

REQUISITOS DE CITI PARA PROVEEDORES

RESPONSABLES:

Jefe de Abastecimiento y Riesgo de Citi

FECHA DE EMISIÓN

Enero de 2015

REVISADO:

Septiembre de 2026

VERSIÓN:

9

ÍNDICE

1	DESCRIPCIÓN GENERAL	3
2	IGUALDAD DE OPORTUNIDADES EN EL EMPLEO	5
3	ANTISOBORNO Y ANTICORRUPCIÓN (AB&C)	6
4	REGALOS Y ENTRETENIMIENTO	6
5	COLABORACIÓN CON LOS PROVEEDORES Y PRINCIPIOS DE PROVEEDORES	7
6	PROHIBICIÓN CONTRA LA ESCLAVITUD MODERNA	7
7	PERSONAL DEL PROVEEDOR	9
8	GESTIÓN DE FRAUDE	11
9	INTERACCIÓN CON LOS MEDIOS Y APARICIONES PÚBLICAS	13
10	COMUNICACIONES ELECTRÓNICAS POR ESCRITO	13
11	ACTIVIDADES Y CONTRIBUCIONES POLÍTICAS	14
12	ANTILAVADO DE DINERO (“AML”).....	15
13	GESTIÓN DE REGISTROS.....	16
14	RESILIENCIA EMPRESARIAL/CONTINUIDAD DEL NEGOCIO	18
15	NORMAS DE INVESTIGACIÓN DE ANTECEDENTES GLOBALES	25
16	GASTOS	27
17	SEGURIDAD DE LA INFORMACIÓN (IS)	28
18	PAUTAS PARA UN LUGAR DE TRABAJO SEGURO	67
19	INTELIGENCIA ARTIFICIAL/APRENDIZAJE AUTOMÁTICO (INCLUIDA LA IA GENERATIVA/IA AGÉNTICA)	68
20	QUEJAS DE LOS CLIENTES	69
21	POLÍTICA DE COMERCIO E INVERSIÓN PERSONAL	70
22	ESTÁNDARES DE FACTURACIÓN Y COBRO	70
23	POLÍTICA DE AUSENCIA OBLIGATORIA	71
	APÉNDICE - DEFINICIONES	72

1 DESCRIPCIÓN GENERAL

1.1. Requisitos generales

Estos Requisitos de Citi para Proveedores (los “**Requisitos**”) detallan algunas de las obligaciones que los Proveedores deben cumplir al hacer 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 ese Proveedor proporcione a Citi (estos últimos se resumen en la Sección 1.2 a continuación y se indican al comienzo de cada disposición incluida 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 obligación en virtud de las Leyes Aplicables (según se define ese término a continuación), cualquier aviso al Proveedor de parte 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 las unidades de negocios o funciones de Citi. Las obligaciones y los requisitos más restrictivos se aplicarán cuando haya un conflicto entre cualquiera de los requisitos anteriores y estos Requisitos. 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 respecto a 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 Proveedor deberá cumplir de inmediato con cualquier solicitud razonable que Citi pueda enviar al Proveedor por los datos que Citi requiera relacionados con los Servicios o el Personal del Proveedor en relación con la obligación de Citi de cumplir con las Leyes Aplicables. El incumplimiento por parte del Proveedor de estas obligaciones se considerará una violación material de los términos de este Acuerdo.

El incumplimiento de estos Requisitos, o de cualquier requisito adicional especificado por una unidad de negocios de Citi con la cual el Proveedor haga negocios, puede resultar en la rescisión del Contrato de un Proveedor con Citi. Además, las violaciones de los Requisitos también pueden ser violaciones de las Leyes Aplicables y pueden dar lugar a daños y perjuicios civiles adeudados a Citi (o terceros) o sanciones penales para el Proveedor. El Proveedor no puede 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
2	IGUALDAD DE OPORTUNIDADES EN EL EMPLEO/ACCIÓN AFIRMATIVA	Aplicable a contratos y órdenes de compra necesarios para la ejecución de un contrato de Citi con el gobierno federal de EE. UU.; si hay incertidumbre respecto a si el contrato o la orden de compra constituye una subcontratación o orden de compra del gobierno federal, incluya “Según corresponda” al comienzo o al final de la cláusula.
12	ANTILAVADO DE DINERO	Aplicable a los Proveedores que prestan ciertos servicios relacionados con clientes (es decir, incorporación, revisión de cuentas y transacciones de clientes) o con la entrega de datos/métricas relacionados con las actividades anteriores; <u>Y/O</u> Proveedores que actúan como intermediarios respecto a efectivo o instrumentos financieros (p. ej., captación remota de depósitos, entregas, o servicios de camiones blindados o cajas de depósito).
13	GESTIÓN DE REGISTROS	Aplicable a Proveedores que acceden a, procesan o almacenan Información de Citi.
14	CONTINUIDAD DEL NEGOCIO	Aplicable a Proveedores que prestan servicios o alojan infraestructura/aplicaciones de tecnología utilizadas 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.
15	NORMAS DE INVESTIGACIÓN DE ANTECEDENTES GLOBALES	Aplicable a Proveedores que prestan servicios a Citi.
16	GASTOS	Aplicable a Proveedores que son elegibles contractualmente para reclamar gastos comerciales reembolsables.
17	SEGURIDAD DE LA INFORMACIÓN (IS)	Aplicable a Proveedores, incluidos Subcontratistas que acceden/procesan/gestionan/almacenan información de Citi; <u>Y/O</u> Proveedores responsables como Host de las aplicaciones de Internet de la marca Citi de cara al público; <u>Y/O</u> Proveedores con conectividad a los recursos de red de Citi; <u>Y/O</u> Proveedores que requieran acceso sin escolta a las instalaciones de Citi.
18	PAUTAS PARA UN LUGAR DE TRABAJO SEGURO	
19	INTELIGENCIA ARTIFICIAL/APRENDIZAJE AUTOMÁTICO (INCLUIDA LA IA GENERATIVA/IA AGÉNTICA)	Aplicable a Proveedores que utilizan Inteligencia Artificial/Aprendizaje Automático (IA/ML), según lo definido por Citi en cualquier parte del producto o servicio que prestan.
20	POLÍTICA DE COMERCIO E INVERSIÓN PERSONAL	Aplicable a Proveedores que requieren acceso regular a MNPI como parte de sus responsabilidades laborales en Citi.
23	POLÍTICA DE AUSENCIA OBLIGATORIA	Esta Política es aplicable a No Empleados (“Trabajadores”) que ocupan Puestos Sensibles (como se define en el Glosario) (“Trabajadores Sensibles”), así como gerentes y supervisores directos de

Número de la Sección	Título de la Sección	Aplicabilidad
		Empleados Sensibles (“Gerentes”) y Contactos Comerciales de Citi de No Empleados Sensibles.

2 IGUALDAD DE OPORTUNIDADES EN EL EMPLEO

2.1 Igualdad de oportunidades en el empleo.

Citi ha desarrollado políticas diseñadas para garantizar la igualdad de oportunidades en el empleo para todas las personas calificadas sin distinción de raza, color, religión, sexo, orientación sexual, identidad de género, origen nacional, estatus de ciudadanía, estatus migratorio, edad, estado civil, información genética, discapacidad, condición de veterano protegido o cualquier otra característica protegida por la ley.

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

Los Proveedores revisarán y tomarán las medidas apropiadas de acuerdo con la Declaración de la Política de Igualdad de Oportunidades en el Empleo de EE. UU. (U.S. Equal Employment Opportunity Policy Statement, EEO) de Citi, que puede encontrarse en www.citigroup.com/global/eeo-aa-policy.

2.2 Contratos gubernamentales

Los contratos y órdenes de compra que sean necesarios para la ejecución de un contrato de Citi con el gobierno federal deben contener la siguiente cláusula textualmente y en negrillas como se muestra a continuación. (Si no se sabe si se trata de una orden de compra/subcontratación del gobierno federal, erre en incluir y agregue “Según corresponda” al comienzo de la sección).

[Según corresponda,] el Proveedor cumplirá con todas las leyes federales contra la discriminación aplicables y certifica que no opera ningún programa que contravenga las leyes federales contra la discriminación aplicables.

2.3 Apéndice de contratos gubernamentales

Los contratos y órdenes de compra que sean necesarios para la ejecución de un contrato de Citi con el gobierno federal deben contener el siguiente aviso en el apéndice de la subcontratación u orden de compra. (Si no se sabe si se trata de una orden de compra/subcontratación del gobierno federal, erre en incluir y agregue “Según corresponda” al final del aviso a continuación).

Como contratista del gobierno federal, por medio de la presente Citigroup proporciona al contratista o proveedor abajo firmante un aviso por escrito de nuestras obligaciones de igualdad de oportunidades en el empleo en favor de los veteranos y personas con incapacidad protegidos. Citigroup cumple plenamente con la sección 503 de la Ley de Rehabilitación y la Ley de Asistencia para el Reajuste de los Veteranos de la Era de Vietnam, así como sus regulaciones aplicables en virtud de 41 C.F.R. § 60-741 y 41 C.F.R. § 60-300, respectivamente. Nuestra Equal Employment Opportunity Policy

Statement puede encontrarse en www.citigroup.com/global/eeo-aa-policy. Cualquier pregunta sobre nuestra EEO Policy Statement puede dirigirse al contacto proporcionado en nuestra Declaración de la Política.

[Según corresponda,] le pedimos que tome las medidas adecuadas de conformidad con nuestra Declaración de la Política y las regulaciones.

3 ANTISOBORNO Y ANTICORRUPCIÓN (AB&C)

Citi cuenta con políticas, procedimientos y controles internos diseñados razonablemente para cumplir con las leyes antisoborno y anticorrupción (AB&C) aplicables y prohíbe estrictamente el soborno o los pagos de facilitación en cualquier forma. Los Proveedores (incluidos los Promotores Comerciales), su Personal o cualquier persona que actúe en nombre de Citi, directa o indirectamente, realizarán sus actividades de acuerdo con los más altos estándares éticos y en cumplimiento de la Ley de Prácticas Corruptas en el Extranjero (FCPA) de EE. UU., la Ley Antisoborno del Reino Unido (UKBA), cada una según sus enmiendas, y todas las demás leyes AB&C locales aplicables de los países en los que opera Citi.

Ni el Proveedor ni ningún miembro de su Personal que opere en nombre de Citi o en relación con algún acuerdo o relación del Proveedor con Citi, (i) hará, conferirá, autorizará u ofrecerá ningún pago, beneficio, ventaja u otra cosa de valor a persona alguna; ni (ii) recibirá o aceptará ningún pago, beneficio, ventaja o cualquier otra cosa de valor de persona alguna, en cada uno de los casos (i)-(ii) en violación de la FCPA, la UKBA o cualquier otra ley AB&C. El Proveedor y su Personal deben realizar sus actividades y transacciones en nombre de Citi, o en relación con cualquier acuerdo o relación del proveedor con Citi, en cumplimiento de los Requisitos, incluida esta Sección. El Proveedor y su Personal también deben mantener un programa de cumplimiento de AB&C, así como políticas y procedimientos diseñados y aplicados para asegurar su cumplimiento de todas las leyes AB&C.

Para obtener una descripción general del Programa Antisoborno y Anticorrupción (AB&C) de Citi, visite [Citigroup's Investor Relations](#) (en Políticas de Citi, seleccione Programa AB&C).

4 REGALOS Y ENTRETENIMIENTO

Ni los Proveedores ni su personal pueden proporcionar regalos ni otorgar nada de valor (incluido entretenimiento) a empleados de Citi, cuando hacerlo pudiera crear un conflicto de intereses real o aparente, comprometer la integridad o el juicio del empleado o influir de manera inadecuada en la toma de decisiones del empleado, causar que el empleado actúe en contra de sus funciones o de otro modo violar las leyes aplicables. Sin limitar lo anterior, el empleado debe cumplir con la Sección de Regalos y Entretenimiento Prohibidos del Estándar de Regalos y Entretenimiento (G&E). Ni los Proveedores ni su

Personal pueden proporcionar a ningún empleado de Citi regalos comerciales no monetarios que superen, en total, los USD \$300 por persona y por año calendario.

Cuando un Proveedor ofrece entretenimiento comercial (p. ej., invitaciones a comer, o bien, a 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. Además, si el Proveedor no asiste al evento, el entretenimiento se considerará un regalo comercial y estará sujeto a los umbrales de reporte aplicables del Estándar de Regalos y Entretenimiento de Citi. El Proveedor no puede, en nombre de Citi o supuestamente en nombre de Citi, proporcionar nada de valor, incluso a costa del propio Proveedor o a costa de un empleado de Citi, a ninguna persona, directa o indirectamente, ni inducir a otra persona a hacer lo mismo, si hacerlo sería, o podría considerarse razonablemente como, corrupto, inapropiado o una violación de la ley aplicable.

5 COLABORACIÓN CON LOS PROVEEDORES Y PRINCIPIOS DE PROVEEDORES

<https://www.citigroup.com/citi/suppliers/> Citi colabora con Proveedores en un número de iniciativas y para crear conciencia sobre el programa de abastecimiento de Citi entre los posibles Proveedores de las comunidades a las que servimos. Además, estas colaboraciones buscan identificar Proveedores con potencial, especialmente aquellos que impulsan soluciones innovadoras para abordar problemas comerciales emergentes. Hay información adicional disponible sobre las expectativas de Citi para los Proveedores en el sitio web [Doing Business with Citi](#) en:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 PROHIBICIÓN CONTRA LA ESCLAVITUD MODERNA

Citi se compromete a mantener prácticas destinadas a identificar y tratar de prevenir 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 suministros. Todos los Proveedores de Citi deberán cumplir con los Requisitos establecidos a continuación y desarrollar políticas y procedimientos y/o prácticas efectivas en toda la empresa para identificar y tratar de prevenir el riesgo de esclavitud moderna y trata de personas dentro de sus propias operaciones y sus cadenas de suministros. Los Proveedores deben completar el Cuestionario de Responsabilidad Corporativa de Citi a pedido de Citi, incluida cualquier información adicional según sea necesario, para permitir que Citi evalúe la exposición al riesgo y los posibles pasos de mitigación, particularmente para Proveedores en sectores y ubicaciones geográficas de mayor riesgo. Se espera que los Subcontratistas del Proveedor sigan el mismo proceso.

6.1 Prevención del Trabajo Infantil

Los Proveedores no emplearán mano de obra infantil. El término “infantil” se refiere a cualquier persona menor de la edad mínima para trabajar según las leyes aplicables, o

en ausencia de dichas leyes, cualquier persona menor de 15 años o menor de la edad en la que se completa la educación obligatoria, según cuál sea mayor. Sujeto a la prohibición de anulación respecto de la contratación de mano de obra infantil, si se emplea a trabajadores menores de 18 años, se debe considerar particularmente qué funciones 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 estén 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 forma alguna, incluidas las horas extra forzadas. Todo trabajo debe llevarse a cabo de forma voluntaria. Las obligaciones del proveedor en virtud del presente incluyen, entre otras, garantizar lo siguiente:

1. **Contratos, Salarios y Horario 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 otros, términos transparentes con respecto al salario, el pago de horas extras, los periodos 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 acuerdos colectivos donde se lleva a cabo el trabajo.
2. **Derecho a Cesar Libremente el Trabajo:** Los trabajadores deben tener el derecho de rescindir la relación laboral con libertad, según corresponda tras un periodo razonable de aviso, de acuerdo con las leyes y los acuerdos colectivos aplicables, sin que se les impongan sanciones inadecuadas.
3. **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.
4. **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 recibir su salario íntegro, a tiempo y con recibos de pago transparentes. No se aplicarán deducciones punitivas ni retenciones de los salarios o beneficios como medida disciplinaria. Las semanas laborales no deben exceder el máximo establecido por las leyes locales, y las horas extras deben

ser voluntarias, dentro de los límites legales, y la negativa a trabajar horas extras no debe ser sancionada.

5. **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.
6. **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 cargos o costos a los trabajadores en relación con el proceso de contratación o se incurre en ellos durante el transcurso del empleo, el Proveedor debe tomar medidas razonables para que se reembolsen dichos costos. Cuando sea necesario contratar trabajadores a través de un tercero, como una agencia de empleo, solo se contratarán agencias de empleo acreditadas y de buena reputación. Cuando los trabajadores sean contratados para ser empleados directamente, solo se trabajará con agencias de contratación acreditadas y de buena reputación. La prohibición de los honorarios de contratación pagados por el trabajador se aplica a todos los reclutadores, agentes y subagentes. Los Proveedores aplicarán controles para garantizar el cumplimiento. **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.
7. **Reclamos sin Represalias:** Los trabajadores tendrán la libertad de presentar reclamos a sus empleadores sobre el trato que les da el empleador y los trabajadores no sufrirán perjuicios, represalias o victimización por haber presentado un reclamo.

7 PERSONAL DEL PROVEEDOR

7.1 Capacitación, 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 incapacidad, impuestos de seguridad social o beneficios, impuestos federales de desempleo, beneficios estatales de seguro de desempleo o retención del impuesto federal 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 Reemplazo del 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 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 las Leyes Aplicables y cualquier acuerdo de negociación colectiva aplicable. Sin limitar la generalidad de lo anterior, el Proveedor declara, garantiza y acuerda además 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 toda 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 de las Leyes Aplicables relacionadas con la inmigración y reemplazará a cualquier Personal que no tenga autorización de trabajo de acuerdo con las Leyes Aplicables con 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 para Citi.

7.4 Propietarios del Proveedor

Para cumplir con las leyes y regulaciones aplicables en las jurisdicciones en las que Citi opera, a solicitud de Citi, los Proveedores están obligados a proporcionar los detalles de los propietarios, que son una persona natural y/o una entidad, incluidos los propietarios inmediatos del Proveedor hasta inclusive el titular beneficiario final que tiene propiedad o control directo o indirecto a través de su influencia u otros medios sobre el contrato, el producto o el servicio.

8 GESTIÓN DE FRAUDE

En relación con los esfuerzos de Citi para identificar y mitigar el riesgo de fraude (“Gestión de Fraude”).

8.1 Todos los Proveedores deberán:

1. Cooperar con cualquier investigación de Citi de presunto o posible robo, fraude u otra posible actividad delictiva o irregularidad, y cualquier enjuiciamiento de conducta fraudulenta o delictiva según las medidas permitidas por la ley.
2. Garantizar la notificación y la derivación oportunas de cualquier posible evento de fraude a Citi a través de la [Ethics Hotline](#). Esto incluye, entre otros, intento, sospecha, presunto caso o caso real de robo, 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, a un agente de Citi o a una persona que no sea un empleado de Citi (p. ej., empleados temporales y contratistas).
3. Permitir el monitoreo y la supervisión por parte de Citi y sus representantes y apoyar a Citi, y a las fuerzas del orden público, en sus investigaciones respecto a posibles actividades fraudulentas que involucren a ese Proveedor.
4. 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
5. 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 prestan servicios que están inherentemente más expuestos al riesgo de fraude **deben**:

1. 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.
2. 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 prestados a Citi.

3. 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 Business Activity Owner (BAO).
4. Proporcionar cualquier información requerida para la diligencia debida, el monitoreo continuo y la evaluación de la exposición al riesgo de fraude al Business Activity Owner (BAO).
5. La Diligencia Debida incluye la Plantilla de Evaluación del Impacto de Fraude de Terceros ("TP-FIAT"), que está diseñada para realizar evaluaciones de control de las capacidades de los Proveedores relacionadas con la mitigación del riesgo de fraude. Este procedimiento operativo describe una serie de pasos que deben seguir el Propietario de la Actividad Comercial (BAO) o el Responsable de Terceros (TPO) y el Responsable de Gestión de Riesgos de Fraude ("FRMO") para identificar y gestionar el riesgo de fraude.

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

1. tienen acceso a datos clasificados como Confidenciales o de nivel superior (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.
2. tienen conectividad a las redes o sistemas de Citi; y
3. 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 aplicación de cambios a datos de Citi o de 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 en las instalaciones de Citi;
 - h) Estados de cuenta financieros: Actividades contables, como contabilización de entradas en el GL/SL;
 - i) Obtención y gasto de recompensas por actividades incentivadas.

9 INTERACCIÓN CON LOS MEDIOS Y APARICIONES PÚBLICAS

Servicios Empresariales y Asuntos Públicos de Citi es el único departamento autorizado para emitir comunicados de prensa o declaraciones públicas en nombre de Citi. Los Proveedores no pueden emitir ningún comunicado de prensa que identifique directa o indirectamente a Citi, a cualquier Contrato o acuerdo alguno entre un Proveedor y Citi ni ningún producto o servicio que Citi haya adquirido 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 websites, 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 que se relacione o no con el suministro de productos o la prestación de servicios a Citi, los Proveedores no podrán usar indicios, marcas comerciales, marcas de servicio, nombres comerciales, logotipos, símbolos o nombres de marca propiedad de Citi, sin obtener, en cada caso, el consentimiento previo y por escrito de Citi. Los Proveedores no podrán usar el nombre, el logotipo ni las marcas comerciales, instalaciones o relaciones de Citi para el beneficio propio o para un trabajo ajeno a Citi (incluso en membretes o websites 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 servicios gratuitos.

10 COMUNICACIONES ELECTRÓNICAS POR ESCRITO

Al interactuar con el personal de Citi, o en cumplimiento de sus obligaciones para o en nombre de Citi, se permite a los Proveedores usar solo los Equipos, Sistemas y Servicios de Comunicaciones Electrónicas Escritas que estén aprobados por Citi. Los Canales de eComm de Citi nuevos, ampliados o modificados, ya sean como herramientas independientes o integrados en una plataforma más amplia, proporcionados por Citi o por terceros, deben ser aprobados de acuerdo con los Requisitos de Citi aplicables respecto a los cuales el Proveedor ha sido notificado por 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, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber 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 acuerdo con los requisitos aplicables para la retención de registros (sujeto a las leyes y regulaciones locales).

<https://policydirectory.citi.net/cpd/ layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 ACTIVIDADES Y CONTRIBUCIONES POLÍTICAS

Una variedad de leyes, como las relacionadas con: influencia extranjera; financiamiento de campañas; regalos y entretenimiento; cabildeo legislativo, de base, de buena voluntad y regulatorio; contratación pública, pay-to-play; y valores, regulan las actividades políticas y las divulgaciones relacionadas con este tipo de actividades, de Citi y sus Proveedores. Se prohíbe cualquier actividad política por parte de los Proveedores que no cumpla con las políticas o normas, leyes o regulaciones relevantes de Citi.

La actividad política incluye pero no se limita a:

1. 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 horario de la empresa en nombre de un candidato que hace campaña para un cargo público, un comité de un partido político o un comité político.
2. Cabildeo o participación en cualquier acercamiento a funcionarios públicos, ya sea directamente o a través de terceros, incluidos los intentos de influir sobre los funcionarios, la legislación y, según la jurisdicción, esto puede incluir intentos de influir sobre la elaboración de normas de la agencia o la adjudicación de contratos gubernamentales; o
3. Buscar, aceptar u ocupar cualquier cargo político asociado con un gobierno, incluida cualquier junta, comisión u otra organización de gobierno similar.

Ningún Proveedor puede emprender o realizar ninguna actividad política en nombre de (o supuestamente en nombre de) Citi, o sus clientes, sin la autorización previa por escrito del Control de Operaciones Globales de Asuntos Gubernamentales de Citi (ggacontrol@citi.com). Aunque Citi puede pagar un cargo y/o reembolsar los costos de bolsillo por los servicios de actividad política contratados y permitidos proporcionados por el Proveedor, como cabildar, Citi nunca reembolsará a un Proveedor ni a ninguno de sus empleados por contribuciones políticas personales o corporativas de ningún tipo.

12 ANTILAVADO 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 actúan como intermediarios 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 de AML:

1. Cumplimiento de los Procesos de Citi y las Leyes Aplicables:

- 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 regulaciones 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 los roles 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 actividades financiera, transacciones y la entrada de efectivo.

2. Elementos de la Capacitación Anual y el Programa para el Personal:

- Asegurarse de que las personas de su Personal que presten Servicios a Citi reciban capacitación anual con respecto a los roles 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 actividades financieras, transacciones y la entrada de efectivo. La capacitación debe incluir, entre otros, los siguientes componentes:
 - a. Generación de informes y escalamiento de actividades sospechosas.
 - b. Un programa de “Conozca a Su Cliente” (KYC), incluido un Programa de Identificación de Clientes (CIP), verificación de sanciones y nombres, diligencia debida para clientes (CDD), diligencia debida mejorada (EDD) y la identificación y verificación de **Titulares Beneficiarios Finales (UBO)**.
 - c. Monitoreo de transacciones en todos los instrumentos y actividades financieras relevantes.

- 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.

3. Cumplimiento de las Disposiciones Contractuales:

- Cumplir con cualquier disposición del Contrato que defina cualquier programa que deba ser instaurado por el Proveedor.

4. Notificación Inmediata de Presuntos Incumplimientos:

- Informar inmediatamente a Citi por escrito de cualquier sospecha de violación de la ley, incluida cualquier actividad observada que parezca inusual o potencialmente inusual relacionada con la entrada de efectivo, actividades financieras o transacciones que implique a Citi o sus clientes.

5. Prevención y Generación de Informes de Evasión Fiscal:

- 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.
- En este sentido, 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 Políticas y Procedimientos Internos del Proveedor:

Los Proveedores deberán mantener políticas y procedimientos internos apropiados para cumplir con todas las leyes y regulaciones de 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 que ejercen custodia sobre la Información de Citi trabajen con su Business Activity Owner (“**BAO**”) o el contacto comercial principal de Citi para (i) identificar y clasificar la Información como Registros o Información 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 Información, disponer adecuadamente de la Información al final del Ciclo de Vida de la Información.

El BAO o el contacto comercial principal de Citi deben trabajar con el Proveedor para garantizar que el Proveedor haya identificado y clasificado los registros de acuerdo con los códigos de registro de Citi en el MRC y que el Inventario 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 que cumplan con los criterios de elegibilidad para su eliminación deben eliminarse apropiadamente lo antes posible, pero no más de seis meses después de que se hayan cumplido los requisitos de retención, a menos que estén sujetos a Retención de Información. La Información Transitoria debe destruirse no más de dos años después de su último uso a menos que esté sujeta a Retención de Información. La Información Transitoria que incluye información personal debe eliminarse una vez que se cumpla el propósito para el cual se recopiló, a menos que esté sujeta a Retención de Información. El Proveedor debe suspender la destrucción o alteración de la Información de Citi cuando se le notifique una Retención de Información. El Proveedor deberá consultar a su principal contacto comercial en Citi o al BAO en caso de cualquier incertidumbre.

Cada trimestre, DRIM revisa y actualiza las reglas de retención listadas en los Cronogramas de Retención del País, según sea necesario, para cumplir con los cambios regulatorios e internos. Cuando se produzca un cambio que afecte al Proveedor, el BAO se lo comunicará. El Proveedor debe evaluar el impacto e implementar los cambios en los respectivos sistemas, procesos e inventarios. Esto respecto a los tipos de Registros que posee y gestiona en un plazo de 90 días a partir de la notificación del BAO.

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. El Proveedor devolverá, a solicitud, la Información de Citi según lo requerido en virtud de los términos contractuales aplicables. Los Proveedores no deben deshacerse de ninguna Información de Citi, independientemente de su clasificación (p. ej., Confidencial, No Confidencial) sin la aprobación de su contacto comercial principal de Citi o del BAO, que debe incluir la confirmación de que no se aplican Retenciones de Información 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 Responsable de Gestión de Registros para revisar y actualizar los nombres de los contactos, los detalles de los procedimientos, los roles y responsabilidades y el Inventario de Registros del Proveedor de Citi.

14 RESILIENCIA EMPRESARIAL/CONTINUIDAD DEL NEGOCIO

Aplicable a Proveedores que prestan servicios o alojan infraestructura/aplicaciones de tecnología utilizadas por Citi. El Business Activity Owner (BAO) de Citi es responsable de comunicar la aplicabilidad y requisitos de COB al Proveedor.

14.1 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 deshabilitadas. Los recursos de recuperación deben colocarse en ubicaciones geográficamente separadas de las ubicaciones principales, con separación suficiente para minimizar o eliminar la amenaza de que el mismo evento de desastre pueda afectar tanto a las ubicaciones primarias como a las de recuperación.

1. 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.
2. Los Proveedores de aplicaciones pueden implementar una arquitectura tipo “Hot/Hot” para garantizar una configuración de Alta Disponibilidad (HA). Esta arquitectura requiere que haya dos (como mínimo) sistemas configurados de forma idéntica que estén en funcionamiento y disponibles para los clientes/usuarios. La característica más importante que ofrece este modelo es que el/los entorno(s) alternativo(s) funcionan simultáneamente con el centro de datos primario (de producción).

14.2 Niveles de Servicio de Recuperación

La continuidad del negocio de los Proveedores debe cumplir con los niveles de servicio establecidos para ser efectiva para Citi. Como mínimo, el Plan de Recuperación ante Desastres del Proveedor deberá establecer valores específicos para:

1. Objetivo de Tiempo de Recuperación
2. Objetivo de Punto de Recuperación
3. Recursos de Recuperación/Capacidad de Tecnología
4. Duración de la Recuperación

14.3 Plan de Recuperación ante Desastres

El Proveedor mantendrá un Plan de Recuperación ante Desastres para la continuidad 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 Productos/Servicios o cumplir con sus otras obligaciones en virtud del presente desde cualquier lugar en particular o mediante los esfuerzos de cualquier persona en particular, el Proveedor pueda proporcionar los Productos/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 Vigor de cada Orden de Trabajo celebrada entre Citi y el Proveedor, y anualmente a partir de entonces mientras cada Orden de Trabajo esté vigente. El Proveedor proporcionará a Citi cualquier instrucción u otra información necesaria para que Citi continúe recibiendo los Productos/Servicios del Proveedor en circunstancias en las que el Proveedor invoque su Plan de Recuperación ante Desastres. El proveedor declara, garantiza y acuerda que su Plan de Recuperación ante Desastres incluirá, como mínimo:

1. Procedimientos y estrategias de recuperación, incluyendo reubicación, transferencia de trabajo y/o acceso remoto para mitigar los efectos de interrupciones incluyendo falta de disponibilidad de tecnología (Denegación de Servicio/DoS), falta de disponibilidad de la ubicación de trabajo principal (Denegación de Acceso/DoA) y falta de disponibilidad del personal (incluidos los subcontratistas);
2. Mantenimiento por parte del Proveedor (incluyendo, entre otros) de un sitio de recuperación ante desastres secundario separado de las ubicaciones del Servicio, el almacenamiento de medios de respaldo en una ubicación separada de las ubicaciones del Producto/Servicio, el uso de líneas de comunicación y servidores redundantes;
3. Procedimientos para el respaldo/la restauración del funcionamiento y la aplicación de los Productos/Servicios, incluido un plan detallado y documentado para responder a una interrupción prolongada de los Productos/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 periodo de tiempo acordado mutuamente;
4. Procedimientos para la protección de todo el Contenido;
5. Procedimientos y cualquier acuerdo con terceros para equipos de reemplazo (p. ej., equipos informáticos);
6. Procedimientos para cualquier instalación de producción fuera del sitio; y
7. El Plan de Recuperación ante Desastres del Proveedor estipulará que:
 - a. El Proveedor notificará de inmediato a Citi cualquier desastre que pueda afectar negativamente a los Productos/Servicios;
 - b. El Proveedor proporcionará a Citi, dentro de las 24 horas posteriores a dicha notificación, un plan para continuar prestando los Productos/Servicios en una instalación de procesamiento alternativa;

- c. Los Productos/Servicios deben estar completamente operativos dentro del Objetivo de Tiempo de Recuperación (RTO) requerido que, si no se define de otro modo en el Contrato aplicable, es de 4 horas o menos para los procesos clasificados por Citi con una clasificación de criticidad “Crítica para la Empresa” o “ALTA”, 24 horas o menos para los procesos clasificados por Citi con una clasificación de criticidad “MEDIA” y 72 horas o menos para los procesos clasificados por Citi con una clasificación de criticidad “BAJA”; y
- d. 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.

14.4 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:

- 1. Procedimientos para el 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 periodo de tiempo acordado mutuamente;
- 2. 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;
- 3. El Proveedor acuerda, 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; y
- 4. 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.

14.5 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.

14.6 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. El Proveedor debe proporcionar una supervisión apropiada de los Subcontratistas, incluida la revisión periódica de sus controles y los resultados de las pruebas, y garantizar la resolución oportuna de cualquier deficiencia identificada.

14.7 Invocación del Plan de Recuperación ante Desastres y Notificación de Crisis

El Proveedor notificará de inmediato al contacto comercial principal de Citi:

1. Cuando el Proveedor invoque su Plan de Recuperación ante Desastres;
y
2. 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 sobre los Servicios o Productos proporcionados a Citi.

14.8 Pruebas

Todos los recursos y planes de recuperación del Proveedor deben probarse en un plazo de 120 días después de la implementación de la producción (90 días en caso de aplicaciones clasificadas por Citi como Críticas para la Empresa) y probarse anualmente (cada 12 meses) como mínimo. Las pruebas deberán demostrar la capacidad del Proveedor para satisfacer los niveles de servicio de recuperación para todos los productos y servicios suministrados a Citi. Estas pruebas deben ser integrales e incluir el alcance completo de los Servicios proporcionados a Citi. Los Proveedores deben notificar a Citi con al menos 30 días calendario de anticipación sobre las pruebas de recuperación de los productos/servicios proporcionados a Citi. Citi puede participar u observar las pruebas de recuperación del Proveedor de las aplicaciones utilizadas por Citi para validar la funcionalidad comercial de la aplicación en el entorno de recuperación. 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. En un plazo de (10) días hábiles después de completar cada prueba, el Proveedor proporcionará a Citi un resumen de los objetivos de la prueba, el plan de la prueba y los resultados de la prueba, incluidos los plazos necesarios para la recuperación y la evidencia de los resultados de la prueba (p. ej., capturas de pantalla).

14.9 Validación del Volumen

Un Proveedor que aloja aplicaciones clasificadas por Citi como Críticas para la Empresa debe demostrar que los volúmenes de Producción se pueden procesar en su entorno de COB/recuperación ante desastres. Citi y el Proveedor deben acordar la metodología a usar para la validación.

14.10 Uso de los Sistemas de Citi para Prestar Servicios

Si Citi o las Empresas Afiliadas 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.

14.11 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 realizará un análisis de causa raíz y corregirá rápidamente todas las deficiencias identificadas. Luego de la implementación de las correcciones, el Proveedor deberá repetir la prueba a más tardar ciento veinte (120) días calendario (90 días calendario en el caso de aplicaciones clasificadas por Citi como Críticas para la Empresa) luego del fallo de la prueba inicial (o el periodo especificado en la Orden de Trabajo correspondiente).

14.12 Gestión de Crisis

Junto con su plan de continuidad del negocio, el Proveedor debe mantener un plan de gestión de crisis para dirigir y controlar las operaciones de recuperación. Como mínimo, el plan de gestión 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 escalamiento para reunir y difundir la información sobre la crisis e incluir protocolos de notificación y escalamiento para comunicarse con Citi en el caso de una crisis.

14.13 Evaluaciones de Continuidad del Negocio

Los Proveedores están sujetos al Proceso de Evaluación de Continuidad del Negocio de Terceros de Citi para la evaluación de las políticas, los procedimientos y los controles del Proveedor con respecto al cumplimiento de los requisitos de Citi y cualquier requisito legal y/o regulatorio (aplicable a Citi o al Proveedor) que se relacione con la continuidad del negocio. La evaluación consta de cuestionarios que requieren respuestas del Proveedor con evidencia de respaldo y puede incluir visitas a las instalaciones del Proveedor. En caso de que las conclusiones de una evaluación revelen o indiquen problemas o inquietudes, Citi documentará las conclusiones y trabajará con el Proveedor para identificar un medio para corregir los problemas. Los Proveedores deben hacer rápidamente las correcciones necesarias y/o agregar controles compensatorios para abordar las inquietudes de Citi hasta que Citi esté razonablemente satisfecho.

14.14 Resiliencia Operacional

Los Servicios Comerciales Críticos son aquellos servicios que, si su entrega se interrumpiera, podrían causar un impacto adverso significativo a Citi, sus clientes o el sistema financiero. El Proveedor se asegurará de que cualquier interrupción en la entrega de elementos de los Servicios que equivalgan a servicios comerciales críticos o respalden la provisión de servicios comerciales críticos por parte de Citi, según lo especifique Citi ocasionalmente ("Servicios Comerciales Críticos") no exceda la duración establecida por Citi ni infrinja de otro modo ninguna métrica relevante establecida por Citi ("Tolerancias a Impactos") según lo notificado al Proveedor ocasionalmente. Estas Tolerancias a Impactos se expresarán como una métrica temporal clara que equivale a la cantidad de tiempo que puede interrumpirse la prestación del servicio. Citi y el Proveedor revisarán las Tolerancias a Impactos anualmente como parte de los procesos

de gobernanza de contratos en curso. Cuando Citi deba establecer más de una Tolerancia a Impactos para un Servicio Comercial Crítico individual debido a los requisitos de más de un Organismo Regulador, Citi puede especificar Tolerancias a Impactos separadas para dicho Servicio Comercial Crítico. El Proveedor deberá:

1. 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 dentro de la(s) Tolerancia(s) a Impactos correspondiente(s) establecida(s) 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;
2. Cuando se le solicite, brindar asistencia razonable a Citi para permitirle identificar a las personas, los procesos, las tecnologías, las instalaciones y la información que son necesarios para que el Proveedor preste el servicio de apoyo a los Servicios Comerciales Críticos;
3. Brindar asistencia razonable a Citi para permitirle realizar:
 - a. cualquier prueba de escenario interno de la capacidad del Proveedor para permanecer dentro de la(s) Tolerancia(s) a Impactos para cada Servicio Comercial 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.

Cuando cualquier prueba de escenario interna realizada por Citi identifique vulnerabilidades o limitaciones en la capacidad del Proveedor para prestar servicios dentro de la(s) Tolerancia(s) a Impacto correspondiente(s) establecida(s) por Citi y luego de que el Proveedor no entregue cualquier servicio dentro de la(s) Tolerancia(s) a Impactos correspondiente(s) establecida(s) 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 incapacidad para permanecer dentro de la(s) Tolerancia(s) a Impactos (según corresponda) tan pronto como sea razonablemente posible.

14.15 Arreglo de Depósito en Garantía

A solicitud de Citi, los Proveedores (i) que proporcionen licencias de software a Citi para su funcionamiento dentro del entorno de Citi o (ii) que proporcionen un Servicio Alojado a Citi, deberán garantizar que los Materiales de Depósito se depositen ante el agente de depósito en garantía designado por Citi, y ejecutar un cronograma de registro de depositantes u otros formularios exigidos por dicho agente de depósito en garantía con respecto a los Materiales de Depósito en virtud del acuerdo de depósito en garantía aplicable. Posteriormente, durante el tiempo restante de la vigencia del acuerdo aplicable con respecto a la licencia o al Servicio Alojado, el Proveedor depositará versiones actualizadas de los Materiales de Depósito ante el agente de depósito en garantía para garantizar que el Código Fuente depositado en garantía y los demás

Materiales de Depósito se mantengan actualizados con la última versión del software aplicable a la versión del software o de los Servicios Alojados que esté utilizando Citi. Las actualizaciones del Código Fuente o de otro Material de Depósito se entregarán al agente de depósito en garantía dentro de los treinta (30) días siguientes a la fecha de cualquier actualización del software con licencia de Citi o de las modificaciones de los Servicios Alojados que utilice Citi. El Proveedor cumplirá plenamente con todas las obligaciones y requisitos de un depositante según lo establecido en el acuerdo de depósito en garantía. El Proveedor es el único responsable de todos los costos y cargos del depósito en garantía, incluidos, entre otros, los cargos de establecimiento, los cargos anuales, los cargos de depósito, los cargos de servicios y cualquier otro cargo y costo de depósito en garantía. En caso de que se produzca un Evento de Liberación, el Agente de Depósito en Garantía liberará los Materiales de Depósito a Citi o al designado de Citi, de conformidad con los términos del acuerdo subyacente y del acuerdo de depósito en garantía.

Si el Código Fuente (u otros Materiales de Depósito) se entrega a Citi o al designado de Citi (ya sea directamente por el Proveedor o por el Agente de Depósito en Garantía en cumplimiento de sus obligaciones en virtud de un acuerdo de depósito en garantía aplicable), en tal caso el Código Fuente y los Materiales de Depósito estarán sujetos a la licencia existente en virtud del acuerdo correspondiente entre el Proveedor y Citi; siempre que, se considere que cada licencia otorga a Citi el derecho a utilizar y modificar el Código Fuente y otros Materiales de Depósito según sea razonablemente necesario para: (i) integrar, y garantizar la compatibilidad, del software y otros Materiales de Depósito con los Sistemas de Citi, (ii) hacer que el software u otros Materiales de Depósito cumplan la Ley Aplicable, los estándares de la industria o las prácticas del mercado, (iii) permitir que el software u otros Materiales de Depósito se mantengan actualizados con las innovaciones tecnológicas, y (iv) permitir que el software y otros Materiales de Depósito cumplan los propósitos comerciales de Citi y sus Empresas Afiliadas dentro del alcance de la Licencia existente. Cualquier versión del Software que incluya una modificación desarrollada por o en nombre de Citi utilizando el Código Fuente estará sujeta a todas las disposiciones de esta Sección y del contrato subyacente; no obstante, el Proveedor no tendrá ningún derecho, título o interés en o sobre cualquier modificación, y todos los derechos de propiedad intelectual en y sobre cualquier modificación corresponderán exclusivamente a Citi.

El Proveedor realizará esfuerzos comercialmente razonables con terceros que proporcionaron cualquier software utilizado en el Software para permitir que el Proveedor coloque el Código Fuente de dicho software de terceros en el Depósito de Código Fuente. En caso de que el tercero se niegue a conceder al Proveedor este derecho, el Proveedor deberá realizar los esfuerzos comercialmente razonables para que el acuerdo de licencia de software de terceros aplicable se transfiera a Citi cuando se produzca un Evento de Liberación.

El Código Fuente entregado a Citi de acuerdo con esta Sección estará sujeto a la Licencia existente para el Software con licencia o los Servicios Alojados aplicables, *siempre que* Citi pueda utilizar y modificar el Código Fuente y el Software en relación con sus requisitos comerciales y operativos, para permitir que dicho Software permanezca actualizado con las innovaciones tecnológicas y para cumplir con las Leyes Aplicables. Cualquier versión del Software que incluya una modificación desarrollada por

o en nombre de Citi utilizando el Código Fuente estará sujeta a todas las disposiciones del acuerdo aplicable; no obstante, el Proveedor no tendrá ningún derecho, título o interés en o sobre cualquier modificación, y todos los Derechos de Propiedad Intelectual en y sobre cualquier modificación corresponderán exclusivamente a Citi.

15 NORMAS DE INVESTIGACIÓN DE ANTECEDENTES GLOBALES

Aplicable a todos los Proveedores Externos que prestan servicios a Citi.

15.1 Descripción General: Investigación de Antecedentes

La investigación de antecedentes debe realizarse de acuerdo con todas las leyes y regulaciones locales aplicables. Los representantes del Proveedor, el personal del Proveedor y sus Subcontratistas deben proporcionar toda la información y los datos personales que se describen en este documento, 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.

Puede encontrar información adicional sobre cómo completar la investigación de antecedentes en https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 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.

15.3 Evaluación de Sanciones

Todo el personal del Proveedor que realice trabajos en nombre de Citi o un propietario con el 25% o más de la propiedad de un Proveedor de Citi, incluidos los Subcontratistas independientemente de si tienen acceso a datos/sistemas/redes Y/O instalaciones de Citi, debe ser evaluado en contraste 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."), así como en contraste con cualquier lista emitida y nombres

de jurisdicciones sujetas a sanciones impuestas por autoridades fuera de los Estados Unidos, incluyendo la Lista Consolidada de Sanciones Financieras de la Unión Europea (UE), la Lista Consolidada del Consejo de Seguridad de las Naciones Unidas (“ONU”), la Lista de Sanciones del Reino Unido (“RU”) y las listas conforme a las leyes y regulaciones aplicables a la jurisdicción local (“Sanciones No Estadounidenses”). Las listas de la OFAC están disponibles públicamente en este website: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Cumplimiento de las Normas de Inmigración

El Proveedor debe demostrar que mantiene e implementa protocolos para verificar que todo su personal esté autorizado para trabajar en los países donde se los asigne. Además, el Proveedor debe: (1) garantizar que todo el personal esté autorizado para el trabajo, y (2) mantener el cumplimiento de todas las leyes, regulaciones y políticas aplicables (incluidos los requisitos de elegibilidad y verificación para el empleo). El Proveedor, además, debe mantener y demostrar que cuenta con protocolos para garantizar que su personal cumpla con todas las leyes y regulaciones migratorias aplicables, y que su personal tenga la clasificación/status de visa correspondiente para las asignaciones y actividades en las que participa.

15.5 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 local. El historial de empleo de una persona debe validarse para garantizar que se hayan declarado correctamente los empleadores, los puestos, las fechas y las funciones correspondientes. Los miembros del Personal del Proveedor también deben declarar cualquier empleo o asignación anterior como consultores o trabajadores temporales de Citi o de cualquiera de sus empresas antecesoras (incluidas, entre otras, Citibank, Citicorp, Travelers, Salomon Brothers y/o Smith Barney).

15.6 Historial Educativo

Los Proveedores deben validar el más alto nivel de educación completado de su personal. La información validada debe incluir las fechas de asistencia, nombre(s) de la(s) institución(es), dirección(es) y título(s) obtenido(s).

15.7 Antecedentes Penales

Cuando esté legalmente permitido, el personal y los subcontratistas del Proveedor deben revelar ante Citi si son objeto de arresto, citación, apercibimiento, procesamiento, acusación formal o condena por cualquier delito penal, incluida una declaración de culpabilidad o nolo contendere y la participación en un programa de rehabilitación previa a un juicio o programas similares. 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, o delitos similares definidos de manera diferente en virtud de las leyes locales,

salvo que las leyes lo prohíban, pueden dar lugar a la denegación y/o inelegibilidad para la asignación a Citi. Otras condenas pueden resultar en la negación y/o inelegibilidad para la asignación con base en las leyes y regulaciones locales aplicables.

15.8 Repetición de la Verificación

El personal del Proveedor cuya asignación finaliza debe volver a verificarse en caso de que sea reasignado a Citi. Para obtener información adicional sobre los requisitos de repetición de la verificación, consulte https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Traslados Internacionales

Toda la verificación debe completarse de acuerdo con las regulaciones del país donde se encuentra la asignación. Si el personal del Proveedor se traslada a un nuevo país, la persona debe ser verificada según los requisitos del nuevo país.

16 GASTOS

Proveedores que son elegibles contractualmente para reclamar gastos comerciales reembolsables.

16.1 Descripción general

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 Gobernanza de Gestión de Gastos Operativos de Citi y sus Normas y Procedimientos relevantes, en su caso, y que estén adecuadamente justificados mediante recibos, facturas, itinerarios u otras formas de documentación que Citi considere aceptables.

16.2 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):

1. El propósito comercial del gasto;
2. El monto y la descripción del gasto;
3. El lugar y la fecha del gasto;
4. El nombre/descripción del proyecto para el cual el Proveedor está prestando servicios;
5. Los nombres y la relación comercial del representante de Citi que solicitó el/los servicio(s) por los que se incurrió en gastos; y
6. El número de la orden de compra, cuando corresponda.

Para obtener información sobre los gastos comerciales reembolsables 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 reembolsos deben cumplir con las disposiciones en el Contrato aplicable o con la Política de Gobernanza de Gastos Operativos de Citi y sus Normas y Procedimientos relevantes, cuando corresponda, y estar aprobados por el negocio patrocinador correspondiente y/o por el principal contacto comercial de Citi, así como por la persona debidamente autorizada y que tiene un monto suficiente para la materia prima correspondiente. Las solicitudes que no cumplan con los requisitos no recibirán reembolso.

17 SEGURIDAD DE LA INFORMACIÓN (IS)

Aplicable a Proveedores incluyendo Subcontratistas que acceden, procesan, almacenan o gestionan cualquier información de Citi según se clasifica y define en el Apéndice; o aplicaciones orientadas a Internet de la marca Host Citi; o tienen conectividad con los recursos de red de Citi; o requieren acceso sin escolta a las instalaciones de Citi.

17.1 Descripción General

Esta Sección proporciona los requisitos mínimos para los Proveedores de Citi, incluidos los subprocesadores o subcontratistas de proveedores, que almacenan, procesan, gestionan o acceden a Información de Citi o alojan aplicaciones de Citi o que tienen conectividad de red con Citi, con respecto a los controles de protección de la información que espera Citi. Estos requisitos aseguran que la información esté protegida de acuerdo con los requisitos legales y regulatorios aplicables y los estándares más altos de la industria (p. ej., ISO/IEC 27001/2) en los lugares donde Citi y sus Proveedores operan. Si las leyes locales, las regulaciones o los 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 de otras políticas de Citi y de términos y condiciones contractuales. Si un Proveedor decide implementar prácticas de seguridad adicionales o procedimientos para la seguridad de la información, este debe asegurar que dichas prácticas y procedimientos no entren en conflicto con los controles mínimos establecidos en esta sección.

17.2 Política y Gobernanza de la Seguridad de la Información

Los Proveedores deben tener políticas y estándares documentados en materia de seguridad de la información. La gobernanza de la política debe incluir roles y responsabilidades claramente definidos y revisión/actualización anual de la política y los estándares para verificar la consistencia con el estado actual de la tecnología, los estándares de la industria, las leyes y los requisitos regulatorios.

17.3 Segregación de funciones

El Proveedor debe tener procesos establecidos que garanticen que ninguna persona individual pueda desempeñar dos funciones comerciales cualesquiera 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.

Tabla A

Funciones	Descripción de la Función
Desarrollo/ingeniería	Diseñar, crear o modificar software, hardware y configuraciones; los ejemplos pueden incluir: - Diseñar y crear un nuevo código de aplicación y esquemas de bases de datos relacionados - Productos de infraestructura de ingeniería y componentes de aplicaciones - Personalizar productos tecnológicos para integrarlos con software y servicios
Aprobación	Aprobar la promoción de cambios de código que se implementarán
Implementación/administración de sistemas	Instalar, desplegar o administrar software, hardware y cambios de configuración. Por ejemplo: - Realizar un lanzamiento de código automatizado o manual a la infraestructura de producción - Instalar un producto o aparato tecnológico - Iniciar o detener servicios para respaldar la resolución de problemas y remediación de sistemas con datos de producción
Revisión de la Actividad con Identificación Privilegiada	Verificación de la actividad de gestión de cambios o eventos del sistema relacionados con la seguridad (p. ej., rastros de auditoría)
Administración de identificaciones	Agregar, modificar y eliminar identificaciones (Usuario, FID y Bots), permisos o contraseñas
Función comercial	Descripción de la función
Iniciación de la transacción comercial	Iniciar (también denominado ingresar, realizar o crear) transacciones comerciales y cambiar la información del cliente

Aprobación de la transacción comercial	Aprobar (también denominado autorizar, verificar o liberar) transacciones comerciales
Función de TI	Descripción de la función
Operaciones de red	Gestión de dispositivos y soporte operacional de productos que proporcionan servicios de infraestructura de red. Algunos ejemplos son los enrutadores de red, conmutadores, cortafuegos y Servicios de Nombres de Dominio (DNS)
Operaciones fuera de red	Gestión de dispositivos y soporte operativo de productos que no proporcionan servicios de infraestructura de red. Algunos ejemplos son los servidores, los teléfonos y las computadoras

17.4 Compromiso de la Dirección con la Seguridad de la Información

Los Proveedores que alojarán una aplicación de Internet con la marca Citi y/o tendrán acceso a la información de Citi con clasificación Confidencial o de nivel superior están sujetos al Proceso de Evaluación de Seguridad de la Información de Terceros (TPISA) de Citi para evaluar las políticas, procedimientos y controles del Proveedor en relación con el cumplimiento de los requisitos de Citi y los requisitos legales y/o regulatorios (aplicables a Citi o al Proveedor) relacionados con la seguridad de la información.

La evaluación consta de cuestionarios de seguridad que requieren respuestas del Proveedor con evidencia de respaldo y puede incluir visitas a instalaciones del Proveedor donde la Información Confidencial o de nivel superior de Citi es almacenada, procesada, gestionada o accedida por el tercero. Además, el Equipo de Monitoreo Continuo de Terceros del TPISA puede monitorear al Proveedor utilizando herramientas de monitoreo de Seguridad Cibernética que utilizan la información disponible de dominio público para identificar sistemas, hosts, aplicaciones y servidores vulnerables orientados a Internet en casos de, por ejemplo, software que ha llegado al final de su vida útil, puertos abiertos explotados, vulnerabilidades u otras situaciones comprometedoras. Si los resultados del TPISA revelan o indican deficiencias de seguridad, Citi dejará constancia de los resultados en un aviso al Proveedor y trabajará con éste para identificar los medios para subsanar dichas deficiencias. Los Proveedores deben realizar rápidamente las correcciones necesarias y/o añadir controles compensatorios para abordar las inquietudes de Citi a su exclusiva discreción y cumplir con los plazos requeridos de 180 días calendario para los problemas de Alto Riesgo, 240 días calendario para los problemas de Riesgo Medio y antes de la próxima fecha de cumplimiento para los problemas de Bajo Riesgo, según la calificación de riesgo de dichos problemas por parte de Citi.

1. El Proveedor debe realizar periódicamente evaluaciones de sus operaciones y controles comerciales con base en sus propios 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 propios de Seguridad de la Información;
 - b) Evaluación de los recursos de apoyo, como las aplicaciones y la infraestructura utilizadas por el Proveedor y los procesos de la IS 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 de nivel superior por Citi.
2. Las excepciones que se identificaron como resultado de cualquier Evaluación de Riesgos de Seguridad de la Información (p. ej., TPISA) deben documentarse y rastrearse hasta el cierre con evidencia de la medida correctiva proporcionada a Citi.
 3. 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.
 4. Si el Proveedor adquiere una nueva entidad, el Proveedor debe completar una evaluación de la entidad adquirida para cumplir con estos Estándares.
 5. El Proveedor no debe subcontratar las funciones de gestión de la seguridad, incluidas, entre otras, la gestión del cortafuegos o firewall, la gestión de la configuración de la seguridad, la gestión de parches o las funciones de 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.
 6. Si el Proveedor aloja un software o website que contiene Información de Citi o lleva la marca de Citi, deben realizarse evaluaciones de vulnerabilidad periódicas de acuerdo con el Estándar de Pruebas de Seguridad del Sistema (SST) de Citi y debe solucionarse cualquier excepción importante identificada en las evaluaciones dentro de los plazos especificados en ese Estándar. Como el SST no está aprobado para su distribución externa, los Proveedores deben trabajar con su Gerente de Relaciones de Citi para asegurar el cumplimiento de la documentación de referencia. Además, el Proveedor debe cumplir con los Estándares de Gestión de Seguridad de la Información ISO/IEC 27001 (o los estándares sucesores de gestión de seguridad de la información que establecen estándares y protocolos más altos) y cumplir con las disposiciones de seguridad de la información contenidas en esta Sección (17).
 7. 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 proporción de conectividad.
 8. El Proveedor debe notificar rápidamente al contacto de Citi que corresponda (Responsable de la Actividad Comercial, BAO) 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.

9. El Proveedor debe asegurarse de que todas las actividades de alto riesgo o los cambios en los datos confidenciales tengan rastros de auditoría que permitan atribuir esas acciones a las personas que las realizaron.
10. El Proveedor debe asegurarse de que todos los datos confidenciales o de nivel superior estén enmascarados en la pantalla y en papel (incluidos, por ejemplo, los informes de seguimiento, de excepción, reglamentarios y de otro tipo).
11. El Proveedor debe restringir la impresión, registro o copia de datos confidenciales, incluso por sus dispositivos propios. El Proveedor debe devolver o destruir toda la información de Citi en un momento acordado durante o al final del acuerdo, a menos que las leyes o las regulaciones lo prohíban de otro modo.
12. El Proveedor debe asegurarse de que todo el personal del Proveedor (empleados fijos y temporales, contratistas, subcontratistas) con acceso a la información de Citi firme un contrato de no divulgación o confidencialidad (NDA).
13. 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 y políticas de recursos humanos del Proveedor que deben reconocerse como parte de su proceso de incorporación.
14. El Proveedor cuenta con un proceso para recuperar todos los activos cuando un empleado o no empleado es despedido o renuncia.
15. Si se mantiene cualquier Información Confidencial o se almacena de cualquier manera en un website o un sistema al que puede accederse desde la web, el Proveedor debe divulgar esta información a Citi. Esta divulgación puede incluirse en la descripción de los Servicios. Si el Proveedor mantiene o almacena Información Confidencial de Citi, el Proveedor hará que se realice una auditoría SSAE 18 (o cualquier evaluación autorizada del sucesor aprobada por Citi) una vez al año, durante el plazo de este Acuerdo, y le proporcionará a Citi, como mínimo una vez al año, una copia de los informes que documenten los resultados de dicha auditoría SSAE 18 o cualquier evaluación autorizada por el sucesor aprobada por Citi.
16. Si el Proveedor es adquirido por otra entidad o adquiere otra entidad en una fusión, adquisición o transacción similar, y dicha transacción pudiera afectar 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 la adquisición o fusión no afecte el cumplimiento del mismo.

17.5 Riesgo de Seguridad de la Información del Subcontratista

El Proveedor debe exigir que los subcontratistas con acceso a los datos confidenciales o de nivel superior de Citi se sometan a evaluaciones de Seguridad de la Información (IS) precontractuales y poscontractuales periódicas llevadas a cabo por personal calificado de Seguridad de la Información. Estas evaluaciones deben realizarse conforme a un proceso aprobado por la gerencia que aborde todas las etapas del proceso de evaluación, desde el inicio hasta la gestión del problema. La evaluación de IS del subcontratista debe basarse en un cuestionario o herramienta equivalente que evalúe la postura del subcontratista dentro de los dominios del IS que se alinean con los incluidos en el Cuestionario de Evaluación de Seguridad de la Información de Terceros (TPAQ) de Citi y debe incluir un método lógico para calcular el riesgo de Seguridad de

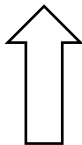
la Información en lo que respecta a la participación del subcontratista. El Proveedor debe realizar un seguimiento de la finalización de la evaluación y gestionar los problemas observados y los planes de acción correctiva hasta su cierre.

17.6 Responsabilidad por los activos:

- 1. 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.
- 2. El Proveedor debe asegurarse de que se mantenga 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.
- 3. El Proveedor debe ser responsable de proteger toda la Información de Citi bajo su control.
- 4. El Proveedor debe garantizar la responsabilidad de la actividad de sus usuarios de manera coherente con las prácticas de la industria.
- 5. El acceso de usuarios a cuentas personales de correo electrónico en Internet con almacenamiento externo y en la nube debe restringirse desde la red global del Proveedor donde resida la Información de Citi.

17.7 Clasificación y Manejo de la Información.

Citi clasifica la información conforme a la siguiente tabla de Clasificación de la Información. Consulte el Apéndice para obtener definiciones y ejemplos de cada clasificación que se lista a continuación.

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

- 1. 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.
- 2. La información con clasificación “Interna” o de nivel 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 los estándares de Citi.
- 3. 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 Cuarto), el Proveedor debe tener una política 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.
- 4. El Proveedor siempre debe proteger la Información de Citi contra el acceso, la modificación o la eliminación no autorizados.

5. La Información de Citi clasificada como Confidencial o de nivel superior transferida a través de Medios Electrónicos Portátiles (ETM) debe cifrarse usando un algoritmo criptográfico aprobado y debe confirmarse la entrega. El Proveedor debe confirmar que el ETM fue recibido por el destinatario. Si no se recibe la confirmación del recibo en o antes de la fecha de entrega esperada, el Proveedor debe notificar a Citi.

17.8 Configuración Segura

1. El Proveedor debe mantener un estándar documentado sobre configuración segura para todos los activos con el potencial para almacenar, procesar, transmitir o tener acceso a Información de Citi.
2. El Proveedor debe incorporar controles de seguridad de la información en sus procesos y procedimientos para la selección, el desarrollo y la implementación de aplicaciones, productos y servicios.
3. El Proveedor debe tener un procedimiento seguro de creación para todos los sistemas donde se almacene, procese y/o transmita Información de Citi.
4. El Proveedor debe mantener una imagen o plantilla segura de todos los sistemas.
5. Todas las cuentas de usuario y contraseñas predeterminadas se eliminan y/o cambian de los sistemas, dispositivos de red y aplicaciones compatibles con el proveedor.
6. Cualquier sistema o servicio que se haya visto comprometido debe ser reconstruido y configurado usando una imagen o plantilla que tenga una integridad comprobada.
7. Cualquier cambio que vaya a aplicarse a una configuración segura debe ser aprobado por la administración a través del proceso de gestión de cambios del Proveedor.
8. El Proveedor debe notificar a Citi cualquier cambio en la configuración segura.
9. El procedimiento seguro de creación debe incluir herramientas para admitir las comprobaciones automatizadas de la configuración para los ajustes estándares y de seguridad de creación al momento de la implementación en producción y el monitoreo continuo para cumplir con la configuración de base y detectar las desviaciones de esta.

17.9 Requisitos de Cifrado

El Proveedor no transmitirá información clasificada como Confidencial o de nivel superior sin cifrar. La información clasificada como Confidencial o de nivel superior debe cifrarse **de extremo a extremo** con herramientas o soluciones aprobadas por Citi. Los protocolos aprobados y los respectivos números de versión para la transmisión cifrada de datos son los siguientes:

1. Al intercambiar información de autenticación y autorización: SAML v2.0, OAuth v2.0 (solo con autorización),
2. Para proteger los canales de comunicación y el intercambio de claves asociado se permiten los siguientes Protocolos de Seguridad de Red:
 - a) Se prefiere TLS v1.3 y se permiten todas las suites TLS v1.3. Si TLS v1.3 es el único protocolo habilitado, no es necesaria una revisión

- adicional.
- b) Si TLS v1.3 no es técnicamente viable y se aprovecha TLS 1.2, entonces es aceptable un grado de B o superior de SSL Labs y no es necesaria una revisión adicional.

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 claves para cifrar datos son los siguientes:

1. **Estándar de Cifrado Avanzado (AES):** Longitudes de clave aprobadas: 256 o más 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: Es obligatorio AES con clave de 256 bits. Se permite AES con una longitud de clave de 128 bits como una opción de cifrado TLS; sin embargo, estas no se permitirán a favor de una longitud de bits de 256 o más al 31 de diciembre de 2028 para permitir la alineación de Citi con los plazos internacionales (Ref. NIST 8547 IPD).
2. **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.

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:

Aviso relacionado con la Preparación Cuántica del Proveedor: Los Proveedores deben presentar su plan sobre la cobertura de la *tabla 2* y la *tabla 4* de NIST IR 8547 (ipd) al equipo del Programa de Preparación Cuántica de Citi a través de ([enlace de encuesta](#)).

1. **Criptosistemas de Clave Pública y Tamaños Mínimos de Longitud de Clave:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 bits.
 - b) Algoritmo de Firma Digital (DSA): 2048 bits. No debe usarse DSA para proteger los datos de Citi procesados o almacenados fuera del Citi.
 - c) Algoritmo de Firma Digital de Curva Elíptica (ECDSA): 256 bits y como se especifica en ANSI X9.62 con curvas recomendadas por NIST.
2. **Mecanismos de Intercambio y Acuerdo de Claves y Tamaños Mínimos de Longitud de Clave:**
 - a) Diffie-Hellman (DH) / Ephemeral Diffie-Hellman (DHE): 2048 bits.
 - b) Curva elíptica Diffie-Hellman (ECDH)/Curva elíptica efímera Diffie-Hellman (ECDHE): 256 bits y como se especifica en ANSI X9.63 con curvas recomendadas por NIST¹.
3. **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.

¹ Se prefiere ECDHE.

- a) Solo se acepta SHA-1 para aplicaciones de firma no digitales. Familia SHA-2, familia SHA-3 y POLY-1305: Se acepta para todas las aplicaciones criptográficas de función hash.
- 4. **Funciones de Derivación de Clave Basadas en Contraseña y Requisitos Mínimos:**
 - a) PBKDF2: Recuento mínimo de iteraciones de 10000 con una sal criptográfica de al menos 16 bytes.
 - b) HKDF: Debe incluirse la sal criptográfica, y debe incluirse el valor de entrada de información.
 - c) SCRYPT: Número mínimo de rondas/factor de costo de 10.
 - d) Está prohibido el uso de NIST SP800-108 KDF para Stream Encryption. Se permiten los modos NIST SP 800-108 KDF, es decir, los modos Counter, Feedback y Double-Pipeline Iteration.
 - e) Se recomienda Argon2.
- 5. **Funciones de Hash de Contraseña y Requisitos Mínimos:**
 - a) Bcrypt (para almacenamiento local del material de autenticación): Número mínimo de rondas/factor de costo de al menos 10.
 - b) Se recomienda utilizar Argon2 o PBKDF2 para el hash de contraseñas cuando se almacenen éstas localmente en cualquier entorno o sistema desplegado con productos del Proveedor.

17.10 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 de nivel 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 regulación y/o la política del Proveedor, puede cumplirse en su totalidad a través del cifrado de transporte (p. ej., cifrado de puerta de enlace a puerta de enlace a través de Transport Layer Security, TLS). Los protocolos de correo electrónico seguro aprobados son:

1. **El Cifrado Basado en la Identificación (IBE)** cuenta con correo electrónico cifrado y solo puede usarse dentro de las soluciones orientadas al cliente de Citi y los sistemas seguros de correo electrónico y entrega electrónica.
2. **TLS Obligatorio (MTLS)** cuenta con cifrado de Sesión (no cifra la carga útil de correo electrónico) y puede utilizarse con proveedores, socios y clientes que hayan negociado previamente acuerdos para su uso.
3. **Domain Keys Identified Mail (DKIM)** cuenta con autenticación y gestión de claves y puede utilizarse con proveedores, socios y clientes.

17.11 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 (p. ej., SWIFT o un banco central) pueden considerarse exentas del requisito de cifrado de PII Confidencial en tránsito hasta que esas redes proporcionen la infraestructura necesaria para soportar completamente las transmisiones cifradas.

17.12 Voz y Fax

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

17.13 Gestión de Claves y Certificados Criptográficos

El término “límite seguro” usado en esta sección se refiere a un límite validado del Programa de Validación de Módulos Criptográficos (CMVP), tal como el Estándar Federal de Protección de la Información (FIPS); (FIPS 140-2/3 Nivel 2 es el nivel de seguridad mínimo aceptable). (Se aceptan los Enclaves de Computación Confidencial, como los Enclaves Nitro de AWS. Otros casos de límites de seguridad únicos deben ser aprobados por Citi).

1. El Proveedor debe desplegar algoritmos criptográficos estándar actuales de la industria y las longitudes mínimas de clave para el cifrado y las firmas (incluidas claves SSH). El Proveedor debe proporcionar certeza a través de su Proceso de Gestión de Cambios cuando dichos algoritmos y longitudes de clave se actualicen para alinearse con los estándares de la industria.
2. El Proveedor debe tener un proceso formal documentado del ciclo de vida de la gestión de claves, secretos y certificados con controles implementados para proteger los materiales sensibles de usos o exposiciones no autorizados. Todos los secretos criptográficos y eventos del ciclo de vida de claves solo deben ocurrir dentro de un límite seguro. Todo acceso a los límites privilegiados y seguros debe estar documentado. El Proveedor debe proporcionar un diagrama de secuencia para todos los eventos del ciclo de vida de claves destacando los actores, entidades y límites involucrados.
3. Las Claves Criptográficas deben tener un propósito único y nunca deben usarse para ningún otro propósito, tal como usar la misma clave de cifrado para el cifrado de disco, así como el cifrado de datos o la misma clave de cifrado para cifrar la carga útil así como cifrar la base de datos. La reutilización de claves criptográficas en múltiples tenants por parte de un proveedor de SaaS está prohibido por defecto y puede permitirse solo para casos de uso no críticos y de bajo riesgo que involucren información de Citi clasificada debajo de PII Confidencial, PII Sensible y Restringida, sujeto a la aprobación explícita del Security Architecture Council.
4. Para todas las claves criptográficas (simétricas o asimétricas), la clave privada o el material de clave privada (tal como semillas, o parte de una clave privada) no deben mostrarse en texto sin cifrar en ningún momento. La clave privada o el material de la clave privada (tal como la semilla o parte de una clave privada) nunca debe salir del límite seguro, con la excepción de las claves efímeras tales como claves de sesión dinámicas. Si el diseño requiere que una clave simétrica o una clave privada o un material de clave privada se transmita entre enclaves seguros/límites de acceso privilegiados, deberá transmitirse únicamente de forma cifrada utilizando una Clave de Envoltura de Clave Simétrica o una Clave de Transporte de Clave Pública únicamente a través de túneles mutuos cifrados TLS, y dicha transmisión deberá ser aprobada por Citi por escrito. En estos casos, la Clave de Transporte de Clave Privada nunca debe salir del límite seguro de acceso privilegiado donde se generó.

5. La Clave de Envoltura de Clave Simétrica 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. La Clave de Envoltura de Clave Simétrica debe tener Listas de Controles de Acceso (ACL) adecuadas asociadas dentro del límite seguro, tal como módulos validados por CMVP y la Clave de Envoltura de Clave Simétrica nunca debe almacenarse fuera del límite seguro.
6. El acceso humano o de servicio o agente automatizado a almacenes de claves o límites seguros que contienen claves o secretos privados o material de claves privadas (tal como la semilla o parte de una clave privada) debe estar debidamente segregado con controles que limiten el acceso solo al personal o a los sistemas autorizados.
7. 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.
8. El Proveedor no debe usar certificados autofirmados y de comodín ni certificados de SSL por defecto.
9. Todas las Claves criptográficas deben tener un periodo de tiempo criptográfico definido como se sugiere en NIST SP800-57 parte 1, revisión 6. Las claves deben actualizarse o rotarse antes de su vencimiento para acomodar periodos de cambio, conflictos de programación y bloqueos del sistema.
 - a) Mientras se reemplaza un certificado vencido, está prohibida la reutilización del antiguo par de claves asimétricas.
10. Las Claves Criptográficas deben tratarse como si estuvieran comprometidas tan pronto como se sospeche que la integridad de la clave, el medio en el que la clave se almacena o comparte, o la confidencialidad de la clave simétrica o privada están comprometidos. Todas las claves que estén comprometidas deben ser retiradas de su uso operativo, y todos los certificados correspondientes deben revocarse.
11. Las redes inalámbricas deben cifrarse con algoritmos de cifrado estándares de la industria.
12. Los Proveedores que utilicen cualquier forma de mecanismo criptográfico deben usar herramientas y técnicas estándares de la industria para la gestión de claves. El rol de gestión de claves debe separarse de la gestión operacional.
13. Los Proveedores pueden aprovechar el KMS y la PKI nativos de la nube solo cuando se garantiza la interoperabilidad con los servicios de PKI & KMS proporcionados por los Servicios de Seguridad de Datos de Citi y el control criptográfico no se delega fuera de la gobernanza criptográfica de Citi.

17.14 Responsabilidad de Control de Acceso

Para proteger todos los Sistemas de Información Controlada usados para almacenar, acceder, gestionar, procesar o transmitir Información Confidencial o de nivel superior de Citi contra el acceso no autorizado, el Proveedor es responsable de hacer cumplir el principio de mínimo privilegio, limitando las autorizaciones de usuario al nivel mínimo de acceso requerido para cada función laboral y gestionando el suministro de acceso lógico

a todos los sistemas y aplicaciones. Los controles deben estar completamente documentados y ser auditables. El suministro y la retirada de acceso, incluido el restablecimiento de contraseñas y su habilitación, deben realizarse mediante un proceso automatizado siempre que sea posible, a fin de mitigar el riesgo de posibles errores humanos que puedan generar sobreasignación de permisos y para alinearse con los estándares de la industria.

1. El Proveedor es responsable de los derechos de acceso de todos los usuarios de su organización.
2. El Proveedor debe implementar controles de acceso que aseguren que a los usuarios se les otorguen solo los privilegios y autorizaciones necesarios para realizar su función.
3. 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.

17.15 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 Información Confidencial o de nivel superior de Citi. Esto incluye:

1. Identificación e inventario de sistemas de autenticación aprobados.
2. El requisito de que todo acceso a los datos de Citi requiere la aprobación de un gerente o del designado de un gerente, así como del responsable del sistema. El Proveedor es responsable de asegurar que a cualquier miembro de su personal con acceso a los datos de Citi se le otorgue dicho acceso según sea necesario.
3. El requisito de que cualquier combinación de privilegios/funciones para un usuario individual no se pueda proporcionar si representa un conflicto de intereses o una violación de las reglas del creador-verificador.
4. Un proceso de monitoreo para supervisar y gestionar los derechos de acceso otorgados/revocados para cada usuario en el sistema.
5. Las solicitudes de acceso no deben basarse en la duplicación o clonación de los permisos de otro usuario; deben especificar roles o permisos explícitos con una justificación comercial para evitar la escalada de privilegios y garantizar el principio del mínimo privilegio.

17.16 Identificación y Autenticación de Usuarios

Todos los sistemas de información controlada del Proveedor deben autenticar la identidad de los usuarios o sistemas que accedan a estas plataformas antes de iniciar una sesión o transacción desde la que se pueda acceder a Información de Citi.

1. Los usuarios deben ser identificados o asignados de manera única a la plataforma de tecnología mediante una Identificación de Usuario.
2. Los usuarios deben ser autenticados en la plataforma de tecnología utilizando un método de autenticación aprobado. El Proveedor debe comunicarse con su principal contacto comercial (BAO) para conocer los métodos aprobados vigentes.

3. Todo uso de infraestructura de autenticación compartida (p. ej., inicio de sesión único, inicio de sesión reducido y otros servicios de autenticación compartida) deben utilizarse de acuerdo con los requisitos de autenticación de Citi. El Proveedor debe comunicarse con su BAO principal para conocer los métodos aprobados vigentes.
4. Los Datos de Verificación de Identidad (IVD) que se usan para autenticar a un usuario en un Sistema de Información deben cifrarse en transmisión y almacenamiento. Consulte la sección 17.9 para conocer los requisitos de cifrado.
5. Cada cuenta utilizada por el personal del Proveedor para acceder a los sistemas de Citi debe mapearse a un identificador único asignado por Citi (p. ej., GEID); se prohíben las ID de usuarios genéricas/compartidas para usuarios humanos para garantizar la trazabilidad, la aplicación de SOD y la preparación para las auditorías.

17.17 Identificación del Acceso Privilegiado y Acceso Privilegiado Temporal

El Proveedor debe mantener un inventario de todas las identidades e identificar aquellas que tienen acceso privilegiado o tienen acceso a depósitos electrónicos (conjuntos de datos o bases de datos que respaldan aplicaciones del negocio) que contienen información clasificada como PII Confidencial o de Nivel Superior. El Proveedor debe implementar controles que protejan contra el uso no autorizado de estas Identidades. Si un trabajador requiere acceso a una ID privilegiada o a los depósitos electrónicos mencionados arriba, el acceso debe otorgarse a través de un proceso de gestión de acceso temporal que:

1. Requiera que el solicitante esté en una lista de usuarios autorizados previamente aprobados o que obtenga una aprobación en el momento del uso.
2. Requiera justificación documentada en un ticket de cambio/problema antes de que se otorgue acceso.
3. Incluya una revisión independiente de la actividad realizada con el acceso.
4. Incluya un proceso para iniciar la revocación/eliminación del acceso al final de la duración de la liberación de acceso temporal.
5. Permita 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.

17.18 Revisión de Derechos de Acceso de los Usuarios

1. El Proveedor debe implementar un proceso documentado para revisar, verificar y eliminar las autorizaciones innecesarias del usuario a los Sistemas de Información Controlada utilizados para almacenar, procesar, administrar y/o transmitir Información de Citi al menos semestralmente.
2. Los usuarios no deben revisar o aprobar sus propias autorizaciones o las de una persona que les haya delegado responsabilidad de revisión.
3. Luego de un cambio de función por parte de un empleado del Proveedor dentro de Citi, el Proveedor tiene 14 días calendario para realizar una revisión

de acceso y autorizaciones y eliminar el acceso a los datos de Citi si ya no es necesario para la nueva función del empleado.

17.19 Procedimientos de Inicio de Sesión Seguro

1. 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.

17.20 Sistema de Gestión de Contraseñas

1. Las contraseñas estáticas de usuarios nunca deben mostrarse en pantalla como texto sin cifrar. La funcionalidad de conmutación de visibilidad de contraseña está exenta de este requisito, siempre que:
 - (1) La entrada de contraseña está enmascarada por defecto,
 - (2) La visibilidad de la contraseña pueda iniciarse sólo mediante una acción explícita del usuario, (3) la contraseña se vuelve a enmascarar automáticamente en un máximo de 15 segundos después de que se interrumpa la acción del usuario.
2. Las contraseñas de identificaciones funcionales privilegiadas no deben ser preprogramadas en texto sin cifrar.
3. Las contraseñas estáticas deben contener un mínimo de diez (10) caracteres e incluir letras y números y ser sensibles a mayúsculas y minúsculas. La sensibilidad a mayúsculas y minúsculas de las contraseñas estáticas debe validarse en cada punto de autenticación. Las contraseñas estáticas de identificaciones funcionales (FID) deben contener un mínimo de 15 caracteres en aplicaciones implementadas después del 31 de agosto de 2026.
4. 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 (p. ej., teclado, teléfono, tarjeta inteligente).
5. Todas las contraseñas estáticas deben cambiarse, como mínimo, cada 90 días calendario.
6. Todas las contraseñas estáticas deben bloquearse después de no más de seis (6) intentos de inicio de sesión fallidos consecutivos, o seis (6) intentos de restablecimiento de contraseña consecutivos. Las contraseñas deben desbloquearse a través de una función de administrador de ID o desbloquearse automáticamente después de al menos 30 minutos.
7. Todos los sistemas de autenticación deben imponer un control de inactividad/falta de uso que no puede exceder los 100 días calendario. Si es técnicamente posible, los inicios de sesión inhabilitados pueden ser rehabilitados por el usuario u otra función autorizada.
8. El proceso de autenticación debe garantizar que no se use la misma contraseña dentro de al menos los últimos seis (6) cambios.

17.21 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 las aplicaciones (p. ej., arrancar desde dispositivos periféricos) esté restringido y controlado.

17.22 Cierre de Sesión por Inactividad

1. Para todos los usuarios de un Sistema de Información Controlada usado para almacenar, procesar y/o transmitir Información de Citi, se debe requerir el inicio de sesión y la reautenticación.
2. La reautenticación de usuarios se debe exigir luego de un periodo de inactividad no superior a los 30 minutos. La actividad incluye cualquier entrada al dispositivo (ratón, 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.

17.23 Terminación del Acceso del Usuario

1. Tras un despido o renuncia, el acceso del usuario o las autorizaciones que podrían permitir el acceso a los datos Confidenciales o de nivel superior de Citi, incluidos el 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 inmediatamente.
2. Si un empleado tiene acceso a sistemas propiedad de Citi y que estén administrados por dicha empresa, el Gerente de Relaciones Comerciales de Citi, el BAO o el respaldo del BAO deben ser notificados inmediatamente después del cambio de función o desvinculación laboral de ese empleado para garantizar que el Gerente del Negocio de Citi inicie la eliminación del acceso para los trabajadores desvinculados antes del final de su fecha de desvinculación laboral.
3. El Proveedor tiene un proceso documentado implementado para recuperar el acceso de todos los activos en línea con los plazos establecidos en la sección 17.23.2 cuando un empleado o no empleado es despedido o renuncia.
4. Si el Proveedor descubre alguna anomalía con respecto a 17.23.1-17.23.3, el Proveedor debe informar inmediatamente al Gerente de Relaciones Comerciales de Citi, el BAO o el respaldo del BAO, proporcionando fundamentos y controles sólidos.

17.24 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 Confidenciales o de nivel superior de Citi que incluyan:

1. 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.
2. 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 haya almacenamiento/procesamiento local de información con una clasificación de

Información Confidencial o de nivel superior de Citi, debe cifrarse con una herramienta de cifrado que cumpla con los estándares de la industria.

3. Solo deben establecerse conexiones remotas a través de soluciones de acceso remoto aprobadas que empleen autenticación de factores múltiples (MFA).
4. 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.
5. 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.
6. Si se utilizan dispositivos que no son propiedad del Proveedor ni estén administrados por éste para acceder a la Información Confidencial o de nivel superior de Citi, se debe usar una solución autorizada que no permita descargas a la máquina local. Se deben implementar los siguientes controles:
 - a) Se impide que los Datos de Citi se descarguen a un dispositivo fuera de una solución administrada por la empresa.
 - 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 (p. ej., Virtual Desktop Interface (VDI)).
 - c) Las soluciones de acceso remoto como Terminal Services y VMware Horizon deben configurarse para deshabilitar el uso compartido del portapapeles y Drive Mapping sobre los protocolos Blast, PCoIP, RDP y SSH.
7. 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 (p. ej., mediante contraseña, datos biométricos, etc.) e impedir su uso si el teléfono móvil tiene modificaciones “jailbreak” o “rooting” (usando un sistema operativo diferente a los certificados y suministrados por el proveedor del dispositivo móvil).
8. 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 brindados a Citi deberán utilizar la autenticación de múltiples factores (MFA) y dicho acceso será registrado y supervisado de forma independiente por el Proveedor para detectar actividad sospechosa y/o acceso no autorizado de conformidad con estos Requisitos.
9. Para dispositivos de propiedad personal y dispositivos propiedad de un tercero, el Proveedor debe tener una solución efectiva para asegurar que dichos dispositivos tengan una versión aprobada del sistema operativo,

niveles de parches, soluciones antivirus y antimalware, antes de que se permita que dichos dispositivos inicien sesión en la red.

10. El Proveedor debe garantizar que todo su personal:

- a) Mantenga un espacio de trabajo remoto dedicado y privado que no contenga ningún dispositivo de asistencia de voz (p. ej., Siri, Alexa), dispositivos de grabación de video y/o cualquier otro dispositivo para capturar fotos y video o para escuchar/grabar 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.
- b) Bloquear el dispositivo informático cuando lo deje desatendido para garantizar que el acceso no autorizado para ver la pantalla se mitigue adecuadamente.

17.25 Política de Escritorio Limpio

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 capacitación sobre SI u otro canal.

17.26 Prevención Contra Incendios

1. 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.
2. El proveedor debe utilizar uno o más sistemas de detección, alarma y supresión de incendios. Estos sistemas deben ser inspeccionados semestralmente y probados anualmente.

17.27 Seguridad Física

1. La Información de Citi debe ser almacenada en áreas seguras con controles que restrinjan el acceso solo a personal autorizado.
2. El Proveedor debe contar con un sistema documentado y auditable de control de acceso físico.
3. 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.
4. 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.

17.28 Procedimientos y Responsabilidad de Seguridad Operacional

1. El proceso de gestión de cambios del Proveedor debe incluir controles de puntos de control clave en torno al registro, revisión, prueba, aprobación, implementación y cierre de los cambios. El Proveedor también debe tener un

proceso de cambios de emergencia que requiera todas las etapas enumeradas sobre incluir una jerarquía de aprobaciones obligatorias.

2. El Proveedor debe tener un proceso auditable en torno a la gestión de capacidad que incluya, entre otros, métricas/indicadores de disponibilidad, capacidad y rendimiento; evaluación de impacto en el negocio; seguimiento proactivo, investigación y tratamiento de excepciones de rendimiento y capacidad.
3. Cuando corresponda, el Proveedor debe asegurarse de que los entornos de Laboratorio, Desarrollo, Pruebas y Producción estén todos separados de manera física y/o lógica entre sí.

17.29 Requisitos para el Desarrollo de Software

Aplicable a Proveedores que entregan software desarrollado para uso exclusivo de Citi. Los Proveedores deben seguir estos requisitos o demostrar un proceso documentado y aprobado del Ciclo de Vida del Desarrollo de Software ("SDLC") con un enfoque equivalente de igual calidad.

17.30 Iniciación y Planificación

El Proveedor debe definir el alcance y los objetivos de la solución en alineación con los requisitos de Citi y sus obligaciones contractuales con Citi. Esto incluye:

1. Documentar los requisitos funcionales y no funcionales;
2. Proporcionar estimaciones de esfuerzos y plazos; e
3. Identificar todos los componentes o dependencias de terceros.

Las actividades de cumplimiento, incluidas las evaluaciones de riesgos de seguridad, deben iniciarse al comienzo del proyecto. Los roles, las responsabilidades y los puntos de control de aprobación deben comunicarse claramente.

Todos los entornos deben clasificarse como Desarrollo (DEV), Pruebas (TEST) o Producción (PROD) y deben permanecer estrictamente segregados durante todo el ciclo de vida. La clasificación del entorno determina los permisos de acceso y el tipo de datos que pueden procesarse. El Proveedor debe restringir el acceso según la designación del entorno y alinear los despliegues con la finalización de la fase del SDLC correspondiente para evitar el acceso no autorizado o la exposición de los datos.

17.31 Diseño

El Proveedor debe documentar un enfoque de diseño que garantice que la solución entregada cumpla con todos los requisitos establecidos (un "Plan de Pruebas"). Como mínimo, un Plan de Pruebas debe incluir y describir:

1. 1.Todas las pruebas que debe ejecutar el equipo de desarrollo, incluidas las pruebas unitarias y las pruebas funcionales y no funcionales, así como las pruebas de aspectos de rendimiento, con trazabilidad a los requisitos;
2. 2.La identificación del/de los aprobador(es) que confirmará(n) la finalización;
3. 3.Los requisitos de pruebas de seguridad, como evaluaciones de vulnerabilidad y modelado de amenazas; y
4. 4.El entorno de pruebas, el enfoque, el proceso y la ruta de promoción.

Se debe preparar una estrategia de lanzamiento que describa los requisitos previos y el proceso para la lanzamiento en entornos TEST y PROD, incluidos los criterios

de preparación del lanzamiento, el contenido y la cadencia de entrega durante la vida útil del proyecto.

Cuando se especifique en el Contrato, las distribuciones de software deben empaquetarse en un formato aprobado por Citi utilizando herramientas y flujos de trabajo aprobados por Citi.

17.32 Pruebas

Las pruebas deben planificarse y ejecutarse en un entorno controlado para validar que la solución cumpla con los requisitos y criterios de éxito definidos. Los casos de prueba deben poder rastrearse a los requisitos y los compromisos de código.

El Proveedor debe preparar un informe que resuma los resultados de aprobado/reprobado, las pruebas adicionales realizadas durante el desarrollo y cualquier prueba no completada (con las razones) (un “Informe de Salida de la Prueba”). Los defectos y las capacidades diferidas deben documentarse junto con los planes de mitigación para problemas no resueltos.

A solicitud de Citi, el Proveedor debe proporcionar evidencia de:

1. Un Plan de Pruebas detallado;
2. Finalización de la prueba y resultados detallados en un Informe de Salida de la Prueba; y
3. Trazabilidad de los resultados de las pruebas a los requisitos y los compromisos de código.

17.33 Implementación

Antes de la implementación, el Proveedor debe completar todas las pruebas de seguridad requeridas, incluidos los análisis de vulnerabilidad y el modelado de amenazas. El proceso de lanzamiento debe estructurarse con registros de cambios documentados, estrategias de reversión y aprobaciones requeridas. Los planes de implementación y los manuales de implementación deben incluir protocolos de monitoreo y escalamiento.

Después de la implementación, el Proveedor debe finalizar los identificadores del sistema y actualizar todos los artefactos relacionados para garantizar la preparación para la auditoría.

17.34 Seguridad

1. Se debe incluir en el SDLC una evaluación estructurada realizada durante la fase de diseño del SDLC para identificar y abordar posibles riesgos de seguridad, vulnerabilidades y deficiencias arquitectónicas antes de escribir el código (una “Revisión de Seguridad del Diseño”) con controles preventivos y detectivos que se alineen con los estándares de la industria como OWASP.
2. Se deben hacer cumplir las prácticas de cifrado seguro.
3. El Proveedor debe incorporar controles de seguridad de la información en sus procesos y procedimientos para la selección, el desarrollo y la implementación de aplicaciones, productos y servicios.
4. El Proveedor debe contar con un procedimiento seguro de creación para todos los sistemas donde se almacene, procese y/o transmita Información de Citi, y debe mantener una imagen o plantilla segura para todos los sistemas.

17.35 Controles contra Malware

El Proveedor debe asegurarse de que se implementen los controles necesarios para prevenir y detectar la introducción de cualquier código malicioso (p. ej., virus, gusanos, virus troyanos, adware, spyware, ransomware u otros ataques cibernéticos similares en los que se puedan comprometer los datos). El Proveedor debe:

1. Implementar, actualizar y mantener tecnología de 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 datos de Citi.
2. Desplegar configuraciones de seguridad para evitar que los usuarios finales desactiven las herramientas de antivirus/antimalware y los análisis programados.
3. Disponer de procedimientos automatizados y gestionados de forma centralizada para configurar y actualizar el software antivirus y antimalware.
4. Garantizar que se implementen procesos para identificar y abordar las computadoras que incumplen con las reglas donde las firmas del antivirus o los motores de análisis están desactualizadas.
5. Controlar el acceso a puertos/interfaces de comunicación que permiten la conexión a dispositivos externos incluidos, entre otros, medios de almacenamiento.

17.36 Controles contra Código Móvil

Los Proveedores deben garantizar la implementación de controles en torno a las prácticas seguras de código móvil. Cuando se autoriza el uso del código móvil, la configuración debe, como mínimo, cumplir con todos los estándares relevantes 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:

1. El código móvil publicado por el Proveedor debe ser firmado por una Autoridad de Certificación aprobada por Citi y el ciclo de vida del certificado debe ser administrado por el Proveedor en cuanto a su vencimiento o rotación.
2. El código móvil firmado con certificados vencidos debe ser retirado de producción.

17.37 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 mantengan rastros de auditoría a nivel de infraestructura o aplicación para registrar los siguientes elementos:

1. Acciones relevantes de seguridad de infraestructura para la plataforma asociada

2. Todas las alarmas del sistema asociadas con un firewall o evento de seguridad generado por IDS/IPS
3. Todos los intentos de violación de la seguridad del sistema (p. ej., intentos fallidos de inicio de sesión de Usuario)
4. Intentos no autorizados de acceder a los recursos (software, datos, procesos, etc.)
5. Acciones del administrador
6. Información relacionada con la recepción de información específica de un usuario u otro sistema
7. 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 Confidencial o PII Sensible
 - c. Actualizaciones en datos Restringidos
 - d. Actualizaciones en datos de Autenticación
8. Todas las sesiones establecidas
9. Los artefactos de sesión, como la identificación única del dispositivo, deben capturarse, cuando sea técnicamente posible, y registrarse para las aplicaciones de cara a Citi (es decir, websites y aplicaciones móviles) para respaldar las investigaciones de fraude. Estos artefactos deben contener al menos direcciones IP. 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.
10. Los rastros de auditoría deben documentar la atribución de una actividad específica a una persona específica para evitar el rechazo.
11. Se deben registrar los eventos Significativos de Administración de Seguridad de la Información (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 Sistemas de Información Controlados
 - d) Restablecimiento de contraseñas
 - e) Cambios en la configuración de seguridad del sistema
 - f) 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:
 - I. Fecha y hora del evento (hora en formato UTC)
 - II. Identificación de Usuario de la persona que realiza la acción
 - III. Tipo de evento
 - IV. Activo o nombre de recurso afectado
 - V. Tipo de acceso (eliminar, modificar, etc.)
 - VI. Éxito o falla del evento
 - VII. Origen (terminal, puerto, ubicación, IP, nombre de host, etc.)

17.38 Protección de la Información de Registro

El Proveedor debe asegurarse de que se implementen controles de acceso para preservar la integridad de los rastros de auditoría durante el inicio, el cierre, el almacenamiento y la transmisión.

1. 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 rastreando.
2. El Proveedor debe proporcionar a Citi un procedimiento de retención de registros para los datos de registro que defina cómo se mantienen los datos e incluya medidas de cumplimiento que hagan referencia a todos los requisitos legales y regulatorios aplicables.
3. 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.

17.39 Monitoreo del Uso del Sistema

El Proveedor debe asegurarse de que los siguientes eventos se capturen, registren y revisen directamente o mediante un proceso de revisión automatizado:

1. Todas las alarmas del sistema asociadas con un evento generado por un firewall o un Sistema de Detección de Intrusiones (IDS)/Sistema de Prevención de Intrusiones (IPS).
2. Todas las actualizaciones de recursos críticos, tal como se identifican en el procedimiento de creación estándar seguro.
3. Toda actividad interactiva realizada por cualquier identificación (funcional, privilegiada, de sistema, temporal, etc.) con acceso a información clasificada como PII Confidencial o de nivel superior.
4. Eventos de ISA significativos enumerados en la sección anterior de registro de Auditoría con la siguiente excepción:
 - a) Eliminación de autorizaciones de usuario, rol o perfil cuando la actividad de Administración de Seguridad de la Información sea ejecutada por un sistema de ejecución o flujo de trabajo automatizado que tenga controles de integridad de extremo a extremo.

17.40 Correlación y Revisión de Registros

1. Cuando un evento registrado activa una alerta, se revisa dicho evento y el Proveedor debe tomar medidas de seguimiento y llevar a cabo una investigación si hay indicios de que es posible que haya ocurrido un incidente potencialmente perjudicial relacionado con la seguridad de la información.
2. 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.
3. Los Proveedores deben revisar y ajustar periódicamente la configuración de su SIEM o herramienta de análisis de registros para mejorar la identificación de eventos procesables.

17.41 Control de Software Operacional

El Proveedor debe asegurarse de que solo se utilicen los sistemas operativos y el software que actualmente sean compatibles con un proveedor comercial aceptado por la industria o que de forma activa y adecuada lancen parches y actualizaciones de configuración para abordar los problemas de seguridad.

El Proveedor debe asegurarse de que se implemente un proceso documentado que especifique los plazos de remediación dentro de los cuales se aplican todas las configuraciones y parches de seguridad aprobados.

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 permita el uso de versiones de software no compatible con vulnerabilidades conocidas y que dicho software sea actualizado y parcheado según sea necesario de manera oportuna.

El software de aplicación usado para procesar Información de Citi debe adquirirse de Proveedores establecidos y debe tener licencia, estar catalogado y contar con soporte.

17.42 Gestión de Vulnerabilidades y Amenazas

1. El Proveedor debe implementar un proceso de gestión de vulnerabilidades y amenazas que aborde y/o incluya de manera integral todo lo siguiente:
 - a. Herramientas y procedimientos para el descubrimiento y la gestión de vulnerabilidades en todos los recursos de información que pueden usarse para procesar, almacenar, transmitir o acceder a la Información Confidencial o de nivel superior de Citi.
 - b. Un requisito de que los análisis se realicen al menos semanalmente usando herramientas de vulnerabilidad reconocidas por la industria y metodología de generación de informes.
 - c. Clasificación de vulnerabilidades de acuerdo con la versión más actual del “Common Vulnerability Scoring System (CVSS)” (ver <https://www.first.org/cvss>), con plazos de remediación basados en la gravedad.
 - d. Un requisito de probar correcciones de vulnerabilidades antes de la implementación total en producción.
 - e. Un proceso operacional documentado y repetible para acelerar la resolución de vulnerabilidades críticas.
 - f. El Proveedor debe hacer un seguimiento de los activos a lo largo de su ciclo de vida con soporte para prepararse para los estados al Final de su Vida Útil (EOL) o al Final del Soporte del Proveedor (EOVS), y contar con procesos para actualizar o reemplazar dichos activos de manera proactiva.
 - g. Cualquier vulnerabilidad crítica identificada mediante recopilación de inteligencia, análisis de vulnerabilidades o pruebas de penetración debe priorizarse y solucionarse dentro de un plazo bien definido acorde al riesgo de la vulnerabilidad.

17.43 Aplicaciones Alojadas por Terceros

Si el Proveedor mantiene o almacena Información Confidencial o datos más sensibles de Citi en un website o sistema accesible por Internet, o un website con la marca de Citi, 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:

1. Designar a un empleado del Proveedor para responder a las consultas de Citi sobre seguridad de la información.
2. Utilizar las mejores prácticas reconocidas por la industria para monitorear, con frecuencia no menor a semanal, fuentes acreditadas de información sobre vulnerabilidades de seguridad informática, como FIRST, CERT/CC, el Catálogo de Vulnerabilidades Explotadas Conocidas de la CISA 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.
3. Probar, al menos trimestralmente, la implementación de sus medidas de seguridad de la información utilizando herramientas de análisis de vulnerabilidades de redes, sistemas y aplicaciones y/o pruebas de penetración.
4. Permitir que Citi o un tercero aprobado por Citi realicen, en intervalos de tiempo razonables, evaluaciones de vulnerabilidad, piratería ética u otras evaluaciones de seguridad con el fin de verificar el cumplimiento por parte del Proveedor de 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, análisis 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.
5. Todo contratista que preste al Proveedor servicios de evaluación de vulnerabilidades debe ser de la lista aprobada por Citi de proveedores de evaluación de vulnerabilidades. Cuando el Proveedor utilice contratistas o subcontratistas para prestar los Servicios, el Proveedor deberá, a sus expensas, garantizar que las evaluaciones de vulnerabilidades requeridas se completen de la misma manera oportuna como si el Proveedor estuviera prestando dichos Servicios directamente y deberá garantizar que el requisito de que cualquier contratista o subcontratista facilite dichas evaluaciones se incluya en el acuerdo entre el Proveedor y el contratista/subcontratista correspondiente al Servicio, incluyendo la redacción que autoriza a Citi a realizar dichas evaluaciones.
6. **Notificación.**
 - a) Cuando el Proveedor identifique una vulnerabilidad que involucre un producto o servicio que afecte a Citi, el Proveedor debe notificar a Citi por escrito dentro de las 24 horas posteriores a la identificación e

incluirá una descripción de las acciones correctivas que tomará el Proveedor.

- b) 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 del 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 24 horas siguientes a dicha publicación. Cada notificación incluirá información sobre la vulnerabilidad, la utilidad del sistema para los servicios relacionados con Citi (es decir, si aloja información de Citi o se utiliza para la prestación de servicios, o ambas cosas), si puede explotarse de forma remota; y la puntuación de Vulnerabilidades y Exposiciones Comunes (CVE). El Proveedor continuará proporcionando 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.

- 7. **Medidas Correctivas.** 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 del riesgo en función del Sistema de Puntuación de Vulnerabilidades Comunes (CVSS) como se establece en el Apéndice A aplicable (ver <https://www.first.org/cvss>). Una vez que las partes hayan asignado y acordado un nivel de riesgo, el Proveedor corregirá cualquier vulnerabilidad media, alta o crítica identificada. Siempre que sea posible, la corrección de cualquier vulnerabilidad 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, 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.

17.44 Controles de Red de Seguridad de Comunicaciones

- 1. 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 puntos cumplimiento de la red.

- a. 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. Las redes usadas para acceder, almacenar, gestionar, procesar y/o transmitir Información de Citi usando Redes de Área Local Inalámbricas (WLAN) u otras soluciones de dispositivos inalámbricos que incluyen controles razonables para prohibir el acceso no autorizado (PEAP-TLS, EAP-TTLS, etc.) pueden conectarse a redes que contienen Información de Citi.
 - b. Todas las conexiones de IP externas a la red global del Proveedor están protegidas por un firewall administrado por el Proveedor.
 - c. 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 la red del Proveedor donde se accede, administra, almacena, procesa o transmite la Información de Citi.
2. Para todas las aplicaciones de Internet con la marca de Citi, el Proveedor debe garantizar que:
- a. Todos los servicios alojados en los sitios del Proveedor estén protegidos por servicios antiDDoS (Denegación de Servicio Distribuido) aprobados por Citi o controles comparables validados por Citi.
 - b. Los sistemas de seguridad "firewall" externos deben estar configurados con una regla de denegación por defecto. Las reglas del sistema de seguridad "firewall" deben configurarse según el principio de privilegios mínimos y deben registrarse todos los intentos de conexión denegados por el firewall (p. ej., pérdida de paquetes).
 - c. El tráfico de comunicaciones de red debe denegarse por defecto y permitirse por excepción en las interfaces gestionadas. Las excepciones deben estar muy limitadas a fuentes, destinos y servicios específicos.
 - d. El tráfico de las aplicaciones web debe contar con controles adecuados y ser filtrado, por ejemplo, mediante cortafuegos de aplicaciones web (WAF).

17.45 Segregación en Redes

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 accedan a través de la zona desmilitarizada del Proveedor (DMZ).

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 (p. ej., filtrado de puertos durante un ataque de virus).

El personal de Acceso Remoto y Seguridad de Host debe implementar controles de acceso basados en grupos (p. ej., 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.

17.46 Identificación de Equipos en Redes

Las plataformas tecnológicas deben identificar y autenticar las plataformas tecnológicas de pares de acuerdo con los niveles de riesgo de IS de la interacción y otros controles de mitigación.

1. Solo los dispositivos del Proveedor (es decir, hardware, incluidas las computadoras de escritorio y portátiles, entre otros) 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 Información de Citi.
2. 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.

17.47 Análisis y Especificación de Requisitos de Seguridad

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.

17.48 Transacciones en Línea

1. Cuando corresponda, el Proveedor debe tener Sistemas de Información que usen contraseñas dinámicas o certificados digitales para validar las credenciales.
2. Todos los certificados de entidad final deben reemplazarse al menos una vez cada 13 meses.
3. Todas las aplicaciones del Proveedor que almacenen, procesen, administren o accedan a información de Citi, alojen aplicaciones de Internet con la marca de Citi o tengan conectividad a los recursos de red de Citi deben:
 - a. Utilizar un método de autenticación basado en los tipos de datos/funciones a los que se accede;
 - b. Realizar una evaluación de cumplimiento de la Autenticación de Múltiples Factores (MFA) e implementar recomendaciones, según sea necesario;
 - c. Realizar una evaluación de incorporación de Monitoreo de Actividades Sospechosas (SAM) e implementar recomendaciones, si es necesario;
 - d. En todos estos casos, el Proveedor debe comunicarse con su principal contacto comercial para conocer los requisitos vigentes de Citi.

17.49 Procedimientos de control de cambios

1. El proveedor debe asegurarse de que los cambios de configuración en los sistemas de seguridad "firewall", 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.

2. El acceso otorgado a producción mediante identificaciones temporales debe ser registrado y monitoreado para hacer un seguimiento de los cambios realizados en el entorno.
3. Para Sistemas de Información Controlada que contengan Información del Cliente clasificada por Citi como Confidencial o de nivel superior o con 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 17.32 (Registros de Auditoría). Las revisiones pueden utilizar una metodología apropiada de muestreo basada en el riesgo.
4. La revisión debe validar que los cambios que forman parte del acceso privilegiado temporal se realizaron según lo previsto.
5. El Proveedor debe documentar todos los cambios, incluso almacenar evidencia del proceso de revisión.

17.50 Fuga de Información

El Proveedor debe tener implementado un estándar de cifrado seguro documentado que evite la fuga de información, que incluya:

1. Información detallada del sistema (p. ej., tecnología y tipo de servidores);
2. Rastros de la pila y errores de excepción que revelen la estructura de árbol de directorios y el tipo de base de datos subyacente.

17.51 Datos de Prueba

La información Confidencial o de nivel superior, 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 el Proveedor debe implementar controles de producción en tiempo real en los entornos de desarrollo y prueba.

17.52 Aceptación del Sistema

El Proveedor debe contar con procesos documentados de Gestión del Alcance del Proyecto y Aceptación de Sistemas que cumplan con los estándares pertinentes de la industria.

17.53 Reporte de Debilidades en la Seguridad de la Información

El Proveedor debe tener un Proceso para asegurar que las vulnerabilidades de aplicaciones e infraestructura que puedan comprometer los recursos de información de Citi **se informen de inmediato a Citi.**

17.54 Responsabilidades y Procedimientos de Incidentes de Seguridad

1. Un SIRT es un evento de seguridad que compromete cualquiera de los siguientes, independientemente de cómo o dónde haya ocurrido el incidente de seguridad, o quién pueda haber causado el compromiso:

- La Confidencialidad, Integridad o Disponibilidad de los datos de Citi.

- La Confidencialidad, Integridad o Disponibilidad de cualesquiera datos (incluida la Información Personal) para los cuales Citi está sujeto a obligaciones contractuales, legales o regulatorias.
 - La Integridad o Disponibilidad de los sistemas de información de Citi que almacenan, procesan o transmiten cualesquiera datos de Citi.
2. Para nuestros fines, un compromiso de la confidencialidad se refiere a la exposición de datos a una persona no autorizada, o a escenarios en los que Citi pierde la custodia y el control de los datos. Se requiere que todos los incidentes de seguridad se reporten de inmediato.
 3. Si el Proveedor ha experimentado un SIRT, el Proveedor debe cooperar con Citi para proporcionar la información solicitada por Citi de conformidad con los propios procesos de respuesta a incidentes de Citi, analizar los datos comprometidos de una manera suficiente para permitir que Citi cumpla con los requisitos legales, regulatorios y/o de gobernanza internos; realizar cualquier notificación requerida conforme a las leyes, reglas o regulaciones o bien solicitada por Citi a su discreción y a solicitud de Citi y a expensas del Proveedor, y solo después de que Citi haya tenido la oportunidad de revisar y enmendar la redacción de la plantilla de notificaciones propuesta; y el Proveedor no debe nombrar a Citi en ninguna de dichas notificaciones a menos que Citi solicite específicamente por escrito que se le nombre.

17.55 Protección de Fugas de Datos (DLP)

El Proveedor debe implementar controles de prevención de fuga de datos (DLP), incluido el monitoreo de contenido y punto final que cubra a todo el personal con acceso a datos Confidenciales o de nivel superior de Citi.

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 su red a través de los siguientes canales:

- a. Correos electrónicos no cifrados
- b. Archivos adjuntos de correos electrónicos cifrados
- c. Impresión de datos de Citi
- d. Transferencias de datos de Citi a ubicaciones fuera de su red (por ejemplo, a través de FTP).
- e. 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. Este privilegio debe prevenirse por defecto.
- f. 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 desde su red hacia otros destinos. Este privilegio debe prevenirse por defecto.
- g. Cargar datos de Citi a sitios web externos, incluyendo SaaS/sitios de intercambio de archivos. Este privilegio debe prevenirse por defecto.

17.56 Navegación Web

1. El Proveedor debe contar con controles de acceso web para evitar el intercambio de información Confidencial o de nivel superior de Citi y la exposición a malware o ataques para aquellos empleados con acceso a los datos de Citi.
2. Para los Proveedores 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, IA generativa, 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 actualice con regularidad; todas las URL no categorizadas deben bloquearse por defecto o todas las URL deben bloquearse por defecto y aprobarse según el caso.
 - f. Los Navegadores Web utilizados por el Proveedor deben ser totalmente compatibles y estar al día con las actualizaciones de seguridad más recientes por parte del proveedor de software.

17.57 Mensajería Electrónica

La mensajería instantánea, las redes punto a punto u otras herramientas colaborativas de Internet no se pueden usar para transmitir o almacenar Información de Citi hacia fuera de la red del Proveedor o desde redes que contienen Información de Citi, a menos que se aplique el cifrado apropiado para todos los datos de Citi según la Sección 17.9 (Política sobre el uso de controles criptográficos).

17.58 Correo Electrónico

El Proveedor debe contar con controles de correo electrónico a fin de evitar el intercambio de Información de Citi y la exposición a malware o ataques. Esto incluye:

1. Los archivos adjuntos entrantes que ingresan en el portal del correo electrónico se escanean y bloquean si suponen un riesgo para el sistema.
2. Se use software de filtrado de correo electrónico (antispam, antiphishing) que está actualizado.
3. Cualquier dato Confidencial o de nivel superior de Citi debe cifrarse cuando se envíe fuera de la organización del Proveedor.
4. 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.

17.59 Medios Extraíbles

1. El Proveedor debe proteger la Información de Citi independientemente del medio en el que se mantenga. Este estándar se aplica, entre otros, a los siguientes tipos de medios en los que se almacena 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.
2. 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.
3. 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. La gerencia debe inventariar los medios extraíbles. Los medios extraíbles que contengan datos de Citi Confidenciales o de nivel superior deben cifrarse automáticamente sin que se exija ninguna acción por parte del usuario.

17.60 Eliminación de Medios

1. Cuando la Información de Citi clasificada como Confidencial o de nivel superior sea elegible para su eliminación de acuerdo con las instrucciones establecidas por Citi (es decir, en el momento en que la información ya no sea necesaria o útil para Citi, o luego de que cualquier periodo adicional de conservación exigido por las leyes, regulaciones y/o políticas de Citi haya expirado), el Proveedor debe destruir dicha Información de modo que resulte inutilizable e irrecuperable.
2. 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 de los medios.
 - b. Desmagnetizar los medios (si corresponde).
3. Destruir los medios físicamente para hacerlos ilegibles (es decir, trituración, destrucción de las unidades).
4. 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 deben poder ser abiertas por el personal autorizado.
 - a. Las copiadoras, impresoras, máquinas de fax y cualquier otro dispositivo que tenga memoria/almacenamiento que pueda contener

información Confidencial o de nivel superior de Citi también deben desinfectarse.

17.61 Gestión y Capacitación en Seguridad de la Información

1. Mantener un programa apropiado de educación y concientización sobre 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 o de nivel superior y el informe de incidentes de seguridad y la gestión de respuestas.
2. 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 de la organización según sea relevante para la función de su puesto de trabajo.
3. El Proveedor debe asegurarse de que el programa de capacitación y concientización se revise y actualice anualmente para abordar los riesgos y amenazas emergentes, las mejores prácticas actuales y las nuevas tecnologías en el panorama de la ciberseguridad.
4. Como mínimo, es necesario incluir los siguientes temas:
 - b. Etiquetado y manejo de la información
 - c. Transmisión segura (correo electrónico seguro, almacenamiento seguro en SharePoint, no enviar datos propiedad de Citi a correos electrónicos personales)
 - d. Reporte de incidentes de seguridad de la información
 - e. Lugar de trabajo seguro (p. ej., uso apropiado de Internet, software no autorizado, prohibiciones sobre la descarga de software no aprobado)
 - f. Gestión de contraseñas (p. ej., contraseñas fuertes, prohibición de compartir contraseñas)
 - g. Ingeniería social (p. ej., phishing, spear phishing, vishing, SMiShing)
 - h. Trabajo remoto (p. ej., conexión protegida/segura, seguridad de dispositivos personales)
5. A los empleados del Proveedor se les debe asignar la capacitación antes o en el momento de obtener acceso a los sistemas que alojan los datos de Citi y deben completarla antes de la fecha límite indicada en la notificación de asignación.
 - a. La capacitación en Seguridad de la Información debe impartirse a todo el personal al menos una vez al año, siempre que lo permita la ley.
6. La capacitación debe incluir una manera para registrar la medida de su efectividad (p. ej., un cuestionario una vez completada con un umbral para aprobar/reprobar) siempre que lo permitan las leyes locales.

17.62 Programa de Gestión de Riesgos Cibernéticos

El Proveedor también deberá mantener un programa adecuado de gestión de riesgos cibernéticos que incluya, como mínimo, lo siguiente:

1. Mantener un programa bien definido y documentado de Gestión de Riesgos de Seguridad de la Información y/o un programa de gestión de riesgos operacionales que tenga un componente de gestión de riesgos cibernéticos/de información claramente definido, que defina el apetito de riesgo cibernético del Proveedor y asegure que su riesgo cibernético residual se alinee con ese apetito.

2. Mantener un sólido programa de gestión de riesgos de seguridad que incluya, entre otros, la recopilación y/o la realización de auditorías y revisiones de seguridad que evalúen el estado general de la seguridad dentro de la organización y reporte al menos una vez al año a su liderazgo ejecutivo para fines de revisión y garantía de que no se ha violado el apetito de riesgo cibernético del Proveedor.
3. Mantener el cumplimiento de cualquier Estándar de Seguridad de los Datos de PCI (PCI-DSS) aplicable al Proveedor cuando el Proveedor procesa, almacena y/o transmite transacciones, pagos y/o información de tarjetas de crédito/débito.
4. Mantener un plan y guía para la gestión de crisis y un Plan del Equipo de Respuesta a Incidentes de Seguridad 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.

17.63 Seguridad de Aplicaciones, API, Código, Sistemas e Infraestructuras

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.

17.64 Seguridad Móvil

Cuando el Proveedor proporciona una solución de aplicación móvil, el Proveedor debe cumplir con los siguientes requisitos:

1. La aplicación móvil debe ser compatible únicamente con las versiones generalmente disponibles (GA)/estables y que no estén al final de su vida útil (EOL)² de las plataformas Google Android (excepto Android Go) y/o Apple iOS/iPadOS. Si la solución móvil está equipada con soporte para otros sistemas operativos, los sistemas operativos/versiones compatibles deberán ser configurables por Citi.
2. La solución móvil no debe ser compatible con plataformas/dispositivos móviles que no estén equipados con conjuntos de instrucciones regulares para trabajar con algoritmos criptográficos que incluyen, pero no se limitan a,

² Versiones del producto que cuentan con soporte activo y reciben actualizaciones regulares de seguridad y mantenimiento por parte del propietario de la plataforma o del Proveedor.

cifrado como se especifica en la Sección 17.9 (Requisitos de Cifrado) de este documento.

3. Las versiones del sistema operativo en fase de preproducción, incluidas, entre otras, las versiones/lanzamientos beta, de acceso anticipado y de vista previa de funciones, no están permitidas en el entorno de producción.
4. El Proveedor debe poder proporcionar una lista de los componentes integrados de terceros que incluya, entre otros, bibliotecas de software libre y de código abierto que son agrupadas/aprovechadas por la solución móvil.
5. La aplicación móvil debe cumplir con los requisitos y las mejores prácticas que permiten que las aplicaciones móviles se publiquen a través de tiendas de aplicaciones públicas, como la Apple App Store o Google Play Store. Las tiendas de aplicaciones públicas que se listan a continuación deberán ser el método preferido y principal para distribuir/publicar la aplicación móvil.
6. Las aplicaciones móviles Android deben aprovechar el esquema de firmas APK v2+. No se debe usar el esquema de firmas APK versión 1 (también conocido como firma JAR).
7. El tipo y la longitud de la clave de firma de la aplicación móvil deben cumplir con la sección 17.9 - Requisitos de **Cifrado** de este documento.
8. Cada clave de firma de la aplicación y el certificado X.509v3 asociado deben gestionarse individualmente y dedicarse a un solo ID de aplicación/ID de paquete. La(s) clave(s) de firma no deben compartirse entre las aplicaciones.
9. Si una aplicación móvil requiere retención de datos en el dispositivo móvil, debe retener solo los datos más recientes en el dispositivo que sean necesarios para los fines de la aplicación/el servicio, o siempre que se requiera conforme a requisitos legales/o regulatorios.
 - a. La recopilación, el procesamiento y/o el almacenamiento de datos de usuarios deben cumplir con las leyes locales, incluidas, entre otras, las regulaciones de privacidad, como el Reglamento General de Protección de los Datos (GDPR) y la Directiva 2002/58/CE (Privacidad Electrónica) o sus equivalentes regionales.
 - b. Los componentes integrados de terceros (p. ej., bibliotecas) no deben recopilar, procesar ni almacenar datos de usuarios.
10. Las aplicaciones móviles no deben permitir que ningún dato de la aplicación sea accesible para todo el público.
 - a. Si se requiere compartir datos con otras aplicaciones, las aplicaciones deben aprovechar técnicas, métodos y controles comercialmente razonables para que los respectivos sistemas operativos compartan solo la cantidad necesaria de datos con el número mínimo de otras aplicaciones cuando dicho intercambio de datos esté debidamente justificado y documentado.

11. Las aplicaciones móviles deben basarse únicamente en facilidades de comunicación seguras proporcionadas por los respectivos sistemas operativos móviles. P. ej.,
 - a. Las aplicaciones para Android deben declarar explícitamente que no se permite un tráfico de red inseguro hacia ningún dominio de red en su manifiesto de la aplicación y/o archivo de configuración de red.
 - b. Las aplicaciones para iOS/iPadOS deben aprovechar la Seguridad del Transporte de Aplicaciones (ATS) sin ninguna excepción.
12. Los materiales criptográficos deben estar unidos a un almacén de claves seguro con respaldo de hardware.
13. Las aplicaciones móviles deben desarrollarse en modo de lanzamiento y no deben contener:
 - a. Ninguna característica o método que pueda omitir controles de seguridad,
 - b. Información de Debug, como nombres de archivos de código fuente, nombres de variables, nombres de símbolos, comentarios etc., que tengan el potencial de facilitar la ingeniería inversa.
14. Las aplicaciones móviles deben estar equipadas con mecanismos antienganche o antimanipulación efectivos para evitar la inyección de código malicioso que podría alterar o monitorear el comportamiento de la aplicación en su tiempo de ejecución.
15. Las aplicaciones móviles deben implementar técnicas integrales de antidebugging o antiingeniería inversa/ofuscación para obstaculizar los ataques de ingeniería inversa.
16. Los paquetes de aplicaciones móviles deben estar equipados con una capacidad que permita verificar la autenticidad e integridad de su contenido (p. ej., usando checksum criptográfico y/o firma digital).
17. Si la aplicación móvil requiere autenticación del usuario, las revisiones de la integridad de la aplicación y/o el dispositivo deben completarse antes de que comience la autenticación del usuario.
18. Las aplicaciones móviles que acceden/procesan/almacenan cualquier información propiedad de Citi con una clasificación de Citi de Confidencial o de nivel superior y/o cuya clasificación de riesgo de Seguridad de la Información sea Media o superior deben utilizar solo modalidades biométricas sólidas (p. ej., cumplir o superar la categoría de Clase 3/Fuerte como se define en el correspondiente [Android Compatibility Definition Document](#)).
19. Las aplicaciones móviles deben implementar contramedidas para protegerse contra ataques de Hombre en el Medio (MitM).
20. Las aplicaciones móviles deben poder detectar dispositivos comprometidos que incluyen, entre otras cosas, dispositivos móviles con modificaciones “jailbreak” o “rooting” y reaccionar de acuerdo con la evaluación de riesgos del negocio y los requisitos regulatorios.
21. Las aplicaciones móviles deben implementar una fuerte vinculación con el dispositivo para evitar que el token del software (p. ej., prueba de posesión) sea clonado.

22. Las aplicaciones móviles deben usar aplicaciones/soluciones de teclado seguras (p. ej., las incorporadas/preinstaladas por los sistemas operativos móviles).
23. Las notificaciones instantáneas no deben contener ninguna información confidencial (p. ej., información de Citi clasificada como Confidencial o de nivel superior). Sin embargo, la contraseña por única vez (OTP) puede distribuirse a través de una notificación instantánea.
24. Las soluciones de aplicaciones móviles deben estar equipadas con una capacidad para rechazar/ignorar intentos de comunicación con clientes móviles que usan una o más versiones de aplicaciones con vulnerabilidades conocidas/explotables.
25. Las aplicaciones móviles deben cumplir con las mejores prácticas de la industria incluyendo, entre otras cosas, las técnicas de prevención publicadas en el [OWASP Mobile Top 10](#).
26. Las aplicaciones móviles que aprovechan las técnicas de inteligencia artificial y aprendizaje automático (IA/ML) deben hacerlo de manera ética y conforme a la Sección 19 - **Error! Reference source not found.** (incluyendo la IA Generativa/IA Agéntica).
27. La aplicación móvil debe aprovechar los permisos mínimos del dispositivo que se requieren para realizar los propósitos o funciones que aprovecha Citi.
28. Las aplicaciones móviles no almacenarán ninguna información no pública en almacenamiento externo/extraíbles, como las tarjetas SD.**Error! Reference source not found.**

17.65 Divulgación de Software

El Proveedor divulgará todos y cada uno de los componentes, incluidos, entre otros, los softwares de código abierto contenidos en los productos o servicios proporcionados a Citi (en conjunto, los "Componentes de Software"). El Proveedor no incorporará, a través de una actualización, mejora o de otro modo, ningún Componente de Software en ninguna versión de los productos o servicios que se instalarán en los Sistemas de Citi sin aviso previo a Citi en cada caso. Además, el Proveedor se asegurará de que sus productos o servicios no incluyan Componentes de Software que se use con licencia en virtud de cualquier término que someta a Citi o sus Empresas Afiliadas a cualquier obligación no divulgada y aceptada expresamente por Citi en un Acuerdo. El Proveedor divulgará a Citi cualquier Componente de Software malicioso detectado en la organización, los productos o los servicios del Proveedor dentro de los 30 días posteriores al descubrimiento. Específicamente, el Proveedor divulgará su uso de Componentes de Software en cada versión y lanzamiento de productos o servicios a través de la provisión a Citi de un Listado de Materiales de Software ("SBOM") en el formato de archivo OWASP CycloneDX o el formato de archivo de especificación ISO/IEC 5962:2021 de Intercambio de Datos de Paquetes de Software ("SPDX"). La divulgación del Proveedor debe incluir dónde se originaron los Componentes de Software (p. ej., proveedor comercial, base de datos integrada, administrador de paquete binario público, construido a partir de código fuente, proveedor de Software Integrado o Componentes de Software seleccionado) y si el Proveedor o cualquiera de sus

dependencias de la cadena de suministros de software ha tomado una copia de los Componentes de Software (conocido como “fork”) y posteriormente lo ha incorporado en su producto o servicios como una dependencia del paquete o como código fuente integrado en el código fuente del Proveedor a partir del cual se compilan los productos y servicios.

17.66 Modelado de Amenazas

El Proveedor debe implementar un proceso de modelado de amenazas que aborde y/o incluya de manera integral todo lo siguiente:

1. Definición del Alcance: El Proveedor debe definir claramente el alcance del modelo de amenazas, centrándose en los componentes del software y los flujos de datos que procesan, almacenan o transmiten información Confidencial y superior de Citi.
2. Identificación de Amenazas: El Proveedor debe identificar sistemáticamente posibles amenazas y vulnerabilidades relevantes para el diseño, la arquitectura y el uso previsto del software, tomando en cuenta varios vectores de ataque y actores maliciosos al principio del ciclo de vida del diseño.
3. Análisis de Riesgos: El Proveedor debe analizar las amenazas identificadas para evaluar su posible impacto y probabilidad, lo que permite la priorización de riesgos de seguridad.
4. Operación de Controles: El Proveedor debe definir e integrar controles de seguridad y estrategias de mitigación apropiados para el diseño y desarrollo del software a fin de abordar estos riesgos priorizados.
5. Documentación: El Proveedor debe documentar el modelo de amenazas, incluidas las amenazas identificadas, los riesgos asociados y las medidas de mitigación correspondientes implementadas.
6. Revisión Periódica: El Proveedor debe revisar y actualizar regularmente los modelos de amenazas, particularmente cuando haya cambios significativos en el diseño, la funcionalidad o el entorno de implementación del software.

17.67 Inteligencia Artificial

1. Los Proveedores deben implementar y cumplir un sólido Ciclo de Vida del Desarrollo de Software Seguro (SSDLC) para todos los sistemas y componentes de IA/ML proporcionados a o integrados con Citi. Esto incluye que haya seguridad en el diseño, el desarrollo, las pruebas, la implementación y el mantenimiento continuo.
2. Los sistemas de IA proporcionados por el Proveedor deben demostrar integridad en sus operaciones y mostrar una sólida resistencia a los ataques adversarios. Esto incluye la implementación de mecanismos para la detección rápida de la inyección, la sanitización de la entrada y el mantenimiento del aislamiento de los datos.
3. Los agentes y componentes de IA proporcionados por los Proveedores deben interactuar con los sistemas de Citi y otras herramientas de manera segura. Esto requiere una fuerte gestión de identidades y acceso, una validación estricta de los argumentos de ejecución de la herramienta y el aislamiento de las operaciones de alto riesgo de la herramienta. Se deben incorporar mecanismos de “humano en el bucle” (HITL) para acciones sensibles o de alto riesgo.

4. Los sistemas de IA del Proveedor deben generar registros integrales, inmutables y auditables para todos los eventos significativos. Estos registros deben protegerse de manipulación, combinarse y retenerse conforme a las políticas de Citi. Se requieren capacidades de monitoreo continuo y detección de anomalías para identificar y alertar sobre incidentes y actividades sospechosas relacionados con la seguridad.
5. Los sistemas de IA del Proveedor deben respaldar la supervisión humana basada en el riesgo, permitiendo una intervención apropiada, y diseñarse con una clara responsabilidad sobre los productos y acciones de la IA. Esto incluye clasificar los resultados de la IA por nivel de riesgo y respaldar las capacidades de anulación humana.
6. Todos los agentes, componentes y sistemas de IA proporcionados por los Proveedores deben implementar controles sólidos de gestión de identidades y acceso. Cada interacción de IA debe ser atribuible a una identidad identificable (humana o no humana), con la autenticación requerida para todo acceso. Los agentes de IA deben usar identidades gestionadas y seguir los principios de mínimo privilegio al acceder a los recursos de Citi.
 - a. Los Proveedores deben facilitar y garantizar que a todos los agentes de IA se les asignen identidades de agentes de la Red de Identidades de Objetos de Citi (COIN), federados con los sistemas de Gestión de Identidades y Acceso (IAM) de Citi, para permitir la aplicación de políticas de seguridad de Citi, gestión centralizada de identidades y auditoría.
 - b. Los Proveedores deben incorporar agentes externos al COIN usando mecanismos de integración aprobados por Citi, incluida la API de COIN disponible a través de puertas de enlace seguras (como SSG Gateway o Apigee), y deben garantizar que dicha incorporación se lleve a cabo de manera segura de acuerdo con los requisitos de seguridad aplicables de Citi.
 - c. Los Proveedores, si están alojados internamente, deben generar su token que se alinee con el COIN; los Proveedores alojados externamente y que autenticuen los entrantes con su propio token federado deben tener un token de intercambio compatible con tokens de Citi, por ejemplo, intercambiando de MSFT a tokens de COIN. Cualquier tipo de token nuevo que actualmente no sea respaldado a través de la bolsa de tokens debe ser revisado para su aprobación por el equipo de IAM en Citi.
7. Cuando los Proveedores utilizan o proporcionan servidores o clientes de Protocolo de Contexto Modelo (MCP), deben implementar el MCP RFC 7591 incluyendo todas las características opcionales.
8. Los sistemas de IA del Proveedor deben proteger las indicaciones del sistema y los trabajos internos de la divulgación o manipulación. La gestión del contexto debe hacer cumplir límites estrictos para evitar la fuga de datos entre tenants, usuarios o entornos.
9. Los Proveedores deben tener procedimientos documentados para detectar, responder y reportar incidentes de seguridad específicos de IA, incluidos ataques adversarios, manipulación de modelos, acciones de IA no

autorizadas o vulneraciones de datos que involucren sistemas de IA. Citi debe ser notificado inmediatamente de dichos incidentes.

18 PAUTAS PARA UN LUGAR DE TRABAJO SEGURO

Aplicable a Proveedores que acceden/procesan/administran/almacenan Información de Citi Y/O Alojamiento 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 (p. ej., de acuerdo con las licencias, términos y condiciones aplicables) y luego solo con respecto a los fines comerciales de Citi y de los Proveedores de 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 malversación o la divulgación no autorizada de recursos 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 recursos de Citi también es un incumplimiento de su obligación con Citi.

Elemento	Requisitos
Información de Citi (documentación electrónica e impresa)	La Información de Citi se debe guardar debidamente y bajo llave después del horario laboral normal y toda vez que el Proveedor se aleje de su espacio de trabajo designado.
Computadoras de Escritorio (PC) y Portátiles	Las computadoras de escritorio y portátiles usadas para ver cualquier Información de Citi o acceder a esta deben protegerse con contraseñas de protectores de pantalla luego de un periodo de inactividad. Cada vez que el Proveedor se aleje del espacio de trabajo designado, debe bloquear la computadora de escritorio o portátil con las teclas CTRL + ALT + DEL [SUPR] y seleccionar "Lock Computer" (Bloquear el equipo). Si el Proveedor utiliza una computadora portátil para ver Información de Citi, debe asegurarse de que la computadora portátil esté conectada con un cable o candado de seguridad a la unidad base durante el horario laboral y de que se guarde bajo llave de forma segura después del horario laboral normal.
Guardar Bajo Llave	Los archivadores y cajones que almacenan Información de Citi deben cerrarse bajo llave después del horario laboral normal.
Áreas de Oficina Abiertas	Las áreas de oficina abiertas 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.

Elemento	Requisitos
Bandejas de impresoras, fotocopadoras y fax	Todo el material relacionado con Citi debe eliminarse 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 ser triturados o colocados en un recipiente de reciclaje seguro o cerrado con llave. Los medios magnéticos deben eliminarse de forma segura después de seguir los procedimientos de borrado adecuados.

19 INTELIGENCIA ARTIFICIAL/APRENDIZAJE AUTOMÁTICO (INCLUIDA LA IA GENERATIVA/IA AGÉNTICA)

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

19.1 El Proveedor no utilizará, y se asegurará de que ningún Subcontratista no utilice, la IA/ML descrita a continuación, a menos que dicho uso haya sido acordado entre las Partes en el Anexo u Orden de Trabajo aplicable bajo el Contrato:

- a. Utilizado, contenido o incorporado de otro modo en cualquier producto o servicio para el cual están bajo Contrato para proporcionarlo 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
2. 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
3. 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 empresariales no comerciales (p, ej., mantenimiento de registros comerciales, mejoras de procesos, investigación y desarrollo, cumplimiento y auditoría interna).

19.2 El incumplimiento por parte del Proveedor de estas obligaciones se considerará una violación material de los términos de este Acuerdo.

19.3 Si lo solicita un regulador, como parte de cualquier inspección regulatoria o investigación forense sobre el uso de IA/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 de IA/ML.

19.4 También se deben respetar los siguientes principios:

Legalidad. El proveedor de AI/ML deberá cumplir con la Ley Aplicable.

Finalidad y Proporcionalidad. El Proveedor no deberá fusionar el Contenido o la Información de Citi con datos del Proveedor o de terceros. El Proveedor no deberá utilizar el Contenido o la Información de Citi para capacitar a la AI/ML sin la aprobación por escrito de Citi. La AI/ML del Proveedor no deberá utilizar el Contenido o la Información de Citi, salvo en la medida en que sea necesario para prestar los Servicios.

20 QUEJAS DE LOS CLIENTES

20.1 Una Queja es una comunicación oral o escrita, que puede recibirse oralmente (en persona o por teléfono) o por escrito (por correo postal o mediante comunicaciones electrónicas como correo electrónico, mensajería instantánea o redes sociales, etc.), que expresa el descontento de un Cliente, alguien que no es Cliente, un Cliente potencial, un Cliente de Citi, un Cliente potencial o un representante autorizado de un Cliente (colectivamente, “Cliente”) sobre una política, un producto o un servicio de Citi ofrecido por o a través de Citi, un empleado de Citi, un contratista de Citi o un proveedor de servicios externo que actúa en nombre de Citi, o cualquier combinación de los anteriores.

20.2 Los Proveedores deben cumplir con la Política de Gestión de Quejas de Clientes de Citi, así como con cualquier Norma y Procedimiento aplicable de Citi relacionado con las Quejas. El Proveedor notificará por escrito a su contacto comercial principal de Citi (o designado) en un plazo de veinticuatro (24) horas cualquier queja o inquietud (cada una de ellas, una “Queja”) recibida por escrito u oralmente por el Proveedor de cualquier Cliente (o no Cliente o Cliente Potencial, según la definición de Queja de Citi) o de cualquier Regulador en relación con los Servicios prestados por el Proveedor en nombre de Citi, o relacionado de otro modo con Citi. A menos que Citi ponga dicho sistema a disposición del Proveedor, este último también desarrollará, implementará y mantendrá un sistema (“Sistema de Seguimiento”) que sea razonablemente satisfactorio para Citi con el fin de realizar un seguimiento de las Quejas y proporcionar a Citi, a su discreción, una copia de los informes o acceso al sistema. El Sistema de Seguimiento:

- a. clasificará las Quejas por tipo, fecha de recepción y fecha en que se notificó la Queja a Citi;
- b. realizará un seguimiento del proceso de tramitación de la Queja hasta su finalización/resolución; y
- c. atenderá cualquier otra cuestión que Citi pueda solicitar razonablemente. El Sistema de Seguimiento debe estar diseñado para permitir al Proveedor determinar si recibe un número excesivo de Quejas sobre un asunto concreto, de modo que el Proveedor (tras consultar con Citi) pueda determinar si existe un problema sistémico en relación con su negocio o la prestación de sus Servicios y corregir rápidamente los problemas.

21 POLÍTICA DE COMERCIO E INVERSIÓN PERSONAL

La Política de Comercio e Inversión Personal (Personal Trading and Investment Policy, PTIP) de Citi define las actividades de comercio e inversión permitidas y prohibidas, los requisitos de autorización previa y los requisitos relativos al mantenimiento, la divulgación y la supervisión de las cuentas de corretaje o de comercio de una Persona Cubierta. Esta establece estándares mínimos para promover el cumplimiento de las leyes y regulaciones con fines de prevenir el uso inapropiado de la posición o relación de una persona con Citi, incluyendo el conocimiento de dicha persona sobre (1) Información Material No Pública o Información Privilegiada (denominadas colectivamente “MNPI”) relacionada con Citi o un tercero; o (2) información relacionada con las posiciones, transacciones y estrategias de los clientes respecto a títulos valores, derivados y materias primas.

Todo el personal del Proveedor que requiera acceso regular a MNPI como parte de sus responsabilidades laborales en Citi y que esté designado como Persona Cubierta y/o Persona con Acceso a Citi debe cumplir con los requisitos establecidos en el PTIP. El personal del Proveedor debe cumplir con todas las solicitudes de ICRM relacionadas con la divulgación de cuentas personales, la autorización previa de actividades de comercio bursátil personales, las restricciones de comercio bursátil personal y la presentación de estados de cuentas periódicos.

22 ESTÁNDARES DE FACTURACIÓN Y COBRO

En relación con los esfuerzos de Citi por mejorar la puntualidad del servicio y optimizar los controles, todos los Proveedores deberán apoyar los métodos preferidos de Citi para el envío de facturas, así como las opciones preferidas de pago de facturas, tal y como se detalla a continuación:

- El Proveedor creará archivos electrónicos que se transmitirán a Citi en el formato comunicado por este último al Proveedor y/o utilizará la herramienta iSupplier de Citi para ingresar los datos necesarios de facturación/cobro para su posterior transmisión digital a Citi.
- El Proveedor proporcionará a Citi toda la información bancaria necesaria y la documentación justificativa para facilitar el pago electrónico al Proveedor y/o utilizar la opción de pago Tarjeta Virtual de Citi (cuando esté disponible).

Nota: Los plazos de pago se calculan a partir de la fecha en que Citi recibe la factura enviada.

Para pagar a tiempo y cumplir con los compromisos contractuales, Citi exige que todos los Proveedores incluyan los siguientes datos en las facturas y sigan las pautas asociadas al facturar a Citi por bienes o servicios:

1. La entidad comercial de Citi, la dirección de facturación y el nombre del contacto comercial asociado de Citi correctos.
2. Número de Factura, Fecha de Factura y Número de Orden de Compra.
3. Las facturas deben enviarse a la ubicación o dirección de correo electrónico de Citi que se detalla en la orden de compra de Citi.
4. Los bienes o servicios facturados deben detallarse de forma clara y descriptiva en la factura.
5. Incluir únicamente los cargos actuales correspondientes a la factura específica (no incluir otros saldos pendientes de pago de otras facturas).
6. Las facturas deben estar redactadas en inglés, incluida la documentación justificativa.

23 POLÍTICA DE AUSENCIA OBLIGATORIA

La Política de Ausencia Obligatoria (Mandatory Absence Policy, MA) de Citi requiere que las personas que realizan actividades sensibles o de alto riesgo, particularmente aquellas que afectan los libros y registros de la empresa, se alejen periódicamente de estas funciones. Esta separación forzada tiene como objetivo fortalecer los controles internos al crear oportunidades para detectar posibles fraudes, robos u otras conductas indebidas que de otro modo podrían permanecer ocultas. La política se alinea con las expectativas de supervisión establecidas por la Junta de la Reserva Federal de EE. UU. con respecto a las ausencias requeridas para personal en cargos sensibles.

Todo el personal del Proveedor que tenga acceso a datos sensibles y como parte de sus responsabilidades laborales en Citi **y** sea designado como personas “Sensibles” debe cumplir con los requisitos establecidos en la MA policy. Cada año, las personas Sensibles deben programar y completar por completo un Periodo de Ausencia Obligatorio, siguiendo todas las reglas y restricciones de la política. Durante este periodo, no deben realizar, instruir, autorizar o aprobar ninguna actividad sensible, ni deben responder sustancialmente a ninguna comunicación, incluidas las interacciones con los clientes, excepto para redirigir las consultas para su cobertura. Si el periodo de ausencia necesita interrumpirse después de que comience, los gerentes o los contactos del negocio de Citi deben cancelarlo en los sistemas de Cumplimiento para que se restablezca el acceso al sistema, después de lo cual el Trabajador debe reprogramar un nuevo periodo de ausencia.

APÉNDICE - DEFINICIONES

Espacio de Aire (Air-Gap): es una medida de seguridad en la que un sistema, una computadora o una red se separa físicamente de otros sistemas, computadoras 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.

Leyes Aplicables incluye: (a) las leyes y regulaciones 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 Regulaciones sobre Señales de Advertencia) 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. Esto incluye todas las categorías de IA establecidas a continuación, así como variaciones de IA, por ejemplo: IA Generativa, IA Agéntica, Modelos de Lenguaje Grandes, Modelos de IA de Propósito General (GPAI), etc.

Las Categorías de IA incluyen:

- **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.
- **IA Dinámica:** Técnicas que, a diferencia de la “IA Estática”, pueden volver a entrenar automáticamente los parámetros periódicamente, en producción.
- **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.

Aprendizaje Automático (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.

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

Promotor Comercial es un Proveedor contratado por Citi que actúa en nombre de Citi para identificar nuevas oportunidades de negocio o gestionar las relaciones con los clientes existentes.

Regalo Comercial es cualquier objeto de valor (que no sea Entretenimiento Comercial) 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 US \$25 o menos.

Información de Citi es la información propiedad de Citi o que Citi está obligada a proteger durante el almacenamiento, procesamiento, transmisión o eliminación tanto en los formatos digital como no digital.

Las Clasificaciones de la Información de Citi Incluyen:

Confidencial es Información sobre negocios de Citi y/o partes relacionadas que no hace referencia a personas físicas y requiere un alto nivel de protección. El compromiso de la confidencialidad, integridad o disponibilidad de esta información podría tener un impacto grave sobre las operaciones, el estado financiero, la franquicia o los clientes corporativos de Citi.

Información de Identificación Personal (PII) Confidencial es Información Personal sobre una persona que tiene el potencial de facilitar una actividad ilegal, como robo de identidad, fraude de crédito u otro fraude financiero contra dicha persona. El compromiso de la confidencialidad, integridad o disponibilidad de esta información podría tener un impacto significativo sobre las personas, incluyendo, entre otros, pérdidas financieras o fraudes.

- Los elementos de datos personales que, cuando se combinan con otros datos personales, constituyen PII Confidencial incluyen nombres de personas o información de contacto (dirección, teléfono o dirección de correo electrónico) en combinación con:
 - Elementos de datos de transacciones que pueden ocasionar movimientos de fondos, o pueden usarse para cometer robo de identidad o fraude, como:
 - Número de tarjeta de Crédito/Débito
 - Valor de Verificación de la Tarjeta (CVV) o PIN
 - Datos del informe de crédito (puntuación de crédito)
 - Fecha de nacimiento completa
 - Desempeño del trabajador (evaluación/comentarios) o información sobre su remuneración
 - Grabaciones en video, incluso registros de CCTV o cajeros automáticos
- Ciertos elementos de datos personales en forma aislada podrían constituir PII Confidencial:
 - Un número de Seguro Social de EE. UU. o un número de identificación emitido por el Gobierno (que es equivalente en uso y/o estatus de protección legal al número de Seguro Social de EE. UU.), número de pasaporte, número de licencia de conducir o el número de identificación fiscal de una persona.

Interna es Información que no es sobre una persona destinada a fines comerciales y requiere un nivel de protección moderado. El compromiso de confidencialidad, integridad o disponibilidad de esta información podría tener un **impacto limitado** sobre un equipo o grupo de trabajo.

- **Información de Identificación Personal (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, respuestas a preguntas de seguridad); o se relaciona con una persona y que podría ser confidencial (como información médica o de salud personal, número de cuenta, valor de cuenta).
- La Información Personal también incluye la Información de Salud Protegida (según la definición de la Ley de Portabilidad y Responsabilidad del Seguro Médico de EE. UU.), la Información Personal Confidencial y la Información Crediticia (según la definición de diversas leyes de protección/privacidad de los datos y confidencialidad bancaria).

Pública es información que está disponible libremente fuera de Citi o destinada a uso público, como comunicados de prensa de Citi o artículos acerca de Citi que aparecen en las noticias.

Restringida es Información limitada en uso por personas o grupos específicos que es más sensible para Citi o sus empresas afiliadas y requiere el nivel más alto de protección. El compromiso de la confidencialidad, integridad o disponibilidad de esta información podría tener un **grave impacto (en toda la empresa, múltiples regiones, múltiples sectores)** sobre las operaciones, el estado financiero, la franquicia o los clientes corporativos de Citi.

- **PII Sensible** es Información Personal que según leyes específicas necesita protección adicional, que podría usarse para discriminar de manera ilegal o causar de otro modo injusticias o daños a una persona. El compromiso de la confidencialidad, integridad o disponibilidad de esta información podría tener un impacto significativo sobre la persona (incluyendo, entre otros, pérdida financiera, fraude o impacto discriminatorio).
- 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 sobre Salud Personal (PHI) que incluye información sobre el historial médico o la condición mental o física de la persona.

Cliente implica cualquier cliente de Citi y puede incluir individuos (es decir, personas naturales), así como empresas, instituciones, organizaciones y personas jurídicas.

Región de la Nube es una ubicación física donde el Proveedor de Servicios en la Nube agrupa el/los centro(s) 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, entre otros, los siguientes: 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, servicios de mensajería instantánea como mensajes de Microsoft Lync, Skype y Bloomberg, websites 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 Empresas Afiliadas o por o en nombre de sus clientes o proveedores de servicios, (b) creados, producidos a través de los Servicios, o (c) derivados de cualquiera de los anteriores.

Contrato es un documento legal escrito firmado por dos o más partes, que incluye una oferta, aceptación, contraprestación 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, apéndices, 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 del Proveedor a los procesos comerciales de Citi que se pueden recuperar dentro del RTO definido.

La Prueba de Denegación de Servicio (DOS) valida que la aplicación del Proveedor y los componentes de la infraestructura subyacente que respaldan la unidad de negocios de Citi se pueden recuperar dentro del RTO definido.

“Materiales de Depósito” se refiere a las siguientes subsecciones (i)-(vi), en conjunto, con respecto a, según corresponda, el software con licencia de Citi para funcionar dentro del entorno de Citi o los materiales utilizados por el Proveedor para los Servicios alojados prestados a Citi:

- (i) Una versión exacta y duplicada del Código Fuente del software utilizado para el desarrollo, funcionamiento, mantenimiento y soporte del software con licencia o los Servicios Alojados establecidos en el acuerdo aplicable con Citi (y todas las versiones posteriores de dicho software o Servicios Alojados), y toda la Documentación de dicho software (independientemente de si Citi ya cuenta con una copia de partes de dicho Código Fuente) (**“Depósito del Código Fuente”**);
- (ii) El Código Fuente de cualquier software de terceros sobre el que el Proveedor tenga derechos con respecto al desarrollo, funcionamiento, mantenimiento y soporte del software con licencia o los Servicios Alojados;
- (iii) Una copia con licencia de todas las herramientas de software, como depuradores, ensambladores y compiladores, necesarias para convertir el Código Fuente incluido en los Materiales de Depósito en un formato ejecutable, según sea necesario para operar, mantener y dar soporte al software o a los Servicios Alojados;
- (iv) En la medida en que no se haya proporcionado anteriormente, cualquier Documentación que incluya lo siguiente: (A) descripciones generales y operaciones de los Materiales de Depósito; (B) arquitectura y funciones básicas del programa; (C) información sobre el flujo de datos; (D) mapa y listado detallados de la memoria; (E) mapas de puertos de entrada/salida; y (F) cualquier otro detalle que permita a un programador con conocimientos estándar en los lenguajes de programación aplicables utilizar y modificar el Código Fuente incluido en los Materiales de Depósito;

- (v) Toda otra información técnica relacionada con el software o los Servicios Alojados que sea razonablemente necesaria para permitir a Citi, o a un tercero competente en nombre de Citi, utilizar, operar, modificar y mejorar el software o los Servicios Alojados; y
- (vi) Una lista de todo el software y la tecnología de terceros utilizados en relación con el software o los Servicios Alojados, incluyendo detalles razonables con respecto a su uso en el software y la información de contacto del proveedor de dicho software o tecnología. Citi reconoce y acepta que los Materiales de Depósito no contienen ningún código fuente de terceros que no sea el establecido en la subsección (ii); y
- (vii) con respecto a los Servicios Alojados:
 - a. una réplica a escala reducida del entorno de producción alojado en la nube o materiales específicos del entorno relacionados con la nube y cualquier otra información necesaria para replicar el entorno de producción de Citi, incluyendo, entre otros: infraestructura como código, scripts de Terraform, recursos en la nube, plantillas de Cloud Formation, archivos de configuración, tenants en la nube, suscripciones en la nube, imágenes de máquina, imágenes de Docker e infraestructura como código fuente del software; y
 - b. una copia de los datos de Citi almacenados en el software.

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 (Identity and Access Management, 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 la Franquicia/Aplicaciones Críticas de la Franquicia (FCA): son aquellos procesos/aplicaciones que Citi ha identificado como esenciales para la ejecución exitosa de sus Funciones Comerciales Críticas para el Negocio

Fraude es un acto, una declaración errónea o una omisión intencional que tiene como objeto engañar a otros para que la víctima sufra una pérdida o el autor obtenga un beneficio

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, websites, 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.

Datos de Verificación de Identidad (IVD) se define como Preguntas de Seguridad (SQ) o preguntas de Autenticación Basada en el Conocimiento (KBA). Las Preguntas de Seguridad generalmente son definidas por la aplicación y respondidas por el usuario final. Ejemplos son el

apellido de soltera de la madre, el lugar de nacimiento, el helado favorito, etc. Ambos tipos de preguntas deben tratarse como Datos de Autenticación.

Seguridad de la Información o “IS” se refiere al estado en el cual una computadora o un sistema informático está protegido contra accesos no autorizados o ataques y, debido a ese estado, (a) la computadora o el sistema informático continúan disponibles y en funcionamiento; (b) se mantiene la integridad de la computadora o el sistema informático; y (c) se mantiene la integridad y la confidencialidad de la información almacenada en, procesada por o transmitida a través de la computadora o el 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 explotada por una o más Amenazas a la Seguridad de la Información.

No Cliente/No Generador de 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) es un acuerdo entre Citi y un Proveedor, cuyos términos rigen el intercambio, uso y divulgación de Información.

Software de código abierto se refiere a un código fuente o un programa de computadora compilado en el que el código fuente está disponible para el público en general para su uso o modificación a partir de su diseño original.

Personal: significa, ya sea que se indique directamente o se derive del contexto, Proveedor y sus empresas afiliadas, directores, ejecutivos, empleados, agentes, auditores, asesores, proveedores de servicios y contratistas (excluyendo al personal de Citi). El personal del Proveedor también incluye directores, ejecutivos, empleados, agentes, auditores, asesores u otros representantes de cualquier Subcontratista.

Inventario de Registros es una lista detallada que incluye los tipos de registro, la ubicación, las fechas, etc., de los registros de Citi y que es necesaria 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, en que el Proveedor es capaz de sostener operaciones mientras está en modo de recuperación.

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 día anterior).

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

“Evento de Liberación” se refiere a uno o varios de los siguientes casos:

- (i) El Proveedor (A) se declara insolvente o admite su incapacidad para pagar sus deudas en general a medida que vencen; (B) se somete, voluntaria o involuntariamente, a cualquier procedimiento en virtud de cualquier ley de quiebra o insolvencia nacional o extranjera que no se haya suspendido completamente en un plazo de siete (7) días hábiles o que no se haya desestimado o anulado en un plazo de cuarenta y cinco (45) días a partir de su presentación; (C) realiza una cesión general en beneficio de los acreedores; o (D) tiene un síndico, fiduciario, custodio o agente similar designado por orden de cualquier tribunal de jurisdicción competente para hacerse cargo de o vender cualquier parte sustancial de su propiedad o negocio.

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 Dotación y el Marco de Gestión de Proveedores.

Gerente de Abastecimiento de la 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 de los Contratos, incluidas las RFP y otras actividades de selección de Proveedores, la administración de los términos y condiciones de los Contratos y los requisitos de acreditación de la evaluación financiera.

Efecto adverso Grave o Catastrófico para una persona significa que el impacto podría razonablemente resultar 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.

Subcontratista: Un subcontratista es un cuarto (persona o entidad) que fue contratado por un tercero para realizar algunas o todas las actividades o servicios que Citi ha contratado con el tercero.

Orientación:

P1: ¿Es necesario reportar todos los subcontratistas de un Tercero?

R1: Solo se debe informar sobre los subcontratistas relacionados con el servicio prestado. Algunos ejemplos de servicios o actividades llevados a cabo por un subcontratista incluyen, entre otros:

*Un subcontratista que preste servicios de tecnología o software que sustenten de manera directa o indirecta el servicio/las actividades que Citi haya contratado con el Tercero; o

*Un subcontratista cuyos servicios incluyan el acceso a información Confidencial o de nivel superior de Citi; o

*Un subcontratista que tenga interacción directa o indirecta con cualquier cliente existente/potencial de Citi; o

*Un subcontratista que no esté acompañado y preste servicios de trituration o archivo de documentos de Citi dentro o fuera de cualquier local de Citi; o

*Un subcontratista que respalde funciones o servicios bancarios básicos, como pagos, cobros, préstamos, etc.

Proveedor: Para los fines de este documento “Requisitos de Citi para Proveedores”, un “Proveedor” se refiere exclusivamente a un Tercero Externo que ha suscrito un acuerdo comercial para prestar productos o servicios directamente a una Entidad de Citi o para respaldar a una Entidad de Citi a fin de que esta cumpla sus objetivos comerciales. Un Tercero Externo se define como una entidad que no pertenece a Citi. Los Proveedores también pueden ser clientes de una Entidad de Citi o pueden respaldar las interacciones con los clientes de Citi; sin embargo, los acuerdos basados exclusivamente en su condición de cliente de Citi no se consideran relaciones con proveedores dentro del alcance de este documento.

Información Transitoria: Un Registro es la versión final más completa de la información que Citi está obligado a retener por razones legales, regulatorias o de negocios aprobadas. Toda la otra información se clasifica como “Información Transitoria”.