FFIEC

Herramienta de Evaluación de Ciberseguridad

Mayo 2017

Ley de Reducción de Trámites (PARA) – Control de la Oficina de Administración y Presupuesto (OMB) N° 1557-0328; Fecha de vencimiento: 31 de agosto de 2019.

El número de control OMB y fecha de vencimiento que anteceden corresponden a la Ley de Reducción de Trámites y su reglamento de implementación la cual declara que una agencia federal no puede conducir o auspiciar una recolección de informaciones, y que una persona u organización no requiere responder a una recolección de informaciones, a no ser que presenten un número de control OMB vigente y, si fuera el caso, la fecha de vencimiento. Vea 44 USC 3506 (c)(1)(B) y 5 CFR.

1320.5(b)(2)(i), 1320.8(b)(1).

Índice

Recursos Adicionales

Overview for Chief Executive Officers and Boards of Directors (Resumen para los Directores Ejecutivos y la Junta Directiva)

Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook (Anexo A: Comparación de las declaraciones de base con el Manual de Evaluación de TI del FFIECT)

Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework (Anexo B: Comparación de la Herramienta de Evaluación en Ciberseguridad con el Marco referencial de Ciberseguridad del NIST)
Appendix C: Glossary (Anexo C: Glosario)

Guía del Usuario

Resumen

En vista del aumento en número y sofisticación de las amenazas cibernéticas, el Consejo de Examen de Instituciones Financieras Federales[1] (FFIEC, por sus siglas en inglés) ha desarrollado la Herramienta de Evaluación de Ciberseguridad (en adelante, Evaluación), en representación de sus miembros, para ayudar a que las instituciones identifiquen sus riesgos y determinen su madurez de ciberseguridad.

El contenido de la Evaluación es consistente con los principios del *Manual de Evaluación de Tecnología de la Información del FFIEC (Manual TIC)* y el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés),[2] así como con las prácticas de ciberseguridad aceptadas en la industria. La Evaluación proporciona a las instituciones un proceso replicable y medible que informa a la administración sobre los riesgos que tiene su institución y su nivel de preparación en ciberseguridad.

La Evaluación comprende dos partes: Perfil de Riesgo Inherente y Madurez de Ciberseguridad. El Perfil de Riesgo Inherente identifica el riesgo inherente de la institución antes de implementar los controles. La Madurez de Ciberseguridad incluye dominios, factores de evaluación, componentes, y declaraciones expositivas individuales a través de cinco niveles de madurez a fin de identificar los controles específicos y las prácticas existentes. Aunque la administración puede determinar el nivel de madurez de la institución en cada dominio, la Evaluación no ha sido diseñada para identificar un nivel de madurez de ciberseguridad en general.

Para completar la Evaluación, la administración evalúa primero el perfil de riesgo inherente basado en cinco categorías:

- Tipos de tecnología y conexión
- Canales de entrega
- Productos online/móviles y servicios tecnológicos
- Características organizativas
- Amenazas externas

Luego, la administración evalúa el nivel de madurez de ciberseguridad para cada uno de los cinco dominios:

- Gestión de riesgos cibernéticos y supervisión
- Inteligencia de amenazas y colaboración
- Controles de ciberseguridad
- Gestión de dependencia externa
- Gestión de incidentes cibernéticos y resiliencia

---

[1] El FFIEC está conformado por representantes de las siguientes entidades: la Junta de Gobernadores del Sistema de la Reserva Federal (FRS), la Corporación Federal de Seguro de Depósitos (FDIC), la Administración Nacional de Cooperativas de Crédito (NCUA), la Oficina del Contralor de la Moneda (OCC), Oficina para la Protección Financiera del Consumidor (CFBP), y el Comité de Enlace del Estado (SLC).

[2] Existe un esquema disponible en el Anexo B: Mapping Cybersecurity Assessment Tool to the NIST Cybersecurity El NIST revisa el Esquema y brinda aportes a fin de garantizar que sea consistente con los principios del Marco de Referencia y para destacar la naturaleza complementaria de estos dos recursos.

Revisando el perfil de riesgo inherente, así como los niveles de madurez de la institución a lo largo de los dominios, la administración puede determinar si sus niveles de madurez son apropiados con relación a su riesgo. Si no lo son, la institución puede tomar acción, ya sea para reducir el nivel de riesgo o para incrementar los niveles de madurez. Este proceso está diseñado para complementar el proceso de gestión de riesgos y el programa de ciberseguridad de una institución. y no para remplazarlos.

Antecedentes

Esta Evaluación está basada en la evaluación de ciberseguridad que los miembros del FFIEC implementaron como plan piloto en el 2014, la cual fue diseñada para evaluar el grado de preparación que las instituciones comunitarias tenían para poder mitigar los riesgos cibernéticos. El Instituto Nacional de Estándares y Tecnología (NIST) define ciberseguridad como “el proceso para proteger la información mediante la prevención, detección, y respuesta a los ataques”. Como parte de la ciberseguridad, las instituciones deben considerar la gestión de amenazas externas e internas y sus vulnerabilidades a fin de proteger la infraestructura y los activos de información. La definición se basa en lo que está definido acerca de seguridad informática en la guía del FFIEC.

Los incidentes cibernéticos pueden tener un impacto financiero, operativo, legal y también afectan la reputación. Recientes ataques cibernéticos notables han demostrado que los incidentes cibernéticos pueden afectar significativamente el capital y las ganancias. Los costos pueden incluir investigaciones forenses, campañas de relaciones públicas, gastos legales, monitoreo del crédito al consumidor, y cambios tecnológicos. En ese sentido, la ciberseguridad necesita estar integrada dentro de una institución como parte de los procesos de gobernabilidad de la empresa, seguridad de la información, continuidad del negocio, y gestión de riesgos de terceros. Por ejemplo, las políticas de ciberseguridad de una institución pueden ser incorporadas dentro del programa de seguridad de la información. Además, los roles y procesos de ciberseguridad a los que se refieren en la Evaluación pueden tener roles separados dentro del grupo de seguridad (o subcontratados) o pueden ser parte de los roles más amplios dentro de la institución.

Completando la Evaluación

La Evaluación está diseñada para proporcionar un proceso medible y replicable que pueda evaluar el nivel de riesgo de ciberseguridad y la preparación que tiene una determinada institución. La primera parte de esta Evaluación comprende el Perfil de Riesgo Inherente, el cual identifica el riesgo inherente de una institución con relación a los riesgos cibernéticos. La segunda parte comprende la Madurez de Ciberseguridad, la cual determina el estado actual de preparación en ciberseguridad representada por los niveles de madurez a través de cinco dominios. Para que esta Evaluación sea una herramienta efectiva de la gestión del riesgo, una institución puede decidir realizarla periódicamente y en la medida que ocurran cambios tecnológicos y operacionales significativos.

Los programas de riesgos cibernéticos se desarrollan y alinean sobre la base de programas de seguridad informática que ya existen, la continuidad del negocio, y la recuperación en caso de desastres. La Evaluación está diseñada para ser utilizada principalmente a nivel de toda la empresa y cuando se incorporan nuevos productos y servicios, tal como sigue:

- **En toda la empresa**. La administración debe revisar el Perfil de Riesgo Inherente y las declaraciones expositivas para comprender qué políticas, procedimientos y controles están funcionando en toda la empresa y dónde pueden existir discrepancias. Después de esta

revisión, la administración puede determinar los niveles de madurez apropiados para la institución en cada dominio o el estado deseado para la Madurez de Ciberseguridad. Luego, la administración puede desarrollar planes de acción para alcanzar el estado de riesgo esperado.

- **Nuevos productos, servicios o iniciativas.** Utilizar la Evaluación antes de lanzar un nuevo producto, servicio o iniciativa puede ayudar a que la administración comprenda cómo esto puede afectar el perfil de riesgo inherente de la institución y el resultado de los niveles de madurez esperados.

Primera Parte: Perfil de Riesgo Inherente

La Primera parte de la Evaluación identifica el riesgo inherente de la institución. El Perfil de Riesgo Inherente detalla actividades, servicios y productos organizados en las siguientes categorías:

- **Tecnologías y tipos de conexión.** Ciertos tipos de conexiones y tecnologías pueden representar un riesgo inherente alto dependiendo de la complejidad y madurez, conexiones, y naturaleza de los productos o servicios tecnológicos específicos. Esta categoría incluye el número del proveedor del servicio de internet (ISP, por sus siglas en inglés) y conexiones de terceros, ya sea que los sistemas estén alojados internamente o sean subcontratados, el número de conexiones no seguras, el uso de acceso inalámbrico, la cantidad de dispositivos de red, el fin de vida útil de los sistemas, el alcance de los servicios en la nube, y el uso de dispositivos personales.
- **Canales de entrega.** Algunos canales de entrega para productos y servicios pueden representar un riesgo inherente alto dependiendo de la naturaleza del producto o servicio específico ofrecido. El riesgo inherente aumenta a medida que hay un incremento en la variedad y número de canales de entrega. En esta categoría se consigna si los productos o servicios están disponibles a través de canales de entrega online o móviles, y el alcance de las operaciones de los cajeros automáticos (ATM, por sus siglas en inglés).
- **Productos online/móviles y servicios tecnológicos.** Diversos productos y servicios tecnológicos ofrecidos por instituciones pueden representar un riesgo inherente alto dependiendo de la naturaleza del producto o servicio específico ofrecido. Esta categoría incluye diversos servicios de pago, tales como tarjetas de crédito y débito, pagos de persona a persona, aquellos originados en la Cámara de Compensación Automatizada (ACH, por sus siglas en inglés), transferencias de dinero de bajo monto, pagos de mayor cuantía, captura remota de depósitos de comerciantes, servicios de tesorería, a clientes y fideicomisos, remesas globales, bancos corresponsales, y actividades de adquisición comercial. Esta categoría también considera si la institución brinda servicios tecnológicos a otras organizaciones.
- **Características organizacionales.** Esta categoría toma en consideración las características organizacionales tales como fusiones y adquisiciones, número de empleados directos y contratistas de ciberseguridad, cambios en el personal de seguridad, número de usuarios con acceso privilegiado, cambios en el entorno de la tecnología de información (TI), locales con presencia comercial, y lugares de operación y centros de datos.
- **Amenazas externas.** La cantidad y tipo de ataques (con o sin éxito) afectan la exposición al riesgo inherente de la institución. Esta categoría considera la cantidad y sofisticación de los ataques que afectan a la institución.

Niveles de riesgo

Los niveles de riesgo incluyen tipo, cantidad y complejidad de las operaciones de la institución y las amenazas dirigidas a la institución. El riesgo inherente no incluye controles de mitigación.

Seleccione el nivel de riesgo inherente más apropiado para cada actividad, servicio o producto dentro de cada categoría. Los niveles varían desde Riesgo Inherente Insignificante a Mayor Riesgo Inherente (Figura 1) e incluye un amplio rango de descripciones. Los niveles de riesgo proporcionan parámetros para determinar el riesgo inherente en cada categoría. Estos parámetros no pretenden ser rígidos sino ilustrativos con el fin de ayudar a determinar un nivel de riesgo dentro de cada actividad, servicio o producto. En situaciones donde el nivel de riesgo cae entre dos niveles, la administración deberá seleccionar el nivel de riesgo más alto.

Figura 1: Diseño del Perfil de Riesgo Inherente

Niveles de riesgo

Actividad, servicio, o producto

Categoría: Tecnologías y tipos de conexión	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Número total de conexiones de proveedores de servicio de Internet (ISP) (incluyendo conexiones de las sucursales)	Sin conexiones	Complejidad mínima (1–20 conexiones)	Complejidad moderada (21–100 conexiones)	Complejidad significativa (101–200 conexiones)	Complejidad considerable (>200 conexiones)
Conexiones externas inseguras, número de conexiones de no usuarios (por ejemplo, protocolo de transferencia de archivo (FTP), Telnet, rlogin)	Ninguna	Pocas ocasiones con conexiones inseguras en (1–5)	Varias ocasiones con conexiones inseguras (6–10)	Significativas ocasiones con conexiones inseguras (11–25)	Considerables ocasiones con conexiones inseguras (>25)
Acceso a la red inalámbrica	Sin acceso inalámbrico	Puntos de acceso inalámbricos separados para corporativos y para invitados	Acceso a la red inalámbrica para invitados y para corporativos están lógicamente separados; número limitado de usuarios y puntos de acceso (1– 250 usuarios; 1–25 puntos de acceso)	Acceso a la red inalámbrica corporativa; número significativo de usuarios y puntos de acceso (251–1,000 usuarios; 26–100 puntos de acceso)	Acceso a la red inalámbrica corporativa; todos los empleados tienen acceso; considerable número de puntos de acceso (>1,000 usuarios; >100 puntos de acceso)

Determinación del Perfil de Riesgo Inherente

La administración puede determinar el Perfil general de Riesgo Inherente de la institución en base al número de declaraciones que se aplican a cada nivel de riesgo para cada una de las actividades (Figura 2). Por ejemplo, cuando la mayoría de las actividades, productos o servicios caen dentro del Nivel de Riesgo Moderado, la administración puede determinar que la institución tiene un Perfil de Riesgo Inherente Moderado. Sin embargo, cada categoría puede representar un nivel de riesgo inherente diferente. Por lo tanto, además de evaluar el número de ocasiones en las que una institución selecciona un nivel de riesgo específico, la administración puede también considerar evaluar si la categoría específica representa un riesgo adicional.

Figura 2: Resumen del Riesgo Inherente

	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Número de declaraciones seleccionadas en cada nivel de riesgo					
En base a los niveles de riesgo individual seleccionados, asigne un perfil de riesgo inherente	**Insignificante**	**Mínimo**	**Moderado**	**Significativo**	**Mayor**

A continuación, se incluye las definiciones de los niveles de riesgo.

- **Riego Inherente Insignificante.** Una institución con un Perfil de Riesgo Inherente Insignificante generalmente utiliza la tecnología de forma muy limitada. Tiene pocas computadoras, aplicaciones, sistemas y no tiene conexiones. La variedad de productos y servicios es limitada. La institución tiene una pequeña presencia geográfica y pocos empleados.
- **Riesgo Inherente Mínimo.** Una institución con un Perfil de Riesgo Inherente Mínimo generalmente tiene una limitada complejidad en términos de la tecnología utilizada. Ofrece una limitada variedad de productos y servicios con menor riesgo. Los sistemas de la institución considerados de misión crítica son subcontratados. La institución utiliza principalmente tecnologías ya instaladas. Mantiene algunos tipos de conexiones con sus

clientes y terceros con una limitada complejidad.

- **Riesgo Inherente Moderado.** Una institución con un Perfil de Riesgo Inherente Moderado generalmente utiliza tecnología que, de alguna manera, puede ser compleja en términos de cantidad y sofisticación. La institución puede subcontratar sistemas y aplicaciones considerados de misión crítica y mantenerlos internamente. Hay una mayor variedad de productos y servicios ofrecidos a través de diversos canales.
- **Riesgo Inherente Significativo.** Una institución con un Perfil de Riesgo Inherente Significativo generalmente utiliza tecnología compleja en términos de alcance y sofisticación. La institución ofrece productos y servicios de alto riesgo que pueden incluir nuevas tecnologías. La institución puede alojar un número significativo de aplicaciones internamente. La institución permite un gran número de dispositivos personales o una amplia variedad de dispositivos. La institución mantiene un número importante de conexiones con sus clientes y con terceros. También se ofrece una variedad de servicios de pagos directos en lugar hacerlos a través de terceros, lo cual se puede reflejar en un nivel significativo del volumen de transacciones.
- **Riesgo Inherente Mayor.** Una institución con un Perfil de Riesgo Inherente Mayor utiliza tecnologías extremamente complejas para entregar una infinidad de productos y servicios. Muchos de estos productos y servicios están en el más alto nivel de riesgo, incluyendo aquellos ofrecidos a otras organizaciones. Se utilizan nuevas y emergentes tecnologías a través de los múltiples canales de entrega. La institución puede subcontratar algunos sistemas o aplicaciones considerados de misión crítica, pero muchos están alojados internamente. La institución mantiene un gran número de tipos de conexiones para transferencia de datos con sus clientes y terceros.

Segunda Parte: Madurez de Ciberseguridad

Después de determinar el Perfil de Riesgo Inherente, la institución se dirige a la parte de la Evaluación sobre Madurez de Ciberseguridad a fin de determinar el nivel de madurez de la institución dentro de cada uno de los cinco dominios siguientes:

- **Dominio 1:** Gestión de riesgos cibernéticos y supervisión
- **Dominio 2:** Inteligencia de amenazas y colaboración
- **Dominio 3:** Controles de ciberseguridad
- **Dominio 4:** Gestión de dependencia externa
- **Dominio 5:** Gestión de incidentes cibernéticos y resiliencia

Dominios, Factores de Evaluación, Componentes y Declaraciones Expositivas

Dentro de cada dominio existen factores de evaluación y componentes que contribuyen a ello. En cada componente hay declaraciones expositivas que describen una actividad que respalda al factor de evaluación en dicho nivel de madurez. El Cuadro 1 proporciona definiciones para cada dominio y los factores de evaluación subyacentes.

Tabla 1: Dominios y Factores de Evaluación definidos

Dominios y Factores de Evaluación Definidos	
Dominio 1 **Gestión del Riesgo Cibernético y Supervisión** La gestión y supervisión de riesgos cibernéticos comprende la supervisión por parte de la Junta Directiva y el desarrollo e implementación de un programa de ciberseguridad efectivo para toda la empresa, llevado a cabo por la administración, con políticas y procesos integrales, a fin de establecer una apropiada supervisión y asignación de responsabilidades.	
Factores de Evaluación	**Gobernabilidad** incluye supervisión, estrategias, políticas y gestión de activos de la TI para implementar una gobernabilidad efectiva del programa de ciberseguridad. **Gestión del riesgo** incluye un programa de gestión del riesgo, un proceso de evaluación del riesgo, y una función de auditoría para gestionar el riesgo de manera efectiva y evaluar la eficacia de los controles claves. **Recursos** comprende al personal, las herramientas y los procesos presupuestarios para asegurar que el personal de la institución, o los que son externos, tengan el conocimiento y la experiencia que corresponde al perfil de riesgo de la institución. **Capacitación y cultura** comprende los programas de capacitación del personal y de concientización de los clientes los cuales contribuyen a una cultura organizacional que pone énfasis en la mitigación de las amenazas de ciberseguridad.
Dominio 2 **Inteligencia de Amenazas y Colaboración** La inteligencia de amenazas y colaboración comprende los procesos para descubrir, analizar y entender, de manera efectiva, las amenazas cibernéticas, con la capacidad de compartir información de forma interna, así como con terceros.	
Factores de evaluación	**Inteligencia de amenazas** se refiere a la adquisición y análisis de la información para identificar, hacer seguimiento y predecir las habilidades cibernéticas, intenciones y actividades que ofrecen rumbos que llevan a mejorar la toma de decisiones. **Monitoreo y análisis** se refiere a la manera cómo una institución monitorea las fuentes de amenazas y qué tipo de análisis se puede realizar para identificar las amenazas específicas para la institución o resolver conflictos en las diversas corrientes de información de amenazas. **Intercambio de información** comprende establecer relaciones con instituciones comparables y con foros que compartan información, además de encontrar la manera de comunicar la información sobre amenazas a dichos grupos, así como también a las partes interesadas dentro de la institución.
Dominio 3 **Controles de Ciberseguridad** Los controles de ciberseguridad son aquellas prácticas y procesos utilizados para proteger activos, infraestructura e información, fortaleciendo la postura defensiva de la institución a través de protección automatizada y monitoreo continuo.	
Factores de Evaluación	Los **controles preventivos** disuaden y previenen ataques cibernéticos, e incluyen la gestión de infraestructura, gestión del acceso, seguridad de los dispositivos y terminales, y un cifrado seguro. Los **controles de detección** incluyen la detección de amenazas y vulnerabilidades, detección de actividades anómalas y detección de incidentes, de esa manera pueden alertar a la institución sobre las irregularidades en el sistema y en la red indicando que ha ocurrido o puede ocurrir un incidente. Los **controles correctivos** se utilizan para solucionar vulnerabilidades del sistema y del software a través de una gestión de parches y la corrección de problemas identificados durante las exploraciones de vulnerabilidades y pruebas de penetración.
Dominio 4 **Gestión de Dependencia Externa** La gestión de dependencia externa consiste en establecer y mantener un programa integral para supervisar y gestionar conexiones externas y relaciones con terceros que tengan acceso a la información y a los activos tecnológicos de la institución.	

Factores de evaluación	Las **conexiones** incorporan la identificación, el monitoreo y la gestión de las conexiones externas y el flujo de datos hacia terceros. La **gestión de relaciones** incluye la diligencia debida, contratos, y monitoreo permanente para ayudar a garantizar que los controles complementan el programa de ciberseguridad de la institución.
Dominio 5 **Gestión de Incidentes Cibernéticos y Resiliencia** La gestión de incidentes cibernéticos consiste en establecer, identificar y analizar los sucesos cibernéticos; priorizar la contención o mitigación de la institución; y comunicar la información a las partes interesadas correspondientes. La resiliencia cibernética comprende tanto la planificación como la realización de pruebas para mantener y recuperar la continuidad de las operaciones durante un incidente cibernético y posterior a este.	
Factores de Evaluación	**La planificación y estrategia para la resiliencia ante incidentes** incluye planificación y pruebas de resiliencia en la continuidad del negocio existente, y planes de recuperación ante desastres para minimizar las interrupciones en el servicio y daños a la información o su destrucción. La **detección, respuesta y mitigación** se refieren a los pasos que la administración sigue para identificar, priorizar, responder y mitigar los efectos de las amenazas internas y externas y sus vulnerabilidades. **El proceso de escalación e informes** garantiza que las partes claves interesadas estén informadas acerca del impacto de los incidentes cibernéticos, y que las entidades reguladoras, las autoridades y los clientes sean notificados según corresponda.

Cada nivel de madurez incluye un grupo de declaraciones expositivas que describen cómo los comportamientos, prácticas, y procesos de una institución pueden producir los resultados deseados de manera consistente.

La Evaluación comienza en un nivel de madurez Básico y progresa hasta llegar al nivel de madurez más alto, el nivel Innovador (Figura 3). El Cuadro 2 brinda definiciones para cada nivel de madurez, los cuales son acumulativos.

Figura 3: Niveles de Madurez en Ciberseguridad

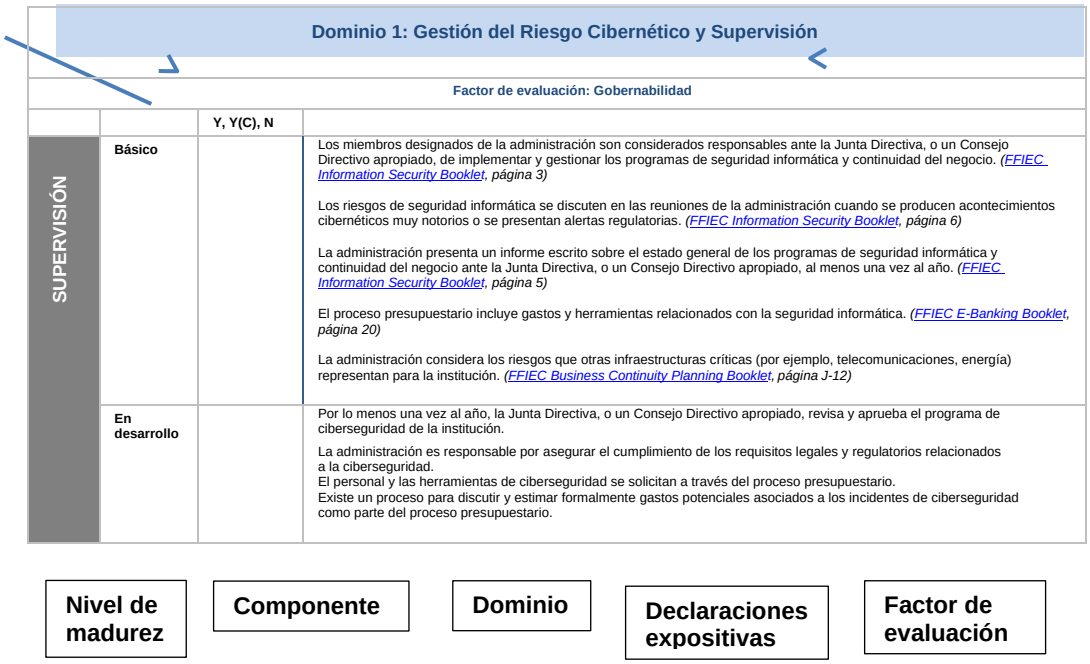
Cuadro 2: Definición de Niveles de Madurez

Niveles de Madurez definidos	
Básico	La madurez a nivel básico se caracteriza por un mínimo de expectativas requeridas por leyes y reglamentos, o recomendadas en la guía de supervisión bancaria. Este nivel incluye objetivos basados en el riesgo de cumplimientos normativos. La administración ha revisado y evaluado la guía.
En desarrollo	La madurez en desarrollo se caracteriza por la formalidad adicional de políticas y procedimientos documentados que hasta el momento no se requerían. Existen objetivos basados en el riesgo. La responsabilidad en cuanto a ciberseguridad es asignada formalmente y ampliada más allá de la protección de la información del cliente para incluir información de activos y sistemas.
Intermedio	La madurez intermedia se caracteriza por procesos formales y detallados. Los controles son validados y consistentes. Las prácticas y el análisis de la gestión del riesgo están integradas en las estrategias del negocio.
Avanzado	La madurez avanzada se caracteriza por las prácticas y el análisis de ciberseguridad que están integrados a lo largo de las líneas del negocio. La mayor parte de los procesos de gestión del riesgo están automatizados e incluyen mejoras permanentes en los procesos. La responsabilidad para la toma de decisiones de riesgo por negocios de primera línea está asignada formalmente.
Innovador	La madurez innovadora se caracteriza por promover la innovación en las personas, los procesos, y la tecnología para que la institución y la industria gestionen los riesgos cibernéticos. Esto puede implicar el desarrollo de nuevos controles, nuevas herramientas, o la creación de nuevos grupos para compartir información. Los análisis predictivos, en tiempo real, están ligados a respuestas automatizadas.

Alcanzar la Madurez de Ciberseguridad

Cada dominio y nivel de madurez tiene una serie de declaraciones expositivas organizadas de acuerdo con los factores de evaluación. A fin de que la institución pueda encontrar temas en común a través de los diferentes niveles de madurez, las declaraciones se han categorizado por componentes. Los componentes son grupos de declaraciones expositivas similares que hace que la Evaluación sea más fácil de utilizar (Figura 4)

Figura 4: Madurez de ciberseguridad



La administración determina qué declaraciones expositivas se ajustan mejor a las actuales prácticas de la institución**.** ***Todas las declaraciones expositivas en cada nivel de madurez, y en niveles anteriores, deben cumplirse y mantenerse para alcanzar el dominio del nivel de madurez.*** Cumplir y mantener requiere respuestas afirmativas, ya sea con "Sí" o "Sí, con controles compensatorios"[3] para cada una de las preguntas declarativas en cada nivel de madurez. La administración puede determinar el nivel de madurez de la institución en cada dominio; sin embargo, la Evaluación no está diseñada para identificar el nivel de madurez de ciberseguridad en general.

La administración puede determinar que una declaración expositiva ha sido suficientemente sustentada con base en los resultados comprobados. Algunas declaraciones expositivas pueden no aplicarse a todas las instituciones si el producto, servicio, o tecnología no se ofrece o no se utiliza. Las declaraciones expositivas que no sean aplicables a todas las instituciones están claramente consignadas y no afectan la determinación de un nivel de madurez específico.

Interpretación y análisis de los resultados de la Evaluación

La administración puede revisar el Perfil de Riesgo Inherente de la Institución con relación a los resultados de su Madurez en Ciberseguridad para cada dominio, a fin de entender si están alineados o no.

El Cuadro 3 presenta la relación entre el Perfil de Riesgo Inherente de una institución y sus

niveles de madurez del dominio, ya que no existe un único nivel esperado para una institución. En general, a medida que el riesgo inherente crece, los niveles de madurez de una institución deben aumentar. El perfil de riesgo inherente de una institución y sus niveles de madurez cambiarán a lo largo del tiempo a medida que cambien las amenazas, sus vulnerabilidades y los entornos operacionales. Por lo tanto, la administración debe poner en consideración la reevaluación periódica de su perfil de riesgo inherente y su madurez de ciberseguridad, y cuando los cambios planeados puedan afectar su perfil de riesgo inherente (por ejemplo, con el lanzamiento de nuevos productos o servicios, nuevas conexiones).

[3]Control de compensación – Un control administrativo, operativo y/o técnico (por ejemplo, salvaguardas o contramedidas) empleado por una organización en lugar de un control de seguridad recomendado como punto de referencia para perfiles de riesgo bajo, moderado o alto, que proporcione una protección equivalente o comparable para un sistema informático.

Cuadro 3: Relación Riesgo/Madurez

Nivel de madurez de ciberseguridad para cada dominio	Niveles de riesgo inherente →				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Innovador				■	■
Avanzado			■	■	■
Intermedio		■	■	■	
En desarrollo	■	■	■		
Básico	■	■			

Si la administración determina que los niveles de madurez de la institución no son los apropiados con relación al perfil de riesgo inherente, esta administración debe considerar reducir el riesgo inherente o desarrollar una estrategia para mejorar los niveles de madurez. Este proceso incluye:

- determinar niveles de madurez objetivo
- realizar un análisis de discrepancias
- priorizar y planificar las acciones a tomar
- implementar los cambios
- reevaluar a lo largo del tiempo
- comunicar los resultados

La administración puede establecer los niveles de madurez objetivo para cada domino o a lo largo de los dominios en base a los objetivos comerciales de la institución y su propensión al riesgo. La administración puede realizar un análisis de discrepancias entre los niveles de madurez actuales y las metas, e iniciar las mejoras en base a las discrepancias. Cada declaración expositiva puede representar un rango de estrategias y procesos con un impacto en toda la empresa. Por ejemplo, las declaraciones expositivas que todavía no se han alcanzado proporcionan conocimiento para políticas, procesos, procedimientos, y controles que pueden mejorar la gestión del riesgo con relación a un riesgo específico o al grado de preparación general en ciberseguridad de la institución.

Al utilizar los niveles de madurez en cada dominio, la administración puede identificar acciones potenciales que incrementarían el grado de preparación general en ciberseguridad de la institución. La administración puede revisar las declaraciones expositivas de niveles de madurez superiores a los que la institución ha conseguido y así poder determinar las acciones necesarias para alcanzar el siguiente nivel e implementar cambios que puedan resolver esas discrepancias. Las reevaluaciones periódicas que la administración realiza sobre el perfil de riesgo inherente y niveles de madurez pueden ayudar aún más a la institución a mantener un apropiado grado de preparación en ciberseguridad. Además, la administración también puede buscar una validación independiente del proceso de Evaluación y sus hallazgos en la institución, mediante la función

de auditoría interna.

Los resultados de la Evaluación deben ser comunicados al Director Ejecutivo (CEO) y a la Junta Directiva. Mayor información y preguntas pertinentes se encuentran en: "Overview for Chief Executive Officers and Boards of Directors." (Resumen para los Directores Ejecutivos y la Junta Directiva.)

Recursos

Además del "*Overview for Chief Executive Officers and Boards of Directors*," el FFIEC ha publicado los siguientes documentos a fin de ayudar a las instituciones con el uso de la Herramienta de Evaluación en Ciberseguridad.

- Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook (Anexo A: Comparación de las declaraciones de base con el Manual de Evaluación de TI del FFIEC)
- Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework (Anexo B: Comparación de la Herramienta de Evaluación en Ciberseguridad con el Marco referencial de Ciberseguridad del NIST)
- Appendix C: Glossary (Anexo C: Glosario)

Perfil de Riesgo Inherente

Categoría: Tecnologías y tipos de conexión	Niveles de riesgo				
	Insignificante	**Mínimo**	**Moderado**	**Significativo**	**Mayor**
Número total de conexiones de proveedores de servicios de Internet, ISP (incluyendo conexiones de las sucursales)	Sin conexiones	Complejidad mínima (1-20 conexiones)	Complejidad moderada (21-100 conexiones)	Complejidad significativa (101-200 conexiones)	Complejidad considerable (>200 conexiones)
Conexiones externas inseguras, número de conexiones de no usuarios (por ejemplo, protocolo de transferencia de archivos (FTP), Telnet, rlogin)	Ninguna	Pocas ocasiones con conexiones inseguras (1-5)	Varias ocasiones con conexiones inseguras (6-10)	Significativas ocasiones con conexiones inseguras (11-25)	Considerables ocasiones con conexiones inseguras (>25)
Acceso a la red inalámbrica (wifi)	Sin acceso inalámbrico (sin wifi)	Puntos de acceso inalámbrico separados para invitados y para corporativos	Acceso a la red inalámbrica para invitados y para corporativos están lógicamente separados; número limitado de usuarios y puntos de acceso (1– 250 usuarios; 1–25 puntos de acceso)	Acceso a la red inalámbrica corporativa; número significativo de usuarios y puntos de acceso (251–1,000 usuarios; 26–100 puntos de acceso)	Acceso a la red inalámbrica corporativa; todos los empleados tienen acceso; considerable número de puntos de acceso (>1,000 usuarios; >100 puntos de acceso)
Se permite que equipos personales se conecten a la red corporativa	Ninguna	Un solo tipo de dispositivo disponible; disponible para <5% de empleados (personal, ejecutivos, administradores); solo acceso a e-mail	Se utilizan diversos tipos de dispositivos; disponible para <10% de empleados (personal, ejecutivos, administradores) y la Junta; solo acceso a e-mail	Se utilizan diversos tipos de dispositivos; disponible para <25% de empleados autorizados (personal, ejecutivos, administradores) y la Junta; acceso a e-mail y a algunas aplicaciones	Se utiliza cualquier tipo de dispositivo; disponible para <25% de empleados (personal, ejecutivos, administradores) y la Junta; todas las aplicaciones tienen acceso

Proveedor o terceras personas, incluso organizaciones y personas ya sean proveedores o subcontratistas, tienen acceso a los sistemas internos (por ej. red privada virtual, modem, intranet, conexión directa)	Ningún proveedor o tercera persona relacionada a este tiene acceso a los sistemas	Número limitado de proveedores (1-5) y número limitado de terceras personas relacionadas a este (<50) tienen acceso; menor complejidad en la forma de acceder a los sistemas	Número moderado de proveedores (6-10) y moderado número de terceras personas relacionadas a este (50-500) tienen acceso; cierta complejidad en la forma de acceder a los sistemas	Número significativo de proveedores (11-25) y número significativo de terceras personas relacionadas a este (501-1,500) tienen acceso; alto nivel de complejidad en la forma de acceder a los sistemas	Considerable número de proveedores (>25) y considerable número de terceras personas relacionadas a este (>1,500) tienen acceso; mayor complejidad en la forma de acceder a los sistemas

Categoría: Tecnologías y tipos de conexión	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Clientes mayoristas con conexiones dedicadas	Ninguno	Pocas conexiones dedicadas (entre 1-5)	Varias conexiones dedicadas (entre 6-10)	Significativo número de conexiones dedicadas (entre 11-25)	Considerable número de conexiones dedicadas (>25)
Aplicaciones del proveedor alojadas internamente y diseñadas o modificadas para dar soporte a actividades consideradas críticas	Ninguna aplicación	Pocas aplicaciones (entre 1-5)	Varias aplicaciones (entre 6-10)	Significativo número de aplicaciones (entre 11-25)	Considerable número de aplicaciones y complejidad (>25)
Aplicaciones diseñadas por el proveedor, alojadas internamente, para dar apoyo a actividades consideradas críticas	Limitadas aplicaciones (0-5)	Pocas aplicaciones (6-30)	Varias aplicaciones (31-75)	Significativo número de aplicaciones (76-200)	Considerable número de aplicaciones y complejidad (>200)
Tecnologías diseñadas por el usuario e informáticas de usuario final para soportar actividades consideradas críticas (incluye la hoja de cálculo Excel y la base de datos Access de Microsoft u otras herramientas diseñadas por el usuario)	Ninguna tecnología diseñada por el usuario	De 1-100 tecnologías	De 101-500 tecnologías	De 501-2,500 tecnologías	>2,500 tecnologías
Fin de vida útil de los sistemas (EOL)	Ningún sistema (software o hardware) que haya pasado el fin de su vida útil o en riesgo de estar cerca en un lapso de 2 años	Pocos sistemas que están en riesgo de llegar al fin de su vida útil y ninguno de ellos soporta operaciones críticas	Varios sistemas que llegarán al fin de su vida útil en el lapso de 2 años y algunos de ellos soportan operaciones criticas	Un gran número de sistemas que soportan operaciones críticas están al fin de su vida útil o en riesgo de alcanzar el fin de su vida útil en 2 años	La mayor parte de las operaciones críticas dependen de sistemas que han llegado al fin de su vida útil o lo harán dentro de los próximos 2 años o un número desconocido de sistemas que ya alcanzaron el fin de su vida útil
Software de Código abierto (OSS)	No es un OSS	OSS limitado y ninguno soporta operaciones críticas	Varios OSS que soportan operaciones críticas	Gran número de OSS que soportan operaciones críticas	La mayoría de las operaciones dependen de OSS

Dispositivos de red (por ej. servidores, routers y firewalls; tanto en físico como virtual)	Dispositivos limitados o no existentes (<250)	Pocos dispositivos (250-1,500)	Varios dispositivos (1,501-25,000)	Significativo número de dispositivos (25,001-50,000)	Considerable número de dispositivos (>50,000)
Proveedores de servicio almacenan y/o procesan información que soporta actividades críticas (No tienen acceso a los sistemas internos pero la institución depende de sus servicios)	No existen proveedores que soportan actividades críticas	De 1-25 proveedores soportan actividades críticas	De 26-100 proveedores soportan actividades críticas	De 101-200 proveedores soportan actividades críticas; 1 o más están localizados en el extranjero	>200 proveedores soportan actividades críticas; 1 o más están localizados en el extranjero

Categoría: Tecnologías y tipos de conexión	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Servicios de computación en la nube alojados externamente para soportar actividades críticas	No existen proveedores de servicio de nube	Pocos proveedores de servicio de nube	Varios proveedores de servicio de nube	Significativo número de proveedores de servicios de nube (8-10); proveedor de servicio de nube incluye localización internacional; uso de nube pública	Considerable número de proveedores de servicio de nube (>10); proveedor de servicio de nube incluye localización internacional; uso de nube pública

Categoría: Canales de entrega	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Presencia online (cliente)	Sin presencia en la Web ni en los medios sociales	Sirve como un sitio web informativo o página de medios sociales (por ej., informa sobre localización de sucursales y cajeros automáticos, y de materiales de marketing)	Sirve como canal de entrega para la banca minorista online; puede comunicarse con los clientes a través de los medios sociales	Sirve como canal de entrega para clientes mayoristas; puede incluir el origen de la cuenta minorista	Aplicaciones de Internet sirven como canales de entrega a clientes mayoristas para gestionar grandes activos
Presencia de teléfono móvil	Ninguna	Solo alertas de mensajes de texto o notificaciones; acceso por navegador	Aplicación de banca móvil para clientes minoristas (por ej. pago de cuentas, captura remota de cheque vía móvil; solo transferencias internas	Aplicación de banca móvil incluye transferencias externas (por ej. para clientes corporativos, transacciones externas recurrentes)	Funcionalidad total, que incluye originar nuevas transacciones (por ej. ACH, transferencias)
Cajeros automáticos (ATM) (Operación)	No hay servicio de cajero automático	Ofrece servicio de cajero automático, pero no es propietario de las máquinas	Servicios de cajero automático administrados por terceros; cajeros automáticos en sucursales locales y regionales; abastecimiento de efectivo por subcontratación	Servicios de cajero automático administrados internamente; cajeros automáticos en sucursales estadounidenses y establecimientos minoristas; abastecimiento de efectivo por subcontratación	Servicios de cajero automático administrados internamente; servicio de cajeros automáticos que sirven a otras instituciones financieras; cajeros automáticos en sucursales locales e internacionales y en establecimientos minoristas; servicio de abastecimiento de efectivo gestionado internamente

Categoría: Productos Online/Móviles y servicios tecnológicos	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Emite tarjetas de crédito o débito	No emite tarjetas de crédito o débito	Emite tarjetas de crédito y/o débito a través de terceros; <10,000 tarjetas vigentes	Emite tarjetas de crédito o débito a través de terceros; entre 10,000-50,000 tarjetas vigentes	Emite tarjetas de crédito o débito directamente; entre 50,000-100,000-tarjetas vigentes	Emite tarjetas de crédito o débito directamente; >100,000-tarjetas vigentes; emite tarjetas a nombre de otras instituciones financieras
Tarjetas prepago	No emite tarjetas prepago	Emite tarjetas prepago a través de terceros; <5,000 tarjetas vigentes	Emite tarjetas prepago a través de terceros; 5,000-10,000 tarjetas vigentes	Emite tarjetas prepago a través de terceros; 10,001-20,000 tarjetas vigentes	Emite tarjetas prepago internamente, a través de terceros; o a nombre de otras instituciones financieras; >20,000 tarjetas vigentes
Tecnologías emergentes de pago (por ej. billetera digital, billetera móvil)	No acepta o usa tecnologías emergentes de pago	Aceptación o uso indirecto de tecnologías emergentes de pago (el uso del cliente puede afectar la cuenta de depósito o de crédito)	Aceptación o uso directo de tecnologías emergentes de pago; socio o franquicia con proveedor no bancarizado; volumen de transacción limitado	Aceptación o uso directo de tecnologías emergentes de pago; volumen de transacción pequeño; no acepta pagos del exterior	Aceptación directa de tecnologías emergentes de pago; moderado volumen de transacciones y pagos del exterior
Pagos de persona a persona (P2P)	No se ofrece	Clientes pueden originar el pago; es usado por <1,000 clientes o volumen mensual de transacciones <50,000	Clientes pueden originar el pago; es usado por 1,000-5,000 clientes o volumen mensual de transacciones es entre 50,000-100,000	Clientes pueden originar el pago; es usado por 5,001-10,000 clientes o volumen mensual de transacciones es entre 100,001-1 millón	Clientes pueden solicitar el pago u originarlo; es usado por >10,000 clientes o volumen mensual de transacciones >1 millón
Iniciar pagos de la Cámara de Compensación Automatizada (ACH)	No se origina con la Cámara de Compensación Automatizada	Origina transacciones de crédito de la ACH; volumen diario <3% del total de activos	Origina transacciones de débitos y créditos de la ACH; volumen diario es 3%-5% del total de activos	Auspiciar procesadores de pagos de terceros; se originan débitos y créditos de la ACH; volumen diario es 6%-25% del total de activos	Auspiciar procesadores de pagos de terceros corresponsales; se originan débitos y créditos de la ACH; volumen diario es >25% del total de activos
Originar pagos a mayoristas (por ej. CHIPS)	No se originan pagos a mayoristas	Volumen de pagos a mayoristas originados a diario <3% del total de activos	Volumen de pagos a mayoristas originados a diario 3%-5% del total de activos	Volumen de pagos a mayoristas originados a diario 6%-25% del total de activos	Volumen de pagos a mayoristas originados a diario >25% del total de activos

Categoría: Productos Online/Móviles y servicios tecnológicos	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Transferencias bancarias	No se ofrece	Solo solicitudes de transferencia en persona; solo transferencias nacionales; volumen diario inalámbrico <3% del total de activos	Solicitudes de transferencia en persona, por teléfono y fax; volumen diario de transferencias nacionales 3%-5% del total de activos; volumen diario de transferencias internacionales <3% del total de activos	Diversos canales de solicitud (por ej., online, por mensaje de texto, e-mail, fax y teléfono; volumen diario de transferencias nacionales 6%-25% del total de activos; volumen diario de transferencias internacionales <3%-10% del total de activos	Diversos canales de solicitud (por ej., online, por mensaje de texto, e-mail, fax y teléfono; volumen diario de transferencias nacionales >25% del total de activos; volumen diario de transferencias internacionales >10% del total de activos
Captura remota de depósito del comerciante (RDC)	No ofrece captura remota de depósito CDR	<100 clientes comerciales; volumen diario de operaciones es <3% del total de activos	100-500 clientes comerciales; volumen diario de operaciones es 3%-5% del total de activos	500-1,000 clientes comerciales; volumen diario de operaciones es 6%-25% del total de activos	>1,000 clientes comerciales; volumen diario de operaciones es >25% del total de activos
Remesas internacionales	No ofrece remesas internacionales	Volumen diario total de operaciones es <3% del total de activos	Volumen diario total de operaciones es 3%-5% del total de activos	Volumen diario total de operaciones es 6%-25% del total de activos	Volumen diario total de operaciones es >25% del total de activos
Servicio de tesorería al cliente	No se ofrece servicio de tesorería	Se ofrece servicio limitado; número de clientes es <1,000	Servicios ofrecidos incluyen caja de seguridad, originar ACH, y captura de depósito remoto; número de clientes está entre 1,000-10,000	Servicios ofrecidos incluyen soluciones para cuentas por cobrar y gestión de liquidez; número de clientes está entre 10,001-20,000	Múltiples servicios ofrecidos incluyen servicios de moneda extranjera, inversiones en línea, y cuentas inversión financiera transitoria; número de clientes es >20,000
Servicios fiduciarios	No se ofrecen servicios fiduciarios	Se ofrecen servicios fiduciarios a través de un proveedor externo; activos bajo la administración totalizan <US$500 millones	Se ofrecen servicios fiduciarios directamente; porfolio de activos bajo la administración totalizan US$500-900 millones	Se ofrecen servicios fiduciarios directamente; activos bajo la administración totalizan US$1,000-10,000 millones	Se ofrecen servicios fiduciarios directamente; activos bajo la administración totalizan >US$10,000 millones

Actúa como banco corresponsal (transferencias interbancarias)	No actúa como banco corresponsal	Actúa como banco corresponsal para <100 instituciones	Actúa como banco corresponsal para 100-250 instituciones	Actúa como banco corresponsal para 251-500 instituciones	Actúa como banco corresponsal para >500 instituciones

Categoría: Productos Online/Móviles y servicios tecnológicos	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Adquiriente comercial (auspicia comerciantes o actividad de procesamiento de tarjetas en el sistema de pagos)	No actúa como adquiriente comercial	Actúa como adquiriente comercial; <1,000 comerciantes	Actúa como adquiriente comercial; subcontrata el procesamiento de pago con tarjeta; 1,000-10,000 comerciantes	Actúa como adquiriente comercial y procesador de pago con tarjeta; 10,001-100,000 comerciantes	Actúa como adquiriente comercial y procesador de pago con tarjeta; <1,000 comerciantes
Servicios de alojamiento TI para otras organizaciones (ya sea por sistemas compartidos o soporte administrativo)	No brinda servicios de TI para otras organizaciones	Da alojamiento o proporciona servicios de TI a organizaciones afiliadas	Da alojamiento o proporciona servicios de TI hasta a 25 organizaciones no afiliadas	Da alojamiento o proporciona servicios de TI para 26-50 organizaciones no afiliadas	Da alojamiento o proporciona servicios de TI a >50 organizaciones afiliadas

Categoría: Características organizativas	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Fusiones y adquisiciones (incluyendo venta de activos y joint ventures)	No hay nada planeado	Abierto para iniciar conversaciones o buscar activamente una fusión o adquisición	En conversaciones por lo menos con una parte interesada	Se ha anunciado públicamente una venta o adquisición en el último año, en negociaciones con uno o más interesados	Están en proceso varias integraciones relacionas con adquisiciones
Empleados directos (incluyendo contratistas de tecnología informática y ciberseguridad)	Número total de empleados <50	Número total de empleados 50-2,000	Número total de empleados <2,001-10,000	Número total de empleados 10,001-50,000	Número de empleados es >50,000
Cambios en el personal de TI y seguridad informática	Cargos claves cubiertos; baja o inexistente rotación de personal	Existen vacantes para personal con roles no indispensables	Cierta rotación de cargos claves o senior	Rotación frecuente en cargos senior o claves	Puestos vacantes por largos periodos en cargos seniors o claves; alto nivel de rotación en TI o seguridad informática

Acceso privilegiado (red de Administradores, base de datos, aplicaciones, sistemas, etc.)	Número limitado de administradores; administradores externos limitados o inexistentes	Nivel de rotación de administradores no afecta las operaciones o actividades; puede utilizar algunos administradores externos	Nivel de rotación de administradores afecta las operaciones; número de administradores para sistemas individuales o aplicaciones excede lo necesario	Alto nivel de confianza en administradores externos; número de administradores no es suficiente para soportar el nivel o ritmo de cambio	Alta rotación de personal en administradores de red; muchos o la mayoría de los administradores son externos (contratistas o proveedores); la experiencia en administración de redes es limitada

Categoría: Características organizativas	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Cambios en el entorno de TI (p. ej. la red, infraestructura, aplicaciones importantes, tecnologías de soporte para nuevos productos o servicios)	Entorno de TI/ informático estable	Mínimos cambios o poco frecuentes en el entorno de TI	Nuevas tecnologías adoptadas con frecuencia	Gran cantidad de cambios significativos	Considerables cambios en el/los proveedores subcontratados para servicios cruciales de TI; con frecuencia ocurren cambios grandes y complejos en el entorno
Ubicación de sucursales /presencia comercial	1 estado	1 región	1 país	1-20 países	>20 países
Lugares de operación/centros de datos	1 estado	1 región	1 país	1-10 países	>10 países

Categoría: Amenazas externas	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Intentos de ciberataques	Ningún intento de ataque o no hubo reconocimiento	Pocos intentos al mes (<100); pueden haber tenido campañas de *phishing* genérico dirigidas a empleados y clientes	Varios ataques al mes (100-500); campañas de *phishing* dirigidas a empleados o clientes de la institución o a terceros que dan soporte a actividades cruciales; puede haber sufrido un ataque de denegación de servicios distribuidos (DDoS) en el último año	Significativo número de intentos al mes (501-100,000) campañas de *spear phishing* dirigidas a clientes con alto patrimonio neto y empleados de la institución o de terceros que dan soporte a actividades cruciales; la institución es mencionada específicamente en informes de amenazas; puede haber sufrido múltiples intentos de ataques DDoS en el último año	Considerable número de intentos de ataque al mes (>100,000) persistentes intentos para atacar a altos funcionarios y/o administradores de la red; frecuentemente dirigido por ataques DDoS (denegación de servicios distribuidos)

Total	Niveles de riesgo				
	Insignificante	Mínimo	Moderado	Significativo	Mayor
Número de declaraciones seleccionadas en cada nivel de riesgo					
En base a los niveles de riesgo seleccionados, asigne un perfil de riesgo inherente	**Insignificante**	**Mínimo**	**Moderado**	**Significativo**	**Mayor**

Madurez de Ciberseguridad

Dominio 1: Gestión y Supervisión del Riesgo Cibernético			
Factor de evaluación: Gobernabilidad			
		Y, Y(C), N	
SUPERVISIÓN	**Básico**		Los miembros designados de la administración son considerados responsables, ante la Junta Directiva o un Consejo Directivo apropiado, de implementar y gestionar los programas de seguridad informática de continuidad del negocio. *(FFIEC Information Security Booklet, página 3)* Los riesgos de seguridad informática se discuten en las reuniones de la administración cuando se producen acontecimientos cibernéticos muy notorios o se presentan alertas regulatorias. *(FFIEC Information Security Booklet, página 6)* La administración presenta un informe escrito, ante la Junta Directiva o Consejo Directivo apropiado, sobre el estado general de los programas de seguridad informática y continuidad del negocio, al menos una vez al año. *(FFIEC Information Security Booklet, página 5)* El proceso presupuestario incluye gastos y herramientas relacionados con la seguridad informática. *(FFIEC E-Banking Booklet, página 20)* La administración considera los riesgos que otras infraestructuras críticas (p.ej., telecomunicaciones, energía) representan para la institución. *(FFIEC Business Continuity Planning Booklet, página J-12)*
	En desarrollo		Por lo menos una vez al año, la Junta Directiva o un Consejo Directivo apropiado revisa y aprueba el programa de ciberseguridad de la institución. La administración es responsable por asegurar el cumplimiento de los requisitos legales y regulatorios relacionados a la ciberseguridad. El personal y las herramientas de ciberseguridad se solicitan a través del proceso presupuestario. Existe un proceso para discutir y estimar formalmente los gastos potenciales asociados a los incidentes de ciberseguridad como parte del proceso presupuestario.

	Intermedio		La Junta Directiva o un Consejo Directivo apropiado tiene conocimientos especializados en ciberseguridad o contrata expertos para ayudar con responsabilidades de supervisión. El paquete estándar para la reunión de la Junta Directiva incluye informes y medidas que van más allá de los eventos e incidentes para poder abordar las tendencias de la inteligencia de amenazas y la postura respecto a la seguridad de la institución. La institución tiene una declaración de propensión al riesgo cibernético aprobada por la Junta Directiva o un Consejo Directivo apropiado. Los riesgos cibernéticos que exceden la propensión al riesgo son elevados a la administración. La Junta Directiva o un Consejo Directivo apropiado garantiza que la autoevaluación anual sobre ciberseguridad evalúe la habilidad de la institución para alcanzar sus estándares de gestión de riesgo cibernético. La Junta Directiva o un Consejo Directivo apropiado revisa y aprueba las decisiones que la administración toma en cuanto a prioridades y asignación de recursos en base a los resultados de las evaluaciones cibernéticas. La Junta Directiva o un Consejo Directivo apropiado garantiza que la administración tome las acciones necesarias para abordar los cambiantes riesgos cibernéticos o los temas importantes de ciberseguridad. El proceso presupuestario para solicitar personal y herramientas adicionales de ciberseguridad está integrado en procesos presupuestarios de las unidades de negocio.
	Avanzado		La Junta Directiva o un Consejo Directivo apropiado aprobó que la declaración de propensión al riesgo cibernético forma parte de la declaración de propensión al riesgo en toda la empresa. La administración tiene un proceso formal para mejorar continuamente la supervisión en ciberseguridad. El proceso presupuestario para solicitar personal y herramientas de ciberseguridad adicionales alinea los recursos y herramientas con la estrategia de seguridad cibernética. La administración y la Junta Directiva o un Consejo Directivo apropiado consideran responsables a las unidades comerciales por administrar efectivamente todos los riesgos cibernéticos asociados a sus actividades. La administración identifica la(s) causa(s) profunda(s) cuando los ataques cibernéticos resultan en pérdidas materiales. La Junta Directiva o un Consejo Directivo apropiado garantiza que las acciones de la administración consideren los riesgos cibernéticos que la institución representa para el sector financiero.

	Innovador		La Junta Directiva o un Consejo Directivo apropiado discute de qué manera la administración puede desarrollar mejoras en ciberseguridad y que estas puedan ser adoptadas en todo el sector. La Junta Directiva o un Consejo Directivo apropiado verifica que las acciones de la administración consideren los riesgos cibernéticos que la institución representa para otras infraestructuras importantes (por ejemplo, telecomunicaciones, energía).
ESTRATEGIAS / POLÍTICAS	**Básico**		La institución tiene una estrategia de seguridad informática que integra tecnología, políticas, procedimientos y capacitación para aliviar el riesgo. *(FFIEC Information Security Booklet, página. 3)* La institución tiene políticas acordes con su riesgo y complejidad que abarcan los conceptos de gestión de riesgos de la tecnología de la información. *(FFIEC Information Security Booklet, página 16)* La institución tiene políticas acordes con su riesgo y complejidad que abarcan los conceptos de intercambio de información de amenazas. *(FFIEC E-Banking Booklet, página 28)* La institución tiene políticas aprobadas por la Junta Directiva que van acordes con su riesgo y complejidad, las cuales abordan la seguridad informática. *(FFIEC Information Security Booklet, página 16)* La institución tiene políticas acordes con su riesgo y complejidad que abarcan los conceptos de dependencia externa o administración por parte de terceros. *(FFIEC Outsourcing Booklet, página 2)* La institución tiene políticas acordes con su riesgo y complejidad que abarcan los conceptos de respuesta a los incidentes y resiliencia. *(FFIEC Information Security Booklet, página 83)* Todos los elementos del programa de seguridad informática están coordinados a través de toda la empresa. *(FFIEC Information Security Booklet, página 7)*
	En desarrollo		La institución amplió su estrategia de seguridad informática para incorporar la ciberseguridad y la resiliencia. La institución tiene un programa formal de ciberseguridad que está basado en los estándares y referencias de la industria de la tecnología y seguridad. Existe un proceso formal para actualizar las políticas a medida que el perfil de riesgo inherente de la institución vaya cambiando.

	Intermedio		La institución tiene un amplio conjunto de políticas que va acorde con su riesgo y complejidad el cual abarca los conceptos de inteligencia de amenazas. La administración revisa periódicamente la estrategia de ciberseguridad para abarcar las cambiantes amenazas cibernéticas y los cambios en el perfil de riesgo inherente de la institución. La estrategia de ciberseguridad está incorporada a la estrategia de la gestión de riesgos en toda la empresa, o conceptualmente se ajusta dentro de ella. La administración enlaza los objetivos estratégicos de ciberseguridad con las metas tácticas. Existe un proceso formal para hacer referencia cruzada y al mismo tiempo actualizar todas las políticas relacionadas a los riesgos cibernéticos
	Avanzado		La estrategia de ciberseguridad delinea el estado futuro de ciberseguridad de la institución con perspectivas a corto y largo plazo. Los estándares de ciberseguridad reconocidos por el sector industrial son utilizados como fuentes durante el análisis de las discrepancias en el programa de ciberseguridad. La estrategia de ciberseguridad identifica y comunica el rol de la institución como un componente de infraestructura primordial en la industria de los servicios financieros. El rol de la institución en infraestructura crítica informa sobre la propensión al riesgo. La administración está continuamente mejorando el programa de ciberseguridad actual para adaptarlo a medida cambia el estado del objetivo de ciberseguridad.
	Innovador		La estrategia de ciberseguridad identifica y comunica el rol de la institución a medida que se relaciona con otras infraestructuras cruciales.
GESTIÓN DE ACTIVOS DE TI	**Básico**		Se mantiene un inventario de los activos de la organización/ de TI (por ejemplo, hardware, software, datos y sistemas alojados de manera externa) *(FFIEC Information Security Booklet, página 9*) Los activos de la organización de TI (por ejemplo, hardware, sistemas, datos y aplicaciones) tienen prioridad para recibir protección dependiendo del tipo de información y el valor comercial. *(FFIEC Information Security Booklet, página 12)* La administración asigna la responsabilidad de mantener un inventario de los activos de TI. *(FFIEC Information Security Booklet, página 9)* Existe un proceso de gestión de cambio para solicitar y aprobar cambios en las configuraciones de los sistemas, en el hardware, software, aplicaciones y herramientas de seguridad. *(FFIEC Information Security Booklet, página 56)*

	En desarrollo		El inventario de los activos, incluyendo la identificación de los activos más importantes, se actualiza por lo menos una vez al año para consignar activos nuevos, reasignados, redefinidos y aquellos que tienen fecha de expiración. La institución tiene un proceso documentado del ciclo de vida de los activos el cual considera si los activos que deben ser adquiridos, tienen o no salvaguardas de seguridad apropiados. La institución gestiona de manera proactiva el sistema de fin de ciclo de vida (EOL) (por ejemplo, remplazo) para limitar los riesgos de seguridad. Los cambios son formalmente aprobados por una persona o comisión con la debida autoridad y con separación de funciones.
	Intermedio		Las configuraciones básicas no pueden ser modificadas sin contar con una solicitud formal de cambio, una aprobación documentada y una evaluación de las implicaciones en seguridad. Un proceso formal de gestión de cambio de TI requiere que se evalúe el riesgo de ciberseguridad durante el análisis, aprobación, pruebas e informe de los cambios.
	Avanzado		El riesgo en la cadena de suministro es revisado antes de la adquisición de sistemas de información considerados de misión crítica, incluyendo los componentes del sistema. Las herramientas automatizadas hacen posible el seguimiento, actualización, priorización de activos y el informe personalizado del inventario de activos. Existen procesos automatizados para detectar y bloquear cambios no autorizados en el software y el hardware. El sistema de gestión de cambios utiliza umbrales para determinar cuándo se requiere una evaluación de riesgo del impacto
	Innovador		Una función formal de gestión de cambios controla las solicitudes de cambio descentralizadas o altamente distribuidas, así mismo, identifica y mide los riesgos de seguridad que puede ocasionar un aumento en la exposición a ciberataques. Se han implementado herramientas de la empresa automatizadas e integrales para detectar y bloquear cambios no autorizados en el software y el hardware.
		Factor de Evaluación: Gestión de Riesgo	
PROGRAMA DE GESTIÓN DE RIESGO	**Básico**		Dentro de la institución, existe(n) la(s) función(es) de gestión de riesgos de seguridad informática y continuidad comercial. *(FFIEC Information Security Booklet, página 68)*
	En desarrollo		El programa de gestión de riesgos incluye la identificación de riesgos cibernéticos, su cuantificación, mitigación, monitoreo e informe. La administración revisa y utiliza los resultados de las auditorías para mejorar las políticas, procedimientos y controles de ciberseguridad existentes.

			La administración monitorea temas de riesgo residual alto y moderado a partir de la evaluación de riesgo de ciberseguridad hasta que los temas son abordados adecuadamente.
	Intermedio		La función de ciberseguridad tiene una clara línea de jerarquía, la cual no presenta conflicto de intereses. El programa de gestión de riesgos aborda específicamente los riesgos cibernéticos más allá de los límites de los impactos tecnológico (por ejemplo, financieros, estratégicos, regulatorios y de cumplimiento). Se han establecido puntos de referencias o mediciones del rendimiento del objetivo para mostrar las mejoras o retrocesos de las condiciones de seguridad a lo largo del tiempo. La administración utiliza los resultados de auditorías independientes y revisiones para mejorar la ciberseguridad. Existe un proceso para analizar y asignar pérdidas potenciales y gastos relacionados a ellas, por centro de costos, en relación con los incidentes de ciberseguridad.
	Avanzado		Las mediciones de ciberseguridad se utilizan para hacer posible una estratégica toma de decisiones y financiar áreas que lo requieran. La gestión de riesgos independiente establece y monitorea los límites relacionados con los riesgos cibernéticos para las unidades comerciales. El personal de la gestión de riesgos independiente eleva a la administración y a la Junta Directiva, o a un Consejo Directivo apropiado, las discrepancias más significativas de la evaluación de riesgos cibernéticos de la unidad comercial. Existe un proceso para analizar el impacto financiero que los incidentes cibernéticos tienen sobre el capital de la institución. La agregación de datos sobre riesgos cibernéticos y las capacidades de informar en tiempo real soportan las necesidades actuales que tiene la institución de informar, especialmente durante incidentes cibernéticos.
	Innovador		La función de gestión de riesgos identifica y analiza los elementos en común en los sucesos cibernéticos que ocurren tanto en la institución como en otros sectores para habilitar una gestión de riesgos más predecible. Existe un proceso para analizar el impacto financiero que un incidente cibernético en la institución puede tener a lo largo del sector financiero.
EVALUACIÓN DE RIESGO	**Básico**		Una evaluación de riesgo enfocada en salvaguardar información del cliente identifica las amenazas internas y externas, las razonables y predecibles, la probabilidad y el daño potencial de las amenazas, y la adecuación de las políticas, los procedimientos y sistemas de información del cliente. *(FFIEC Information Security Booklet, página 8)* La evaluación de riesgo identifica los sistemas basados en internet y las transacciones de alto riesgo que garantizan controles de autenticación adicional. *(FFIEC Information Security Booklet, página 12)*

			La evaluación de riesgo se actualiza para abordar nuevas tecnologías, productos, servicios y conexiones antes del despliegue. *(FFIEC Information Security Booklet, pág. 13)*
	En desarrollo		Las evaluaciones de riesgo se utilizan para identificar los riesgos de ciberseguridad provenientes de nuevos productos, servicios o relaciones. El enfoque de la evaluación de riesgo se ha expandido más allá de la información del cliente para abordar toda la información de los activos. La evaluación de riesgo considera el riesgo de utilizar componentes de software y hardware en el fin de su vida útil.
	Intermedio		La evaluación de riesgo se ajusta para tomar en consideración riesgos ampliamente conocidos o prácticas de gestión de riesgos.
	Avanzado		Una función de gestión de riesgos en toda la empresa incorpora el análisis de una amenaza cibernética y la exposición específica al riesgo como parte de la evaluación de riesgo de la empresa.
	Innovador		La evaluación de riesgo es actualizada en tiempo real a medida que ocurren cambios en el perfil de riesgo, se lanzan o actualizan nuevos estándares aplicables y se anticipan nuevas exposiciones. La institución utiliza información de las evaluaciones de riesgo para predecir amenazas y obtener resultados en tiempo real. Los análisis automatizados o avanzados ofrecen información predictiva y medidas de riesgo en tiempo real.
AUDITORÍA	**Básico**		Una auditoría o revisión independiente evalúa las políticas, procedimientos y controles a través de toda la institución buscando riesgos importantes y temas de control asociados a las operaciones de la institución, incluyendo riesgos en nuevos productos, tecnologías emergentes y sistemas de información. *(FFIEC Audit Booklet, página 4)* La función de auditoría independiente valida los controles relacionados al almacenamiento o transmisión de información confidencial. *(FFIEC Audit Booklet, página 1)* Las prácticas de acceso (logging) son revisadas periódicamente para asegurar una gestión apropiada del acceso (por ejemplo, controles de acceso, retención y mantenimiento). *(FFIEC Operations Booklet, página 29)* Se realiza formalmente un seguimiento de los asuntos y acciones correctivas de auditorías internas y pruebas/evaluaciones independientes a fin de asegurar que las fallas sean resueltas de manera oportuna. *(FFIEC Information Security Booklet, página 6)*

	En desarrollo		La función de auditoría independiente valida que la función de gestión de riesgos esté de acuerdo con la complejidad y riesgo de la institución. La función de auditoría independiente valida que el intercambio de información sobre amenazas de la institución esté de acuerdo con la complejidad y riesgo de esta. La función de auditoría independiente valida que la función de controles de ciberseguridad de la institución esté de acuerdo con la complejidad y riesgo de esta. La función de auditoría independiente valida que la gestión de las relaciones con terceros de la institución esté de acuerdo con la complejidad y riesgo de esta. La función de auditoría independiente valida que el programa de respuesta ante incidentes y la resiliencia de la institución estén de acuerdo con la complejidad y riesgo de esta.
	Intermedio		Existe un proceso formal para que la función de auditoría independiente actualice sus procedimientos en base a cambios en el perfil inherente de riesgo de la institución. La función de auditoría independiente valida que la inteligencia y colaboración sobre amenazas de la institución estén de acuerdo con la complejidad y riesgo de esta. La función de auditoría independiente revisa regularmente la declaración de propensión a riesgos cibernéticos de la administración. Las auditorías o revisiones independientes se utilizan para identificar discrepancias en cuanto a los conocimientos especializados y habilidades existentes en temas de seguridad.
	Avanzado		Existe un proceso formal para que la función de auditoría independiente actualice sus procedimientos en base a cambios que ocurren en el cambiante panorama de amenazas a través de todo el sector. La función de auditoría independiente revisa regularmente la declaración de propensión a riesgos cibernéticos en comparación con los resultados de la evaluación e incorpora las discrepancias dentro de la estrategia de auditoría. Las auditorías o revisiones independientes se utilizan para identificar debilidades en ciberseguridad, causas subyacentes e impacto potencial para las unidades de negocio.
	Innovador		Existe un proceso formal para que la función de auditoría independiente actualice sus procedimientos en base a cambios que ocurren en el cambiante panorama de amenazas a través de otros sectores de los que depende la institución. La función de auditoría independiente utiliza sofisticadas herramientas de minería de datos para realizar un monitoreo continuo de los procesos o controles en ciberseguridad.

Factor de Evaluación: Recursos			
PERSONAL	**Básico**		Se han identificado los roles y responsabilidades de la seguridad informática. *(FFIEC Information Security Booklet, página 7)* Existen procesos para identificar conocimientos especializados adicionales que se requieren para mejorar las defensas de la seguridad informática. *(FFIEC Information Security Work Program, objetivo I: 2-8)*
	En desarrollo		Se utiliza un proceso formal para identificar las herramientas y los conocimientos especializados que puedan ser necesarios. La administración cuenta con un apropiado conocimiento y experiencia para conducir los esfuerzos en ciberseguridad de la institución. El personal con responsabilidades en ciberseguridad cuenta con las calificaciones requeridas para realizar las tareas que corresponden a su cargo. Los candidatos para algún puesto de trabajo, contratistas y terceros están sujetos a una verificación de antecedentes correspondiente a la confidencialidad de la información a la que tienen acceso, los requisitos comerciales), y riesgos aceptables.
	Intermedio		La institución cuenta con un programa para reclutamiento de talentos, retención y planificación de la sucesión del personal de ciberseguridad y resiliencia.
	Avanzado		La institución compara a su personal/equipo de ciberseguridad con sus similares para identificar si su reclutamiento, retención y planes de sucesión están de acuerdo con los otros. El personal especializado en ciberseguridad desarrolla, o contribuye al desarrollo, de la seguridad integrada a nivel de empresa y de las estrategias de ciberdefensa.
	Innovador		La institución activamente colabora con asociaciones industriales y del ámbito académico para informar sobre el currículo basado en las futuras necesidades del personal de ciberseguridad en la industria.
Factor de Evaluación: Capacitación y Cultura			
CAPACITACIÓN	**Básico**		Se proporciona capacitación anual en seguridad informática. *(FFIEC Information Security Booklet, página 66)* La capacitación anual en seguridad informática incluye respuesta ante incidentes, amenazas cibernéticas actuales (por ejemplo, *phishing*, *spear phishing*, ingeniería social, y seguridad en telefonía móvil), y otros temas que puedan ir surgiendo. *(FFIEC Information Security Booklet, página 66)* Se pone a disposición de los empleados material sobre Consciencia Situacional cuando acontecen eventos cibernéticos muy visibles o por alertas regulatorias. *(FFIEC Information Security Booklet, página 7)* Materiales sobre Concientización del Cliente están disponibles fácilmente (por ejemplo, DHS' Cybersecurity Awareness Month materials). *(FFIEC E-Banking Work Program, Objetivo 6-3)*

	En desarrollo		La institución tiene un programa de capacitación continua en ciberseguridad y desarrollo de habilidades para el personal de ciberseguridad. La administración recibe capacitación en ciberseguridad adecuada a las responsabilidades del cargo. Empleados que tienen permisos para cuentas privilegiadas reciben capacitación adicional en ciberseguridad de acuerdo con sus niveles de responsabilidad. Las unidades de negocio reciben capacitación en ciberseguridad adecuada a los riesgos específicos de sus negocios. La institución valida la efectividad de la capacitación (por ejemplo, ingeniería social o pruebas de *phishing*).
	Intermedio		La administración incluye las lecciones aprendidas de la ingeniería social y los ejercicios de phishing para mejorar los programas de concientización de los empleados. Los clientes minoristas y los clientes comerciales reciben información sobre concientización en ciberseguridad por lo menos una vez al año. Las unidades de negocio reciben capacitación en ciberseguridad adecuada a los riesgos específicos del negocio, además de lo solicitado en la institución como un todo. La institución actualiza habitualmente la capacitación de su personal de seguridad para adaptarlo a las nuevas amenazas.
	Avanzado		Los directores independientes reciben capacitación en ciberseguridad la cual aborda cómo los productos complejos, servicios y líneas de negocio afectan los riesgos cibernéticos de la institución.
	Innovador		Se utilizan indicadores clave de rendimiento para determinar si la capacitación y los programas de concientización tienen influencia positiva en el comportamiento.
CULTURA	**Básico**		La administración responsabiliza a los empleados por el cumplimiento del programa de seguridad informática. *(FFIEC Information Security Booklet, página. 7)*
	En desarrollo		La institución tiene normas de conducta formales que responsabilizan a todos los empleados por el cumplimiento de las políticas y procedimientos en ciberseguridad. Los riesgos de ciberseguridad son ampliamente discutidos en las reuniones de las unidades de negocio Los empleados saben claramente cómo identificar y elevar los problemas potenciales de ciberseguridad.

	Intermedio		La administración garantiza que los planes de rendimiento estén ligados al cumplimiento de las políticas y estándares en ciberseguridad, de tal manera que los empleados se responsabilicen de ello. La cultura de riesgo requiere de una consideración formal de riesgos cibernéticos en todas las decisiones del negocio. En las reuniones de gestión de riesgos independiente se presentan y discuten los informes sobre los riesgos cibernéticos.
	Avanzado		La administración garantiza una permanente mejora en la cultura de toma de conciencia de los riesgos cibernéticos.
	Innovador		La institución lidera los esfuerzos para promover la cultura de ciberseguridad en todo el sector y en otros sectores de los que dependen.

Dominio 2: Inteligencia de Amenazas y Colaboración

Factor de Evaluación: Inteligencia de Amenazas

		Y, Y(C), N	
INTELIGENCIA DE AMENAZAS Y COLABORACIÓN	**Básico**		La institución pertenece o está suscrita a una o más fuentes de intercambio de información de amenazas y vulnerabilidades que brindan información sobre amenazas (por ejemplo, Centro de Análisis e Intercambio de Información de Servicios Financieros [FS-ISAC], Equipo de Preparación para Emergencias Informáticas de los Estados Unidos [US-CERT] *(FFIEC E-Banking Work Program, página 28)* La información de amenazas se utiliza para monitorear amenazas y vulnerabilidades. *(FFIEC Information Security Booklet, página 83)* La información de amenazas se utiliza para mejorar la gestión y controles de los riesgos internos. *(FFIEC Information Security Booklet, página 4)*
	En desarrollo		La información de amenazas recibida por la institución incluye análisis de tácticas, patrones y recomendaciones para mitigar el riesgo.
	Intermedio		Se ha implementado un programa formal de inteligencia de amenazas el cual incluye una suscripción a informes sobre amenazas informáticas de proveedores externos y fuentes internas. Se han implementado protocolos para recolectar información de instituciones comparables en la industria y del gobierno. Se mantiene un repositorio central de inteligencia de amenazas cibernéticas solo para lectura.
	Avanzado		Se utiliza un modelo de inteligencia cibernética para recolectar información sobre amenazas. Se recibe automáticamente la inteligencia de amenazas desde diversas fuentes en tiempo real. La inteligencia de amenazas de la institución incluye información relacionada a eventos geopolíticos que podrían aumentar los niveles de amenaza de ciberseguridad.
	Innovador		Un sistema de análisis de amenazas correlaciona automáticamente la información de amenazas con riesgos específicos, y luego toma acciones automatizadas basadas en el riesgo, al mismo tiempo que ponen en alerta a la administración. La institución está invirtiendo en el desarrollo de una nueva inteligencia de amenazas y mecanismos de colaboración (por ejemplo, tecnologías, procesos de negocios) que transformarán la manera de recolectar y compartir la información

Factor de Evaluación: Monitoreo y Análisis			
MONITOREO Y ANÁLISIS	**Básico**		Los registros de auditoría y otros registros relacionados a eventos de seguridad se revisan y conservan de forma segura. *(FFIEC Information Security Booklet, página 79)* Los registros de eventos informáticos se utilizan para investigaciones una vez que estos eventos hayan ocurrido. *(FFIEC Information Security Booklet, página 83)*
	En desarrollo		Implementación de un proceso para monitorear información de amenazas y así descubrir amenazas emergentes. El proceso de información de amenazas y análisis es asignado a un grupo específico o a una determinada persona. Los procesos de seguridad y tecnología están centralizados y son coordinados por el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) o una entidad equivalente. Los sistemas de monitoreo funcionan continuamente con el apoyo adecuado para ofrecer un eficiente manejo de los incidentes.
	Intermedio		Existe un equipo de inteligencia de amenazas que evalúa, desde varias fuentes, la inteligencia de amenazas en cuanto a credibilidad, relevancia y exposición. Se ha creado un perfil para cada amenaza que identifica un posible intento, la capacidad y el objetivo de la amenaza. Las fuentes de información de amenazas que abordan todos los componentes del perfil de amenaza tienen prioridad y son monitoreadas. Se analiza la inteligencia de amenazas para elaborar resúmenes de amenazas cibernéticas incluyendo los riesgos para la institución y las acciones específicas que la institución debe tener en consideración.
	Avanzado		Existe un comité o un equipo destinado al análisis e identificación de amenazas cibernéticas a fin de centralizar y coordinar iniciativas y comunicaciones. Se han definido procesos formales para resolver conflictos potenciales en cuanto a información recibida de centros de análisis e intercambio de información o de otras fuentes. Para predecir futuros ataques se utiliza el análisis de registros correlacionados y la inteligencia de amenazas internas o externas emergentes. La inteligencia de amenazas es considerada dentro del contexto del perfil de riesgo y la propensión al riesgo de la institución a fin de dar prioridad a las acciones que mitiguen con anticipación las amenazas. La inteligencia de amenazas es utilizada para actualizar la arquitectura y los estándares de configuración.

	Innovador		La institución utiliza diversas fuentes de inteligencia, análisis de registros correlacionados, alertas, flujos de tráfico interno y eventos geopolíticos a fin de predecir futuros posibles ataques y tendencias de ataques. Para predecir amenazas contra objetivos específicos del negocio se utilizan escenarios del más alto riesgo. Los sistemas de TI detectan automáticamente las debilidades en la configuración en base a la inteligencia de amenazas y a la gestión de alertas de tal manera que se pueda dar prioridad a las acciones a tomar.
			Factor de Evaluación: Intercambio de Información
INTERCAMBIO DE INFORMACIÓN	**Básico**		Las amenazas de seguridad informática son recolectadas y compartidas con empleados correspondientes de la institución. *(FFIEC Information Security Booklet, página 83)* Se conservan y actualizan regularmente los datos de contacto de las autoridades de la ley y los entes reguladores. *(FFIEC Business Continuity Planning Work Program, Objetivo I: 5-1)* La información acerca de amenazas es compartida con las autoridades de la ley y los entes reguladores cuando se requiera o lo soliciten. *(FFIEC Information Security Booklet, página 84)*
	En desarrollo		Existe un proceso seguro y formal para compartir información sobre amenazas y vulnerabilidad con otras entidades. Un representante de la institución participa en reuniones de las organizaciones de intercambio de información y otras autoridades.
	Intermedio		Existe un protocolo formal para compartir, con los empleados, información de amenazas, vulnerabilidad e incidentes en base a las funciones de trabajo específicas. Los acuerdos de intercambio de información se utilizan según se requiera o lo soliciten a fin de facilitar el intercambio de información sobre amenazas con otras organizaciones del sector financiero o de terceros. La información es compartida de manera proactiva con la industria, las autoridades, los entes reguladores, y los foros de intercambio de información. Existe un proceso para comunicar y colaborar con el sector público respecto a las amenazas cibernéticas.
	Avanzado		La administración comunica a las unidades de negocio sobre la inteligencia de amenazas con el contexto de riesgo del negocio y las recomendaciones de la administración de riesgo específico. Existen relaciones con empleados de instituciones similares para intercambiar inteligencia de amenazas cibernéticas Se ha establecido una red de relaciones confiables (formales y/o informales) para evaluar información acerca de amenazas cibernéticas.

	Innovador		Existe un mecanismo para intercambiar inteligencia de amenazas cibernéticas con las unidades de negocios en tiempo real incluyendo el impacto potencial financiero y operacional de la inacción. Un sistema informa automáticamente a la administración acerca del nivel de riesgo del negocio específico para la institución, así como del progreso de los pasos recomendados para mitigar los riesgos La institución está realizando esfuerzos para crear nuevos canales que compartan información a través de todo el sector a fin de abordar las discrepancias en los mecanismos de intercambio de información orientados hace entidades externas.

Dominio 3: Controles de Ciberseguridad

Factor de Evaluación: Controles preventivos

		Y, Y(C), N	
GESTIÓN EN INFRAESTRUCTURA	**Básico**		Se utilizan herramientas de defensa del perímetro de la red (por ejemplo, router de área perimetral y firewalls. *(FFIEC Information Security Booklet, página 33)* Los sistemas a los que se tiene acceso desde el Internet o a través de terceros externos están protegidos por firewalls o por otros dispositivos semejantes. *(FFIEC Information Security Booklet, página 46)* Todos los puertos son monitoreados. *(FFIEC Information Security Booklet, página 50)* Se utilizan antivirus actualizados y herramientas anti-malware. *(FFIEC Information Security Booklet, página 78)* Las configuraciones de los sistemas (para servidores, computadoras, routers, etc.) siguen los estándares de la industria y deben ser cumplidos. *(FFIEC Information Security Booklet, página 56)* Están prohibidos los puertos, funciones, protocolos y servicios si ya no son necesarios para el negocio. *(FFIEC Information Security Booklet, página 50)* El acceso para realizar cambios en la configuración de los sistemas (incluyendo máquinas virtuales e hipervisores) es controlado y monitoreado. *(FFIEC Information Security Booklet, página 56)* Están restringidos los programas que permiten tomar control manual del sistema, objetos, la red, la máquina virtual y los controles de aplicaciones. *(FFIEC Information Security Booklet, página 41)* Las sesiones del sistema se cierran después de un período de inactividad preestablecida y se dan por concluidas una vez que se cumplan las condiciones preestablecidas. *(FFIEC Information Security Booklet, página 23)* Los entornos de la red inalámbrica necesitan una configuración de seguridad con un sólido encriptado para autenticación y transmisión. (*No se aplica si no hay redes inalámbricas.) *(FFIEC Information Security Booklet, página 40)*
	En desarrollo		Existe un firewall en cada conexión de internet y también entre cualquier Zona Desmilitarizada (DMZ) y una o varias redes internas. Los antivirus y sistemas de detección/prevención de una intromisión (IDP/IPS) detectan y bloquean ataques o intromisiones reales o fallidas. Los controles técnicos evitan que los dispositivos no autorizados, incluyendo los puntos de acceso inalámbrico no autorizado y medios extraíbles, puedan conectarse a una o varias redes internas.

			Existe una solución basada en el riesgo en la institución o del proveedor de servicio de internet para mitigar ciberataques perjudiciales (por ejemplo, ataques DDoS). Las redes inalámbricas para invitados están totalmente separadas de la red o redes internas (*No se aplica si no existen redes inalámbricas.) Se han implementado extensiones de seguridad para el sistema de nombres de dominio (DNSSEC) en toda la empresa. Se revisan periódicamente los sistemas cruciales soportados por tecnologías heredadas para identificar vulnerabilidades potenciales, oportunidades de mejoras, o nuevas capas de defensa. Se implementan y prueban controles para sistemas sin soporte.
	Intermedio		La red de la empresa está segmentada en varias zonas separadas de confianza o seguridad, con estrategias de defensa en profundidad (por ejemplo, segmentación de red lógica, copias de respaldo, *air-gapping*) a fin de mitigar ataques. Se utilizan controles de seguridad para acceso remoto a todas las consolas administrativas, incluyendo los sistemas virtuales restringidos. Los entornos de red inalámbricos tienen cortafuegos perimetrales que están implementados y configurados para restringir el tráfico no autorizado. (*No se aplica si no hay redes inalámbricas.) Las redes inalámbricas utilizan un encriptado sólido con claves que se cambian frecuentemente. (*No se aplica si no hay redes inalámbricas.) El rango de transmisión de la red o redes inalámbricas está limitada a las fronteras controladas de la institución. (*No se aplica si no hay redes inalámbricas.) Existen medidas técnicas para evitar la ejecución de un código no autorizado en un dispositivo, una infraestructura de redes o en componentes de sistemas de propiedad de la institución o administrados por ella.
	Avanzado		Los entornos de red y las instancias virtuales están diseñadas y configuradas para restringir y monitorear el tráfico entre zonas confiables y zonas no confiables. Solo se permite una función primaria por servidor para prevenir funciones que requieran diferentes niveles de seguridad Existen medidas contra la suplantación de identidad (*anti-spoofing*) a fin de detectar y bloquear direcciones IP de fuentes falsificadas, y evitar que ingresen a la red.

	Innovador		La institución evalúa el riesgo de los activos de su infraestructura y lo actualiza en tiempo real basado en amenazas, vulnerabilidades o cambios operacionales. Se han implementado controles automatizados basados en la evaluación del riesgo de los activos de infraestructura, incluyendo la desconexión automática de los activos afectados. La institución busca proactivamente identificar discrepancias en el control que puedan ser utilizadas como parte del ataque del día cero. Los servidores que tratan con el público se rotan de forma rutinaria y se restablecen para comenzar de cero, y así limitar la ventana de tiempo a la que un sistema se expone a amenazas potenciales.
ACCESO Y GESTIÓN DE DATOS	**Básico**		A los empleados se les otorga acceso a los sistemas de datos e información confidencial en base a las responsabilidades propias del puesto y a los principios del menor privilegio. *(FFIEC Information Security Booklet, página 19)* El acceso de los empleados a los sistemas e información confidencial prevé la separación de funciones. *(FFIEC Information Security Booklet, página 19)* Los mayores privilegios (por ejemplo, privilegios del administrador) están limitados y fuertemente controlados (por ejemplo, asignados a personas, no compartido, y requieren controles con contraseñas más sólidas. *(FFIEC Information Security Booklet, página 19)* Periódicamente, se revisan los accesos de los usuarios a todos los sistemas y aplicaciones en base a los riesgos de la aplicación o del sistema. *(FFIEC Information Security Booklet, página 18)* Cambios en el acceso del usuario a físico y lógico, incluyendo aquellos que resultan de terminaciones voluntarias e involuntarias, se presentan/envían y aprueban por el personal apropiado. *(FFIEC Information Security Booklet, page 18)* Para gestionar el acceso a los sistemas, aplicaciones y hardware es necesario contar con identificación y autenticación. *(FFIEC Information Security Booklet, página 21)* Los controles de acceso requieren complejidad en la formulación de contraseñas y que el número de intentos de uso sea limitado. *(FFIEC Information Security Booklet, página 66)* Todas las contraseñas por defecto y cuentas por defecto innecesarias se cambian antes de la implementación del sistema. *(FFIEC Information Security Booklet, página 61)* Para que los clientes tengan acceso a los productos o servicios en internet es necesario que existan controles de autenticación (por ejemplo, controles de capas, múltiples factores) y que estos estén de acuerdo con el riesgo. *(FFIEC Information Security Booklet, página 21)* Los entornos de producción y no producción están separados para evitar acceso no autorizado o cambios en los activos de información

			(*No se aplica si no existen entornos de no producción en la institución o terceros de la institución.) *(FFIEC Information Security Booklet, página. 64)* Los controles de seguridad física son utilizados para evitar acceso no autorizado a los sistemas de información y sistemas de telecomunicaciones. *(FFIEC Information Security Booklet, página 47)* Todas las contraseñas están encriptadas en almacenamiento y en tránsito. *(FFIEC Information Security Booklet, página 21)*
			La información confidencial está encriptada cuando se transmite a través de las redes públicas o redes no confiables (por ejemplo, Internet). *(FFIEC Information Security Booklet, página 51)* Los dispositivos móviles (por ejemplo, laptops, tabletas y medios extraíbles) están encriptados si se utilizan para almacenar información confidencial. (*N/D si no se usa un dispositivo móvil). *(FFIEC Information Security Booklet, página 51)* El acceso a los sistemas críticos por parte de los empleados, contratistas y terceros utiliza conexiones encriptadas y autenticación de múltiples factores. *(FFIEC Information Security Booklet, página 45)* Existen controles administrativos, físicos o técnicos para evitar que los usuarios sin responsabilidades administrativas instalen software no autorizado. *(FFIEC Information Security Booklet, página 25* El servicio de atención al cliente (por ejemplo, el centro de llamadas) utiliza procedimientos formales para autenticar a los clientes de acuerdo con el riesgo de la transacción *(FFIEC Information Security Booklet, página 19)* Los datos se descartan o destruyen de acuerdo con los requerimientos documentados y dentro de los marcos de tiempo esperados. *(FFIEC Information Security Booklet, página 66)*
	En desarrollo		Cambios en los permisos de acceso para el usuario activan notificaciones para el personal correspondiente. Los administradores tienen dos cuentas: una para uso administrativo y otra para fines generales, tareas no administrativas. El uso de información del cliente en ambientes de no producción cumple con los requerimientos de política interna, regulatoria y legal para ocultar o retirar elementos de información confidencial. El acceso físico a los sistemas confidenciales o de alto riesgo está restringido, el registro y el acceso no autorizado está bloqueado. Existen controles para evitar el acceso no autorizado a las claves encriptadas.

	Intermedio		La institución ha implementado herramientas para evitar el acceso no autorizado o la extrusión de información confidencial. Existen controles para evitar la asignación no autorizada de los privilegios del usuario. Existen controles de acceso para los administradores de la base de datos para evitar la descarga no autorizada o la transmisión de información confidencial. Se retiran todos los accesos físicos y lógicos inmediatamente después que haya sido notificada la terminación involuntaria y dentro de las 24 horas de la salida voluntaria de un empleado. Se han implementado controles de capas y/o autenticación de múltiples factores para proteger a la red de la institución y/o sistemas y aplicaciones de cualquier acceso de terceros. Se utilizan técnicas de autenticación de múltiples factores (p. ej., tokens, certificados digitales) para el acceso de los empleados a los sistemas de alto riesgo según lo identificado en evaluación(es) de riesgo. (*No se aplica si no hay sistemas de alto riesgo.) La información confidencial está encriptada cuando está en tránsito en conexiones privadas (p. ej., retransmisión de trama y T1) y dentro de las zonas de confianza de la institución. Existen controles para evitar el acceso no autorizado a dispositivos y aplicaciones informáticas de uso compartido (por ejemplo, pizarras blancas en red, cámaras, micrófonos, aplicaciones online tales como mensajería instantánea y compartir documentos). (*No se aplica si no se utilizan equipos informáticos de uso compartido.)
	Avanzado		El encriptado de información seleccionada contenida es determinado por la clasificación y evaluación de riesgo de la información de la institución. La autenticación del cliente para el caso de transacciones de alto riesgo incluye métodos para evitar ataques de malware y ataques de intermediario (por ejemplo, firma de transacciones fuera de banda).

	Innovador		Controles de acceso adaptivo desprovee o aísla las credenciales de un empleado, un cliente o terceros para minimizar el daño potencial si es que se sospecha de un comportamiento malicioso. Se realiza un seguimiento y se asegura la información confidencial no estructurada a través de un sistema de almacenamiento de plataforma cruzada *identity-aware*, que proteja contra las amenazas internas, el acceso a usuarios monitores y control de cambios. Se utiliza *toquenización* para sustituir valores únicos de una información confidencial (por ejemplo, tarjeta de crédito virtual). La institución está realizando esfuerzos para crear nuevas tecnologías y procesos para gestionar la verificación y el acceso de clientes, empleados y terceros. Se realiza la mitigación del riesgo en tiempo real en base a la puntuación de riesgo automatizado de las credenciales del usuario.
SEGURIDAD DEL DISPOSITIVO / TERMINALES	**Básico**		Existen controles que restringen el uso de medios extraíbles al personal autorizado. *(FFIEC Information Security Work Program, Objetivo I: 4-1)*
	En desarrollo		Las herramientas bloquean automáticamente cualquier intento de acceso realizado desde dispositivos sin parches sean estos de un empleado o de terceros. Las herramientas bloquean automáticamente cualquier intento de acceso a las redes internas realizado desde dispositivos no registrados. La institución tiene controles para evitar que se agreguen nuevas conexiones no autorizadas. Existen controles para evitar que personas no autorizadas puedan copiar información confidencial a medios extraíbles. Se han implementado antivirus y anti-malware en los terminales (por ejemplo, computadoras, laptops y dispositivos móviles). Los dispositivos móviles que tienen acceso a la información de la institución están fundamentalmente administrados para la instalación de antivirus y la implementación de parches. (*No se aplica si no se utilizan teléfonos móviles.) La institución borra toda información de los dispositivos móviles de manera remota cuando un dispositivo se pierde o es robado. (*No se aplica si no se utilizan dispositivos móviles.)
	Intermedio		Se han implementado controles o dispositivos para la prevención de fuga de datos tanto para comunicaciones de salida como de entrada (por ejemplo, e-mail, FTP, Telnet, prevención de transferencia de archivos pesados). La gestión de los dispositivos móviles incluye el escaneo integral (por ejemplo, *jailbreak / rooted detection* (*No se aplica si no se utilizan dispositivos móviles.) Los dispositivos móviles que se conectan a la red corporativa para almacenar y acceder a la información de la compañía permiten el uso

			de la versión de escritorio remoto y la validación de parches. (*No se aplica si no se utilizan dispositivos móviles.)
	Avanzado		Los dispositivos de empleados y de terceros (incluyendo los móviles) que no cuenten con los parches de seguridad más recientes deben entrar en cuarentena y luego se deben instalar los parches antes de que el dispositivo tenga acceso a la red. Solo se puede tener acceso a información confidencial y aplicaciones en los dispositivos móviles a través de un aislamiento de procesos seguro (*sandbox*) o un contenedor seguro.
	Innovador		Una herramienta de gestión de terminales centralizados proporciona un parche totalmente integrado, configuración y gestión de vulnerabilidad, mientras que también es capaz de detectar cuando ingresa un malware para así evitar que haga daño.
CODIFICACIÓN SEGURA	**Básico**		Los desarrolladores que trabajan para la institución siguen las prácticas de un programa de codificación segura, como parte del ciclo de vida del desarrollo de sistemas (SDLC) que cumple con los estándares de la industria. *(FFIEC Information Security Booklet, página 56)* Los controles de seguridad del software desarrollado de manera interna son periódicamente revisados y probados. (*No se aplica si no hay desarrollo de software). *(FFIEC Information Security Booklet, página 59*) Los controles de seguridad del software desarrollado internamente son revisados independientemente antes de migrar el código a producción. (No se aplica si no existe desarrollo de software). *(FFIEC Development and Acquisition Booklet, página 2*) La propiedad intelectual y el código de producción se guardan en depósito. (No se aplica si no hay código de producción guardado en depósito). *(FFIEC Development and Acquisition Booklet, página 39*).
	En desarrollo		Las pruebas de seguridad se realizan en todas las fases posteriores al diseño del SDLC, para todas las aplicaciones, incluidas las aplicaciones móviles. (*No se aplica si no hay desarrollo de software).
	Intermedio		Existen procesos para mitigar las vulnerabilidades identificadas como parte del desarrollo seguro de sistemas y aplicaciones. La seguridad de las aplicaciones, incluidas aquellas basadas en la web con conexión a internet, se comprueba frente a los tipos de ataques cibernéticos conocidos (por ejemplo, inyección SQL, secuencia de comandos en sitios cruzados, desbordamiento de búfer) antes de su implementación o después de cambios significativos. Los ejecutables del código fuente y de la secuencia de comandos tienen una firma digital para confirmar al autor del software y garantizar que el código no se haya alterado ni dañado. Una función de aseguramiento de la información independiente y basada en el riesgo evalúa la seguridad de las aplicaciones internas.

	Avanzado		Las vulnerabilidades identificadas mediante un análisis de código estático se corrigen antes de implementar aplicaciones recién desarrolladas o modificadas en producción. Se han identificado todas las interdependencias entre aplicaciones y servicios. Las revisiones de código independiente se completan en aplicaciones desarrolladas internamente o personalizadas proporcionadas por el proveedor para garantizar que no haya discrepancias en la seguridad.
	Innovador		El código de software se explora activamente mediante herramientas automatizadas en el entorno de desarrollo para que las debilidades de seguridad se resuelvan inmediatamente durante la fase de diseño.
		Factor de Evaluación: Controles de detección	
DETECCIÓN DE AMENAZAS Y VULNERABILIDADES	**Básico**		Las pruebas independientes (incluidas las pruebas de penetración y la exploración de vulnerabilidades) se llevan a cabo de acuerdo con la evaluación de riesgos para los sistemas dirigidos al público y a la red interna. *(FFIEC Information Security Booklet, página 61*) Se utilizan herramientas como antivirus y anti-malware para detectar ataques. *(FFIEC Information Security Booklet, página 55*) Las reglas del firewall se auditan o verifican por lo menos cada 3 meses. *(FFIEC Information Security Booklet, página 82)* Los mecanismos de protección del correo electrónico se utilizan para filtrar amenazas cibernéticas comunes (por ejemplo, malware adjunto o enlaces maliciosos). *(FFIEC Information Security Booklet, página 39)*
	En desarrollo		Las pruebas de penetración independientes de los límites de la red y de las aplicaciones web cruciales se realizan de forma rutinaria para identificar las discrepancias en el control de seguridad. Las pruebas de penetración independientes se realizan en aplicaciones o sistemas conectados a internet antes de que se lancen o experimenten un cambio significativo. Las herramientas antivirus y anti-malware se actualizan de forma automática. Las reglas del firewall se actualizan de forma rutinaria. La exploración de vulnerabilidades se realiza y analiza antes del despliegue o redespliegue de dispositivos nuevos o ya existentes. Existen procesos para monitorear la actividad de un potencial intruso que pueda llevar a la sustracción de información o a su destrucción
	Intermedio		Los recursos de auditoría o gestión del riesgo revisan el alcance y los resultados de las pruebas de penetración para ayudar a determinar la necesidad de rotar a las empresas en base a la calidad del trabajo. Los correos electrónicos y los archivos adjuntos se exploran automáticamente para detectar malware y se bloquean cuando este se presenta.

	Avanzado		La exploración semanal de vulnerabilidades se rota entre los entornos para analizarlos durante todo el año. Las pruebas de penetración incluyen simulaciones de ataques cibernéticos y/o tácticas y técnicas del mundo real, tal como las pruebas del equipo rojo para detectar discrepancias de control en el comportamiento de los empleados, las defensas de seguridad, las políticas y los recursos. Las herramientas automatizadas identifican de forma proactiva el comportamiento de alto riesgo, el cual indica que un empleado puede representar una amenaza interna.
	Innovador		Las tareas y el contenido del usuario (por ejemplo, abrir un archivo adjunto del correo electrónico) se aíslan automáticamente en un contenedor seguro o en un entorno virtual para que el malware pueda analizarse, pero no pueda acceder a información vital, a sistemas operativos terminales o a aplicaciones en la red de la institución. La exploración de vulnerabilidades se realiza semanalmente en todos los entornos
DETECCIÓN DE ACTIVIDAD ANÓMALA	**Básico**		La institución es capaz de detectar actividades anómalas mediante el monitoreo en todo el entorno. *(FFIEC Information Security Booklet, página 32)* Las transacciones de los clientes que generan alertas de actividad anómala son monitoreadas y revisadas. *(FFIEC Wholesale Payments Booklet, página 12)* Los registros de acceso físico y/o lógico se revisan después de los eventos. *(FFIEC Information Security Booklet, página 73)* El acceso de terceros a los sistemas cruciales es monitoreado a fin de detectar alguna actividad no autorizada o inusual. *(FFIEC Outsourcing Booklet, página 26)* Se monitorean los mayores privilegios. *(FFIEC Information Security Booklet, página 19*)
	En desarrollo		Existen sistemas para detectar automáticamente comportamientos anómalos durante la autenticación de clientes, empleados y terceros. Los registros de seguridad se revisan regularmente. Los registros proporcionan rastreabilidad para todos los accesos al sistema realizados por usuarios individuales. Se han establecido umbrales para determinar una actividad dentro de los registros que garantice la respuesta de la gestión.

	Intermedio		Las transacciones en línea realizadas por los clientes son monitoreadas activamente a fin de detectar comportamientos anómalos. Se utilizan herramientas para detectar la minería de datos no autorizada. Las herramientas monitorean activamente los registros de seguridad para detectar comportamientos anómalos y alertas dentro de los parámetros establecidos. Los registros de auditoría tienen copia de respaldo en un servidor de registros centralizado o en un medio difícil de alterar. Los umbrales para el registro de seguridad son evaluados de manera periódica. La actividad anómala y otras alertas de la red y del sistema se correlacionan con todas las unidades de negocio para detectar y prevenir ataques multifacéticos (por ejemplo, un ataque simultáneo para tomar el control de una cuenta y la denegación de servicio (DDoS).
	Avanzado		Una herramienta automatizada activa alertas de fraude y/o del sistema cuando el inicio de sesión del usuario ocurre dentro de un corto período de tiempo, pero desde una ubicación IP físicamente distante. Las transferencias externas desde las cuentas de los usuarios generan alertas, además requieren revisión y autorización si se detecta un comportamiento anómalo. Existe un sistema para monitorear y analizar el comportamiento de los empleados (patrones de uso de la red, horas de trabajo y dispositivos conocidos) a fin de alertar sobre actividades anómalas. Existe una o varias herramientas automatizadas para detectar y prevenir la minería de datos ocasionada por amenazas de intrusos. Se utilizan etiquetas en archivos o información confidencial ficticia para proporcionar alertas avanzadas sobre una posible actividad maliciosa cuando se accede a la información.
	Innovador		La institución cuenta con un mecanismo automatizado para la calificación del riesgo de las amenazas, en tiempo real. La institución está desarrollando nuevas tecnologías que detectarán posibles amenazas de intrusos y bloquearán la actividad en tiempo real.

DETECCIÓN DE EVENTOS	**Básico**		Se establece una base de referencia para la actividad normal de redes. *(FFIEC Information Security Booklet, página 77)* Existen mecanismos (por ejemplo, alertas de antivirus, alertas de eventos de registro) para alertar a la administración sobre posibles ataques. *(FFIEC Information Security Booklet, página 78)* Existen procesos para monitorear la presencia de usuarios, dispositivos, conexiones y software no autorizados *(FFIEC Information Security Work Program, Objetivo II: M-9)* Se han asignado responsabilidades para monitorear e informar sobre actividades sospechosas en los sistemas. *(FFIEC Information Security Booklet, página 83)* El entorno físico se monitorea para detectar cualquier posible acceso no autorizados. *(FFIEC Information Security Booklet, página 47)*
	En desarrollo		Existe un proceso para correlacionar la información de eventos de diversas fuentes (por ejemplo, red, aplicación o firewall).
	Intermedio		Existen controles o herramientas (por ejemplo, prevención de fuga de información) para detectar posibles transmisiones de información confidencial no autorizadas o no intencionales. Los procesos de detección de eventos han demostrado ser fiables. El monitoreo de seguridad especializado se utiliza para activos críticos en toda la infraestructura.
	Avanzado		Las herramientas automatizadas detectan cambios no autorizados en archivos críticos del sistema, firewalls, IPS, IDS u otros dispositivos de seguridad. Se implementa el monitoreo y detección de la red en tiempo real e incorpora información sobre eventos en todo el sector. Se envían automáticamente alertas en tiempo real cuando se producen cambios, o existe hardware o software no autorizado. Existen herramientas para correlacionar activamente la información sobre eventos de diversas fuentes y enviar alertas basadas en parámetros establecidos.
	Innovador		La institución está realizando esfuerzos para desarrollar sistemas de detección de eventos que se correlacionen en tiempo real, cuando los eventos estén a punto de ocurrir. La institución está realizando esfuerzos para desarrollo el diseño de nuevas tecnologías que detecten amenazas de un potencial intruso y bloqueen la actividad en tiempo real.

Factor de Evaluación: Controles correctivos			
GESTIÓN DE PARCHES	**Básico**		Se ha implementado un programa de gestión de parches el cual garantiza que los parches de software y firmware se apliquen de manera oportuna. *(FFIEC Information Security Booklet, página 62)* Los parches son sometidos a pruebas antes de ser aplicados a los sistemas y/o al software. *(FFIEC Operations Booklet, página 22)* Se revisan los informes de gestión de parches y reflejan los parches de seguridad faltantes. *(FFIEC Development and Acquisition Booklet, página 50)*
	En desarrollo		Existe un proceso formal para adquirir, probar e implementar parches de software según su criticidad. Los sistemas se configuran para recuperar parches automáticamente. El impacto operativo se evalúa antes de implementar los parches de seguridad. Se utilizan herramientas automatizadas para identificar los parches de seguridad faltantes, así como el número de días desde que cada parche estuvo disponible. Los parches faltantes en todos los entornos se priorizan y se rastrean.
	Intermedio		Los parches para vulnerabilidades de alto riesgo se someten a prueba y se aplican cuando son lanzados o cuando se acepta el riesgo y se asigna la responsabilidad.
	Avanzado		El software de monitoreo de parches se instala en todos los servidores para identificar si le falta algún parche al software del sistema operativo, el middleware, la base de datos y otro software clave. La institución monitorea los informes de gestión de parches para garantizar que los parches de seguridad sean sometidos a prueba y que se implementen dentro de un corto período de tiempo (por ejemplo, de 0 a 30 días).
	Innovador		La institución desarrolla parches de seguridad, correcciones de errores o contribuye al desarrollo de código fuente abierto para los sistemas que utiliza. Existen sistemas diferenciados o separados que reflejan los sistemas de producción, lo cual permite probar e implementar los parches de manera rápida, y proporciona un respaldo veloz cuando se necesita.

CORRECCIÓN	**Básico**		Los problemas identificados en las evaluaciones se priorizan y resuelven en función de su criticidad y dentro de los plazos establecidos en respuesta al informe de evaluación. *(FFIEC Information Security Booklet, página 87)*
	En desarrollo		La información se destruye o se borra del hardware y los medios portátiles/móviles cuando un dispositivo falta, ha sido robado o ya no se necesita. Existen procesos formales para resolver las debilidades identificadas durante las pruebas de penetración.
	Intermedio		Los esfuerzos de corrección se confirman realizando una exploración de seguimiento de la vulnerabilidad. Las pruebas de penetración se repiten para confirmar que se han resuelto las vulnerabilidades explotables de medio y alto riesgo. Las investigaciones de seguridad, los análisis forenses y las correcciones son realizadas por personal calificado o por terceros. Se utilizan procedimientos forenses apropiados y generalmente aceptados, inclusive la cadena de custodia, para recopilar y presentar evidencia que pueda respaldar una posible acción legal. El mantenimiento y la reparación de los activos organizacionales o de TI son realizados por personas autorizadas que cuentan con herramientas aprobadas y controladas. El mantenimiento y reparación de los activos organizacionales o de TI se registran de manera oportuna.
	Avanzado		Todos los problemas de medio y alto riesgo identificados en las pruebas de penetración, exploración de vulnerabilidades y otras pruebas independientes son puestos a consideración de la Junta Directiva, o un Consejo Directivo apropiado, para la aceptación del riesgo si no se resuelven de manera oportuna.
	Innovador		La institución está desarrollando tecnologías que corregirán los sistemas dañados por ataques de día cero para mantener el actual tiempo objetivo de recuperación (RTO).

Dominio 4: Gestión de Dependencia Externa

Factor de Evaluación: Conexiones

		Y, Y(C), N	
CONNECTIONS	**Básico**		Se han identificado los procesos de negocios críticos que dependen de la conectividad externa. *(FFIEC Information Security Booklet, página 9)* The institution ensures that third-party connections are authorized. La institución garantiza que las conexiones de terceros son autorizadas. *(FFIEC Information Security Booklet, página 17)* Existe un diagrama de red que identifica todas las conexiones externas. *FFIEC Information Security Booklet, página 9)* Existen diagramas de flujo de datos y flujo de información de documentos hacia grupos externos. *(FFIEC Information Security Booklet, página 10)*
	En desarrollo		Los procesos de negocios críticos han sido asociados a las conexiones externas de apoyo. El diagrama de red se actualiza cuando cambian las conexiones con terceros, o por lo menos una vez al año. Los diagramas de redes y sistemas se almacenan de manera segura con las restricciones de acceso adecuadas. Los controles para las conexiones primarias y de respaldo de terceros son monitoreadas y sometidas a pruebas de manera regular.
	Intermedio		Se utiliza un inventario de activos validado para crear diagramas integrales que representen repositorios de datos, flujo de datos, infraestructura y conectividad. Los controles de seguridad están diseñados y verificados para detectar y evitar intromisiones de conexiones de terceros. Los controles de monitoreo cubren todas las conexiones externas (por ejemplo, proveedores de servicios, socios comerciales, clientes). Los controles de monitoreo cubren todas las conexiones internas de red a red.
	Avanzado		Se valida y documenta la arquitectura de seguridad antes de que cambie la infraestructura de conexión de red. La institución trabaja en estrecha colaboración con los proveedores externos de servicios para mantener y mejorar la seguridad de las conexiones externas.

	Innovador		Los diagramas de conexiones externas son interactivos, muestran en tiempo real los cambios en infraestructura de la conexión de red, nuevas conexiones, fluctuaciones de volumen, y alertas cuando surgen riesgos. Las conexiones de la institución se pueden segmentar o dividir inmediatamente para evitar la propagación de ataques cibernéticos.
Factor de Evaluación: Gestión de Relaciones			
DILIGENCE DEBIDA	**Básico**		La diligencia debida basada en el riesgo se realiza con las posibles terceras partes antes de firmar los contratos, lo cual incluye revisión de sus antecedentes, reputación, situación financiera, estabilidad y controles de seguridad. *(FFIEC Information Security Booklet, página 69)* Se mantiene una lista de proveedores externos de servicios. *(FFIEC Outsourcing Booklet, página 19)* Se realiza una evaluación de riesgos para identificar la criticidad de los proveedores de servicios. *(FFIEC Outsourcing Booklet, página 6)*
	En desarrollo		Existe un proceso formal para analizar las evaluaciones de los controles de ciberseguridad de terceros. La Junta Directiva, o un Consejo Directivo apropiado, revisa un resumen de los resultados de la diligencia debida, que incluye las recomendaciones de la administración para utilizar a terceros que afectarán el perfil de riesgo inherente de la institución.
	Intermedio		Existe un proceso para confirmar que los proveedores externos de servicios de la institución realicen la diligencia debida de sus terceros (por ejemplo, subcontratistas). Previa al contrato, las visitas físicas al lugar por parte de los proveedores de alto riesgo son realizadas por la institución o por un tercero calificado.
	Avanzado		Existe un programa continuo de mejora de los procesos para la actividad de diligencia debida de terceros. Anualmente, se realizan auditorías de proveedores de alto riesgo.
	Innovador		La institución promueve esfuerzos en todo el sector para construir mecanismos de diligencia debida que conduzcan a revisiones de seguridad y resiliencia profundas y eficientes. La institución está realizando esfuerzos para desarrollar nuevos procesos auditables y para llevar a cabo la diligencia debida y el monitoreo permanente de los riesgos de ciberseguridad planteados por terceros.

CONTRATOS	**Básico**		Existen contratos formales que abordan los requisitos de seguridad y privacidad relevantes para todos los terceros que procesan, almacenan o transmiten información confidencial o brindan servicios críticos. *(FFIEC Information Security Booklet, página 7)* Los contratos reconocen que los terceros son responsables de la seguridad de la información confidencial que la institución posee, almacena, procesa o transmite. *(FFIEC Information Security Booklet, página 12)* Los contratos estipulan que los controles de seguridad de terceros sean revisados y validados regularmente por otro tercero independiente. *(FFIEC Information Security Booklet, página 12)* Los contratos identifican el recurso disponible para la institución en caso de que los terceros no cumplan con los requisitos de seguridad definidos. *(FFIEC Outsourcing Booklet, página 12)* Los contratos establecen responsabilidades para actuar ante incidentes de seguridad. *(FFIEC E-Banking Booklet, página 22)* Los contratos especifican los requisitos de seguridad para la devolución o destrucción de datos al finalizar el contrato. *(FFIEC Outsourcing Booklet, página 15)*
	En desarrollo		Las responsabilidades para gestionar dispositivos (por ejemplo, firewalls, routers) que protegen las conexiones con terceros están documentadas formalmente en el contrato. La responsabilidad de notificar sobre incidentes directos e indirectos de seguridad y vulnerabilidades se documenta en los contratos o acuerdos de nivel de servicio (SLA, por sus siglas en inglés). Los contratos estipulan límites geográficos sobre el lugar dónde se pueden almacenar o transmitir los datos.
	Intermedio		Existen acuerdos de nivel de servicio (SLA) de terceros o medios similares que requieren la notificación oportuna de los eventos de seguridad.
	Avanzado		Los contratos requieren que las políticas de seguridad del proveedor de servicios cumplan o excedan las de la institución. Se ha establecido y validado con la administración una estrategia de terminación/salida de terceros.
	Innovador		La institución promueve el esfuerzo en todo el sector para influir en los requisitos contractuales en el caso de terceros críticos en la industria.

MONITOREO PERMANENTE	**Básico**		La evaluación de riesgos de terceros se actualiza regularmente. *(FFIEC Outsourcing Booklet, página 3)* Las auditorías, las evaluaciones y los informes de rendimiento operativo se obtienen y revisan regularmente para validar los controles de seguridad en el caso de terceros críticos. *(FFIEC Information Security Booklet, página 86)* Las prácticas de monitoreo permanente incluyen la revisión de planes de resiliencia de terceros críticos. *(FFIEC Outsourcing Booklet, página 19)*
	En desarrollo		Existe un proceso para identificar nuevas relaciones con terceros, incluso la identificación de nuevas relaciones que se establecieron sin aprobación formal. Un programa formal asigna la responsabilidad de supervisar de forma permanente el acceso a terceros. El monitoreo de terceros es escalado, en términos de profundidad y frecuencia, de acuerdo con el riesgo de los terceros. Existen recordatorios o avisos automáticos para identificar cuándo es necesario obtener o analizar una información de terceros requerida.
	Intermedio		Se realiza un seguimiento activo al acceso del personal de terceros a los datos confidenciales de la institución basado en los principios del mínimo privilegio. Se realizan evaluaciones periódicas *in situ* de los proveedores de alto riesgo para garantizar que existan controles de seguridad adecuados.
	Avanzado		Se realiza un seguimiento activo a través de informes y alertas automatizados al acceso del personal de terceros a los datos confidenciales en los sistemas que alojan a terceros.
	Innovador		La institución realiza esfuerzos para desarrollar nuevos procesos auditables para el monitoreo permanente de los riesgos de ciberseguridad planteados por terceros.

Dominio 5: Gestión de Incidentes Cibernéticos y Resiliencia

Factor de Evaluación: Planificación y Estrategias para la Resiliencia ante incidentes

		Y, Y(C), N	
PLANIFICACION	**Básico**		La institución tiene documentado cómo reaccionará y actuará ante incidentes cibernéticos. *(FFIEC Business Continuity Planning Booklet, página 4)* Existen canales de comunicación que proporcionan a los empleados un medio para informar oportunamente acerca de eventos de seguridad de la información. *(FFIEC Information Security Booklet, página 83)* Los roles y responsabilidades de los miembros del equipo de respuesta ante incidentes están definidos. *(FFIEC Information Security Booklet, página 84)* El equipo de respuesta incluye personas con una formación en diversos campos y conocimientos especializados, provenientes de diversas áreas de la institución (por ejemplo, administración, legal, relaciones públicas, así como tecnología de información). *(FFIEC Information Security Booklet, página 84)* Existe un plan formal de respaldo y recuperación de información para todas las líneas comerciales críticas. *(FFIEC Business Continuity Planning Booklet, página 4)* La institución planea utilizar los programas de continuidad del negocio, recuperación de desastres y respaldo de la información para recuperar las operaciones después de un incidente. *(FFIEC Information Security Booklet, página 71)*
	En desarrollo		El plan y proceso de corrección delinea las acciones de mitigación, los recursos y los parámetros de tiempo. Los planes corporativos de recuperación ante desastres, continuidad del negocio y gestión de crisis contienen un análisis integrado de los incidentes cibernéticos. Se han establecido procesos alternativos para continuar con la actividad crítica dentro de un período de tiempo razonable. Los análisis de impacto del negocio han sido actualizados para incluir la ciberseguridad. Se ha realizado la diligencia debida en fuentes técnicas, consultores o empresas de servicio forense a las que se podría recurrir para que ayuden a la institución durante o después de un incidente.

	Intermedio		Existe una estrategia para coordinar y comunicarse con las partes interesadas internas y externas durante o después de un ataque cibernético. Existen planes para redirigir o sustituir funciones y/o servicios críticos que pueden verse afectados por un ataque exitoso a los sistemas conectados a internet. Existe un acuerdo o acuerdos contractuales o cooperativos directos con organizaciones o proveedores de respuesta ante incidentes para ayudar rápidamente con los esfuerzos de mitigación. Las lecciones aprendidas de incidentes y ataques cibernéticos a la institución y a otras organizaciones en la vida real se utilizan para mejorar las habilidades de mitigación de riesgos y el plan de respuesta de la institución.
	Avanzado		Los métodos de respuesta y recuperación ante incidentes cibernéticos están fuertemente entrelazados en los planes de recuperación ante desastres, continuidad del negocio y gestión de crisis de las unidades de negocio. Se han implementado diversos sistemas, programas o procesos dentro de un programa de resiliencia cibernética integral para mantener, minimizar y recuperar las operaciones de una variedad de incidentes cibernéticos potencialmente perjudiciales y destructivos. Existe un proceso para mejorar continuamente el plan de resiliencia.
	Innovador		El plan de respuesta ante incidentes está diseñado para garantizar la recuperación de la interrupción de los servicios, la garantía de la integridad de los datos y la recuperación de datos perdidos o dañados a consecuencia de un incidente de ciberseguridad. El proceso de respuesta ante incidentes incluye acciones detalladas y activadores basados en reglas para una respuesta automatizada.
PRUEBAS	**Básico**		Se utilizan escenarios para mejorar la detección y respuesta ante incidentes. *(FFIEC Information Security Booklet, página 71)* Las pruebas de continuidad del negocio implican la colaboración con terceros críticos. *(FFIEC Business Continuity Planning Booklet, página J-6)* Los sistemas, las aplicaciones y la recuperación de datos se somete a prueba por lo menos una vez al año. *(FFIEC Business Continuity Planning Booklet, página J-7)*
	En desarrollo		Los escenarios de recuperación incluyen planes para recuperarse de la destrucción de información y los impactos en la integridad de los datos, la pérdida de ellos y la disponibilidad del sistema y de los datos. Los eventos ampliamente reportados se utilizan para evaluar y mejorar la respuesta de la institución. Las copias de respaldo de la información se someten a prueba periódicamente para verificar que sean accesibles y legibles.

	Intermedio		Se analizan los escenarios de ataques cibernéticos para determinar el impacto potencial en los procesos críticos de negocios. La institución participa en ejercicios o escenarios cibernéticos específicos para un sector (por ejemplo, ataque cibernético (contra) Procesadores de pago (CAPP) de FS-ISAC). Las pruebas de resiliencia se basan en el análisis y la identificación de amenazas realistas y muy probables, así como de las amenazas nuevas y emergentes que enfrenta la institución. Los sistemas y procesos críticos en línea se someten a prueba para resistir tensiones durante períodos prolongados (por ejemplo, DDoS). Los resultados de los ejercicios de eventos cibernéticos se utilizan para mejorar el plan de respuesta ante incidentes y los activadores automatizados.
	Avanzado		Las pruebas de resiliencia son integrales y coordinadas en todas las funciones críticas del negocio. La institución valida que es capaz de recuperarse de eventos cibernéticos similares a los ataques sofisticados conocidos en otras organizaciones. Las pruebas de respuesta ante incidentes evalúan a la institución desde la perspectiva de un atacante, para determinar cómo se puede atacar a la institución o a sus activos en terceros críticos. La institución corrige las causas fundamentales de los problemas descubiertos durante las pruebas de resiliencia de la ciberseguridad. Los escenarios de incidentes de ciberseguridad que implican pérdidas financieras significativas se utilizan para realizar pruebas de estrés en relación con la gestión de riesgos de la institución.
	Innovador		La institución somete a prueba la capacidad de cambiar los procesos o funciones de negocio entre diferentes centros de procesamiento o sistemas de tecnología para incidentes cibernéticos sin interrumpir el negocio, la pérdida de productividad o de datos. La institución ha validado que es capaz de corregir los sistemas dañados por ataques de día cero para mantener los objetivos de tiempo de recuperación actuales. La institución está liderando el desarrollo de entornos de prueba más realistas. Los escenarios de incidentes cibernéticos se utilizan para realizar pruebas de estrés ante posibles pérdidas financieras en todo el sector.

Factor de Evaluación: Detección, Respuesta y Mitigación			
DETECCIÓN	**Básico**		Se establecen parámetros de alerta para detectar incidentes de seguridad de la información que puedan activar acciones de mitigación. *(FFIEC Information Security Booklet, página 43)* Los informes de rendimiento del sistema contienen información que puede ser utilizada como un indicador de riesgo para detectar incidentes de seguridad de la información. *(FFIEC Information Security Booklet, página 86)* Existen herramientas y procesos para detector, alertar, y activar el programa de respuesta ante un incidente. *(FFIEC Information Security Booklet, página 84)*
	En desarrollo		La institución tiene procesos para detectar y alertar al equipo de respuesta ante incidentes cuando se manifiesta alguna actividad de un potencial intruso que pueda conducir al robo o destrucción de la información.
	Intermedio		El programa de respuesta ante incidentes se activa cuando se detectan comportamientos anómalos y firmas o patrones de ataque. La institución tiene la capacidad de descubrir alguna infiltración antes de que el atacante atraviese los sistemas, establezca un punto de apoyo, robe información, o cause daño a la información y sistemas. Los incidentes se detectan en tiempo real a través de procesos automatizados que incluyen alertas instantáneas para que el personal apropiado pueda responder. Se correlacionan las alertas del sistema y de la red con las unidades de negocio para detectar y prevenir, de la mejor manera, ataques multifacéticos (por ejemplo, ataques simultáneos de DDoS y toma de control de una cuenta) Los procesos de detección de incidentes son capaces de correlacionar eventos a través de toda la empresa.
	Avanzado		Se han implementado tecnologías adaptables y sofisticadas que pueden detectar y alertar al equipo de respuesta ante incidentes sobre tareas específicas cuando los indicadores de amenazas a través de toda la empresa indican potenciales amenazas externas e internas Se han implementado herramientas automatizadas para proporcionar monitoreo especializado en seguridad basado en el riesgo de los activos, para detectar y alertar en tiempo real a los equipos de respuesta ante incidentes.
	Innovador		La institución es capaz de detectar y bloquear los intentos de ataque de día cero e informar, en tiempo real, a la administración y al equipo de respuesta ante incidentes.

RESPUESTA Y MITIGACIÓN	**Básico**		Se han tomado los pasos apropiados para contener y controlar un incidente a fin de evitar un nuevo acceso no autorizado a la información del cliente o el uso de dicha información. *(FFIEC Information Security Booklet, página 84)*
	En desarrollo		El plan de respuesta ante incidentes está diseñado para priorizar los incidentes, permitiendo una respuesta rápida ante importantes incidentes o vulnerabilidades de ciberseguridad. Existe un proceso para ayudar a contener los incidentes y restablecer las operaciones con una mínima interrupción del servicio. Se han desarrollado estrategias de contención y mitigación para diversos tipos de incidentes (por ejemplo, DDoS, malware). Los procedimientos incluyen estrategias de contención y notificación a terceros potencialmente afectados. Existen procesos para activar el programa de respuesta ante incidentes cuando estos ocurren con un tercero. Se generan registros para respaldar la investigación y mitigación de incidentes. La institución recurre a terceros, según sea necesario, para brindar servicios de mitigación. Se utiliza el análisis de eventos para mejorar las medidas y políticas de seguridad de la institución.
	Intermedio		El análisis de los incidentes de seguridad se realiza en las primeras etapas de una intromisión para minimizar el impacto del incidente. Cualquier cambio en los sistemas/aplicaciones o en los derechos de acceso necesarios para la gestión de incidentes, los revisa la administración para su aprobación formal antes de ser implementados. Existen procesos para garantizar que aquellos activos afectados por un incidente de seguridad y que no pueden volver a su estado operativo, se pongan en cuarentena, se retiren, descarten y/o se reemplacen. Existen procesos para garantizar que los activos restablecidos sean reconfigurados de forma adecuada, y sometidos a prueba minuciosamente antes de ponerlos en funcionamiento nuevamente.
	Avanzado		La función de gestión de incidentes colabora de manera efectiva con la función de inteligencia de amenazas cibernéticas durante un incidente. Los vínculos entre la inteligencia de amenazas, las operaciones de red y la respuesta ante incidentes hacen posible una respuesta proactiva ante incidentes potenciales. Las medidas técnicas aplican estrategias de defensa en profundidad, tal como la inspección profunda de paquetes y agujeros negros para la detección y la respuesta oportuna ante ataques basados en la red asociados con patrones de tráfico anómalos de entrada o salida y/o ataques DDoS.

	Innovador		La gestión de riesgos de la institución sobre los incidentes cibernéticos significativos da como resultado limitadas interrupciones a ninguna interrupción de los servicios críticos. La infraestructura tecnológica ha sido diseñada para limitar los efectos de un ataque cibernético en el entorno de producción desde que migra hasta el entorno de respaldo (por ejemplo, procesos y entornos con brecha de aire (air gap)).
Factor de Evaluación: Proceso de Escalación y Registro			
PROCESO DE ESCALACIÓN Y REGISTRO	**Básico**		Existe un proceso para contactar al personal responsable de analizar y responder ante un incidente. *(FFIEC Information Security Booklet, página 83)* Existen procedimientos para notificar a los clientes, reguladores, y autoridades, según sea necesario o requerido, cuando la institución se da cuenta de un incidente que involucra el acceso autorizado o el uso de información confidencial del cliente. *(FFIEC Information Security Booklet, página 84)* La institución prepara un informe anual de incidentes o violaciones de seguridad para la Junta Directiva, o un Consejo Directivo apropiado. *(FFIEC Information Security Booklet, página 5)* Los incidentes son clasificados, registrados y rastreados. *(FFIEC Operations Booklet, página 28)*
	En desarrollo		Se han establecido criterios para elevar los incidentes cibernéticos o vulnerabilidades ante la Junta Directiva y alta administración en base al impacto potencial y criticidad del riesgo. Reguladores, autoridades y proveedores de servicios, según corresponda, son notificados cuando la institución se da cuenta de algún acceso no autorizado a los sistemas o cuando ocurre un incidente cibernético que pueda resultar en degradación de los servicios. Los incidentes cibernéticos rastreados son correlacionados para el análisis de tendencia e informes.
	Intermedio		Los empleados que cumplen una función fundamental para la mitigación del riesgo (por ejemplo, fraude, resiliencia del negocio) saben a quién asignar el problema en caso de algún incidente. Se utiliza un plan de comunicación para notificar a otras organizaciones, incluyendo a terceros, acerca de incidentes que pueden afectarlos o afectar a sus clientes. Se utiliza un plan de comunicación externa para notificar a los medios con relación a los incidentes cuando corresponde.
	Avanzado		La institución ha establecido medidas cuantitativas y cualitativas para el proceso de respuesta ante incidentes de ciberseguridad. Se proporcionan métricas detalladas, cuadros de mando y/o registros de datos indicadores que describen los incidentes y eventos cibernéticos a la administración y forman parte del paquete de las reuniones de la Junta Directiva.

	Innovador		Existe un mecanismo para proporcionar notificación inmediata a la administración y a empleados claves sobre la ocurrencia de incidentes, a través de diversos canales de comunicación con rastreo y acuse de recibo.