación de la Vulnerabilidad en la Base de datos nacional de vulnerabilidades (NVD) o a través del catálogo de amenazas proporcionado a proveedores de seguridad externos), el Proveedor notificará a Citi por escrito dentro de las 48 horas siguientes a dicha publicación. Cada notificación incluirá información sobre la Vulnerabilidad, si la Vulnerabilidad afecta a Citi, si se puede explotar de forma remota; y la puntuación de vulnerabilidades y exposiciones comunes (CVE). El Proveedor continuará brindando actualizaciones a Citi hasta que se resuelva la Vulnerabilidad. En los casos en que Citi identifique una Vulnerabilidad, Citi puede notificar al Proveedor sobre la misma, y el Proveedor deberá corregir la Vulnerabilidad de inmediato de acuerdo con esta Sección.

18.44 Medidas Correctivas. Cuando el Proveedor identifique una Vulnerabilidad, el Proveedor notificará a Citi por escrito dentro de las 48 horas posteriores a la identificación e incluirá una descripción de las acciones correctivas que está tomando el Proveedor. Para cada notificación de Vulnerabilidad proporcionada en virtud de esta Sección, la Parte notificante evaluará el nivel de riesgo y el impacto de dicha Vulnerabilidad en función de la gravedad y el riesgo para Citi y asignará un nivel de prioridad de riesgo en función del Sistema de Puntuación de Vulnerabilidad Común (CVSS) como se establece en el Apéndice A aplicable (ver <https://www.first.org/cvss>). Una vez que se asigna y acuerda un nivel de riesgo, el Proveedor corregirá cualquier Vulnerabilidad media, alta o crítica identificada. Siempre que sea posible, la corrección de cualquier Vulnerabilidad que impacte debe estar disponible en un paquete de seguridad contra la versión implementada actualmente. Si el Proveedor no tiene la capacidad o la disposición de corregir la Vulnerabilidad a satisfacción de Citi dentro del plazo designado, entonces Citi puede rescindir la licencia aplicable sin ninguna responsabilidad u obligación financiera adicional (por la parte rescindida) y el Proveedor reembolsará de inmediato a Citi la parte prorrateada de los derechos de licencia pagados.

18.45 Controles de Red de Seguridad de Comunicaciones.

- i. Las redes de proveedores utilizadas para acceder, almacenar, administrar, procesar y/o transmitir información de Citi deben protegerse de las amenazas y la seguridad debe mantenerse para los sistemas de información que utilizan la red. Esto incluye información que se encuentra en tránsito en la red.
- ii. La información clasificada como Confidencial o de nivel superior de Citi no debe almacenarse de forma continua en un sistema dentro de una zona desmilitarizada (Demilitarized Zone, DMZ) conectada a Internet.
- iii. Con respecto a las redes utilizadas para acceder, almacenar, administrar, procesar y/o transmitir Información de Citi, el Proveedor debe asegurarse:
- iv. Que solo las redes inalámbricas de área local (Wireless Local Area Network, WLAN) u otras soluciones de dispositivos inalámbricos que incluyan controles razonables para prohibir el acceso no autorizado (PEAP-TLS, EAP-TTLS, etc.) se puedan conectar a redes que contengan Información de Citi;
- v. Que todas las conexiones IP externas a la red global del Proveedor estén protegidas por un firewall administrado por el Proveedor;
- vi. Existe un Sistema de detección de intrusiones (IDS) o un Sistema de prevención de intrusiones (IPS) en tiempo real que monitorea y protege las conexiones de Internet a su red donde se accede, administra, almacena, procesa o transmite la Información de Citi.
- vii. Todas las aplicaciones y servicios de Internet de la marca Citi alojados en los sitios del Proveedor deben tener servicios anti-DDoS (Denegación de Servicio Distribuido) aprobados por Citi o controles comparables validados por Citi.
- viii. Que los firewalls externos se configuren con la opción “denegar todo” como regla predeterminada. Las reglas del firewall deben configurarse según el principio de privilegios mínimos y todos los intentos de conexión denegados por el firewall (p. ej., descartar paquetes).

18.46 Segregación en Redes.

- i. El Proveedor debe asegurarse de que todos los Sistemas de Información y aplicaciones utilizados para acceder, almacenar, procesar, administrar y/o transmitir Información de Citi y sean accesibles a través de Internet, solo se accede a través de la zona desmilitarizada del Proveedor (DMZ).
- ii. Durante un evento de emergencia, el Proveedor debe ser capaz de filtrar el acceso entre las distintas partes de la red para reducir el impacto de eventos de seguridad de red (por ejemplo, filtrado de puertos durante un ataque de virus).
- iii. El personal de Acceso Remoto y Seguridad de Host debe implementar controles de acceso basados en grupos (por ejemplo, personal, subcontratistas) para limitar el acceso a recursos de red en la red del Proveedor. A nivel de host, el control de acceso puede realizarse a nivel grupal o individual.

18.47 Identificación de Equipos en Redes.

- i. Las plataformas tecnológicas deben identificar y autenticar las plataformas tecnológicas pares de acuerdo con los niveles de riesgo de IS de la interacción y otros controles de mitigación.
- ii. Solo los dispositivos del Proveedor (es decir, hardware, incluidas las computadoras de escritorio y portátiles) que cumplan con estos Requisitos y que estén autorizados por el Proveedor pueden acceder a la Red del Proveedor donde se almacena, procesa o transmite la información de Citi.

- iii. Solo los dispositivos del Proveedor (es decir, hardware, incluidas las computadoras de escritorio, computadoras portátiles y medios de almacenamiento de datos extraíbles, entre otros) que cumplan con estos Requisitos y que sean autorizados por Citi podrán acceder a la red de Citi.

18.48 Análisis y Especificación de Requisitos de Seguridad.

- i. El Proveedor debe incorporar procedimientos de seguridad de la información en sus procesos y procedimientos para la selección, desarrollo e implementación de aplicaciones, productos y servicios.
- ii. El Proveedor debe tener un procedimiento seguro de creación para todos los sistemas donde se almacene, procese y/o transmita Información de Citi.
- iii. El procedimiento seguro de creación debe incluir herramientas para admitir la comprobaciones automatizadas de configuración para los ajustes estándares y de seguridad de creación al momento de la implementación en producción.

18.49 Transacciones en Línea.

- i. Cuando corresponda, el Proveedor debe tener sistemas de información que usen contraseñas dinámicas o certificados digitales para validar las credenciales.
- ii. La vigencia de todos los certificados debe renovarse, al menos, una vez cada dos (2) años.
- iii. En el caso de todos los sitios web conectados a Internet y comunicaciones punto a punto entre Citi y el Proveedor, se deben usar certificados de Validación extendida (Extended Validation, EV).
- iv. Todas las aplicaciones del Proveedor que almacenan, procesan, administran o acceden a información de Citi, alojan aplicaciones de Internet de marca Citi o tienen conectividad a los recursos de red de Citi deben:
- v. Tener un método de autenticación basado en los tipos de datos/funciones a los que se accede;
- vi. Realizar una evaluación de cumplimiento de Autenticación de Múltiples Factores (MFA);
- vii. Implementar una solución de gestión de actividades sospechosas (SAM) en línea
- viii. En todos estos casos, el Proveedor debe comunicarse con su contacto comercial principal para conocer los requisitos actuales.

18.50 Procedimientos de Control de Cambios.

- i. El proveedor debe asegurarse de que los cambios de configuración en los firewalls, los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) se enruten a través del proceso de gestión de cambios del proveedor.
- ii. El acceso otorgado a producción mediante identificaciones temporales debe ser registrado y monitoreado para hacer un seguimiento de los cambios realizados en el entorno.
- iii. Para Sistemas de información controlada que contengan información del Cliente clasificada como Confidencial o de nivel superior en un valor de componente de riesgo de seguridad de la información para “integridad” o una “disponibilidad” de nivel alto, el Proveedor debe revisar los registros captados de acuerdo con la Sección 10.7q (Registros de auditoría) a partir de muestras. Las revisiones pueden utilizar una metodología apropiada de muestreo basada en el riesgo.
- iv. La revisión debe validar que los cambios que forman parte del acceso privilegiado temporal se realizaron según lo previsto.

18.51 Fuga de Información. El proveedor debe haber documentado la norma de codificación segura que evite la fuga de información, que incluye:

- i. Información detallada del sistema (por ejemplo, tecnología y tipo de servidores);
- ii. Rastros de la pila y errores de excepción que revelen la estructura de árbol de directorios y el tipo de base de datos subyacente.

18.52 Datos de Prueba. La información confidencial o de mayor riesgo, tal como la define Citi, no será utilizada ni almacenada por el Proveedor en entornos de prueba o desarrollo de aplicaciones de software, a menos que esa información sea desidentificada, enmascarada y/u ofuscada utilizando herramientas y métodos que cumplan con los estándares de la industria para que dichos datos ya no sean sensibles o se implementen los mismos controles que en un sistema de producción.

18.53 Transmisión de Datos. El Proveedor no transmitirá información Confidencial o de mayor riesgo a través de ninguna red pública (como Internet) sin cifrar. En caso de que se envíe información confidencial o de mayor riesgo, según la definición de Citi, a través de redes públicas, esa información debe cifrarse utilizando un algoritmo de cifrado, fortaleza, recuperación de datos y almacenamiento de claves que sean consistentes con las políticas y estándares de Citi y/o el estándar industrial actual acordado mutuamente de protocolos de cifrado.

18.54 Acceso del Personal del Proveedor a los Sistemas de Información del Proveedor. Todo el Personal del Proveedor, incluyendo, entre otros, empleados permanentes o temporales, contratistas y subcontratistas, que requieran acceso especial, privilegiado y/o de nivel administrativo a sistemas, depósitos de datos, aplicaciones y/o infraestructura, incluidos, entre otros, administradores de sistemas, administradores de bases de datos, administradores de control de acceso, administradores de firewall, administradores de sitios web, etc., que estén relacionados directa o indirectamente con los Servicios prestados para Citi deberán utilizar la autenticación multifactor y dicho acceso será registrado y supervisado de forma independiente por el Proveedor para actividad sospechosa y/o acceso no autorizado de acuerdo con los Requisitos de Citi para Proveedores, como se indica anteriormente.

18.55 Almacenamiento de Datos Fuera de la Red. El Proveedor deberá, cuando almacene información confidencial o de mayor riesgo de Citi fuera de la red del Proveedor (por ejemplo, respaldo de Recuperación de Desastres), garantizar que dicha información se cifre cuando esté en reposo utilizando un algoritmo de cifrado aprobado por Citi y/o un protocolo de cifrado estándar de la industria actual acordado mutuamente, así como el almacenamiento de claves.

18.56 Requisitos del Proceso Comercial de Acceso Remoto del Proveedor.

- i. Si el Proveedor proporciona servicios de subcontratación de procesos comerciales y recibe la aprobación expresa por escrito de Citi para permitir que el Personal del Proveedor se conecte de forma remota desde su ubicación (por ejemplo, trabajar desde casa) a los sistemas del Proveedor que tienen acceso, almacenar y/o transmitir datos confidenciales o de mayor riesgo (por ejemplo, datos privados, transacciones monetarias, etc.) se deben cumplir los siguientes requisitos de seguridad para los elementos aplicables relacionados con el acceso remoto proporcionado por el Proveedor. El Proveedor debe presentar la documentación completa, incluidos, entre otros, diagramas de arquitectura de red, flujos de datos, sistemas de autenticación, sistemas de seguridad y cualquier otro detalle técnico o atestación que pueda ser necesaria, a juicio de Citi, para garantizar el cumplimiento de los estándares de Citi y mantener la postura de seguridad de Citi.
- ii. Las Soluciones de Acceso Remoto del proveedor deben, como mínimo:
 - a. Tener o establecer una conexión de red de empresa a empresa privada y segura con Citi. Esta conectividad debe cumplir con los estándares de conectividad de red de terceros y ser revisada y aprobada por la Oficina de CISO de Citi.

- b. Emplear en todas las comunicaciones de la red el cifrado de extremo a extremo, utilizando algoritmos de cifrado aprobados por Citi
- c. Asegurar que la red y los sistemas del Proveedor incluyan Sistemas Unificados de Gestión de Amenazas/Detección y Prevención de Intrusos, junto con el registro y monitoreo de estos sistemas de seguridad para detectar amenazas y anomalías y que los procedimientos de respuesta a incidentes apropiados estén documentados y probados para proteger, detectar, contener, responder y recuperar de una manera oportuna.
- d. Tener una solución de acceso remoto VPN segura y resistente (sin puntos únicos de falla) que requiera autenticación multifactor ("MFA") de conformidad con los estándares MFA de Citi. Además, esta solución de acceso remoto debe garantizar que solo la propiedad del Proveedor, administrada, aprobada y mantenida (por ejemplo, configuración de seguridad, administración de parches, protección antivirus, administración de acceso e identificación, firewalls, etc.) se utilicen para conectarse de forma remota y realizar servicios relacionados con Citi. Si se utilizan tokens de software para MFA, como una aplicación de software en un dispositivo móvil, el software de autenticación de token de software debe autenticar al usuario (por ejemplo, mediante contraseña, datos biométricos, etc.) e impedir su uso si el teléfono móvil tiene jailbreak o rooteo (usando un sistema operativo diferente a los certificados y suministrados por el proveedor del dispositivo móvil).
- e. Debe, como mínimo, proporcionar documentación completa que incluya, entre otros, todos los diagramas de red de acceso remoto relevantes, flujos de datos, todos los controles y tecnologías operativos y de seguridad, y debe proporcionarse a Citi para su revisión y aprobación antes de que se presten servicios de acceso remoto proporcionados al Personal del Proveedor.
- f. Todo el Personal de acceso remoto del Proveedor debe atestiguar y aceptar mediante evidencia documentada lo siguiente:
 - 1. Cumplimiento del Código de Conducta de terceros de Citi, la Política de Comunicaciones Electrónicas y todas las Políticas y Estándares de Citi aplicables.
 - 2. Mantendrá un espacio de trabajo remoto dedicado y privado que no contenga ningún dispositivo de asistencia de voz (p.ej., Alexa), dispositivos de grabación de video y/o cualquier otro dispositivo para escuchar/grabar fotos, videos o audio. No se permitirá que personal no autorizado vea ningún dato, sistema o aplicación que pueda aparecer en la(s) pantalla(s) de los sistemas informáticos remotos.
 - 3. Bloquear el dispositivo informático cuando lo deje desatendido para garantizar que el acceso no autorizado para ver la pantalla se mitigue adecuadamente.
- g. Restringir el acceso remoto solo a dispositivos informáticos administrados y propiedad del Personal autorizado y del Proveedor (por ejemplo, una computadora portátil) que restringe al usuario solo a aquellos servicios ÚNICAMENTE expresamente requeridos (por ejemplo, una solución segura de cliente ligero) para prestar los Servicios. Específicamente, el sistema informático remoto debe configurarse para evitar que el usuario pase por alto la solución de seguridad de "cliente ligero", evitar cualquier impresión remota, evitar el uso de dispositivos de almacenamiento portátiles externos (p.ej., memorias USB, discos duros portátiles, lectores de tarjetas SD, etc.), evitar capturas de pantalla, evitar copiar/pegar fuera de la solución Citi VDI, evitar la instalación de cualquier software y evitar cualquier cambio de configuración no autorizado en el

sistema. El proveedor debe garantizar que se mantenga una higiene cibernética adecuada de estos sistemas informáticos remotos a través de actualizaciones apropiadas y oportunas, parches de seguridad, actualizaciones de configuración, etc. El dispositivo informático remoto también debe requerir que el usuario se vuelva a autenticar después de un máximo de 30 minutos de inactividad y protección de punto final implementada para prevenir, detectar y recuperarse de la introducción de cualquier código malicioso (por ejemplo, virus, gusanos, virus troyanos, adware o spyware). No se permite el uso de dispositivos informáticos de propiedad personal del Personal del Proveedor (por ejemplo, computadoras portátiles/de escritorio BYOD) para proporcionar los Servicios.

- h. Asegurar de que se realice un registro y monitoreo adecuados para rastrear la actividad del usuario y del punto final a través de la ubicación, dirección IP, inicios de sesión/tiempos de espera, actividad sospechosa, malware, etc. Registrar todos los intentos de violación de la seguridad del sistema (p. ej., intentos fallidos de inicio de sesión de usuarios de acceso remoto).
- iii. Si el proveedor permite la administración remota de TI (p. ej., red, sistema, aplicación, base de datos, etc.), el proveedor se asegurará de que todo el acceso remoto lo realice únicamente personal autorizado a través de una conexión cifrada y segura (p. ej., VPN, interfaz de escritorio virtual, etc.) que requiere autenticación multifactor, y todas las actividades se monitorean en busca de actividades sospechosas.

18.57 Aceptación del sistema. El Proveedor debe contar con procesos documentados de aceptación de sistemas y gestión del alcance de proyectos que cumplan con los estándares pertinentes de la industria.

18.58 Reporte de debilidades en la seguridad de la información. El Proveedor debe tener un Proceso para garantizar que las Vulnerabilidades de Infraestructura y Aplicaciones que resulten en un compromiso de los Activos de Información de Citi sean **informadas a Citi inmediatamente**.

18.59 Responsabilidades y procedimientos de incidentes de seguridad. El Proveedor debe garantizar que se aplique un enfoque eficaz a la gestión de incidentes de seguridad de la información que afecten a la Información de Citi. El Proveedor debe mantener procesos para responder a los Incidentes de SI y notificar a Citi dentro de un período de tiempo acordado, cualquier incidente con una probabilidad de clasificación de Gravedad alta que pueda implicar un riesgo significativo para los clientes de Citigroup o la franquicia (incluso cuando el incidente involucre un número significativo de clientes; una gran cantidad de dólares; que probablemente sea objeto de cobertura de prensa; o que probablemente resulte en la notificación no rutinaria de un regulador) debe informarse dentro de un plazo de 2 horas y todos los demás incidentes de seguridad deben informarse dentro de no más de 24 horas de detección de una Amenaza de SI o una Vulnerabilidad de SI las 24 horas del día, los 7 días de la semana. Esto incluye, entre otros, incidentes de seguridad de la información, amenazas a o vulnerabilidades de la seguridad de la información generadas por IDS/IPS/la Detección de Anomalías de Comportamiento en la Red (Network Behavior Anomaly Detection, NBAD).

18.60 Reporte de Incidentes de Seguridad.

- i. Los Proveedores están obligados a informar sobre cualquier Incidente de Seguridad que comprometa o ponga en peligro la confidencialidad, integridad o disponibilidad de los datos confidenciales o de nivel superior que sean propiedad de Citi o estén administrados por Citi, o de los datos que Citi tenga la obligación de custodiar, o de los sistemas de información que albergan dichos datos; independientemente de cómo, quién (personal de Citi o un proveedor o socio de Citi) o dónde (dentro o fuera de la propiedad de Citi) se haya producido el incidente de seguridad. Esto incluye, pero no se limita a, la alteración, destrucción, divulgación, pérdida, robo o uso indebido de dichos datos o sistemas, dispositivos o medios físicos o electrónicos que contengan estos datos. Esto también podría incluir activos públicos de cualquier clasificación de datos, así como cualquier información de identificación personal (PII) / (Datos personales) violación de datos donde es probable que resulte en un alto riesgo para los derechos y libertades de las personas físicas, donde tal los derechos y libertades están definidos por las leyes o reglamentos locales.
- ii. Los proveedores externos deben informar los incidentes de seguridad reales o potenciales a su gerencia, quien debe notificar de inmediato a un funcionario de Citi en caso de cualquier divulgación real o probable de información confidencial de Citi o superior. El representante de Citi debe notificar a su ISO de inmediato.

18.61 Protección de Fugas de Datos (DLP).

- i. El proveedor debe implementar controles de prevención de fuga de datos (DLP), incluido el monitoreo de contenido y punto final que cubre a todo el personal con acceso a datos confidenciales o superiores de Citi.
- ii. El Proveedor debe contar con controles para detectar y/o prevenir instancias en las que los datos confidenciales o de nivel superior de Citi salgan de la red a través de los siguientes canales:
 - a. Correos electrónicos no cifrados.
 - b. Archivos adjuntos de correo electrónico cifrados.
 - c. Carga de datos de Citi a la Web.
 - d. Impresión de datos de Citi.
 - e. Transferencias de datos de Citi a ubicaciones fuera de su red (por ejemplo, a través de FTP).
 - f. Intentos de copiar datos confidenciales o de nivel superior de Citi a medios extraíbles tales como unidades USB, discos duros extraíbles, unidades de CD/DVD y otros dispositivos extraíbles con capacidades de almacenamiento de datos.
 - g. La solución DLP debe registrar y alertar al Proveedor acerca de todos los eventos que representen intentos (ya sean exitosos o bloqueados) de mover, transmitir o copiar datos confidenciales o de nivel superior de Citi de su red a otros destinos.

18.62 Navegación Web.

- i. El proveedor debe contar con controles de acceso web para evitar el intercambio de información confidencial o superior de Citi y la exposición a malware o ataques para aquellos empleados con acceso a los datos de Citi.
- ii. Para los empleados que tienen acceso a los datos confidenciales o de nivel superior de Citi:
 - a. Todas las solicitudes de URL deben quedar registradas.
 - b. Los intentos de acceder a sitios que pueden usarse para compartir datos de Citi sin autorización (es decir, correo web, chat, redes sociales, almacenamiento en línea, etc.) deben ser bloqueados.

- c. Se debe bloquear el acceso a los sitios que puedan exponer el entorno a malware o ataques.
- d. Se debe bloquear todo intento de tener acceso a sitios que se consideren no relacionados con el negocio.
- e. El proveedor debe suscribirse a un servicio de categorización de URL que se actualiza periódicamente; todas las URL no categorizadas se bloquean de manera predeterminada o todas las URL se bloquean de manera predeterminada y las URL se aprueban caso por caso. Los proveedores de bajo riesgo quedan exentos de este requisito.
- f. Los navegadores web utilizados por el Proveedor son totalmente compatibles y están al día con las actualizaciones de seguridad más recientes por parte del proveedor de software.

18.63 Mensajería Electrónica. La mensajería electrónica, las redes peer-to-peer u otras herramientas colaborativas de Internet no se pueden usar para transmitir o almacenar Información de Citi fuera de la red del Proveedor o desde redes que contienen Información de Citi, a menos que se haya implementado el cifrado adecuado para todos los datos de Citi según la Sección 18.7. (Política sobre el uso de controles criptográficos).

18.64 Correo electrónico. El Proveedor cuenta con controles de correo electrónico a fin de evitar el intercambio de información de Citi y la exposición a malware o ataques. Esto incluye:

- i. Los archivos adjuntos entrantes que ingresan en el portal del correo electrónico se escanean y bloquean si suponen un riesgo para el sistema.
- ii. Se utiliza software de filtrado de correo electrónico (antispam, antiphishing) y está actualizado.
- iii. Cualquier dato confidencial o de nivel superior de Citi debe cifrarse cuando se envía fuera de la organización.
- iv. Los clientes de correo electrónico utilizados por el Proveedor son totalmente compatibles y están al día con las actualizaciones de seguridad más recientes por parte del proveedor de software.

18.65 Medios Extraíbles.

- i. El proveedor debe proteger la información de Citi independientemente de los medios en los que se mantenga. Este estándar se aplica, pero no se limita a, los siguientes tipos de medios sobre los que se contiene información: tarjeta, casete, disco compacto (CD), disquete u otro dispositivo de almacenamiento extraíble, copia impresa, disco magnético, cinta magnética, microfilm, microficha, disco óptico o documento en papel.
- ii. La configuración predeterminada para acceder a dispositivos de almacenamiento y medios portátiles en los sistemas donde se almacena Información de Citi debe ser de “sin acceso”. Si se otorgan excepciones y se permite el acceso de lectura y escritura, los datos del dispositivo de almacenamiento portátil deben estar cifrados.
- iii. Si se permite el uso de medios extraíbles, dicho uso debe contar con un proceso de aprobación de gestión, incluida la justificación comercial que requiere el uso de medios extraíbles.
- iv. Los medios extraíbles deben inventariarse.
- v. Los medios extraíbles que contengan datos de Citi de carácter confidencial o nivel superior deben cifrarse automáticamente sin que se exija ninguna acción por parte del usuario.

18.66 Eliminación de Medios.

- i. Cuando la información de Citi con una clasificación de Citi de Confidencial o superior sea elegible para su eliminación de acuerdo con las instrucciones proporcionadas por Citi (es decir, en el punto en el que la información ya no sea necesaria o útil para Citi, más cualquier período adicional de retención requerido por ley, regulación y/o políticas de Citi), el Proveedor debe destruir dicha Información de manera que quede inutilizable e irrecuperable.
- ii. Se debe utilizar una herramienta aprobada que sobrescriba al azar los sectores del disco con diferentes caracteres específicos a fin de borrar de manera segura los medios montables con base en las siguientes reglas:
 - a. En el caso de los medios que almacenan información clasificada como Confidencial o de nivel superior, la herramienta debe completar tres pasadas.
 - b. Desmagnetizar los medios.
- iii. Destruir los medios físicamente para hacerlos ilegibles (es decir, triture, aplaste las unidades).
- iv. Los medios de almacenamiento impresos y no electrónicos de otro tipo que contengan Información Confidencial o de nivel superior deben recopilarse y almacenarse de manera segura en una "Papelera Confidencial" protegida antes de su eliminación definitiva. Las Papeleras Confidenciales siempre deben cerrarse bajo llave y solo pueden ser abiertas por el personal autorizado.
- v. Las copiadoras, impresoras, máquinas de fax y cualquier otro dispositivo que tenga memoria/almacenamiento que pueda contener información confidencial de Citi o superior también deben desinfectarse.

18.67 Manejo de Datos Adicionales.

- i. El Proveedor debe asegurarse de que todos los datos confidenciales estén enmascarados en la pantalla y en papel (incluidos, por ejemplo, los informes de seguimiento, de excepción, reglamentarios y de otro tipo).
- ii. El Proveedor debe restringir la impresión, grabación o copia de datos confidenciales, incluso por 'dispositivos propios'. El proveedor debe realizar todos los esfuerzos razonables para devolver o destruir toda la información de Citi en un momento acordado durante o al final del acuerdo.

18.68 Gestión y Formación en Seguridad de la Información.

- i. El Proveedor debe asegurarse de que todos los empleados, incluidos contratistas y miembros del personal temporal, reciban la educación y capacitación apropiadas para la concientización acerca de las políticas y los procedimientos organizativos según sea relevante para la función de su puesto de trabajo.
- ii. Debe garantizar que el programa de capacitación y concientización se revise y actualice cada año.
- iii. Como mínimo, es necesario incluir los siguientes temas:
 - a. Uso aceptable de los recursos de información
 - b. Etiquetado y manipulación de la información
 - c. Transmisión segura (correo electrónico seguro, almacenamiento seguro en SharePoint, no enviar datos pertenecientes a Citi al correo electrónico personal)
 - d. Informe de incidentes en materia de seguridad de la información
 - e. Centro de trabajo seguro (uso apropiado de Internet, software no autorizado, no descargar software no aprobado por Citi)
 - f. Manejo de contraseñas (contraseñas seguras, uso compartido de contraseñas)
 - g. Controles de malware
 - h. Ingeniería social (phishing, spear fishing, vishing, smishing)
 - i. Trabajo remoto (conexión protegida/segura, seguridad de dispositivos personales)

- iv. El proveedor debe asegurarse de que todos los empleados, incluidos los contratistas y el personal temporal, completen las capacitaciones de concientización sobre la seguridad de la información dentro de los 30 días posteriores a la contratación.
- v. El Proveedor debe asegurarse de que todos los empleados, incluidos contratistas y miembros del personal temporal, completen una capacitación anual de actualización de conocimientos.
- vi. La capacitación debe incluir una medición de su efectividad.

18.69 Programa de Gestión de Riesgos Cibernéticos. El proveedor también deberá, como mínimo, mantener un programa adecuado de gestión de riesgos cibernéticos que incluya lo siguiente:

- i. Mantener un programa bien definido y documentado de gestión de riesgos de seguridad de la información y/o un programa de gestión de riesgos operativos que tenga un componente de gestión de riesgos cibernéticos/de información claramente definido, que defina el apetito por el riesgo cibernético del proveedor y asegure que su riesgo residual cibernético se alinea con ese apetito.
- ii. Un sólido programa de gestión de riesgos de seguridad que incluye, entre otros, la recopilación y/o la realización de auditorías y revisiones de seguridad que evalúan el estado general de la seguridad dentro de la organización, e informa periódicamente al menos una vez al año a su liderazgo ejecutivo para revisión y garantía de que no se ha violado el apetito por el riesgo cibernético del proveedor.
- iii. Mantener el cumplimiento de los Estándares de seguridad de datos PCI (PCI-DSS) aplicables al Proveedor cuando el Proveedor procesa, almacena y/o transmite transacciones, pagos y/o información con tarjeta de crédito/débito.
- iv. Mantener un plan de gestión de crisis y una guía de Plan del Equipo de Respuesta a Incidentes de Seguridad (SIRT) consistente con los estándares de la industria para asegurar que el Proveedor tiene la capacidad suficiente y adecuada para detectar, contener, investigar, responder y recuperarse de cualquier intento, sospecha y/o incidente real de ciberseguridad incluyendo, pero no limitado a ransomware, acceso no autorizado, exfiltración de datos no autorizada, robo de código fuente de aplicaciones, etc.
- v. Mantener un programa de higiene cibernética efectivo que asegure que se instalen parches de software y que las configuraciones de redes, sistemas y/o aplicaciones se apliquen y mantengan de manera consistente y segura.
- vi. Mantener un programa apropiado de educación y concientización sobre privacidad y seguridad de la información/cibernética que incluya, entre otros, la prevención del phishing y otros ataques de ingeniería social, el manejo adecuado de la información confidencial y/o regulada por privacidad, y el informe de incidentes de seguridad y la gestión de respuestas.

18.70 Seguridad de aplicaciones, API, código, sistema e infraestructura. Cuando el Proveedor aloje, desarrolle, codesarrolle, proporcione entornos de desarrollo y/o suministre aplicaciones de software, el Proveedor deberá realizar revisiones de código de dicho software y/o parches para el software en busca de fallas de seguridad, prevención de acceso no autorizado, modificación y/o inserción de malware u otras formas de código malicioso, y pruebas de vulnerabilidad para garantizar que la aplicación (incluidas las API), junto con los servicios del sistema subyacente, el sistema operativo y las redes estén libres de vulnerabilidades y defectos conocidos que podrían resultar en un incidente de seguridad, violación de la privacidad, fraude, acceso no autorizado y/o divulgación de Información Confidencial, pérdida de integridad de la información procesada, almacenada o transmitida por la(s) aplicación(es), y/o pérdida de disponibilidad que podría afectar la calidad de productos y/o servicios que el proveedor proporciona a Citi.

19 PAUTAS PARA UN LUGAR DE TRABAJO SEGURO

Aplicable a Proveedores que acceden/procesan/administran/almacenan Información de Citi Y/O Alojamiento de aplicaciones de Internet de la marca Citi Y/O tienen conectividad a los recursos de red de Citi Y/O requieren acceso sin escolta a las instalaciones de Citi.

Los Proveedores tienen la obligación de proteger los activos tangibles e intangibles de Citi y de sus Clientes. Los activos de Citi y del Cliente pueden usarse solo para fines autorizados y de maneras aprobadas (por ejemplo, de acuerdo con las licencias, términos y condiciones aplicables) y luego solo con respecto a los fines comerciales de los Proveedores de Citi y Citi. Los activos incluyen dinero en efectivo, títulos valores, bienes físicos, servicios, planes de negocios, Información de Citi, información de proveedores, información de distribuidores, propiedad intelectual (programas informáticos, modelos y otros elementos), y toda otra Información confidencial, personal y de propiedad exclusiva. La apropiación indebida o la divulgación no autorizada de los activos de Citi es un incumplimiento de su obligación con Citi y puede constituir un acto de fraude contra Citi. Del mismo modo, el descuido, el desperdicio o el uso no autorizado con respecto a los activos de Citi también es un incumplimiento de su obligación con Citi.

Artículo	Requisitos
Información de Citi (documentación electrónica e impresa)	La Información de Citi se debe guardar debidamente y bajo llave después del horario normal de trabajo y toda vez que el Proveedor se aleje de su espacio de trabajo designado.
Computadoras de escritorio y portátiles	Las computadoras de escritorio y portátiles usadas para ver Información de Citi o acceder a esta deben protegerse con protectores de pantalla y contraseña luego de un período de inactividad. Cada vez que el Proveedor se aleje del lugar de trabajo designado, debe bloquear la computadora de escritorio o portátil con las teclas CTRL + ALT + SUPRIMIR y seleccionar "Lock Computer" (bloquear el equipo). Si el Proveedor utiliza una computadora portátil para ver Información de Citi, debe asegurarse de sujetar la computadora con un cable o candado de seguridad a la base durante el horario de trabajo y guardarla de forma segura después del horario normal de trabajo.
Guardado bajo llave	Los archivadores y cajones que almacenan información de Citi deben cerrarse después de las horas normales de trabajo.
Áreas de Oficina Abiertas	Las áreas abiertas de la oficina no deben usarse como servidores de archivos/mini centros de datos para almacenar información de Citi, a menos que estén diseñadas específicamente para tal uso y documentadas con Citi.
Bandejas de impresoras, fotocopadoras y fax	Todo el material relacionado con Citi debe borrarse de impresoras, fotocopadoras y bandejas de fax.
Eliminación	Elimine la Información de Citi que ya no sea necesaria (siga los programas de conservación específicos). Los documentos deben triturarse o colocarse en una papelería de reciclaje segura. Los medios magnéticos deben eliminarse de forma segura después de seguir los procedimientos de borrado adecuados.

20 INTELIGENCIA ARTIFICIAL/APRENDIZAJE AUTOMÁTICO

Aplicable a Proveedores que utilizan Inteligencia Artificial/Aprendizaje Automático (AI/ML), según lo define Citi en estos Requisitos para Proveedores, en cualquier parte del producto/servicio que están brindando.

- 20.1** El Proveedor deberá entregar una notificación por escrito a Citi que identifique expresamente AI/ML, según lo definido por Citi en el Apéndice del presente, donde tal AI/ML es:
- i. utilizado, contenido o incorporado de otro modo en cualquier producto o servicio para el cual están bajo Contrato para proporcionar directa o indirectamente a Citi, o en cualquier parte del mismo, incluido cualquier producto o servicio de terceros contenido o integrado en el mismo; o
 - ii. utilizado de cualquier manera en la ejecución de cualquier Contrato por parte del Proveedor, ya sea que dicho AI/ML se use, contenga o incorpore de otro modo en el producto o servicio real que se entrega a Citi; o
 - iii. utilizado por el Proveedor de cualquier manera que pueda exponer la Información de Citi a dicho AI/ML, incluidos, entre otros, cualquier AI/ML utilizado por el Proveedor en sus operaciones comerciales no comerciales (por ejemplo, mantenimiento de registros comerciales, mejoras de procesos, investigación y desarrollo, cumplimiento y auditoría interna).
- 20.2** El Proveedor se asegurará de que cualquier acuerdo que rija su relación con un subcontratista (o el propio acuerdo de ese subcontratista con otra parte relevante) que se comprometa a realizar o ayudar con las obligaciones del Proveedor en virtud de cualquier Contrato, o cualquier acuerdo entre el Proveedor y un tercero que rija la responsabilidad de dicho tercero de proporcionar servicios en apoyo de cualquier operación no comercial del negocio del Proveedor como se hace referencia anteriormente, contiene disposiciones que son, como mínimo, tan completas y estrictas como las contenidas en esta Sección 20, y el Proveedor ejercerá sus derechos en virtud de dichas disposiciones en beneficio de Citi a pedido de Citi. Además, a lo largo de la vigencia del Contrato, cualquier uso de AI/ML como se describe en esta Sección 20 en cualquier etapa debe notificarse de inmediato a Citi por escrito, y el Proveedor deberá cumplir de inmediato con cualquier solicitud de Citi de más información de respaldo relacionada con dicha AI/ML y su utilización, y puede estar sujeto a revisión adicional, cambios y supervisión de dicho AI/ML, cuando corresponda.
- 20.3** Si lo solicita un regulador, como parte de cualquier inspección regulatoria o investigación forense sobre el uso de AI/ML en cualquier parte del producto/servicio, el Proveedor debe ayudar a Citi a responder a la solicitud del regulador, incluida la realización y/o facilitación de la realización de auditorías de algoritmos necesarias para descubrir las operaciones reales de los algoritmos incluidos en los modelos AI/ML.
- 20.4** También se deben respetar los siguientes principios:
- i. Legalidad. Se espera que los sistemas AI/ML del proveedor estén diseñados para adherirse y cumplir con la ley aplicable y los tratados internacionales que son más seguros para los clientes, usuarios y empleados de Citi.
 - ii. Finalidad y Proporcionalidad. Nuestros sistemas AI/ML estarán diseñados para el cumplimiento de los fines previstos de los servicios prestados a Citi, y operarán únicamente de manera proporcional en la medida necesaria, adecuada y relevante en relación con los fines antes mencionados.

APÉNDICE - DEFINICIONES

Air – Gap es una medida de seguridad en la que una computadora, sistema o red se separa físicamente de otras computadoras, sistemas o redes. Una arquitectura de respaldo de datos con espacio de aire limita la exposición a un ciberataque y permite la restauración de datos a un punto en el tiempo antes de que el ataque se haya iniciado.

Ley Aplicable incluye: (a) las leyes y reglamentos estatales de ejecución hipotecaria y (b) las reglas, pautas y otros comunicados emitidos por varias agencias federales de los Estados Unidos, incluida la Oficina del Contralor de la Moneda (a veces denominada Pautas y reglamentos de bandera roja) que implementan la sección 114 de la Ley de Transacciones de Crédito Justas y Precisas de 2003.

Zona de Disponibilidad es donde el proveedor de servicios en la nube tiene un grupo de centros de datos lógicos. Una zona de disponibilidad es uno o más centros de datos discretos con energía, redes y telecomunicaciones redundantes en una Región de la Nube.

Inteligencia Artificial (IA) se refiere a un método, sistema o enfoque cuantitativo ('técnicas') que emula la inteligencia humana a través de programas informáticos para realizar estimaciones, predicciones, recomendaciones o decisiones de maneras que van más allá de los enfoques estadísticos, matemáticos, econométricos o financieros clásicos. **Las categorías de IA incluyen:**

- **IA automática:** Técnicas de "IA dinámica" que además son capaces de cambiar automáticamente su estructura básica (por ejemplo, hiperparámetros, variables de entrada)
- **IA Cognitiva:** Técnicas que pueden tomar decisiones de forma autónoma y actuar en consecuencia, incluso en asuntos para los que no fueron entrenados específicamente.
- **IA Dinámica:** Técnicas que, a diferencia de la "IA Estática", pueden volver a entrenar automáticamente los parámetros periódicamente, en producción
- **IA Estática:** Técnicas de IA entrenadas manualmente fuera de línea o cuyos parámetros se programan explícitamente y luego se usan para hacer estimaciones, predicciones, recomendaciones o decisiones.

Machine Learning (ML) es el subconjunto de IA que deriva representaciones o inferencias de datos sin programar explícitamente cada representación de parámetro o paso de computadora, por ejemplo, bosques aleatorios, enfoques basados en redes neuronales. Por el contrario, las técnicas de IA que no son miembros del subconjunto ML incluyen técnicas como la lógica difusa, técnicas de análisis de dependencias complejas para el procesamiento del lenguaje natural.

Business Activity Owner (BAO) es un empleado de Citi responsable de realizar y administrar activamente ciertas actividades asociadas con las relaciones con los Proveedores.

Regalo de Negocios: cualquier objeto de valor (que no sea Entretenimiento de Negocios) dado o recibido por un empleado de Citi en relación con negocios de Citi o negocios de la parte externa, que, por lo general, no incluye objetos valuados en \$25 o menos.

Información de Citi es información que Citi posee o está obligada a proteger durante el almacenamiento, procesamiento, transmisión o eliminación en formatos digitales y no digitales. **Información de Citi Sus clasificaciones incluyen:**

- **Confidencial:** información que los Negocios de Citi están obligados a proteger, lo que incluye la información perteneciente a los clientes, a trabajadores, a terceros o a los Negocios de Citi. La información confidencial es cualquier combinación de datos sujeta a restricciones normativas o contractuales relativas a su divulgación. También es información que el negocio considera que posee el potencial de brindar una ventaja competitiva o producir un impacto considerable en el negocio si se divulga a personas no autorizadas.
- **La Información Confidencial de Identificación Personal (CPPI)** tendrá una clasificación de protección

de información de Confidencial si podría esperarse razonablemente que el compromiso de la confidencialidad, la integridad o la disponibilidad de la PII tenga un efecto adverso grave en las personas afectadas o en Citi, o que el compromiso de la confidencialidad, la integridad o la disponibilidad de la PII desencadenaría requisitos de notificación de incumplimiento conforme a la ley aplicable. Un efecto adverso serio sobre una persona significa que el impacto podría razonablemente resultar en una pérdida financiera moderada o fraude, o bien vergüenza o angustia personal. Ejemplos de datos que cuando se combinan con otra información constituyen PII Confidencial:

- Nombre o información de contacto de la persona (dirección, número telefónico o dirección de correo electrónico) en combinación con:
 - Número de pasaporte, número de licencia de conducir, número de identificación nacional o gubernamental o el número de identificación fiscal de una persona;
 - Número de identificación de cliente, número de tarjeta de crédito/débito, identificadores de cuentas que pueden resultar en movimientos de fondos u otros números de cuentas financieras;
 - Elementos de datos transaccionales que pueden usarse para efectuar robos de identidad o fraudes;
 - Información sobre la solicitud de cuenta del cliente, datos de informes de crédito, puntaje crediticio;
 - Información sobre la valoración de rendimiento del trabajador o su remuneración;
 - Grabaciones en video, incluso registros de CCTV o cajeros automáticos
 - Estos elementos se consideran PII Confidencial bien sea por sí mismos o en combinación con otros elementos: Un número de Seguro Social de EE. UU. o un número de identificación emitido por el gobierno (que es equivalente en uso y/o estado de protección legal al número de Seguro Social de EE. UU.) solamente.
- **Información Interna** se comparte comúnmente dentro de Citi, no está destinada a distribuirse a nadie fuera de Citi y es información que no está clasificada como Restringida o Confidencial. Entre los ejemplos de información Interna se incluyen nuestros estándares y políticas.
 - **Información Personal Identificable (PII):** es cualquier Información Personal que:
 - identifica o se puede usar para identificar a una persona u hogar (como nombre, firma, dirección, identificador nacional único, como número de seguro social, número de registro de residente, fecha de nacimiento, número de licencia de conducir).
 - se relaciona con, describe, es capaz de asociarse a, o podría vincularse razonablemente (directa o indirectamente) con una persona física o un hogar;
 - se puede utilizar para autenticar a una persona o proporcionar acceso a una cuenta (como un nombre de usuario, dirección de correo electrónico, contraseña, PIN, número de identificación, responde preguntas de seguridad); o se relaciona con un individuo y que podría ser confidencial (como información médica o de salud personal, número de cuenta, valor de cuenta).
 - La información personal también incluye información de salud protegida (según lo definido por la Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU.), información personal confidencial e información crediticia (como se define en varias leyes de protección de datos/privacidad y confidencialidad bancaria).
 - **Pública** es información que está disponible gratuitamente fuera de Citi o está destinada al uso público, como comunicados de prensa de Citi o artículos que aparecen en las noticias sobre Citi.
 - **Restringida** es aquella Información que, si se revela a cualquier persona no autorizada, incluidas las personas que trabajan en Citi, podría tener un impacto significativo en las obligaciones legales y reglamentarias de Citi o en su estado financiero, clientes o Franquicia.
 - **PII Restringida** tendrá una clasificación de protección de la información de Restringida si se puede esperar razonablemente que el compromiso de la confidencialidad, la integridad o la disponibilidad de la PII tenga un efecto adverso grave o catastrófico en las personas afectadas o en Citi o si, según la ley de la jurisdicción, aumenta se requieren controles de seguridad debido a la naturaleza de la PII (por ejemplo, PII sensible o de 'categoría especial'). Los ejemplos de PII Restringida incluyen cualquier información de PII Pública, PII Interna y PII Confidencial en combinación con:

- Datos relacionados específicamente con: raza, religión, creencias religiosas o filosóficas, raíces étnicas, afiliación u opiniones políticas, participación en sindicato, información sobre antecedentes penales u ofensas criminales, datos genéticos, datos biométricos o datos referentes a la orientación o la actividad sexual de una persona.
- Información de salud personal (PHI), que incluye información sobre el historial médico o la condición física o mental de la persona, la prestación de atención médica a una persona y el pago por la prestación de atención médica a la persona.

Ciente implica cualquier cliente de Citi y puede incluir individuos (es decir, personas físicas), así como empresas, instituciones, organizaciones y entidades legales.

Región de la Nube es una ubicación física donde el proveedor de servicios de la nube agrupa los centros de datos.

Equipos, Sistemas y Servicios de Comunicaciones son cualquier hardware, software o aplicación utilizada en la transmisión de comunicaciones electrónicas escritas, de voz o de video. Los canales eComm incluyen pero no se limitan a: computadoras, computadoras portátiles, tabletas, dispositivos móviles o teléfonos móviles, incluidos "Bring Your Own Device" (BYOD), BlackBerry, teléfono, fax (servicios de fax), intranet y acceso a Internet, servicios Wi-Fi, servicios de correo electrónico, mensajería instantánea servicios como mensajes de Microsoft Lync, Skype y Bloomberg, sitios web y aplicaciones con funciones de comunicación integradas, reuniones de video o plataformas de colaboración como Zoom o Microsoft Teams, y servicios de redes sociales, servicios interactivos para compartir información, salas de chat de terceros, tableros de anuncios electrónicos y blogs.

Contenido implica la Información Confidencial de Citi y cualquier otro dato, informe, estadística o información de cualquier tipo (a) proporcionado o puesto a disposición directa o indirectamente al Proveedor por o en nombre de Citi o sus Afiliadas o por o en nombre de sus clientes, clientes o proveedores de servicios, (b) creados, producidos a través de los Servicios, o (c) derivados de cualquiera de los anteriores.

Contrato: documento legal escrito firmado por dos o más partes, que incluye ofertas, aceptaciones, contraprestaciones y obligaciones de las partes, y una legalidad de propósitos. Estos contratos pueden incluir, por ejemplo, Acuerdos maestros para productos y servicios, declaraciones de trabajo u órdenes de trabajo, enmiendas y anexos, esquemas, pedidos o cualquier otro tipo de documento por escrito firmado por una entidad de Citi y un Proveedor. Un Acuerdo de Confidencialidad (NDA) también se considera un Contrato a los efectos de estas Normas.

La Prueba de Denegación de Acceso (DOA) valida la dotación de personal y el soporte para los procesos comerciales de Citi que se pueden recuperar dentro del RTO definido.

La Prueba de Denegación de Servicio (DOS) es donde Citi inicia sesión en una aplicación o administrada por el Proveedor o en los sistemas del Proveedor, el Proveedor debe realizar, al menos una vez al año de acuerdo con los requisitos de Citi para cada centro de datos/sala de tecnología donde residen estas aplicaciones, una prueba de DOS para demostrar que la aplicación se puede recuperar en el sitio DR especificado en el Plan de Recuperación Ante Desastres del Proveedor.

Comunicaciones Electrónicas son mensajes o información enviados, recibidos o utilizados por el Personal utilizando medios electrónicos, transmitidos por cable o por señales inalámbricas. Las Comunicaciones Electrónicas incluyen, entre otros, mensajes de texto, correo electrónico, mensajes instantáneos o entre pares, publicaciones en blogs, publicaciones en redes sociales, mensajes enviados a través de aplicaciones de mensajería como WhatsApp, WeChat, Line, Signal o Viber, e incluyen archivos adjuntos, capturas de pantalla, archivos de voz o video grabados, voz o video en vivo y archivos creados, recibidos, descargados, almacenados, transmitidos, eliminados o utilizados a través de Equipos, Sistemas y Servicios de Comunicaciones Electrónicas.

ID Funcionales son ID genéricas, como ADMIN o ROOT, que utiliza una persona o un proceso para acceder a un sistema de seguridad. Una iniciativa clave en la operación

de Gestión de Identidad y Acceso (IAM) es garantizar que Citi tenga controles específicos y definidos para protegerse contra los riesgos que rodean el uso de Identificaciones Funcionales.

Procesos Críticos de Franquicia/Aplicaciones Críticas de Franquicia (FCA) son aquellos procesos o aplicaciones que han sido identificados por Citi como esenciales para la ejecución exitosa de sus Funciones Comerciales Críticas de Franquicia.

Fraude es un acto, declaración errónea u omisión intencional diseñado para engañar a otros, lo que resulta en que la víctima sufra una pérdida o que el perpetrador obtenga una ganancia.

Servicios Alojados incluyen cualquier Aplicación Instalada y cualquier instalación y entorno administrado o utilizado por el Proveedor para proporcionar los Servicios Alojados, todas las aplicaciones y otro software, bases de datos, sitios web, servidores, hardware, redes, telecomunicaciones y otros equipos, y otra tecnología instalada o utilizada dentro del entorno de Servicios Alojados y, en cada caso, todas las Actualizaciones y Servicios de soporte, pero excluyendo todo el Contenido y los Sistemas de Citi.

Seguridad de la Información o “SI” significa el estado en el que una computadora o sistema informático está protegido contra accesos no autorizados o ataques, y debido a ese estado, (a) la computadora o sistema informático continúa estando disponible y operativo; (b) se mantiene la integridad de la computadora o del sistema informático; y (c) se mantenga la integridad y confidencialidad de la información almacenada, procesada o transmitida a través de la computadora o sistema informático.

Amenaza a la Seguridad de la Información: significa un acto o actividad (conocida o sospechada) llevada a cabo en o a través de una computadora o sistema informático que puede poner en riesgo o afectar negativamente la seguridad de la información o la seguridad de otra computadora u otro sistema informático.

Vulnerabilidad de la Seguridad de la Información: se refiere a cualquier vulnerabilidad en una computadora o sistema informático que puede ser aprovechada por una o más amenazas a la seguridad de la información.

La **generación sin clientes/sin ingresos** se define como actividades críticas del negocio no asociadas con actividades generadoras de ingresos, incluidas las actividades legales, de supervisión, regulatorias y de continuidad del negocio.

Acuerdo de Confidencialidad (NDA): acuerdo entre Citi y un Proveedor, cuyos términos rigen el intercambio, uso y divulgación de Información.

Inventario de Registros es una lista detallada que incluye los tipos de registro, la ubicación, las fechas, etc., de los registros de Citi y es necesario para que una empresa administre adecuadamente sus registros a lo largo del Ciclo de Vida de la Información.

Retención de Registros es un requisito impuesto sobre registros e información que suspende la modificación o eliminación de estos hasta que la autoridad que dictó dicha orden la levante.

Capacidad de Recuperación: es el volumen, la cantidad o la velocidad de entrega de los productos y servicios del Proveedor, expresada como un porcentaje de la entrega normal de productos y servicios.

Duración de la Recuperación es la duración máxima, en días calendario, que el Proveedor es capaz de sostener operaciones mientras está en modo de recuperación.

El Punto de Recuperación Objetivo: es el momento en el pasado, expresado en horas, en el que los datos deben recuperarse después de una interrupción comercial. Es el período objetivo máximo en que podrían perderse los datos de un servicio de TI debido a un incidente mayor. RPO solo es una medida del período máximo en que podrían perderse los datos si hubiera un incidente mayor que afectara el servicio de TI, No es una medida directa de la cantidad de datos que podrían haberse perdido (por ejemplo, al final del procesamiento del turno anterior).

Tiempo de Recuperación Objetivo: es la duración en horas entre el momento de una interrupción del servicio y la restauración de productos y servicios.

Organización de Gestión de Recursos (RMO) es responsable de la gestión global de recursos de extremo a extremo para Citi, incluido el abastecimiento estratégico, las operaciones de compra para pagar, la oficina de personal y el marco de gestión de proveedores.

Gerente de Abastecimiento de RMO es una persona dentro de la Organización de Gestión de Recursos (RMO) que es responsable de la negociación de los términos comerciales, los requisitos y los precios del Contrato, incluidas las RFP y otras actividades de selección de Proveedores, la administración de los términos y condiciones del Contrato y los requisitos de acreditación de la evaluación financiera.

Efecto adverso Grave o Catastrófico para una persona significa que el impacto podría resultar razonablemente en efectos adversos significativos para la persona, incluida la pérdida financiera, la pérdida del empleo o la pérdida o dificultad para obtener un empleo, la pérdida de derechos humanos, la humillación personal o pública o aprisionamiento indebido.

Capacidad de Tiempo de Recuperación de Tecnología (TRTC) es el tiempo de restauración total estimado para que una aplicación/servicio empresarial y sus componentes de infraestructura subyacentes se recuperen en su recuperación ante desastres o sitio alternativo después de una invocación.