
Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de investigación aplicada 2

# Aplicación de un modelo de madurez para una entidad bancaria en Costa Rica

Alejandro Bolaños Alpízar

Fecha: junio, 2019

## DECLARATORIO DE DERECHOS DE AUTOR

# CARTA DEL FILÓLOGO

Cartago, 13 de agosto de 2019

Los suscritos, Elena Redondo Camacho, mayor, casada, filóloga, cédula de identidad número 3 0447 0799 y Daniel González Monge, mayor, casado, filólogo, cédula de identidad número 1 1345 0416, vecinos de Quebradilla de Cartago, en calidad de filólogos, revisamos y corregimos el trabajo final de graduación que se titula: *NIST (National Institute of Standards and Technology). Aplicación de un modelo de madurez para una entidad bancaria en Costa Rica*, sustentado por Alejandro Bolaños Alpízar.

Hacemos constar que se corrigieron todos los aspectos de forma, redacción, estilo y otros vicios del lenguaje que se pudieron trasladar al texto.

Esperamos que nuestra participación satisfaga los requerimientos de la Universidad Cenfotec.


Elena Redondo Camacho
Céd. 3 0447 0799
Bachiller en Filología Española
Carné ACFIL 0247

Daniel González Monge
Céd. 1 1345 0416
Bachiller en Filología Española
Carné ACFIL 0245

## DEDICATORIA

Esta tesis es producto del esfuerzo y constancia que me fueron inculcados, gracias a mi familia, amigos, compañeros y colegas, que me han dado la fuerza y motivación para seguir adelante.

## AGRADECIMIENTOS

Este proyecto el fruto del aporte de muchos profesores que han sacrificado su tiempo por enseñar lo que les apasiona, sin ellos y su esfuerzo no hubiese sido posible.

Al señor Alex Araya por acompañarme en este último esfuerzo. Entre otros muchos profesores, colegas y compañeros de carrera que han aportado sus conocimientos, ideas y consideraciones profesionales.

A la señora María Eugenia Ucros y demás colaboradores de la U Cenfotec por acompañarme en esta defensa y colaborar con la logística.

A don Gerald Segura, por aportar su grano de arena con la experiencia y consejo como lector y consejo diario.

A mi compañera Andrea Elizondo Aguilar, por sus recomendaciones y apoyo.

## TRIBUNAL EXAMINADOR

## TABLA DE CONTENIDO

# ÍNDICE DE ILUSTRACIONES

# Capítulo 1. Introducción

## 1.1. Generalidades

La información es un derecho fundamental y, en cualquier lugar, se debe garantizar la confiabilidad, de forma integral, con una altísima disponibilidad y con la capacidad para auditarse. Estos son los pilares en el ámbito mundial que buscan proteger la información como el activo más preciado de cualquier organización.

## 1.2. Antecedentes del Problema

La información de clientes, productos, proveedores y colaboradores es crítica, es un activo casi invaluable, esto hace que sea apetecida por delincuentes o grupos delictivos, con el fin de utilizarla de una forma poco ética o incorrecta, lo que puede causar estafas, pérdidas financieras, incluso problemas sociales. Esta es la razón por la que en los últimos años se han doblado esfuerzos para mantener la información segura de forma que se minimicen las capacidades de acceso no autorizado. La información aumenta su valor cada día, su mal uso ha llegado a considerarse un *peligro potencial*, en manos equivocadas y puede propiciar el terrorismo, delitos económicos o afectar la seguridad de naciones y la integridad de las personas.

## 1.3. Definición y Descripción del Problema

La información debe fluir en gran parte de las organizaciones y estas dependen de su acceso para brindar sus productos y servicios, lo que hace necesario incrementar la seguridad. Con este fin, se idearon controles para mitigar los posibles riesgos, adicionalmente, se crearon formas de monitoreo que registran y reportan los comportamientos relacionados con la información, todo con el fin de mantenerla segura.

A través del tiempo, los controles se han establecido como un mecanismo válido para proteger la información almacenada, ya sea al limitar su acceso o al restringir las calidades. Estos fueron mecanismos que se usaron para incrementar la percepción de seguridad, en algunos casos fueron exitosos, pero en otros no tanto. Cada responsable

de información, entiéndase gobierno, compañía, u organización que almacene datos es responsable de la misma. Cada una tenía su forma de hacerlo, el método para realizarlo podía variar de una organización a otra, aunque las razones de ser fuesen muy similares, cada uno tenía su manera

Los múltiples factores relacionados con la seguridad de la información tornaban la labor más complicada, existían omisiones, procesos poco ordenados, reprocesos y, de esta forma, la tarea se tornaba más compleja. La forma ideada para controlar esto fue crear normativas que buscaban una alineación de los controles. Después de establecer las normativas en el proceso, se comenzó a ver los resultados positivos. Inmediatamente después, se debía pensar en la trasmisión de conocimiento de una forma más metódica y sistemática, es ahí cuando nacen diferentes normativas con nombres muy conocidos en la actualidad, como: COBIT, ITIL, ISO.

Con las normativas a disposición de los administradores de la seguridad se debía determinar ¿cuál es la correcta?, ¿cuál utilizar y por qué?, ¿cuál conviene aplicar a la organización? Aunque no existe una receta o recomendación infalible, las herramientas manuales, normativas o metodologías son la forma de expresar algo complicado en conceptos simples, segmentados y de asimilación rápida para la mayor cantidad de involucrados. Son formas de lograr que el método complicado sea replicable y compresible. La NIST, ISO 27001, COBIT, ITIL, son más que formas ideadas para transmitir los controles, son metodologías funcionales de trabajo, para que las organizaciones logren mejorar el control, en el área tecnológica, este caso se aplica concretamente a la Ciberseguridad.

Sobre este estudio no existen antecedentes relacionados con la seguridad de la información, adicionalmente, no se cuenta con documentación previa de la aplicación del capítulo de Ciberseguridad del Instituto de Estándares en Tecnología (NIST, *en sus siglas en inglés National Institute of Standars and Technology*) en alguna entidad financiera en Costa Rica. Este es un motivo pertinente: crear un análisis con el fin de revelar el estado de la seguridad desde la perspectiva de la NIST.

## 1.4. Justificación

La información en las organizaciones es un activo que, además de dar soporte a negocio como la banca, es la esencia misma de un servicio. Conocer al cliente es crítico y la información dejó de ser líneas de datos relacionados entre sí, ahora es más descriptiva, es la esencia, es un principio más *vivo*. Se puede aseverar que la información, su pérdida, robo o forma de uso puede hacer a un negocio crecer o sostenerlo, pero también ser el principio de su fin.

Actualmente, la ciberseguridad se toma en cuenta en el momento de establecer aliados comerciales, tener una normativa robusta como parte de su postura de ciberseguridad sería un pilar fundamental de la organización, pocas veces y pocas son las organizaciones que se cuestionan esta postura, incluso algunas veces obvian como podrían sufrir afectación. La clave es autoevaluarse y realizarse la pregunta ¿qué puede hacer un cibercriminal para afectar grupos u organizaciones con un ciberataque? Las formas pueden ser muchas:

- Costo de afectación de imagen o reputación: el activo más valioso de una empresa es su imagen, un daño en la imagen afectaría su valor en mercado, minimizaría su alcance como marca y daría ventajas a la competencia.

- Pérdida o secuestro de datos: la información del cliente en los centros de datos es clave, contactos, proveedores, aliados comerciales, pérdida de información o secuestros serían una *mala señal* de la seguridad de la información. No recuperarla complicaría la operación normal y mantener el volumen de movimientos empresariales.

- Afectación de servicios: consiste en la caída de los servicios prestados, ya sea por caída de página *web*, consulta de servicios o demás posibles afectaciones a los clientes, esto afecta la imagen, la oportunidad de servicios y todos los demás daños que implica no tener las plataformas tecnológicas en funcionamiento.

- Coste de remediación o recuperación: un estudio realizado por CISCO

de Referencia de las Capacidades de Seguridad de Cisco (2018) ofrece y compara resultados con los de los estudios de 2017, 2016 y 2015, se muestra que los ataques causan un daño económico real, daños que pueden tardar meses o años en resolverse o incluso hacer desaparecer una empresa.

- Ese mismo estudio de Cisco (2018), realizado con más de 3600 personas en 26 países indica: “Según los encuestados del estudio, más de la mitad (53 por ciento) de todos los ataques resultaron en daños financieros de hasta de USD $5,000,000; sustentados en pérdida de ingresos, clientes, oportunidades y costos de bolsillo, entre otros” (s. p.).

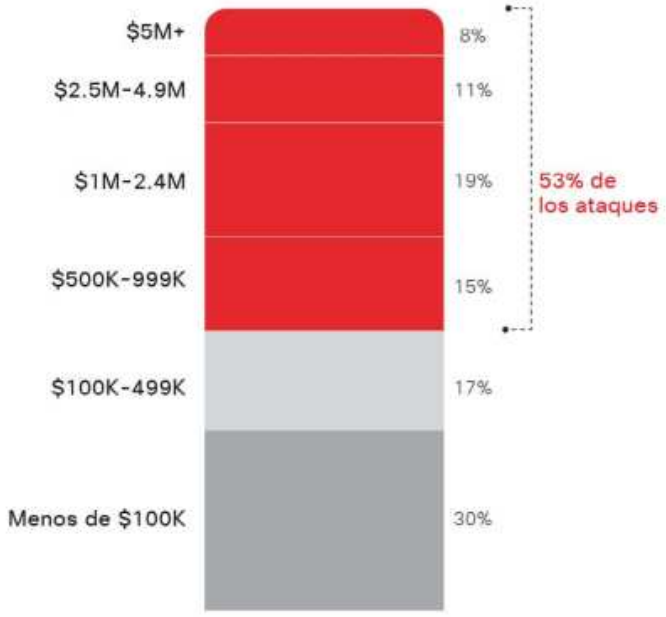



Ilustración 1. Reflejo de Impacto de Ciberataques en el Año 2018 en Dólares

Fuente: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

Si se analizan los resultados por afectación y toman en cuenta las brechas de seguridad; las operaciones y los costos financieros, están en primera línea. En un segundo plano se encuentran los robos de información o derechos de autor, robo de clientes y reputación de marca son los otros aspectos que sufren por fallas en la ciberseguridad. Al parecer, también son comportamientos que se han mantenido del año 2017 al 2018, por lo que no se trata de casos aislados, sino que es un escenario

consistente.


Ilustración 2. Principales Afectaciones de Negocio Reflejadas por los Negocios en el Año 2018

Fuente: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

A partir de lo que muestra esta investigación se puede ver la importancia de la ciberseguridad. Por eso, se tratará la ciberseguridad, como un insumo que no solo sea aplicable en la entidad en la que se elaborará el trabajo, sino que podrá replicarse en otras empresas o instituciones, sin importar la actividad comercial o región geográfica.

El problema de la seguridad de la información no es nuevo, pero en épocas recientes ha adquirido una visibilidad sin precedentes. Por ejemplo, los ciberataques han sustituido formas tradicionales de atacar a países o grupos de personas. En Estados Unidos, se considera a los ciberataques como una de las mayores amenazas y los gobernantes impulsan la ciberseguridad. Uno de los primeros esfuerzos fue la creación de la orden 13636, dictada por el expresidente Barack Obama y que señala: “las repetidas instrucciones cibernéticas en la infraestructura critica demuestra la necesidad de mejorar la ciberseguridad” (Obamawhitehouse.archives.gov, 2012, s. p.).

Este es un tema tan importante en los Estados Unidos que han creado una entidad dedicada al Marco de Seguridad Cibernética, que desarrolla la ciberseguridad en pequeñas y grandes organizaciones: el Instituto Nacional de Estándares Tecnología NIST, expone la importancia de la ciberseguridad y la expresan de una forma visiblemente seria.

Este marco que la NIST expone es de aplicación y edición flexible y abierta a la

comunidad, a investigadores, áreas interesadas, personal civil y cualquier persona o grupo que considere que puede adaptarla como propia, incluso se pueden proponer mejoras, no se hacen distinciones o filtros de origen. Además, existe una comisión que las evalúa e incorpora los cambios a la normativa, estos insumos hacen que el marco de la NIST crezca y se fortalezca constantemente, también incorpora extractos de importantes normas como COBIT, ITIL e ISO.

Esta mezcla no quita valor, todo lo contrario, las integra y complementa de forma consistente, con el único fin de proteger a las empresas y organizaciones. La NIST incorpora las experiencias de especialistas, de empresas, población educativa, individuos de forma civil, etc. Todos estos aportan para formar un abanico de intereses que enriquecen y hacen evolucionar de forma fluida la norma, para crear un producto final que sin duda beneficia a todos, en lo relacionado a ciberseguridad.

La globalidad y la libreta expresa en NIST, hacen que este marco pueda aplicarse en Costa Rica, esto sin duda es una ventaja, debido a que se tiene una relación estrecha con Estados Unidos, en la que la normativa NIST toma relevancia. Implementarla en el ámbito comercial a mediano plazo podría ser una fortaleza, ya que las pequeñas ventajas pueden determinar aliados de negocio.

Esta investigación busca aplicar una normativa quizá no tan replicada en Costa Rica, pero si en otras latitudes, principalmente en los Estados Unidos de América, en donde este marco fue concebido ha sido adoptado. Además, se ha puesto en práctica por diferentes organizaciones gubernamentales, instituciones privadas, universidades, organismos de bien social, incluso en países como Uruguay y algunas naciones del Caribe.

## 1.5. Viabilidad

### 1.5.1. Punto de Vista Técnico

No requiere pruebas técnicas.

### 1.5.2. Punto de Vista Operativo

Desde la operatividad de organización, solo cabe subrayar que en caso de encontrar alguna vulnerabilidad o debilidad se mantendrá de forma confidencial y se informará a las autoridades competentes, incluso antes de cualquier resultado académico, es decir, la integridad de la organización priva sobre lo académico.

### 1.5.3. Punto de Vista Económico

No implica costos asociados a la investigación, el costo es un aspecto teórico, se requiere tiempo de análisis, investigación y observación, con el fin de obtener el conocimiento necesario para obtener los resultados que se desea en la investigación, estos serán sufragados por el investigador.

## 1.6. Objetivos

### 1.6.1. Objetivo General

Crear las bases para definir un modelo que permita la evaluación de la ciberseguridad de las entidades financieras, principalmente bancos de Costa Rica, con base en el marco de ciberseguridad de la NIST.

### 1.6.2. Objetivos Específicos

- Definir los insumos para la medición de los niveles de riesgo necesarios para que se aplique el marco de referencia de la NIST.
- Fundamentar las mejoras a la ciberseguridad con la aplicación del Marco NIST.
- Crear las bases para una guía básica de análisis de la ciberseguridad desde el marco NIST.

## 1.7. Alcances y Limitaciones

### 1.7.1. Alcances

La investigación contempla un análisis de aspectos de seguridad delicados de una entidad financiera, el producto de la investigación es realizar un aporte a la Ciberseguridad, el análisis se realiza en un marco de tiempo específico, con un fin académico.

### 1.7.2. Limitaciones

La principal limitante es el tiempo para realizar la investigación, la cual busca sentar las bases robustas para trabajos posteriores. Como es un proyecto académico, la investigación es reducida, con tiempos moderados, por lo que el enfoque principal será dar y fundamentar los primeros pasos para un análisis de ciberseguridad, como el caso del riesgo inherente. Los pasos para aplicar la normativa son varios y tan profundos como se desee.

Esta investigación será elaborada en una entidad financiera, por lo que algunos datos serán reservados por motivos de seguridad, confidencialidad e integridad de la información. En caso de tener hallazgos sensibles o que pueden afectar el negocio, se le comunicará al área responsable, además, algún dato se mantendrá de forma confidencial para no exponer a la organización.

En caso de requerir pruebas o cambios sugeridos, deberán ser implementados por la entidad en la que se elabora la investigación.

Es una propuesta académica, no se desarrollará ningún tipo de implementación, tiene como fin mostrar una base sólida para implementar NIST.

La versión de NIST es la 1.1 vigente a setiembre 2019, además de COBIT 4. No implica material o aporta insumos adicionales a los expresos en este documento.

## 1.8. Marco de Referencia Organizacional

### 1.8.1. Historia

La entidad lleva alrededor de siete años en el mercado como marca actual, pero, anteriormente, era soportada por marcas internacionales que marcaron la razón de ser. Es una entidad en crecimiento constante y esto se ha visto reflejado en el último semestre del año 2017, en el que fue una de las tres entidades financieras que creció más porcentualmente.

### 1.8.2. Tipo de Negocio y Mercado Meta

La entidad bancaria se dedica a brindar soluciones financieras con calidad y atención personalizada, además de un valor agregado, con lo que contribuye con la descentralización de servicios en busca de una cobertura global. Aplica recursos tecnológicos y humanos para satisfacer las necesidades financieras de los clientes. Todo esto con estándares nacionales en Costa Rica y respetando el estándar global de banca y finanzas. El único fin es mantener la confianza del cliente de que los servicios que se ofrecen están respaldados en todo momento, desde la perspectiva legal, financiera y tecnológica.

### 1.8.3. Misión

La entidad bancaria será la entidad financiera de clase mundial más respetada en Costa Rica por prestar a las familias e individuos los más convenientes servicios en forma amable, alegre, moderna y sencilla.

Debido a que está comprometida con el país y con su desarrollo sostenible, la entidad desarrollará su objetivo social enmarcando sus actuaciones dentro de los más elevados principios éticos y morales.

Será una organización flexible apoyada en tecnología de punta: el diseño y la integración de sus productos, así como la efectividad y diversidad de sus canales de servicios y ventas le permitirán estar al nivel de las mejores del mundo y ser líder en los mercados en los que compita. Además, desarrollará sus estrategias de negocios y

servicios a través de la segmentación del mercado, con información de excelente calidad sobre el comportamiento, preferencias y potencialidad de sus clientes, anticipándose a las tendencias y cambios que se produzcan en el entorno, para lograr el deleite de sus clientes.

Está conformada por el grupo humano más idóneo en el país, con gran sentido de pertenencia y con quienes estará comprometida para lograr su desarrollo personal y profesional. Además, se identifica plenamente con su misión, principios y valores, por lo cual cooperará y compartirá habilidades, canales y servicios para lograr sinergia en los resultados del conjunto.

Ofrecerá a sus accionistas una atractiva rentabilidad y alta valorización de su inversión con el propósito fundamental de maximizar el valor patrimonial de la empresa y generar recursos para desarrollar nuevos negocios e inversiones que permitan su permanencia y crecimiento a largo plazo.

### 1.8.4. Visión

La entidad bancaria es una entidad de intermediación y servicios financieros, orientada a los individuos y familias, especializada en la promoción de ahorro y la financiación de vivienda.

Procura el liderazgo del sector financiero con imagen, rentabilidad y participación en el mercado, con base en innovación, mayor eficiencia en sus operaciones y mejor calidad de los productos ofrecidos a sus clientes.

### 1.8.5. Políticas Institucionales[i]

El término *Gobierno Corporativo* es un concepto que puede tener varios significados, no obstante, para la entidad bancaria será entendido como el conjunto de políticas y principios de dirección, administración y supervisión empresarial que permiten que se definan estructuras para crear valor y generar confianza y transparencia en los diferentes Grupos de Interés del Banco.

Todo sin perjuicio de lo establecido por la normatividad vigente en Costa Rica,

es interés prioritario asegurar la transparencia, eficiencia y probidad de sus actuaciones, ya que estos atributos son un presupuesto básico para que pueda desempeñarse cabalmente, promoviendo la sana competencia en el mercado en el cual se desarrolla.

Cada una de las áreas está comprometida con la adopción de buenas prácticas de transparencia, Gobierno corporativo, ética y conducta, que permitan generar seguridad a sus accionistas y, en general, a todos sus grupos de interés.

De acuerdo con lo anterior, este Código de Buen Gobierno recopila las políticas de la entidad pretende comunicar a todos sus Grupos de Interés, los principios de Gobierno Corporativo, la misión y la visión, la información financiera y no financiera a revelar en el mercado, los órganos de control y las medidas para verificar el cumplimiento de las normas de Buen Gobierno, entre otros.

## 1.9. Marco de Referencias

### 1.9.1. Revisión Sistemática

Este estudio presenta una revisión sistemática en la que expone un análisis ontológico desde el punto de vista de la ciberseguridad. Se desea tener conciencia del estado de ciberseguridad desde este punto de vista relacionado con el marco de referencia de la NIST, por esta razón, el estudio tiene un carácter relevante en la entidad financiera.

### 1.9.2. Repositorios

Para esta investigación, la lista de repositorios utilizados es:

- https://books.google.co.cr (Book Google)
- http://scholar.google.com (Google Scholar)

### 1.9.3. Cadenas de Búsquedas

Se consideró para el estudio una cadena de búsqueda a partir de las siguientes opciones.

NIST and cybersecurity.

### 1.9.4. Inclusión y Exclusión

#### *1.9.4.1. Inclusión*

NIST: tema pilar de la investigación.

Cybersecurity: es la especificación y distinción de los diferentes elementos.

#### *1.9.4.2. Exclusión*

El factor de tiempo será tomado en cuenta y en la investigación solo se valorarán publicaciones posteriores al 2012. Año de la creación de NIST. Además, la investigación solo incorpora idioma español e inglés.

| **Identificación** | |
|---|---|
| Titulo: | *Framework* for Improving Critical Infrastructure Cybersecurity |
| Publicación: | Versión 1.0, febrero 12 2014 |
| Autores: | National Institute of Standards and Technology |
| Referencia: | [1] |
| **Descripción** | |
| Área: | CiberSeguridad. |
| Resumen: | Actualización de marco al marco de referencia. |
| **Aspectos por destacar** | |
| Descripción del marco desde su creación, bases y objetivos. | |

| **Identificación** | |
|---|---|
| Titulo: | *Framework* for Improving Critical Infrastructure Cybersecurity |
| Publicación: | Versión 1.1, abril 16 2018 |
| Autores: | National Institute of Standards and Technology |
| Referencia: | [2] |

| Descripción | |
|---|---|
| Área: | CiberSeguridad. |
| Resumen: | Actualización de marco al marco de referencia. |
| **Aspectos por destacar** | |
| Dentro de lo más significativo de esta actualización esta:<br>El término cumple se aclaró la terminología.<br>Se agregó la Sección 4.0 Autoevaluación del Riesgo de Ciberseguridad con el Marco para explicar cómo el Marco puede utilizarse por organizaciones y con esto comprender y evaluar su riesgo de ciberseguridad, incluyendo el uso de medidas | |

| Identificación | |
|---|---|
| Titulo: | Controles de Seguridad propuesta inicial de un *Framework* en el Contexto de la CiberDefensa |
| Publicación: | 2015 |
| Autores: | Pablo Gastón Sack, Jorge S Ierache, |
| Referencia: | [3] |
| **Descripción** | |
| Área: | CiberSeguridad. |
| Resumen: | Este resume los aspectos de ciberseguridad. |
| **Aspectos por destacar** | |
| Menciona múltiples conceptos de ciberseguridad:<br>Controles de seguridad, Ciberespacio.<br>Ciberguerra.<br>Además, toca diferentes modelos de marcos de referencias de ciberseguridad. | |

# Capítulo 2. Marco Teórico

A pesar de que la ciberseguridad es un tema relativamente nuevo, existen varios métodos para orientar el estado de una empresa en este aspecto. Es importante conocer algunos de estos para comprender qué es el NIST y su importancia, de modo que sea posible potenciar este análisis y que sea perdurable.

## 2.1. COBIT

COBIT 4 es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: *Information Systems Audit and Control Association*) y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992, algunos de sus componentes de la versión cuatro establecen:

- 4 dominios.
    - PO - Planear y organizar.
    - DS – Entregar y dar soporte.
    - AI – Adquirir e implantar.
    - ME – Monitorear y evaluar.
- 34 procesos
- 210 objetivos de control

Entre sus ventajas señalan:

- Alineación de objetivos de TI y del negocio.
- Ayuda a empresa a alcanzar objetivos.
- Es un método holístico, incluye todo el proceso.
- Establecer una orientación a procesos.

- Ser consistente con las mejores prácticas (COSO).
- Proporciona un lenguaje común.

Es importante mencionar que quizás es la norma más utilizada en Costa Rica, por regulación financiera, además, se mantiene en un proceso de mejora continua donde periódicamente se liberan nuevas versiones.

## 2.2. ISACA

La norma de la Asociación de Auditoría y Control de Sistemas de Información, (Information Systems Audit and Control Association) contempla una asociación internacional que apoya actividades como auditorías y controles en los sistemas de información. Se creó en 1967 y contempla 180 países con 170 capítulos de contenido, además, provee certificaciones internacionales, entre las que se pueden mencionar:

- CISA - Certified Information Systems Auditor, certificación de auditores de sistemas de información. Existen cerca de noventa mil personas certificadas (2012).
- CISM - Certified Information Security Manager, certificación de gestores de seguridad. Existen cerca de dieciséis mil personas certificadas.
- CGEIT - Certified in the Governance of Enterprise IT, certificación de gestores de la gobernanza empresarial TI. Existen cerca de cuatro mil seiscientas personas certificadas (2007).
- CRISC - Certified in Risk and Information Systems Control, certificación de gestores de control de riesgos en sistemas de información. Existen cerca de quince mil personas certificadas (2010).

ISACA es una asociación muy activa en el ámbito mundial, valida sus certificaciones en función de diferentes áreas como:

- Aseguramiento.
- Gobierno.

- Seguridad de la información.

### 2.3. Marco ISO 27032:2017

Es otro marco de referencia para la gestión de la seguridad de la información, es muy utilizado en el ámbito mundial, es decir, se aplica a un concepto más amplio que la ciberseguridad, se incluyen otros aspectos como técnicos, legales y organizativos.

Con esta norma:

- Se pretende garantizar la seguridad en los intercambios de información en la Red.
- Crear un nuevo marco para el mejoramiento de la seguridad en Internet. La norma ISO 27032 pretende garantizar un entorno seguro, a través de directrices de seguridad.

### 2.4. NIST

Con la evolución y masificación de la tecnología, los aspectos de seguridad han elevado su exposición, por esto, diferentes organizaciones, incluso gobiernos, dependen de una información confiable. Las amenazas de ciberseguridad pueden afectar la economía, la seguridad pública de naciones, la salud y sectores financieros o reputacional de la organización; esto provocó que, en Estados Unidos de América, el presidente emitiera la Orden Ejecutiva 13636, *Mejorando la crítica Infraestructura Ciberseguridad,* el 12 de febrero de 2013. Entre sus objetivos están mejorar la seguridad y mejorar la capacidad de recuperación de la infraestructura, con esto se pretende mantener un entorno cibernético que aliente la eficiencia, la innovación y la prosperidad económica, que promueva la seguridad empresarial, la privacidad y las libertades civiles.

Esta política exige el desarrollo de un marco de riesgo en ciberseguridad, es decir, un conjunto de estándares y mejores prácticas para que las organizaciones gestionen los riesgos en este ámbito.

El marco se enfoca en impulsores de negocios, para guiar las actividades de ciberseguridad y considerar los riesgos de seguridad cibernética como parte de los procesos de gestión de riesgos de la organización. El marco consta de tres partes: Marco Central o CORE, Perfil del Marco y los Niveles de Implementación del Marco. Mediante el uso de los perfiles, se busca alinear sus actividades de ciberseguridad con sus requisitos comerciales, tolerancias de riesgo y recursos y los niveles proporcionan un mecanismo para que las organizaciones puedan ver y comprender las características de su enfoque.

El marco permite a las organizaciones, independientemente de su tamaño, grado de seguridad cibernética o sofisticación de ciberseguridad, aplicar los principios y las mejores prácticas de gestión de riesgos, para mejorar la seguridad y la capacidad de recuperación de la infraestructura crítica, esto es el pilar de la investigación. El marco hace referencia a los estándares mundialmente reconocidos, con el propósito de utilizarse sin restricción y aplicarlo en diferentes escenarios, con diferentes riesgos, vulnerabilidades y amenazas, además de su tolerancia al riesgo.

Es una herramienta que evoluciona constantemente por los diferentes aportes de las áreas interesadas y con frecuencia incorpora mejoras, se dice que es una herramienta viva que suple las necesidades de ciberseguridad en entornos dinámicos y cambiantes, ante las nuevas amenazas y riegos, es decir, es una solución que se debe valorar.

## 2.5. FFIEC

El proceso para la evaluación de la ciberseguridad, con el fin de mantener una línea de análisis congruente, holístico y alineado con un mismo orden, se contempla la herramienta creada por el Consejo de Examen de Instituciones Financieras Federales (FFIEC por sus siglas en inglés *Federal Financial Institutions Examination Council*), en el año 2014, con el objetivo de mitigar ataques cibernéticos. Esta entidad insta a las instituciones a considerar la gestión de vulnerabilidades y amenazas, tanto internas como externas. La definición se basa en la seguridad de la información, tal como se define en la guía FFIEC: “Los incidentes cibernéticos pueden tener un impacto

financiero, operativo, legal y de reputación. Los recientes ataques cibernéticos de alto perfil demuestran que los incidentes cibernéticos pueden afectar significativamente el capital y las ganancias” (s. f., s. p.).

# Capítulo 3. Marco Metodológico

## 3.1. Tipo de Investigación

El tipo de investigación es aplicada, se enfoca en un entorno actual, a partir del que se fundamenta la investigación sobre el problema presentado. Suchman (1967) define como evaluativa a la investigación aplicada cuya meta no es el descubrimiento del conocimiento, sino que se enfatiza la utilidad de la investigación.

## 3.2. Alcance Investigativo

La investigación será de alcance descriptivo, se presentará una herramienta para análisis de riesgo actual, además, se establecerán las bases para aplicar un marco de referencia, en este caso NIST, con el fin de brindar soporte para un análisis de ciberseguridad aplicado. Es importante señalar que la NIST hace referencia a los instrumentos y referencias para aplicar la normativa, por lo que esta investigación quiere impactar no solo donde se aplica como primer escenario, sino que se espera que sea replicable en otro escenario en el ámbito local, puede ser en la misma área de negocio.

## 3.3. Enfoque

El enfoque de esta investigación utiliza un abordaje cualitativo, según los autores Blasco y Pérez (2007), la investigación estudia el contexto natural como sucede, muestra e interpreta fenómenos de acuerdo con las personas involucradas.

Con el enfoque se determinará el comportamiento de un estado, su reacción y acción en cuanto a condiciones o pruebas determinadas. El estudio no busca representar o defender las cualidades o estado actual con cantidades o valores.

## 3.4. Diseño

Esta investigación busca definir una base en la que mediante un marco de referencia como el elaborado por NIST, una entidad (en este caso bancaria) pueda evaluar de una manera práctica su ciberseguridad, con un marco reconocido

mundialmente y en constante evolución, crecimiento y actualización.

Un marco de referencia como NIST traería muchas ventajas, requeridas para una implementación adecuada de metodologías, es fácil de comprender, su implantación es simple y es actualizada constantemente por parte de diferentes organismos interesados.

# Capítulo 4. Propuesta de Solución

Antes de medir cualquier nivel de madurez aplicado a la ciberseguridad, se debe conocer el negocio y su manejo del riesgo, además de tener claras las prioridades de negocio, así como los intereses o políticas de las organizaciones, cualesquiera que sean. Asimismo, se deben conocer las áreas en las que la entidad tiene poco interés, esto es clave en el momento de evaluar la ciberseguridad y determinar las áreas de mejora.

## 4.1. NIST

Con este par de insumos a nuestro se puede iniciar con el análisis del marco de referencia NIST, hacer una propuesta efectiva sobre cómo analizar la ciberseguridad de una organización, de una forma integral y holística. Para esto, se deben entender los componentes de la NIST:

### 4.1.1. Núcleo

Núcleo es el conjunto de actividades de seguridad, resultados y referencias aplicadas, presenta también directrices o prácticas de la industria que permiten la comunicación y presentan resultados de seguridad, desde un nivel simple de implementación u operación hasta un nivel ejecutivo. Se compone de un ciclo de cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar, es un ciclo de vida que cubre de forma holística la organización. En cada una de las cinco funciones se pueden encontrar categorías y subcategorías, incluso categorías subyacentes que se podrían comparar con otros estándares, directrices o prácticas del mercado.

### 4.1.2. Los Niveles

De los niveles se puede decir que proporcionan un contexto, describen un grado de administración de la ciberseguridad por las prácticas mencionadas, reflejan progreso o lo que se conoce como madurez de la norma y cuantifican el proceso por niveles que orientan sobre el estado de aplicación del modelo.

### 4.1.3. El Perfil

En el perfil se pueden revisar las categorías y subcategorías, determinar cuáles son las más importantes para incluirlas en el análisis de riesgo de la organización, además, se puede crear un perfil objetivo. Esto significa que se puede priorizar objetivos, en relación con las necesidades de las empresa, rentabilidad e innovación.

En respuesta a los comentarios de la industria, en el desarrollo del marco el NIST, se trabaja para permitir que las pautas se apliquen más fácilmente a las organizaciones, gracias a los *perfiles* específicos por sector.

Para evaluar NIST se requieren insumos básicos y la FFIEC suministra las a través del Consejo de Coordinación del Sector de Servicios Financieros (FSSCC por sus siglas en inglés *Financial Services Sector Coordinating Council*) una hoja de cálculo como herramienta FSSCC_ACAT_v2.1_SPA para la protección de la infraestructura critica, una de sus partes u hojas, llamada Entrada perfil riesgo inherente (anexo 1) brinda datos sobre el riesgo inherente (abarcado en esta investigación) y la segunda Resultados perfil riesgo inherente (anexo 2), es la que permite cuantificar la madurez de la organización con cinco dominios, con estos insumos es posible iniciar la evaluación.

# Capítulo 5. Herramienta de Riesgo Inherente

## 5.1. Entrada Perfil Riesgo Inherente

La herramienta es una hoja llamada *Entrada perfil riesgo inherente*, comprende diferentes áreas o categorías, entre las que se pueden citar:

- Tecnologías y tipos de conexión.

Relacionado a los ISP, *wireless*, red cableada, dispositivos que pueden conectarse, proveedores de actividades críticas, ciclos de vida de productos, indicar en casos de *software* abierto, aspectos relacionados con la nube, entre otros.

- Canales de entrega.

Si tiene servicio en línea, presencia móvil, cajeros o ATM en operación.

- Móviles en línea productos y servicios de tecnología.

Es más operativo, por ejemplo, si poseen emisión de tarjetas, billeteras móviles, trasferencias internacionales, remesas, servicios de tesorería, también incluye pagos P2P o persona a personas, como se conoce en Costa Rica, transferencias SINPE del Banco Central, entre otros.

- Organizacional Características.

Este apartado incluye fusiones o adquisiciones, cantidad de colaboradores, rotación del personal crítico, distribución de privilegios, lugares de presencia, ubicación de los edificios principales u operaciones y adhiere cambios en la red o infraestructura critica.

- Amenazas externas.

Examina lo relacionado a los ataques cibernéticos o intentos, como denegación de servicios.

En cada uno de estos puntos se debe categorizar el riesgo inherente con métricas definidas de uno a cinco, según el nivel:

1. Sin afectar.

Es donde no se presenta riesgo o el casi inexistente.

2. Con una mínima afectación.

Existe riesgo, pero con una afectación mínima.

3. Con un riesgo moderado.

Existe riego considerable, con una afectación considerable.

4. Riesgo significativo.

Es un riesgo de atención inmediata y podría afectar muy seriamente.

5. Riesgo el más alto.

Afección o riesgo severo de impacto máximo para el negocio.

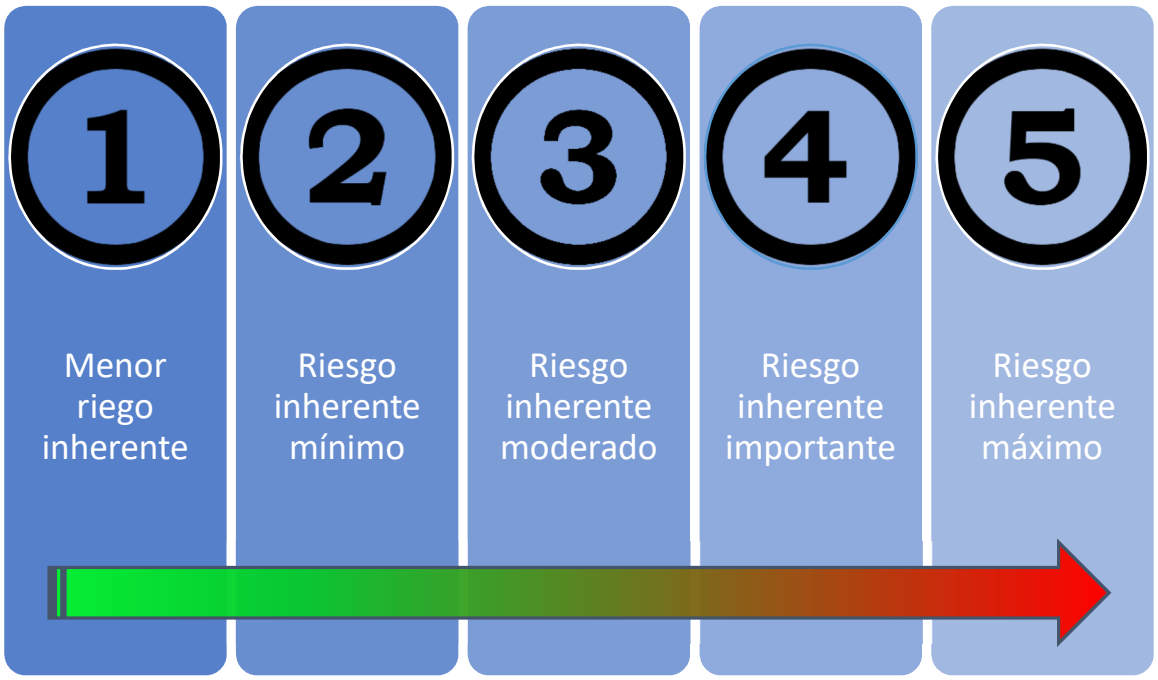



Ilustración 3. Niveles de Riesgo Inherente

1. Menor riego inherente.
2. Riesgo inherente mínimo.
3. Riesgo inherente moderado

4. Riesgo inherente importante
5. Riesgo inherente máximo.

### 5.2. Aplicación de la Herramienta de Riesgo Inherente

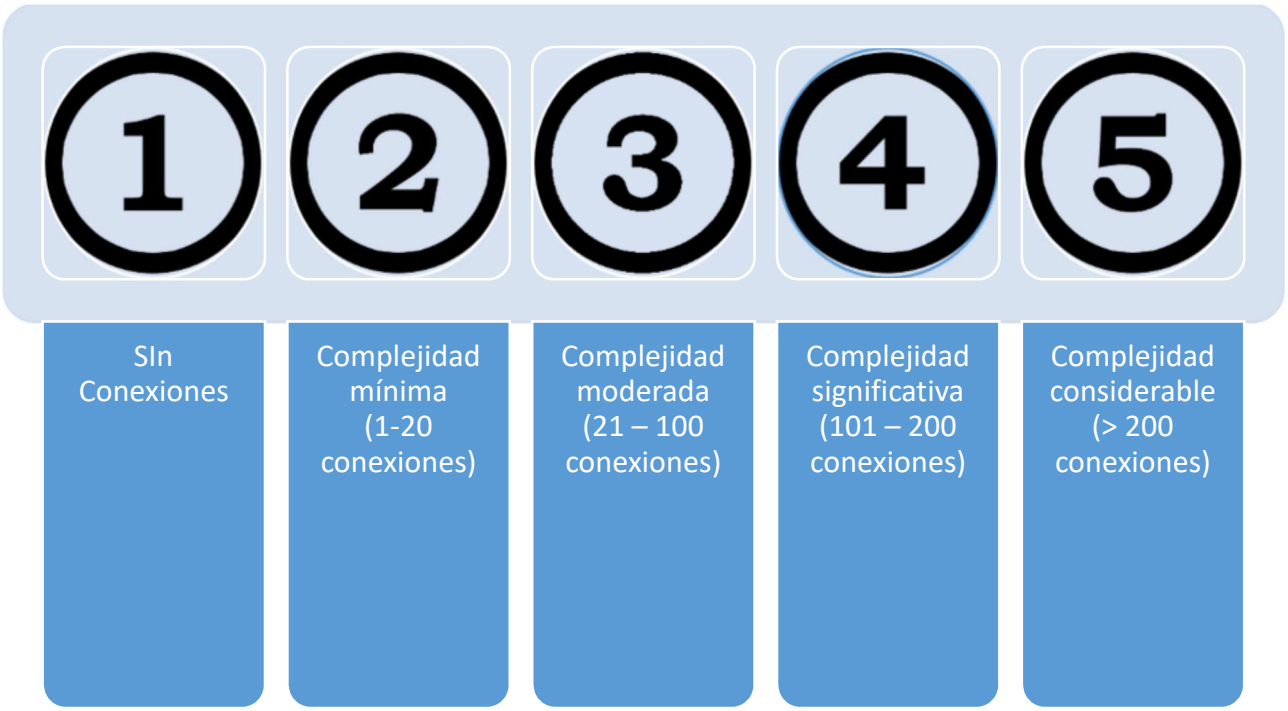
La herramienta consiste en segregar la medición, con el propósito de abarcar los diferentes procesos de tecnología, además de la interrelación con todos los servicios recibidos o los brindados. La herramienta de medición asigna un nivel, según los parámetros definidos por: un atributo, servicio, actividad o producto. El resultado se refleja en una tabla para determinar el riego inherente.

La primera parte para analizar es el riesgo inherente que incorpora el tipo, volumen y la complejidad de las operaciones, además, las amenazas. El riesgo inherente no incluye controles de mitigación. El perfil de riesgo inherente incluye descripciones de las actividades en categorías de riesgo, con las definiciones para la mayoría de los niveles de riesgo inherente. Determinar la exposición al riesgo de las actividades, servicios o productos, para plantearlos a la organización, ayuda en el proceso.

Se definen cinco categorías, evaluadas a continuación:

### 5.2.1. Categoría: Tecnologías y Tipos de Conexión

1. Número total de conexiones a Internet servicio proveedor (ISP) incluyendo conexiones.




Comentarios:

2. Conexiones externas, el número de conexiones no usuarios (por ejemplo, archivo transferencia protocolo (FTP), Telnet, rlogin).

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Ninguna | Pocos casos de conexiones sin garantía (1-5) | Varios casos de conexiones no garantizados (6 – 10) | Hasta importantes de conexiones pecado garantía (11 – 25) | Hasta importantes de conexiones pecado garantía (> 25 |

Comentarios:

3. Acceso a red inalámbrica.


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Sin acceso wireless | Puntos de acceso separados para huéspedes wireless y corporativa inalámbrica | Huésped y acceso a la red inalámbrica corporativa lógicamente están separados; número limitado de usuarios y puntos de acceso (1 a 250 usuarios, puntos de acceso de 1 – 25) | Acceso a la red inalámbrica de la empresa; número significativo de usuarios y puntos de acceso (251 – 1.000 usuarios; 26 – 100 puntos de acceso) | Acceso a la red inalámbrica de la empresa; todos los empleados tienen acceso; número considerable de puntos de acceso (> 1.000 usuarios; > 100 puntos de acceso) |

Comentarios:

4. Dispositivos personales pueden conectarse a la red corporativa.


Comentarios:

5. Terceras partes, incluyendo el número de organizaciones y de individuos de proveedores y subcontratistas, con acceso a sistemas internos (por ejemplo, red privada virtual, módem, intranet, conexión directa).

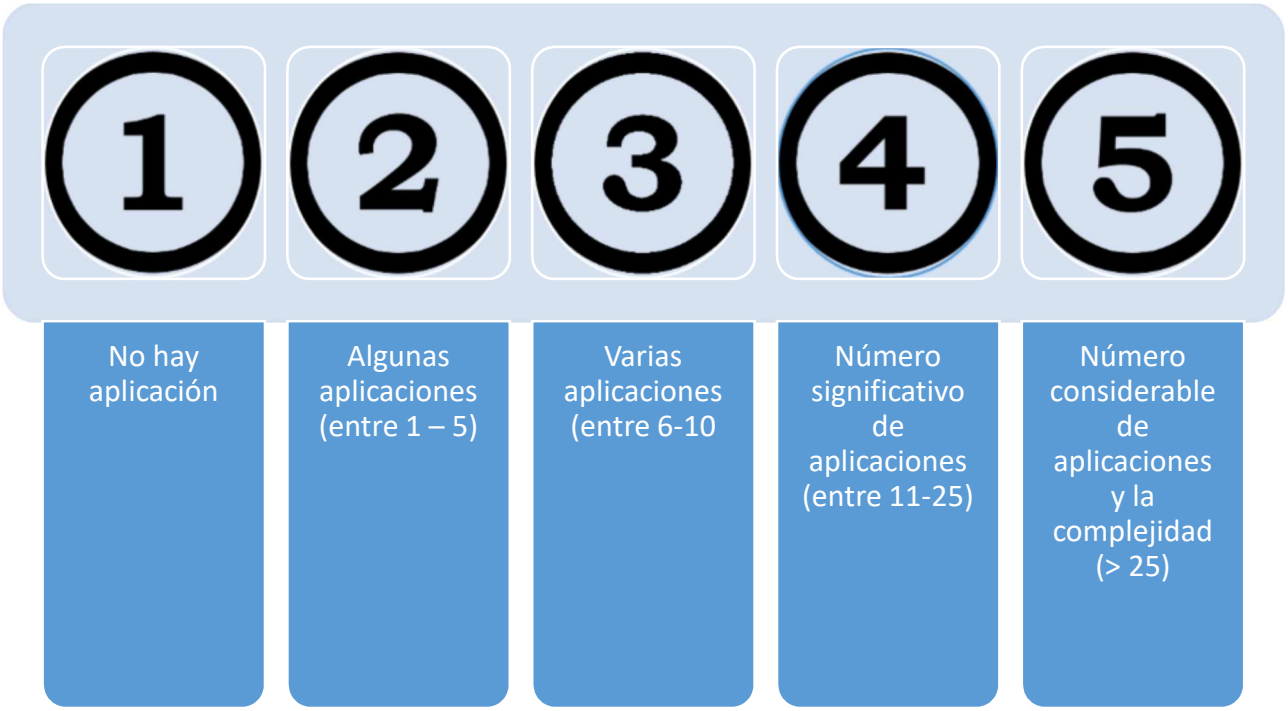

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No hay terceras personas y no individuos de terceros con acceso a los sistemas | Limitado número de terceros (1 – 5) y el número limitado de personas por parte de terceros (< 50) con acceso; baja complejidad en cómo acceden a los sistemas | Número moderado de terceros (6 – 10) y moderado número de individuos por parte de terceros (50 – 500) con acceso; cierta complejidad en cómo acceden a los sistemas | Número significativo de terceros (11 – 25) y gran número de individuos por parte de terceros (501 – 1.500) con acceso; alto nivel de complejidad en cuanto a cómo acceder a los sistemas | Gran número de terceros (> 25) y considerable número de individuos por parte de terceros (> 1.500) con acceso; alta complejidad en cómo acceden a los sistemas |

Comentarios:

6. Clientes externos con conexiones dedicadas.

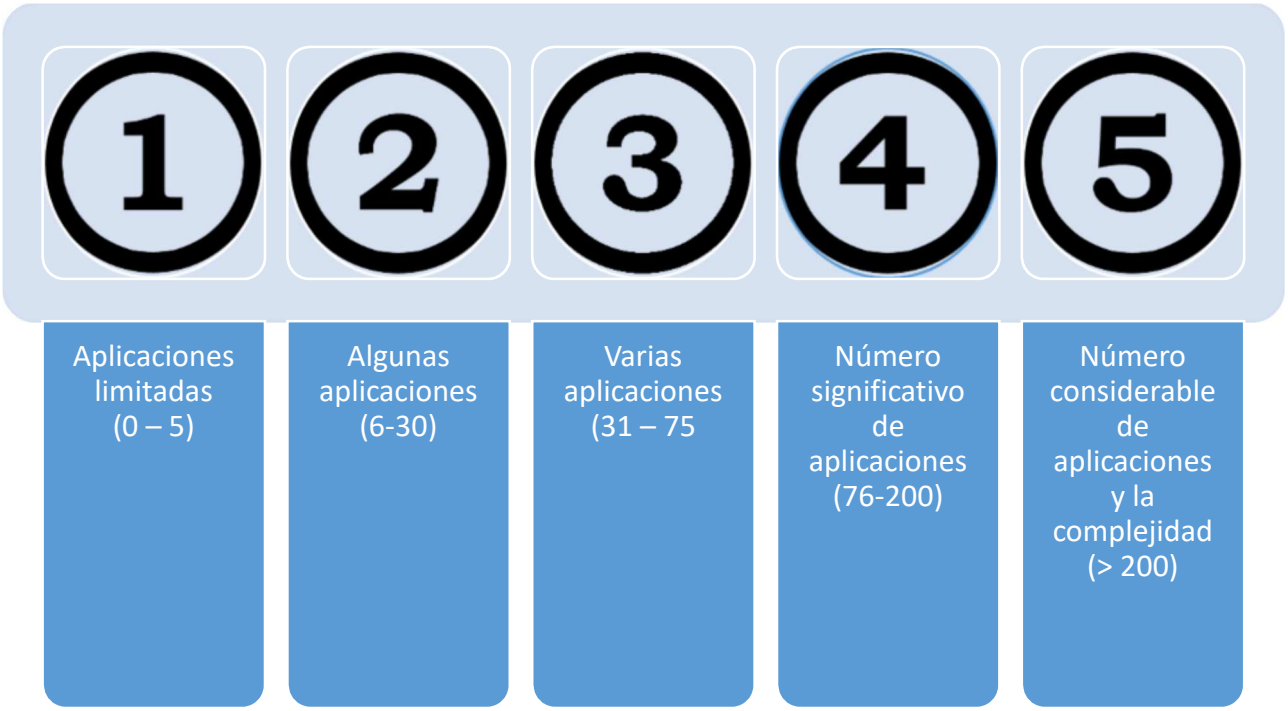

Comentarios:

7. Aplicaciones de proveedor interno alojado y desarrollado, apoyando actividades críticas.



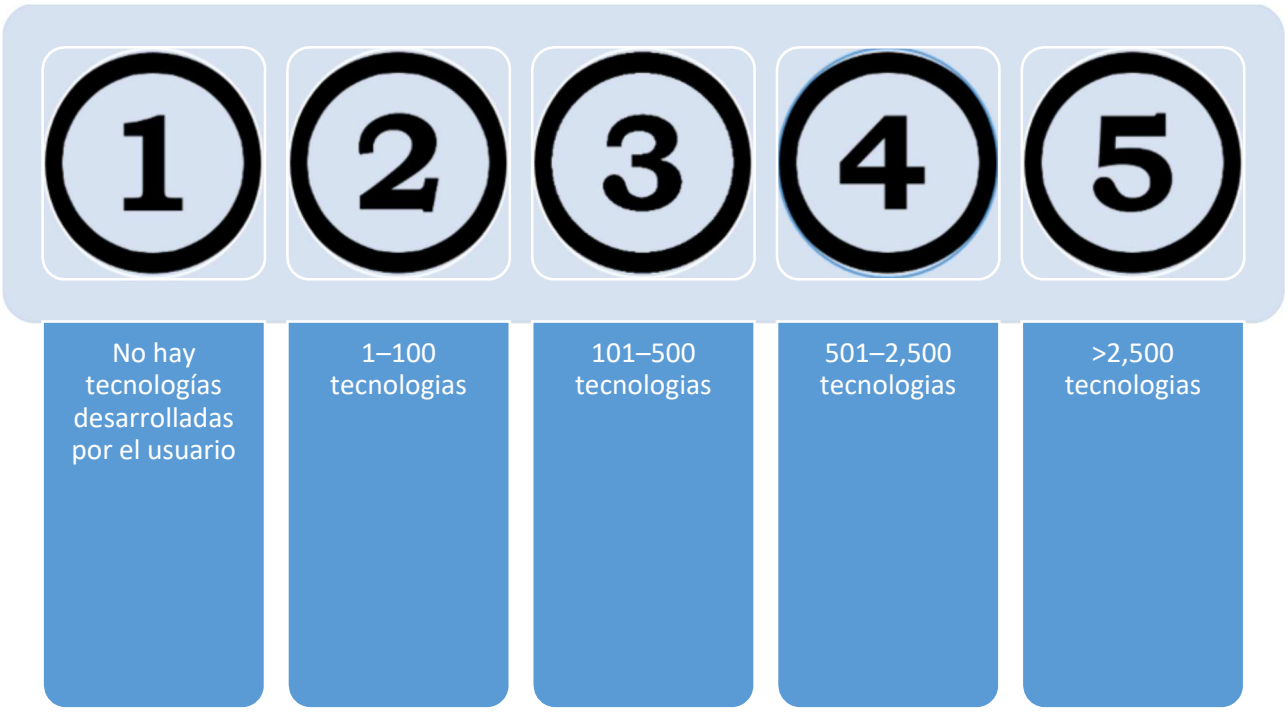

Comentarios:

8. Internamente, organizado, desarrollado por el proveedor de aplicaciones apoyando actividades críticas.



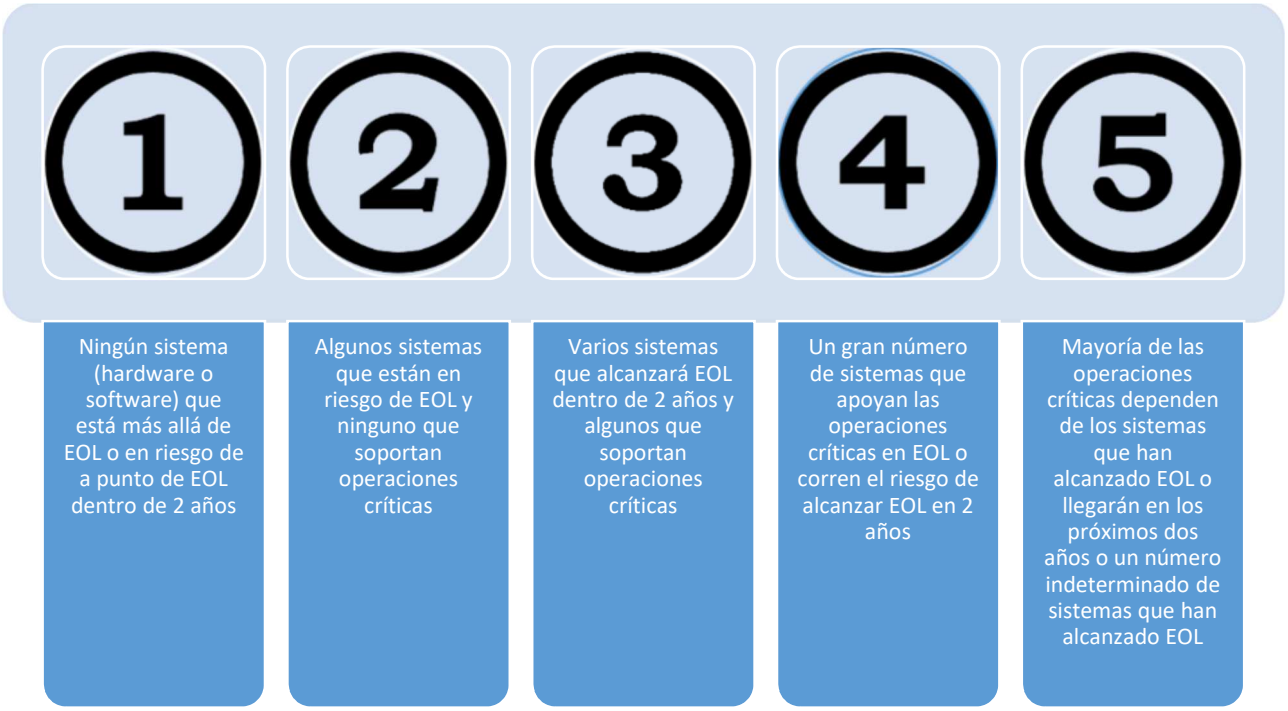

Comentarios:

9. Tecnologías desarrolladas por el usuario y usuario de computación que soportan actividades críticas (incluye hojas de cálculo Microsoft Excel y bases de datos Access u otras herramientas desarrolladas por el usuario).




Comentarios:

10. Sistemas al final de la vida (EOL).




Comentarios:

11. *Software* de código abierto (OSS).


Comentarios:

12. Dispositivos de red (por ejemplo, servidores, *routers* y *firewalls*; son físicos y virtuales).


Comentarios:

13. Proveedores de servicios de terceros, almacenamiento o procesamiento de información que apoyan actividades críticas (no tienen acceso a sistemas internos, pero la institución se basa en sus servicios).


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No hay terceras personas que apoyan actividades críticas | 1-25 terceros que admiten actividades críticas | 26-100 terceras personas que apoyan actividades críticas | 101-200 terceros que admiten actividades críticas; 1 o más son extranjeros | > 200 terceras personas que apoyan actividades críticas; 1 o más son basados en extranjeros |

Comentarios:

14. *Cloud computing*, servicios alojados externamente para apoyar actividades críticas.


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No hay proveedores de nube | Pocos proveedores de nube; nube privada (1-3) | Varios proveedores de nube (4 – 7) | Número significativo de proveedores cloud (8 – 10); proveedor de la nube localizaciones utilizado incluye internacional; uso de nube pública | Número importante de los proveedores de cloud (> 10); proveedor de la nube localizaciones utilizado incluye internacional; uso de nube pública |

Comentarios:

### 5.2.2. Canales de Entrega

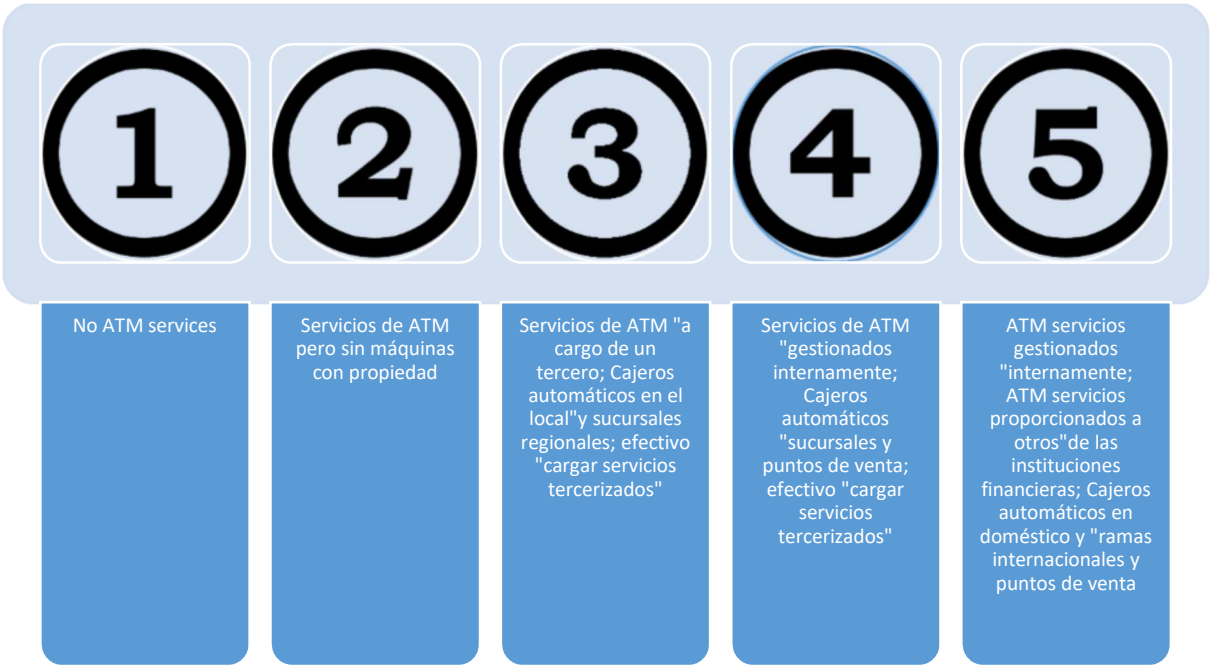
1. *Online* presencia (customer).


Comentarios:

2. Mobile presencia.


Comentarios:

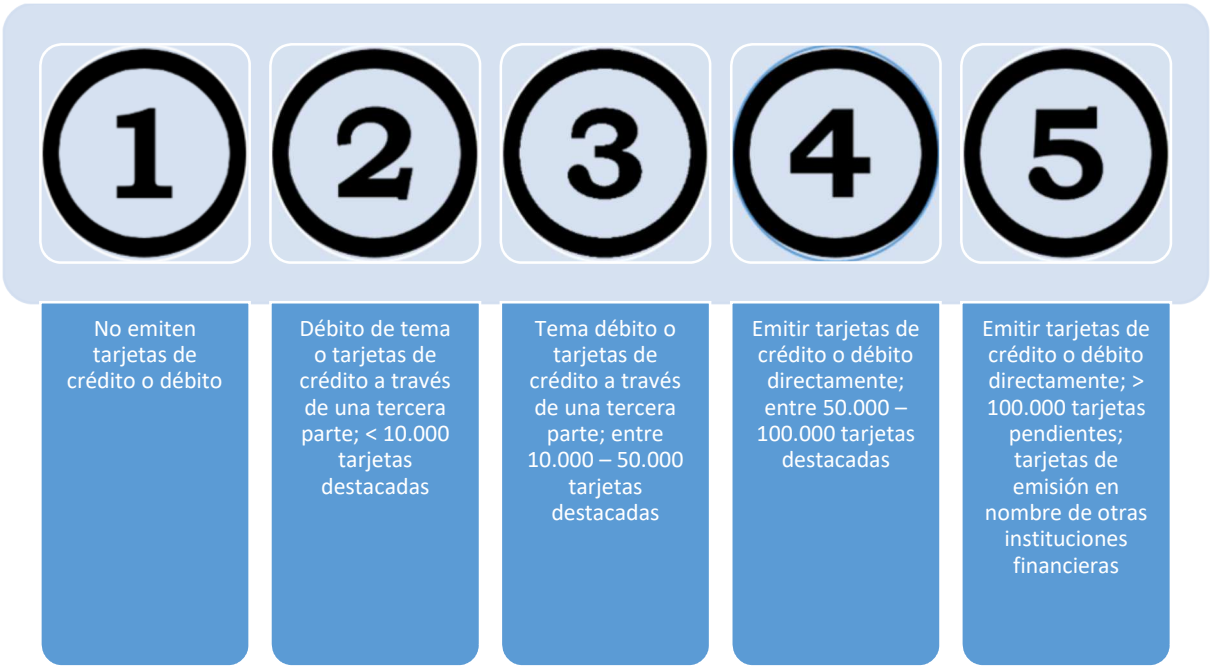
3. Cajeros automáticos (ATM) (operación).




Comentarios:

### 5.2.3. Categoría: Móviles en Línea Productos y Servicios de Tecnología

1. Tarjetas de crédito o débito de tema.




Comentarios:

2. Tarjetas prepagadas


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No emiten tarjetas de prepago | Emitir tarjetas prepagadas a través de un tercero; < 5.000 tarjetas destacadas | Emitir tarjetas prepagadas a través de un tercero; 5.000 – 10.000 tarjetas destacadas | Emitir tarjetas prepagadas a través de un tercero; 10.001-20.000 tarjetas destacadas | Emitir tarjetas prepagadas internamente, a través de un tercero, o en nombre de otras instituciones financieras; > 20.000 tarjetas destacadas |

Comentarios:

3. Tecnologías emergentes para pagos (por ejemplo, billeteras digitales, billeteras móviles).

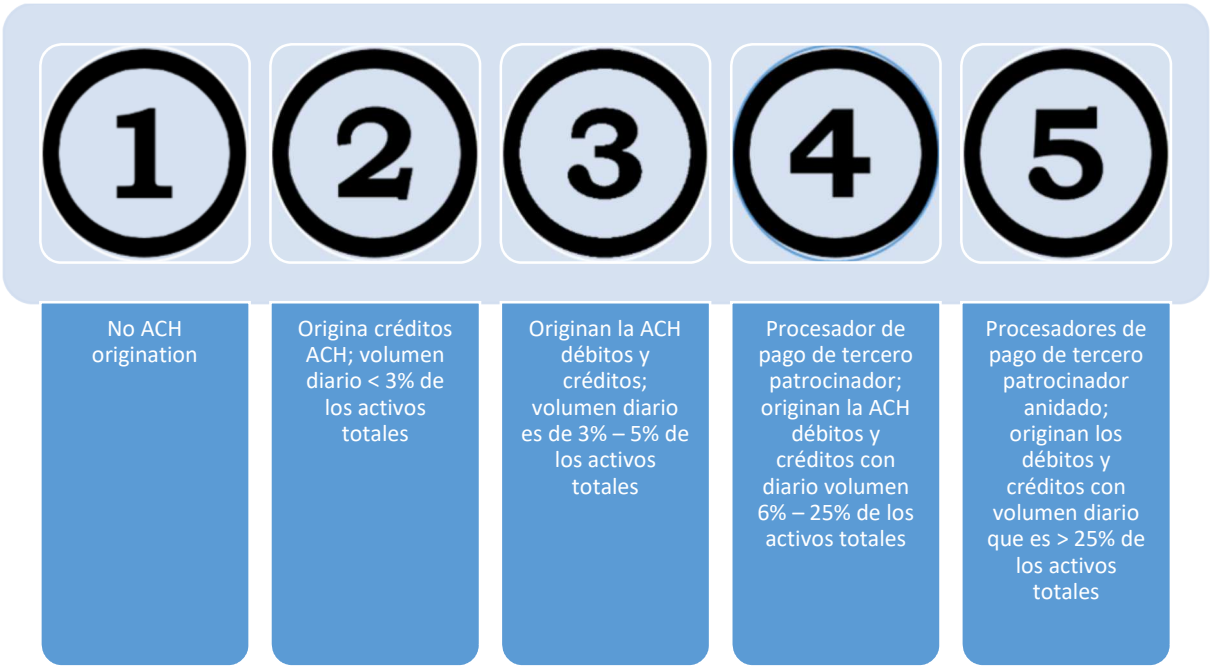

Comentarios:

4. Pagos de persona a persona (P2P).


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Servicio no ofresido | Clientes permitidos originar pagos; utilizado por < 1.000 clientes o volumen de transacción mensual es < 50.000 | Clientes permitidos originar pagos; utilizado por los clientes o transacciones mensuales 1.000 – 5.000 volumen es entre 50.000-100.000 | Clientes permitidos originar pagos; utilizado por los clientes o transacciones mensuales 5.001 – 10.000 volumen es entre 100001 millones | Clientes que permite solicitar el pago u originan pago; utilizado por > 10.000 clientes o volumen de transacción mensual > 1 millón |

Comentarios:

5. Originan pagos ACH compensados, transacciones financieras mediante una red electrónica.




Comentarios:

6. Originario los pagos por mayor (por ejemplo, fichas).


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No originan pagos venta por mayor | Diariamente originó volumen de venta por mayor pago < 3% de los activos totales | Diariamente originó de volumen de venta por mayor pago 3% – 5% de los activos totales | Diariamente originó de volumen de venta por mayor pago 6% – 25% de los activos totales | Diariamente originó volumen de pago por mayor > 25% de los activos totales |

Comentarios:

7. Transferencias bancarias.


Comentarios:

8. Captura de depósito remoto del comerciante (RDC).


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No ofrecido | < 100 clientes mercantiles; volumen diario de transacciones es < 3% de los activos totales | 100 – 500 clientes mercantiles; volumen diario de operaciones es 3% – 5% de los activos totales | 501-1.000 clientes mercantiles; volumen diario de transacciones es 6% – 25% de los activos totales | > 1.000 clientes mercantiles; volumen diario de transacciones es > 25% de los activos totales |

Comentarios:

9. Remesas al exterior.


Comentarios:

10. Clientes y servicios de tesorería.


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No hay servicios de gestión de tesorería se ofrecen | Servicios limitados; número de clientes es < 1.000 | Los servicios ofrecidos incluyen caja de seguridad, originación ACH y captura remota de depósitos; número de clientes es entre 1.000 – 10.000 | Los servicios ofrecidos incluyen cuentas por cobrar soluciones y gestión de la liquidez; número de clientes es entre 10.001-20.00 | Múltiples servicios incluyendo servicios de divisas, invertir en línea y las cuentas de inversión; número de clientes es de > 20.000 |

Comentarios:

11. Servicios de confianza.


| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| No se ofrecen servicios de confianza | Se ofrecen servicios de confianza a través de un proveedor de terceros; activos bajo gestión total < $ 500 millones | Confianza servicios prestados directamente; cartera de activos bajo gestión total $ 500 millones – $ 999 millones | Confianza servicios prestados directamente; total de activos bajo gestión 1 billón | Confianza servicios prestados directamente; activos bajo gestión total >$ 10 billones |

Comentarios:

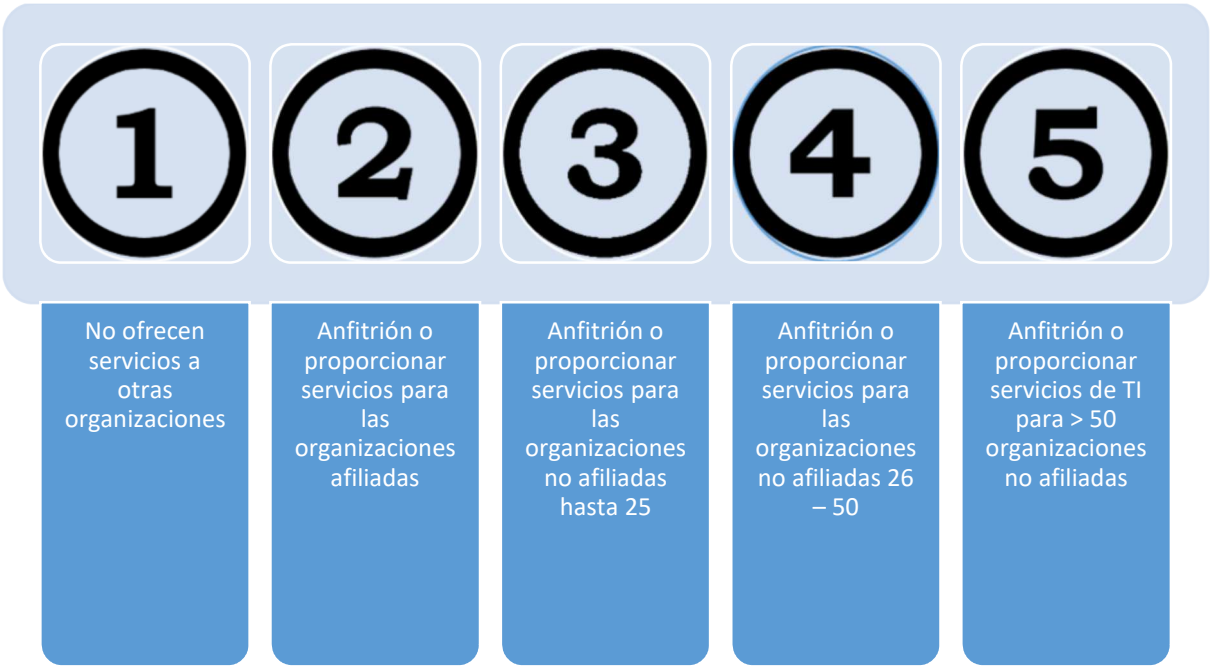
12. Actuar como un banco corresponsal (transferencias Interbancarias).


Comentarios:

13. Empresa adquirente mercantil (comerciantes de patrocinador o actividad de procesador de tarjeta en el sistema de pago).


Comentarios:

14. Es anfitrión de servicios de otras organizaciones (a través de sistemas de unión o apoyo administrativo).




Comentarios:

### 5.2.4. Categoría: Organizacional Características

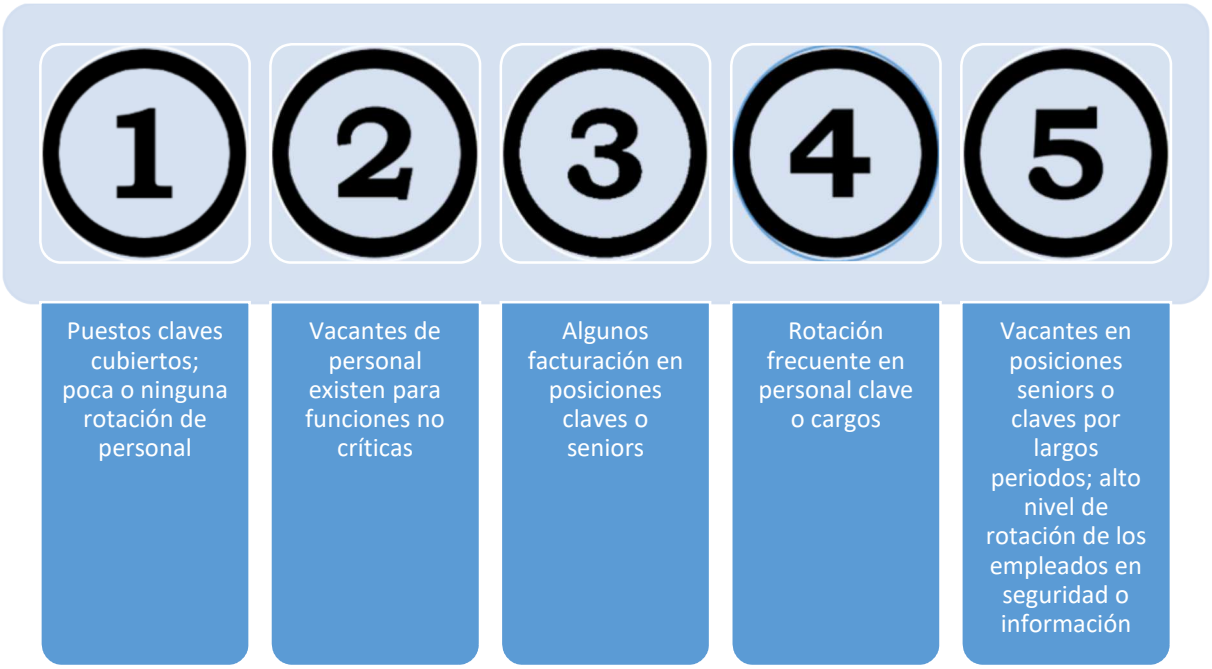
1. Fusiones y adquisiciones (incluyendo desinversiones e inversiones conjuntas).


Comentarios:

2. Empleados (incluyendo contratistas de tecnología y seguridad cibernética de información).


Comentarios:

3. Cambios en el personal de seguridad de información.

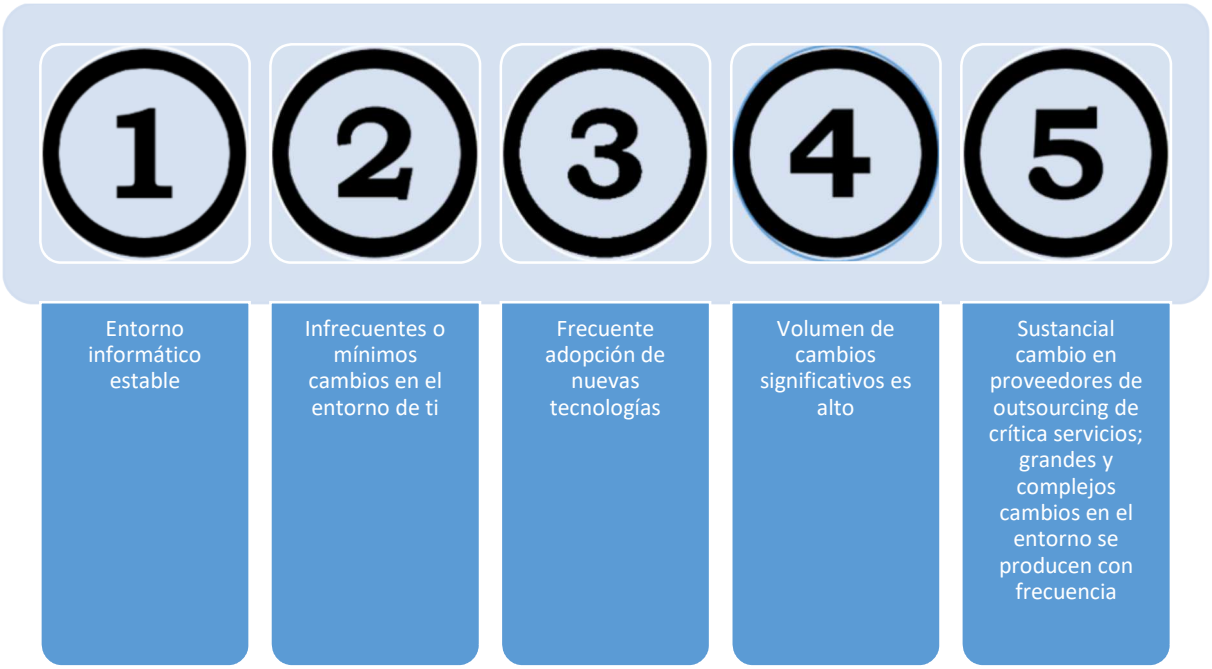



Comentarios:

4. Acceso privilegiado (administradores-red, base de datos, aplicaciones, sistemas, etc.).

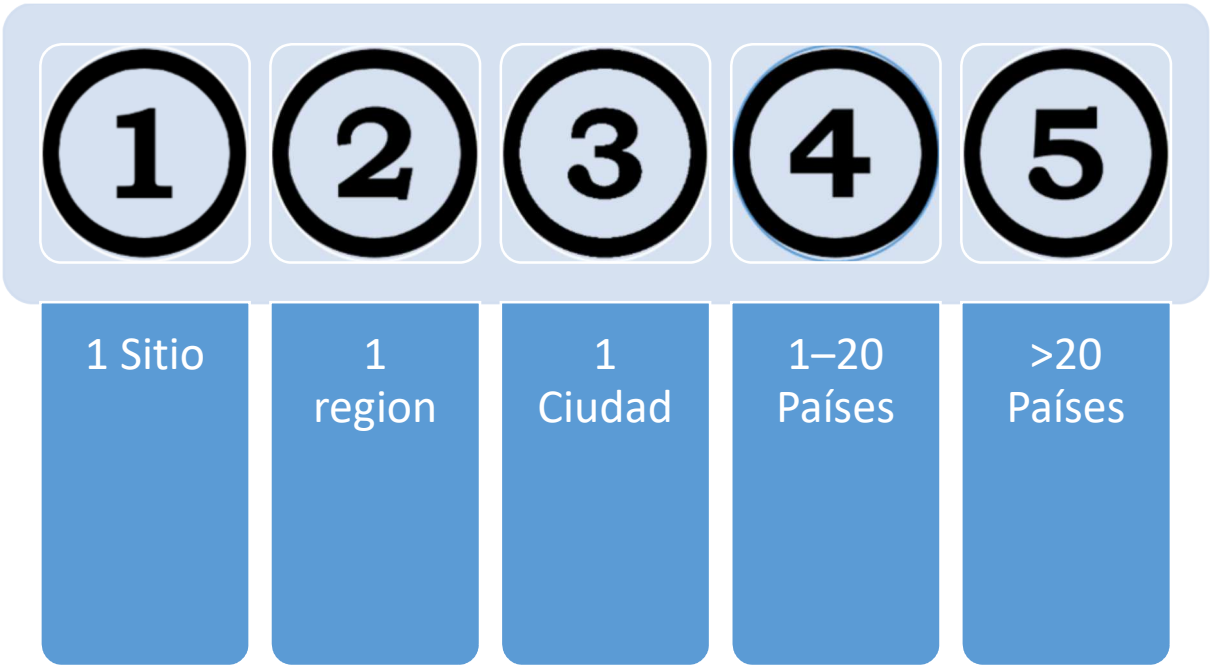

Comentarios:

5. Cambios en el entorno de TI (red, infraestructura, aplicaciones críticas, tecnologías de apoyo a los nuevos productos o servicios).



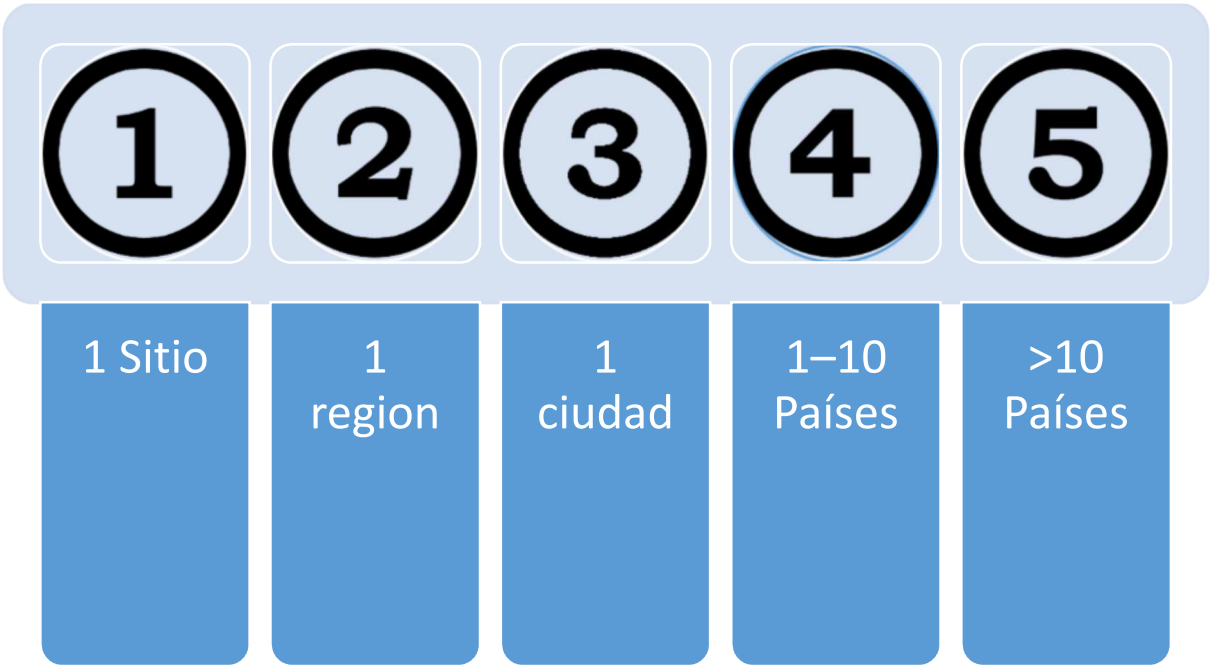

Comentarios:

6. Lugares de presencia de sucursales y negocio.




Comentarios:

7. Ubicaciones de centros de datos de operaciones.




Comentarios:

### 5.2.5. Categoría: Amenazas Externas

1. Intento de ataques cibernéticos.


Comentarios:

# Capítulo 6. Guía de Evaluación

## 6.1. Herramienta de Riesgo Inherente

La forma recomendada para la medición es tabular por atributo, actividad, servicio o producto y luego el grado de riesgo inherente, desde no presente hasta el máximo riesgo. Se categoriza y asigna un valor de 1 al menor y 5 al riesgo inherente máximo.

Lo que se busca con esta tabla es que se pueda parametrizar el riesgo inherente, por ejemplo, completamos los valores enmarcados, obtendríamos algo como esto:

| **Categoría: Tecnologías y tipos de conexión** | **Mínimo** | **2.43** | **34** | **Menor** *1* | **Mínimo** *2* | **Moderado** *3* | **Significativo** *4* | **Máximo** *5* |
|---|---|---|---|---|---|---|---|---|
| Número total de conexiones a Internet servicio proveedor (ISP) (incluyendo conexiones de rama) | | **Menor** | **1** | **Ninguna** | Complejidad mínima (1-20 conexiones) | Complejidad moderada (21 – 100 conexiones) | Complejidad significativa (101 – 200 conexiones) | Complejidad considerable (> 200 conexiones) |
| Conexiones externas, el número de conexiones no usuarios (por ejemplo, archivo transferencia protocolo (FTP), Telnet, rlogin) | | **Moderado** | **3** | Ninguna | Pocos casos de conexiones sin garantía (1-5) | **Varios casos de conexiones no garantizados (6 – 10)** | Hasta importantes de conexiones pecado garantía (11 – 25) | Hasta importantes de conexiones pecado garantía (> 25) |
| Acceso a red Wireless | | **Significativo** | **4** | No Wireless Access | Puntos de acceso separados para huéspedes Wireless y corporativa inalámbrica | Huésped y acceso a la red inalámbrica corporativa lógicamente están separados; número limitado de usuarios y puntos de acceso (1 a 250 usuarios, puntos de acceso de 1 – 25) | **Acceso a la red inalámbrica de la empresa; número significativo de usuarios y puntos de acceso (251 – 1.000 usuarios; 26 – 100 puntos de acceso)** | Acceso a la red inalámbrica de la empresa; todos los empleados tienen acceso; número considerable de puntos de acceso (> 1.000 usuarios; > 100 puntos de acceso) |

Ilustración 4. Ejemplo de Parametrización del Riesgo Inherente

Después de esto, mediante la aplicación de una fórmula, se producen la mayor cantidad de elementos asociados al tipo de riesgo, con esto categoriza de forma más representativa en cada perfil de riesgo.

Seguidamente, se presentan los resultados en un cuadro, de la siguiente forma:

| Perfil de riesgo inherente (por categoría) | Nivel de Riesgo Inherente | Promedio de Risgo | Resultado del riesgo | # de preguntas |
|---|---|---|---|---|
| *1. Tecnologías y tipos de conexión* | *Minimo* | 2.43 | *34* | 14 |
| *2. Canales de entrega* | *Moderate* | *3.33* | 10 | 3 |
| *3. Móvil online productos y servicios de tecnología* | *Mínimo* | *1.64* | 23 | 14 |
| *4. Caracteristicas Organizacionales* | *Mínimo* | *1.57* | 11 | 7 |
| *5. Amenazas externas* | *Mínimo* | *2.00* | 2 | 1 |
| ***Compuesto - resultados riesgo inherente*** | *Mínimo* | ***2.05*** | 80 | 39 |

Ilustración 5. Ejemplo de Resultado de Análisis del Riesgo Inherente

Debido a la visibilidad por categoría se tiene un nivel más representativo demostrado y un resultado del riesgo, según la cantidad de enunciados que se analicen, se determinarán los casos en los que todavía faltan aspectos por completar, se define el riesgo inherente como incompleto, o bien, los canales de entrega deben fortalecer los controles o asumir los riesgos inherentes de primera instancia por tener un promedio de riesgo alto o muy alto.

El FFIEC proporciona un cuadro general que muestra la intersección entre el nivel de riesgo inherente obtenido con este perfil de riesgo y los niveles de madurez de seguridad cibernética. Al completar el perfil de riesgo inherente, los resultados podrían indicar *Moderada*, por lo que la institución debe esforzarse por tener una madurez de ciberseguridad *Evolucionando*, *Intermedia* o *Avanzada*.

La ficha de resultados inherentes de riesgo calcula cuál es el nivel de madurez ciberseguridad.

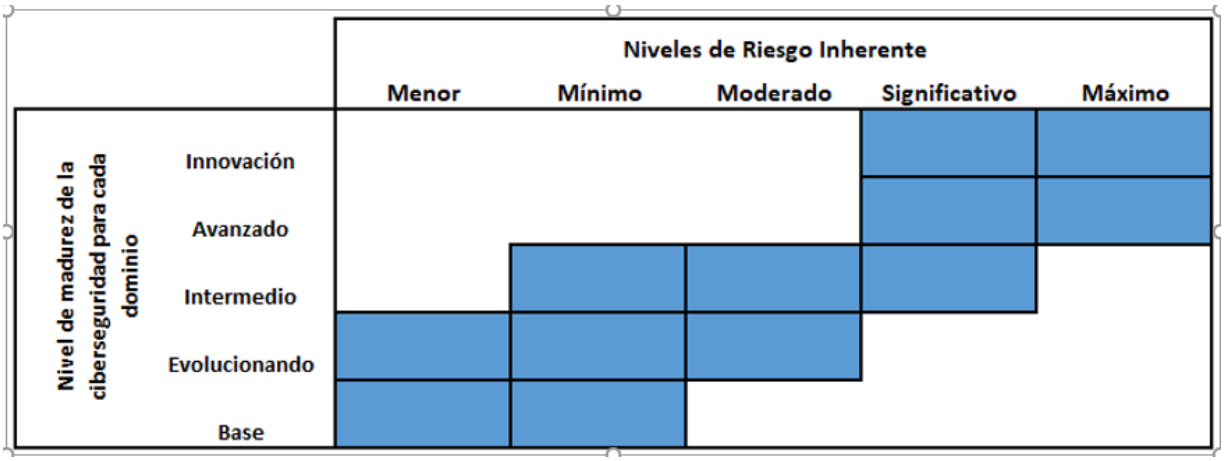



Ilustración 6. Niveles de Riesgo Inherente, Obligatorio por Niveles de Dominio

Otra manera de representarlo es con relación con cada nivel de riesgo por categoría, una representación clara de forma gráfica resumida del perfil de riesgo inherente.

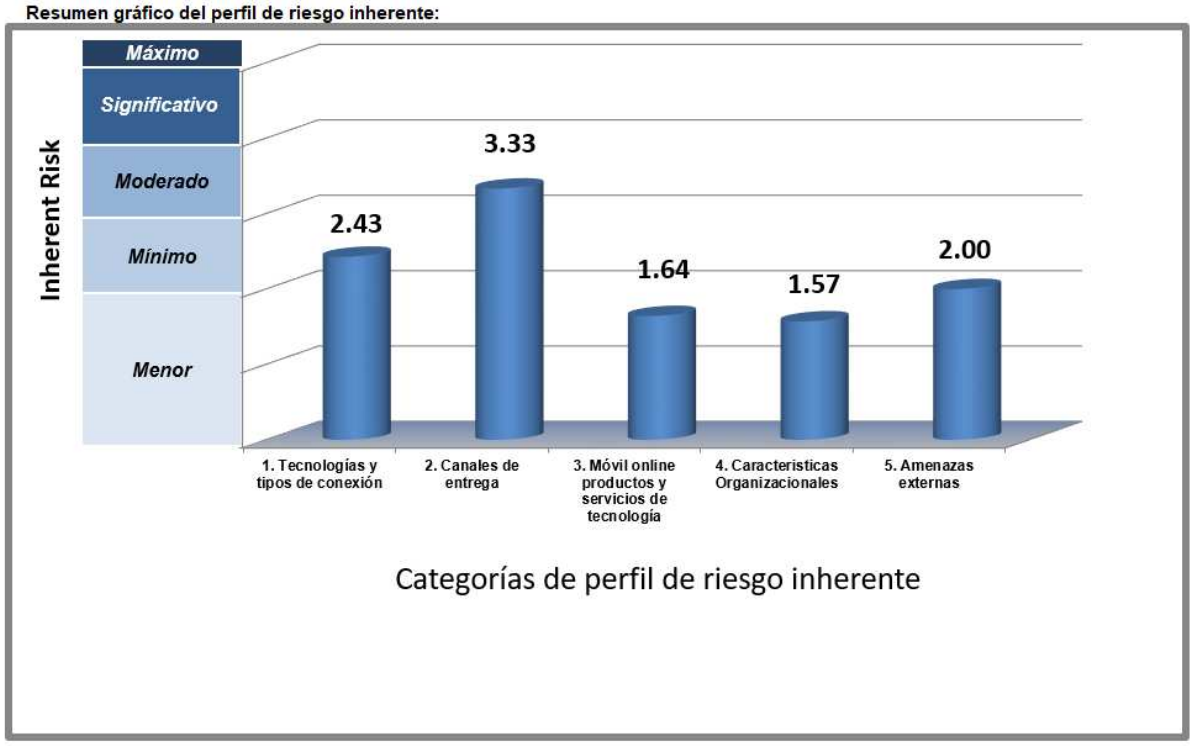



Ilustración 7. Ejemplo de Grafico del Perfil de Riesgo Inherente

# Capítulo 7. Conclusiones y Recomendaciones

## 7.1. Conclusiones

- Los marcos de referencias son tan importantes en las organizaciones que a lo largo del tiempo se han preocupado por darles visibilidad, además, han desarrollado varios tipos de herramientas de comparación con otras normas, de recopilación de información, de pasos, etc. Los organismos responsables de las normativas son serios y se han propuesto no dejar nada al azar o interpretación, como con la herramienta de FFIEC, una herramienta flexible que puede llegar a dar los insumos necesarios para tener éxito en la aplicación de una norma como la NIST.
- Se requieren de varios componentes para completar un análisis de ciberseguridad con un marco de referencias, como NIST en este caso, herramientas, colaboración de la Gerencia, recursos para el analista, conocimientos de negocio, noción de vulnerabilidades y del riesgo; es necesario visibilizar todos estos componentes en el momento de realizar el análisis.
- Las aplicaciones de marcos de ciberseguridad hacen que la organización sea más fuerte y tenga menor exposición al riesgo, por ende, a pérdidas, ya sea por brechas de ciberseguridad o por ataques de informáticos de cualquier tipo.
- Se confirmó que la aplicación de este modelo recorre de forma holística la organización y da profundidad al análisis de ciberseguridad.

## 7.2. Recomendaciones para Implementación

- Consideramos importante analizar otros marcos de referencia en ciberseguridad, ya que la suma de varios análisis enriquece el producto, esto se refleja en el músculo de prevención de la ciberseguridad de cualquier organización.

- Recomendamos aplicar las herramientas antes de la aplicación de NIST, los entes, como el FFIEC, las crearon porque consideran importantes los detalles, para aplicar una norma eficientemente, es necesario que estos se conozcan. Herramientas como la desarrollada en esta investigación de riesgo y madurez, o bien, las que menciona NIST y otros estándares, aportan y sustentan la implementación de la norma.

### 7.3. Reflexiones Finales

- El análisis de varios marcos de referencia en ciberseguridad enriquece el producto del análisis, esto se crea un músculo para la prevención, debido al impacto positivo de la aplicación de la ciberseguridad en cualquier organización.
- Los marcos de referencia o normativas vigentes no pueden ser herramientas rígidas o poco flexibles, deben tener en sus principios la capacidad de cambiar constantemente, por ejemplo, deben contemplar la creación de tecnologías nuevas o con la priorización de entes como el Gobierno Corporativo. Estos son términos que hace algunos años no formaban parte de las normas, en el futuro cercano posiblemente veremos la importancia de otros componentes.
- Consideramos que la aplicación de estas normas permite mejorar la ciberseguridad. En el mercado existen múltiples formas de atender la ciberseguridad, algunas no son tan conocidas como COBIT, ITIL o las ISO, pero todas las normativas aportan a la ciberseguridad y la interrelación de cada una enriquece cualquier proceso de análisis

### 7.4. Trabajos Futuros

- Completar el proceso de la NIST es un reto, requiere mucho tiempo de análisis y evaluación, pero contar con estos recursos enriquece a cualquier organización y aporta seguridad, esto se reflejará en la ciberseguridad, además, su ausencia se podrá ver en los estados

financieros de la organización.

### 7.4.1. Herramienta de Medición de Madurez de Riesgo

- El segundo paso para lograr una evaluación efectiva mediante la NIST, es completar la herramienta de un análisis de madurez de la ciberseguridad, esta se divide en cinco dominios (anexo 3).

  1. Gestión y supervisión del riesgo cibernético.
     - Gobernanza.
     - Gestión de riesgos.
     - Recursos.
     - Entrenamiento y cultura.
  2. Inteligencia de amenazas y colaboración.
     - Inteligencia de amenazas.
     - Monitoreo y análisis.
     - Intercambio de información.
  3. Controles de ciberseguridad.
     - Preventivos.
     - Detectives.
     - Correctivos.
  4. Gestión de la dependencia externa.
     - Conexiones.
     - Gestión de relaciones.
  5. Gestión de incidentes cibernéticos y resiliencia.
     - Planificación y estrategia de Resiliencia de Incidentes.

- Detección, respuesta y mitigación.
- Escalado y presentación de informes.

La herramienta provee un apéndice o base en la que se puede apoyar para determinar un resultado, incluso tiene la capacidad de evaluar que, aunque no se controle la tarea, existe una compensación de control para no afectar el resultado final, ya que mitiga el riesgo de otra forma y es válido. Todo este análisis tiene como producto final una tabla (anexo 3) en la que aparecen:

- Los dominios.
- El factor de madurez de los dominios.
- El factor de evaluación.
- El dominio del factor de evaluación.
- El componente.
- Su grado de madurez en porcentaje.
    - Básico.
    - Evolucionando.
    - Intermedio.
    - Avanzado.
    - Innovador.

Los resultados del análisis de riesgo se determinan con los intereses aptitudes de la organización, la herramienta tiene la capacidad de mostrar resultados por dominio, factor y el nivel de riesgo deseado (anexo 4).

## Capítulo 8. Referencias


CISCO. (2018). Reporte anual de ciberseguridad 2018. Recuperado de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

Deloitte. (2018). Diagnóstico de madurez | Deloitte México. Recuperado de https://www2.deloitte.com/mx/es/pages/audit/articles/madurez-procesos-financieros.html

FFIEC. (2018). Federal Financial Institutions Examination Council's. Recuperado de https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

FFIEC. (2018). Perfil de riesgo inherente. Recuperado de https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Inherent_Risk_Profile.pdf

NIST. (2018). Cybersecurity framework. Recuperado de https://www.nist.gov/cyberframework

NIST. (2018). Framework for improving critical infrastructure cybersecurity. Recuperado de https://translate.googleusercontent.com/translate_c?depth=1&hl=es&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.nist.gov/sites/default/files/*framework*-for-improving-critical-infrastructure-cybersecurity-core.xlsx&xid=17259,15700019,15700124,15700149,15700168,15700173,15700186,15700191,15700201,15700205&usg=ALkJrhhr8ZzSRqjh_r3K0mHMvLvzGNAvvA

NIST. (2018). National Institute of Standards and Technology. Recuperado de https://www.nist.gov/sites/default/files/documents/2018/11/07/frameworkesmellrev_20181102mn_clean.pdf

The White House President Barack Obama. (2018). Orden ejecutiva - Mejora de la infraestructura de ciberseguridad crítica. Recuperado de https://translate.googleusercontent.com/translate_c?depth=1&hl=es&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity&xid=17259,15700019,15700124,15700149,15700168,15700173,15700186,15700191,15700201,15700205&usg=ALkJrhhWshs0kM4Urrh9oIMyBOepdTg_7A

## Capítulo 9. Glosario

- ACH

*Automated Clearing House*, terminología usada para transacciones financieras mediante una red electrónica.

- ATM

*Automated Teller Machine*, es un equipo informático conectado electrónicamente a un banco.

- Ciberataque

Se refiere a la acción ofensiva de un individuo, grupo a un sistema informático con un fin no autorizado.

- Cloud computing

Es un término aplicado a servicios brindados por una empresa, ya sea por *hardware* o *software*, en lugares remotos accedidos mediante Internet.

- Conexiones dedicadas.

Es la forma de comunicación entre dos sitios de forma que se reserva un espacio o ancho de banda para la comunicación entre por lo menos dos sitios.

- DDOS

Es una forma de ataque que busca la denegación de por lo menos un servicio, mediante diferentes técnicas.

- EOL

Se refiere a proceso de vida del *hardware* cuando, por ejemplo, cuando un fabricante anuncia que no dará soporte para cierto *hardware*, se dice que inicia su EOL, es una indicación de que el *hardware* debe remplazarse.

- Firewalls

Es un *software* que permite proteger un equipo informático.

- FTP

Es el protocolo de transferencia de archivo.

- ITGI

Significa instituto para la gobernanza de IT.

- Módem

Es un dispositivo o *hardware* que permite cambiar señales digitales en analógicas o viceversa, para ser transmitidas a través de líneas de teléfono, cables coaxiales, fibras ópticas y microondas, conectado a una computadora, permite la comunicación con otra computadora.

- OSS

*Open source software*, es decir, todos los programas creados libremente para modificarse y utilizados por otras personas,

- rlogin

Aplicación que permite la administración de equipos de forma remota a un equipo anfitrión u *host*.

- Routers

Equipos de comunicación cuya función es enrutar los paquetes a través de las redes de datos.

- Telnet

Protocolo que permite gestión de equipos de forma remota, ha evolucionado a otros protocolos más seguros como SSH Secure Shell, usa la arquitectura cliente-servidor también.

# Capítulo 10. Anexos

## 10.1. Anexo 1. FSSCC_ACAT_V2.1_SPA

- Tecnologías y tipos de conexión.

| Categoría: Tecnologías y tipos de conexión | Minimo | 1.86 | 26 | Menor 1 | Minimo 2 | Moderado 3 | Significativo 4 | Máximo 5 |
|---|---|---|---|---|---|---|---|---|
| Número total de conexiones a Internet servicio proveedor (ISP) (incluyendo conexiones de rama) | | Menor | 1 | None | Complejidad mínima (1-20 conexiones) | Complejidad moderada (21 – 100 conexiones) | Complejidad significativa (101 – 200 conexiones) | Complejidad considerable (> 200 conexiones) |
| Conexiones externas, el número de conexiones no usuarios (por ejemplo, archivo transferencia protocolo (FTP), Telnet, rlogin) | | Significativo | 4 | None | Pocos casos de conexiones sin garantía (1-5) | Varios casos de conexiones no garantizados (6 – 10) | **Hasta importantes de conexiones pecado garantía (11 – 25)** | Hasta importantes de conexiones pecado garantía (> 25) |
| Acceso a red Wireless | | Maximo | 5 | No wireless access | Puntos de acceso separados para huéspedes wireless y corporativa inalámbrica | Huésped y acceso a la red inalámbrica corporativa lógicamente están separados; número limitado de usuarios y puntos de acceso (1 a 250 usuarios, puntos de acceso de 1 – 25) | Acceso a la red inalámbrica de la empresa; número significativo de usuarios y puntos de acceso (251 – 1.000 usuarios; 26 – 100 puntos de acceso) | **Acceso a la red inalámbrica de la empresa; todos los empleados tienen acceso; número considerable de puntos de acceso (> 1.000 usuarios; > 100 puntos de acceso)** |
| Dispositivos personales peden conectarse a la red corporativa | | Menor | 1 | None | Tipo de dispositivo sólo uno disponible; a < 5% de los empleados (personal, ejecutivos, gerentes); acceso a correo electrónico únicamente | Múltiples tipos de dispositivos utilizados; a < 10% de los empleados (personal, ejecutivos, gerentes) y tablero; acceso a correo electrónico únicamente | Múltiples tipos de dispositivos utilizados; a < 25% de los empleados autorizados (personal, ejecutivos, gerentes) y tablero; correo electrónico y aplicaciones acceder a | Cualquier tipo de dispositivo utilizado; a > 25% de los empleados (personal, ejecutivos, gerentes) y tablero; todas las aplicaciones de acceso |
| Terceras partes, incluyendo el número de organizaciones y de individuos de proveedores y subcontratistas, con acceso a sistemas internos (por ejemplo, red privada virtual, módem, intranet, conexión directa) | | Moderado | 3 | No hay terceras personas y no individuos de terceros con acceso a los sistemas | Limitado número de terceros (1 – 5) y el número limitado de personas por parte de terceros (< 50) con acceso; baja complejidad en cómo acceden a los sistemas | **Número moderado de terceros (6 – 10) y moderado número de individuos por parte de terceros (50 – 500) con acceso; cierta complejidad en cómo acceden a los sistemas** | Número significativo de terceros (11 – 25) y gran número de individuos por parte de terceros (501 – 1.500) con acceso; alto nivel de complejidad en cuanto a cómo acceder a los sistemas | Gran número de terceros (> 25) y considerable número de individuos por parte de terceros (> 1.500) con acceso; alta complejidad en cómo acceden a los sistemas |
| Clientes mayoristas con conexiones dedicadas | | Significativo | 4 | Ninguna | Pocas conexiones dedicadas (entre 1 – 5) | Varias conexiones dedicadas (entre 6-10) | **Número importante de conexiones dedicadas (entre 11-25)** | Número importante de conexiones dedicadas (> 25) |
| Aplicaciones de proveedor interno alojado y desarrollado o modificado, apoyando actividades críticas | | Minimo | 2 | No hay aplicación | **Algunas aplicaciones (entre 1 – 5)** | Varias aplicaciones (entre 6-10) | Número significativo de aplicaciones (entre 11-25) | Número considerable de aplicaciones y la complejidad (> 25) |
| Internamente organizado, desarrollado por el proveedor de aplicaciones apoyando actividades críticas | | Moderado | 3 | Aplicaciones limitadas (0 – 5) | Algunas aplicaciones (6-30) | **Varias aplicaciones (31 – 75)** | Número significativo de aplicaciones (76-200) | Número considerable de aplicaciones y la complejidad (> 200) |
| Tecnologías desarrolladas por el usuario y usuario de computación que soportan actividades críticas (incluye hojas de cálculo Microsoft Excel y bases de datos Access u otras herramientas desarrolladas por el usuario) | | Menor | 1 | **No hay tecnologías desarrolladas por el usuario** | 1–100 tecnologías | 101–500 tecnologías | 501–2,500 tecnologías | >2,500 tecnologías |

- Tecnologías y tipos de conexión.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Sistemas de final de la vida (EOL) | **Minimo** | **2** | Ningún sistema (hardware o software) que está más allá de EOL o en riesgo de a punto de EOL dentro de 2 años | **Algunos sistemas que están en riesgo de EOL y ninguno que soportan operaciones críticas** | Varios sistemas que alcanzará EOL dentro de 2 años y algunos que soportan operaciones críticas | Un gran número de sistemas que apoyan las operaciones críticas en EOL o corren el riesgo de alcanzar EOL en 2 años | Mayoría de las operaciones críticas dependen de los sistemas que han alcanzado EOL o llegarán en los próximos dos años o un número indeterminado de sistemas que han alcanzado EOL |
| Software de código abierto (OSS) | **Least** | **0** | No OSS | OSS limitado y ningunos que soportan operaciones críticas | Varios OSS que soportan operaciones críticas | Gran número de sistemas operativos que soportan operaciones críticas | Mayoría de las operaciones depende de OSS |
| Dispositivos de red (por ejemplo, servidores, routers y firewalls; son físicos y virtuales) | **Minimal** | **0** | Limitada o no dispositivos de red (< 250) | **Algunos dispositivos (250-1.500)** | Varios dispositivos (1.501 – 25.000) | Gran número de dispositivos (25.001-50.000) | Número considerable de dispositivos (> 50.000) |
| Proveedores de servicios de terceros almacenamiento o procesamiento de información que apoyan actividades críticas (no tienen acceso a sistemas internos, pero la institución se basa en sus servicios) | **Minimal** | **0** | No hay terceras personas que apoyan actividades críticas | **1-25 terceros que admiten actividades críticas** | 26-100 terceras personas que apoyan actividades críticas | 101-200 terceros que admiten actividades críticas; 1 o más son extranjeros | > 200 terceras personas que apoyan actividades críticas; 1 o más son basados en extranjeros |
| Cloud computing servicios alojados externamente para apoyar actividades críticas | **Minimal** | **0** | No hay proveedores de nube | **Pocos proveedores de nube; nube privada (1-3)** | Varios proveedores de nube (4 – 7) | Número significativo de proveedores cloud (8 – 10); proveedor de la nube localizaciones utilizado incluye internacional; uso de nube | Número importante de los proveedores de cloud (> 10); proveedor de la nube localizaciones utilizado incluye internacional; uso de nube |

- Canales de entrega.

| Categoría: Canales de entrega | Moderate | 3.33 | 10 | Menor 1 | Mínimo 2 | Moderado 3 | Significativo 4 | Máximo 5 |
|---|---|---|---|---|---|---|---|---|
| Online presencia (customer) | | **Moderado** | **0** | No aplicaciones Web o presencia en los medios sociales | Sirve como un sitio Web informativo o página de redes sociales (por ejemplo, proporciona sucursales y cajeros y materiales de marketing) | **Sirve como un canal de entrega para la banca en línea; puede comunicar a los clientes a través de los medios de comunicación social** | Sirve como un canal de entrega para clientes mayoristas; puede incluir creación de cuenta de venta por menor | Aplicaciones de Internet sirven como un canal para los clientes mayoristas para administrar activos de gran valor |
| Mobile presencia | | **Máximo** | **5** | Ninguna | Alertas de texto SMS o notificaciones acceso basado en navegador | Aplicación de banca móvil para los clientes minoristas (por ejemplo, pago, móvil "comprueba la captura, traslados internos solamente)" | Aplicación de banca móvil incluye a traslados externos (por ejemplo, para "clientes corporativos, transacciones externas recurrentes)" | **Completa funcionalidad, incluyendo originando nuevas transacciones (por ejemplo, ACH, alambre)** |
| Cajeros automáticos (ATM) (operación) | | **Máximo** | **5** | No ATM Servicios | Servicios de ATM pero sin máquinas con propiedad | Servicios de ATM "a cargo de un tercero; Cajeros automáticos en el local" y sucursales regionales; efectivo "cargar servicios tercerizados" | Servicios de ATM "gestionados internamente; Cajeros automáticos en sucursales y puntos de venta; efectivo "cargar servicios tercerizados" | **ATM servicios gestionados "internamente; ATM servicios proporcionados a otros" de las instituciones financieras; Cajeros automáticos en doméstico y "ramas internacionales y puntos de venta;" "efectivo recarga servicios gestionados internamente"** |

- Móviles en línea productos y servicios de tecnología.

| Categoria: Tecnologías y tipos de conexión | Minimo | 2.43 | 34 | Menor 1 | Mínimo 2 | Moderado 3 | Significativo 4 | Máximo 5 |
|---|---|---|---|---|---|---|---|---|
| Tarjetas de crédito o débito de tema | | **Menor** | 1 | **No emiten tarjetas de crédito o débito** | Débito de tema o tarjetas de crédito a través de una tercera parte; < 10.000 tarjetas destacadas | Tema débito o tarjetas de crédito a través de una tercera parte; entre 10.000 – 50.000 tarjetas destacadas | Emitir tarjetas de crédito o débito directamente; entre 50.000 – 100.000 tarjetas destacadas | Emitir tarjetas de crédito o débito directamente; > 100.000 tarjetas pendientes; tarjetas de emisión en nombre de otras instituciones financieras |
| tarjetas prepagas | | **Menor** | 1 | **No emiten tarjetas de prepago** | Emitir tarjetas prepagadas a través de un tercero; < 5.000 tarjetas destacadas | Emitir tarjetas prepagadas a través de un tercero; 5.000 – 10.000 tarjetas destacadas | Emitir tarjetas prepagadas a través de un tercero; 10.001-20.000 tarjetas destacadas | Emitir tarjetas prepagadas internamente, a través de un tercero, o en nombre de otras instituciones financieras; > 20.000 tarjetas destacadas |
| Tecnologías emergentes de los pagos (por ejemplo, digitales billeteras, billeteras móviles) | | **Mínimo** | 2 | No aceptar o utilizar tecnologías emergentes de los pagos | **Aceptación indirecta o el uso de nuevas tecnologías de pagos (el uso del cliente puede afectar el depósito o cuenta de crédito)** | Aceptación directa o el uso de nuevas tecnologías de pagos; pareja o co-brand con proveedores no bancarias; volumen de transacciones limitado | Aceptación directa o el uso de nuevas tecnologías de pagos; volumen de transacciones pequeñas; no hay pagos extranjeros | Aceptación directa de las nuevas tecnologías de pagos; volumen moderado de transacciones o pagos extranjeros |
| Pagos de persona a persona (P2P) | | **Menor** | 1 | **No ofrecido** | Clientes permitidos originar pagos; utilizado por < 1.000 clientes o volumen de transacción mensual es < 50.000 | Clientes permitidos originar pagos; utilizado por los clientes o transacciones mensuales 1.000 – 5.000 volumen es entre 50.000- | Clientes permitidos originar pagos; utilizado por los clientes o transacciones mensuales 5.001 – 10.000 volumen es entre 100001 | Clientes que permite solicitar el pago u originan pago; utilizado por > 10.000 clientes o volumen de transacción mensual > 1 millón |
| Origen de ACH pagos | | **Moderado** | 3 | No se originan pagos ACH | Origina créditos ACH; volumen diario < 3% de los activos totales | **Originan la ACH débitos y créditos; volumen diario es de 3% – 5% de los activos totales** | Procesador de pago de tercero patrocinador; originan la ACH débitos y créditos con diario volumen 6% – 25% de los activos totales | Procesadores de pago de tercero patrocinador anidado; originan los débitos y créditos con volumen diario que es > 25% de los activos totales |
| Originario los pagos por mayor (por ejemplo, fichas) | | **Mínimo** | 2 | No originan pagos venta por mayor | **Diariamente originó volumen de venta por mayor pago < 3% de los activos totales** | Diariamente originó de volumen de venta por mayor pago 3% – 5% de los activos totales | Diariamente originó de volumen de venta por mayor pago 6% – 25% de los activos totales | Diariamente originó volumen de pago por mayor > 25% de los activos totales |
| Transferencias bancarias | | **Moderado** | 3 | No ofrecido | En las solicitudes de alambre persona solamente; cables domésticos volumen diario de alambre < 3% de los activos totales | **En persona, teléfono y faz del alambre de peticiones; diario nacional cable volumen 3% – 5% de los activos totales; volumen diario internacional del alambre < 3% de los activos totales** | Múltiples canales de petición (por ejemplo, en línea, texto, correo electrónico, fax y teléfono); volumen diario de alambre interno 6% – 25% de los activos totales; volumen diario del alambre internacional 3% – 10% de los activos totales | Múltiples canales de petición (por ejemplo, en línea, texto, correo electrónico, fax y teléfono); volumen diario de alambre interno > 25% de los activos totales; volumen del alambre internacional diario > 10% de los activos totales |

- Móviles en línea productos y servicios de tecnología.

| Categoría: Tecnologías y tipos de conexión | Mínimo | 2.43 | 34 | Menor 1 | Mínimo 2 | Moderado 3 | Significativo 4 | Máximo 5 |
|---|---|---|---|---|---|---|---|---|
| Captura de depósito remoto del comerciante (RDC) | **Menor** | 1 | **No ofrecido** | < 100 clientes mercantiles; volumen diario de transacciones es < 3% de los activos totales | 100 – 500 clientes mercantiles; volumen diario de operaciones es 3% – 5% de los activos totales | 501-1.000 clientes mercantiles; volumen diario de transacciones es 6% – 25% de los activos totales | > 1.000 clientes mercantiles; volumen diario de transacciones es > 25% de los activos totales |
| Remesas Globales | **Menor** | 1 | **Ofrecen las remesas mundiales** | Es el volumen de transacciones diario bruto < 3% de los activos totales | Volumen bruto de transacciones diarias es de 3% – 5% de los activos totales | Volumen de transacción diaria bruto es 6% – 25% de los activos totales | Volumen de transacción diaria bruto es > 25% de los activos totales |
| Clientes y servicios de tesorería | **Menor** | 1 | **No hay servicios de gestión de tesorería se ofrecen** | Servicios limitados; número de clientes es < 1.000 | Los servicios ofrecidos incluyen caja de seguridad, originación ACH y captura remota de depósitos; número de clientes es entre 1.000 – 10.000 | Los servicios ofrecidos incluyen cuentas por cobrar soluciones y gestión de la liquidez; número de clientes es entre 10.001-20.000 | Múltiples servicios incluyendo servicios de divisas, invertir en línea y las cuentas de inversión barrido; número de clientes es de > 20.000 |
| Servicios de confianza | **Menor** | 1 | **No se ofrecen servicios de confianza** | Se ofrecen servicios de confianza a través de un proveedor de terceros; activos bajo gestión total < $ 500 millones | Confianza servicios prestados directamente; cartera de activos bajo gestión total $ 500 millones – $ 999 millones | Confianza servicios prestados directamente; total de activos bajo gestión 1000000000 billones | Confianza servicios prestados directamente; activos bajo gestión total > $ 10 billones |
| Actuar como un banco corresponsal (transferencias Interbancarias) | **Mínimo** | 2 | No actúan como un banco corresponsal | **Actuar como un banco corresponsal para < 100 instituciones** | Actuar como un banco corresponsal para 100 – 250 instituciones | Actuar como un banco corresponsal para instituciones de 251 a 500 | Actuar como un banco corresponsal para > 500 instituciones |
| Empresa adquirente mercantil (comerciantes de patrocinador o actividad de procesador de tarjeta en el sistema de pago) | **Moderado** | 3 | No actúan como un comerciante adquirente | Actuar como un comerciante adquirente; < 1.000 comerciantes | **Actuar como un comerciante adquirente; subcontratar la tarjeta de pago; 1.000 – 10.000 comerciantes** | Actuar como un comerciante comprador y procesador de tarjeta de pago; comerciantes de 10.001 – 100.000 | Actuar como un comerciante comprador y procesador de tarjeta de pago; > 100.000 comerciantes |
| Es anfitrión de servicios de otras organizaciones (ya sea a través de sistemas de unión o apoyo administrativo) | **Menor** | 1 | **No ofrecen servicios a otras organizaciones** | Anfitrión o proporcionar servicios para las organizaciones afiliadas | Anfitrión o proporcionar servicios para las organizaciones no afiliadas hasta 25 | Anfitrión o proporcionar servicios para las organizaciones no afiliadas 26 – 50 | Anfitrión o proporcionar servicios de TI para > 50 organizaciones no afiliadas |

- Características Organizacionales

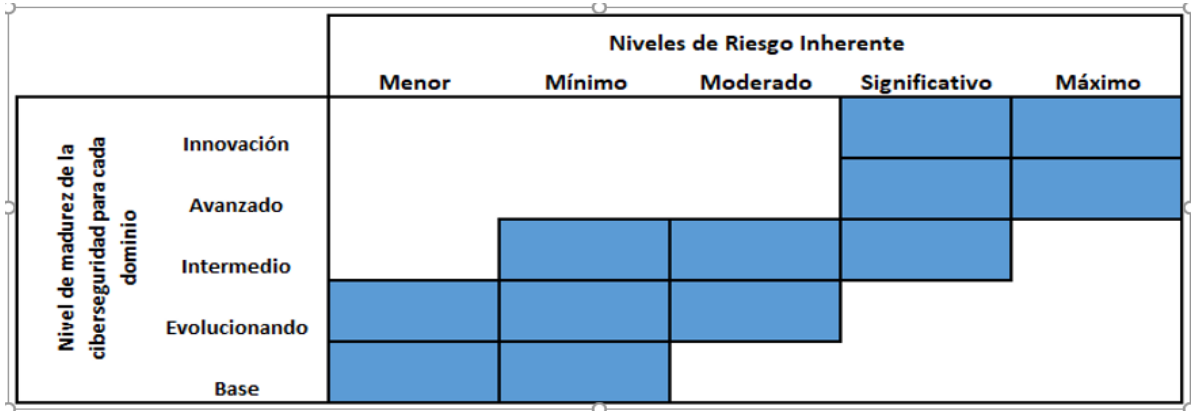
| Categoría: Características Organizationales | Mínimo | 1.57 | 11 | Menor 1 | Mínimo 2 | Moderate 3 | Significantivo 4 | Máximo 5 |
|---|---|---|---|---|---|---|---|---|
| Fusiones y adquisiciones incluyendo desinversiones e inversiones conjuntas | **Menor** | | **1** | **No hay Planeadas** | Abierto a iniciar discusiones o buscando una fusión o adquisición | En conversaciones con al menos 1 parte | Una venta o adquisición ha anunciado públicamente en el último año, en las negociaciones con 1 o más partes | Múltiples integraciones continuas de adquisiciones están en proceso de fusión |
| Directa de empleados (incluyendo contratistas de tecnología y seguridad cibernética de información) | **Menor** | | **1** | **Número del total de empleados < 50** | Número de empleados asciende a 50-2.000 | Número de empleados asciende a 2.001 – 10.000 | Número de empleados asciende a 10.001-50.000 | Número de empleados es > 50.000 |
| Cambios en él y personal de seguridad de información | **Menor** | | **1** | **Puestos claves cubiertos; poca o ninguna rotación de personal** | Vacantes de personal existen para funciones no críticas | Algunos facturación en posiciones claves o seniors | Rotación frecuente en personal clave o cargos | Vacantes en posiciones seniors o claves por largos periodos; alto nivel de rotación de los empleados en seguridad o información |
| Acceso privilegiado (administradores – red, base de datos, aplicaciones, sistemas, etcetera.) | **Mínimo** | | **2** | Número limitado de los administradores; limitada o no administradores externos | **Nivel de facturación en los administradores no afecta a las operaciones o actividades; puede utilizar algunos administradores externos** | Nivel de facturación en los administradores afecta a las operaciones; número de los administradores de aplicaciones o sistemas individuales excede lo que es necesario | Alta dependencia de los administradores externos; número de administradores no es suficiente a nivel de soporte o ritmo de cambio | Alta rotación en los administradores de red; muchos o la mayoría de los administradores son externos (contratistas o proveedores); experiencia en administración de redes es limitada |
| Cambios en el entorno de ti (p. ej., red, infraestructura, aplicaciones críticas, tecnologías de apoyo a los nuevos productos o servicios) | **Menor** | | **1** | **Entorno informático estable** | Infrecuentes o mínimos cambios en el entorno de ti | Frecuente adopción de nuevas tecnologías | Volumen de cambios significativos es alto | Sustancial cambio en proveedores de outsourcing de crítica servicios; grandes y complejos cambios en el entorno se producen con frecuencia |
| Lugares de presencia de sucursales y negocios | **Mínimo** | | **2** | 1 Sitio | **1 region** | 1 ciudad | 1–20 Países | >20 Países |
| Ubicaciones de centros de datos de operaciones | **Moderado** | | **3** | 1 Sitio | 1 region | **1 ciudad** | 1–10 Países | >10 Países |

- Amenazas externas

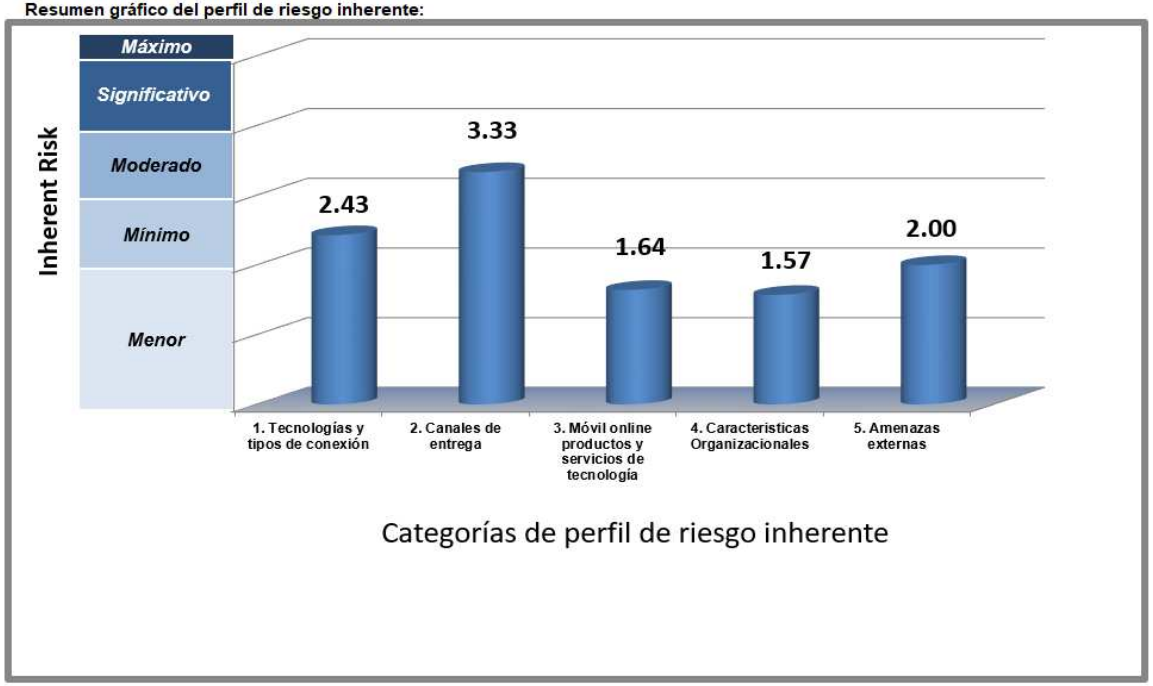
| Categoría: Amenazas externas | Mínimo | 2.00 | 2 | Menor 1 | Mínimo 2 | Moderate 3 | Significantivo 4 | Máximo 5 |
|---|---|---|---|---|---|---|---|---|
| Intentó ataques cibernéticos | | Mínimo | 2 | No como intentados o el reconocimiento | **Algunos intentos mensuales (< 100); puede haber tenido campañas de phishing genéricos recibidos por empleados y clientes** | Varios intentos mensuales (100– 500); campañas de phishing dirigida a empleados o clientes a la institución o de terceros actividades críticas; puede haber experimentado un ataque de denegación de servicio distribuida (DDoS) intento en el último año | Número significativo de intentos mensuales (501 – 100.000); lanza campañas de phishing dirigida a los grandes patrimonios de clientes y empleados de la institución o de terceros actividades críticas; Institución es nombrada específicamente en los informes de amenaza; puede haber experimentado varios ataques DDoS ha intentado en el último año | Número considerable de intentos mensuales (> 100.000); persistentes intentos de atacar los directivos o los administradores de red; con frecuencia blanco de ataques DDoS |

## 10.2. Anexo 2. Resultados del Perfil de Riesgo Inherente

| Perfil de riesgo inherente (por categoría) | Nivel de Riesgo Inherente | Promedio de Risgo | Resultado del riesgo | # de preguntas |
|---|---|---|---|---|
| *1. Tecnologías y tipos de conexión* | *Mínimo* | 2.43 | *34* | 14 |
| *2. Canales de entrega* | *Moderate* | *3.33* | 10 | 3 |
| *3. Móvil online productos y servicios de tecnología* | *Mínimo* | *1.64* | 23 | 14 |
| *4. Caracteristicas Organizacionales* | *Mínimo* | *1.57* | 11 | 7 |
| *5. Amenazas externas* | *Mínimo* | *2.00* | 2 | 1 |
| ***Compuesto - resultados riesgo inherente*** | *Mínimo* | ***2.05*** | 80 | 39 |



**Resumen gráfico del perfil de riesgo inherente:**



## 10.3. Anexo 3. Herramienta de Madurez

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.B.1 | Miembros designados de gestión rindan cuentas por la Junta Directiva o un Comité apropiado para implementar y administrar el Programas de continuidad de negocio y seguridad de información. (FFIEC seguridad folleto, página 3) | "Fuente: IS.I: pg3: La junta, o el comité designado de la junta, debe ser responsable de supervisar el desarrollo, la implementación y el mantenimiento del programa de seguridad de la información de la institución y responsabilizar a la alta gerencia por sus acciones.<br>IS.I: pg4: La junta debe proporcionar a la administración sus expectativas y requisitos, y responsabilizar a la administración por la supervisión y coordinación central, la asignación de responsabilidades y la eficacia del programa de seguridad de la información.<br>IS.WP.2.3: Determine si la junta directiva responsabiliza a la administración por lo siguiente: Supervisión y coordinación central, Asignación de responsabilidad, Apoyo del programa de seguridad de la información y Efectividad del programa de seguridad de la información.<br>MGT.III.C.3: pg28: La junta directiva es responsable de supervisar el desarrollo, la implementación, la administración y el mantenimiento del programa de seguridad de la información de la institución. Esta supervisión incluye la asignación de responsabilidades y responsabilidades específicas para la implementación del programa y la revisión de los informes de la gerencia.<br>MGT.WP.2: Determine si la junta directiva supervisa y la alta gerencia establece adecuadamente una estructura de gobierno efectiva que incluye la supervisión de las actividades de TI.<br>MGT.WP.2.2.g: revise si la junta o un comité de la junta responsabiliza adecuadamente a la administración por la identificación, medición y mitigación de los riesgos de TI " | JDM GV-4: Gobernabilidad y procesos de gestión de riesgo dirección riesgos de ciberseguridad. (p. 22)...<br>JDM RM-1: Procesos de gestión de riesgo son administrados y acordados por los actores organizacionales. (p. 23) |
| D1.G.Ov.B.2 | Los riesgos de seguridad de la información se discuten en las reuniones de gestión cuando se le solicite por eventos cibernéticos altamente visible o avisos reglamentarios. (FFIEC seguridad folleto, página 6) | Fuente: IS. I.B:PG4: Gestión también debe hacer lo siguiente: participar en evaluar el efecto de las amenazas de seguridad o de incidentes en la institución y sus líneas de negocio y procesos.<br>ES. III. A:pg47: La gestión debe desarrollar procedimientos para obtención, supervisión, evaluación y respuesta a la evolución de la amenaza y la información sobre la vulnerabilidad. | Existe una conciencia de riesgo de seguridad cibernética a nivel organizacional, pero no se ha establecido un acercamiento de toda la organización a administrar los riesgos de la ciberseguridad. (p. 10) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.B.3 | Administración proporciona un informe escrito sobre el estado general de la seguridad de la información y Programas de continuidad de negocio para la Junta o un Comité apropiado por lo menos anualmente. (FFIEC seguridad folleto, página 5) | Fuente: IS-I.B: pág. 4: La junta, o el comité designado de la junta, debe aprobar el programa escrito de seguridad de la información de la institución; afirmar responsabilidades para el desarrollo, implementación y mantenimiento del programa; y revisar un informe sobre el estado general del programa al menos una vez al año. La gerencia debe proporcionar un informe a la junta directiva al menos una vez al año que describa el estado general del programa y los asuntos materiales relacionados con el programa, incluidos los siguientes ...<br>IS-WP.2.4: Determine si la junta aprueba un programa escrito de seguridad de la información y recibe un informe sobre la efectividad del programa de seguridad de la información al menos una vez al año.<br>MGT.III.C.3 (a): pg30: La junta también debe revisar anualmente un informe escrito, preparado por la gerencia, sobre las acciones de la institución financiera con respecto al cumplimiento de GLBA.<br>MGT.III.C.4: pg30: La administración también debe proporcionar a la junta un informe escrito sobre el estado general del programa de continuidad del negocio y los resultados de las pruebas del plan y los sistemas de respaldo.<br>MGT.WP.12.7.f: Verifique que la junta es responsable de revisar anualmente el informe de la administración sobre el estado de las acciones del banco para lograr o mantener el cumplimiento del Estándar de seguridad de la información.<br>MGT.WP.12.9.a & c: Determine si la junta directiva aprobó las políticas y la gerencia estableció e implementó políticas, procedimientos y responsabilidades para un programa de continuidad de negocios en toda la empresa, incluidos los siguientes: Revisión anual y aprobación de la continuidad del negocio Programa de la junta directiva e informes anuales de la administración de los resultados de las pruebas de continuidad del negocio y recuperación de desastres a la junta directiva. | ID.GV-4: Gobierno y Gestión de riesgos procesos Dirección Cibernético seguridad del Riesgo. (p. 22) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.B.4 | El proceso de presupuestarían incluye información de seguridad relacionados con gastos y herramientas. (FFIEC E-Banking folleto, página 20) | "Fuente: es. IC: PG5: Financiación, junto con el talento técnico y empresarial, también para mejorar el programa de seguridad de la información. Gestión debe tener, y la Junta debe, la adecuada para desarrollar, implementar y mantener un Programa de seguridad de la información exitosa. ISWP.2.9: Determinación de la información exitosa. ADMINISTRACIÓN DE I.B.6: pg14: Gestión debe esforzarse por lograr un proceso de planificación que se ajuste constantemente a nuevos riesgos u oportunidades y maximizar su valor. ADMINISTRACIÓN DE I.B.6 (c): pg17 cuando dice nuevos proyectos, la gerencia debe buscar en los costos de la entrada de la tecnología y los costos de soporte post-implementación. ADMINISTRACIÓN DE I.B.6 (c): pg17: algunas instituciones como un presupuesto separado. Un análisis financiero de un departamento de TI debe incluir una comparación de la rentabilidad de la operación interna contra la contratación con un tercero proveedor. El análisis- .. | Ninguno |
| D1.G.Ov.B.5 | La dirección considera que los riesgos planteados por otras infraestructuras críticas (por ejemplo, telecomunicaciones, energía) a la institución. (FFIEC negocio continuidad planificación folleto, página J-12) | Fuente: BCP. BJ-12: Ataques cibernéticos también pueden llevarse a cabo en conjunto con eventos físicos disruptivos y pueden afectar a múltiples sectores de las infraestructuras críticas (por ejemplo, los sectores de telecomunicaciones y energía). Las instituciones financieras y TSPs deberían considerar la susceptibilidad a los ataques simultáneos en su resistencia del negocio planificación, recuperación y estrategias de prueba.<br>BCP. WP.10: Determinar si la institución financiera y de TSP estrategias están diseñadas para lograr la resiliencia como la capacidad de responder con eficacia a perturbaciones de gran escala, incluyendo ciberataques y ataques contra varios críticos de la gestión del riesgo sectores de infraestructura. | Ninguno |
| D1.G.Ov.E.1 | Por lo menos anualmente, la Junta Directiva o un Comité apropiado revisa y aprueba Programa de ciberseguridad de la institución. | N/A | ID. GV-4: Gobernabilidad y procesos de gestión de riesgo dirección riesgos de ciberseguridad. (p. 22) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.E.2 | Administración es responsable de garantizar el cumplimiento de requisitos legales y reglamentarios relacionados con la ciberseguridad. | N/A | ID. GV-3: Requisitos legales y reglamentarios sobre ciberseguridad, incluyendo privacidad y libertades civiles obligaciones, están entendidos y manejados.<br>DE (p. 21). DP-2: Actividades de detección cumplen con todos los requisitos aplicables.<br>Perfil de marco (p. 32): identificar y tratar la privacidad individual y las implicaciones de las libertades civiles que resulten de operaciones de ciberseguridad (p. 15) gestión de riesgos de la ciberseguridad.<br>Identificar y autorizar el acceso. Conciencia y las medidas de capacitación.<br>Detección de actividad anómala revisado por cuestiones de privacidad.<br>Informe sobre el intercambio de información personal dentro y fuera de la organización. |
| D1.G.Ov.E.3 | Personal y herramientas de seguridad cibernética se solicita a través del proceso de presupuesto. | N/A | Ninguna |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.E.4 | Existe un proceso para discutir formalmente y estimar gastos potenciales asociados a incidentes de seguridad cibernética como parte del proceso de presupuestario. | N/A | Ninguna |
| D1.G.Ov.Int.1 | La Junta Directiva o un Comité apropiado tiene experiencia de ciberseguridad o contrata expertos para asistir con responsabilidades de supervisión. | N/A | ID. GV-4: Gobernabilidad y procesos de gestión de riesgo dirección riesgos de ciberseguridad.<br>Intro de marco (p. 22): expresa una tolerancia al riesgo (p. 5) |
| D1.G.Ov.Int.2 | El tablero estándar de la reunión incluye informes y métricas que van más allá de incidentes y eventos dirección amenaza inteligencia tendencias y postura de seguridad de la institución. | N/A | Ninguna |
| D1.G.Ov.Int.3 | La institución tiene una declaración de apetito de riesgo Cibernético aprobada por la Junta o un Comité apropiado. | N/A | ID. RM-2: Tolerancia al riesgo organizacional determina y expresa claramente. ID. (p. 23)<br>GV-4: Gobernabilidad y procesos de gestión de riesgo dirección riesgos de ciberseguridad. (p. 22) |
| D1.G.Ov.Int.4 | Riesgos cibernéticos que exceden el apetito de riesgo se escalan a la gestión. | N/A | Ninguna |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.Int.5 | La Junta Directiva o un Comité apropiado asegura anual sobre ciberseguridad autoevaluación de gestión evalúa la capacidad de la institución para cumplir con sus estándares de gestión de riesgo de Cibernético. | N/A | ID. BE-3: Se establecen prioridades para la misión, objetivos y actividades. (p. 21) riesgo informado Descripción: priorización de las actividades de la ciberseguridad es informada directamente por objetivos de riesgo organizacional, el ambiente de amenaza o requisitos de misión de negocios. (p. 10) |
| D1.G.Ov.Int.6 | La Junta Directiva o un Comité apropiado revisa y aprueba de prioridades y recursos asignación decisiones basadas en los resultados de las evaluaciones de Cibernético. | N/A | Ninguna |
| D1.G.Ov.Int.7 | La Junta Directiva o un Comité apropiado asegura gestión toma acciones apropiadas de dirección cambio de riesgos cibernéticos o cuestiones de ciberseguridad significativa. | N/A | Ninguna |
| D1.G.Ov.Int.8 | El proceso de presupuesto para solicitar personal adicional sobre ciberseguridad y herramientas está integrado en los procesos de presupuesto de | N/A | Ninguna |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | unidades de negocio. | | |
| D1.G.Ov.A.1 | El Consejo o junta Comité aprobada Cibernético declaración de apetito de riesgo es parte de la declaración de apetito de riesgo de toda la empresa. | N/A | Ninguna |
| D1.G.Ov.A.2 | Gestión cuenta con un proceso formal para mejorar de manera continua supervisión de la seguridad cibernética. | N/A | PR. IP-7: Procesos de protección son mejorados continuamente. proceso de evolucionar (p. 27) de la conciencia de anteriores actividades, la información compartida por otras fuentes y la continua conciencia de actividades sobre sistemas y redes. (p. 11) |
| D1.G.Ov.A.3 | El proceso de presupuesto para solicitar personal adicional sobre ciberseguridad y herramientas mapas actuales recursos y herramientas para la estrategia de ciberseguridad. | N/A | Ninguna |
| D1.G.Ov.A.4 | Administración y la Junta Directiva o un Comité apropiado responsabilizar a unidades de negocio para gestionar con eficacia | N/A | Ninguna |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | todos Cibernético los riesgos asociados con sus actividades. | | |
| D1.G.Ov.A.5 | Gestión identifica causa raíz cuando Cibernético ataques resultado en pérdida de material. | N/A | Descripción de nivel 4: administración el riesgo de la seguridad cibernética a través de un enfoque de toda la organización con políticas conclusión en el riesgo, los procesos y procedimientos para enfrentar posibles eventos de ciberseguridad. (p. 11) |
| D1.G.Ov.A.6 | La Junta Directiva o un Comité apropiado garantiza que acciones de la administración consideren los riesgos cibernéticos que la institución plantea para el sector financiero. | N/A | Ninguna |
| D1.G.Ov.Inn.1 | La Junta Directiva o un Comité apropiado analiza formas de gestión desarrollar mejoras de ciberseguridad que pueden ser adoptados todo el sector. | N/A | Ninguna |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.Ov.Inn.2 | La Junta Directiva o un Comité apropiado verifica que las acciones de la administración consideren los riesgos de Cibernético que la institución plantea a otras infraestructuras críticas (por ejemplo, telecomunicaciones, energía). | N/A | Ninguna |
| D1.G.SP.B.1 | La institución tiene una estrategia de seguridad de la información que integra tecnología, políticas, procedimientos y entrenamiento para mitigar el riesgo. (FFIEC seguridad folleto, página 3) | "Fuente: IS-Introducción: pg2: La seguridad de la información es mucho más efectiva cuando la administración hace lo siguiente: Integra los procesos, las personas y la tecnología para mantener un perfil de riesgo que esté de acuerdo con el apetito de riesgo de la junta. Alinea el programa de seguridad de la información con el programa de gestión de riesgos empresariales e identifica, mide, mitiga y controla el riesgo. IS-WP.6.3: Determine si la institución evalúa continuamente la capacidad de la tecnología necesaria para mantener un nivel apropiado de seguridad de la información en función del tamaño, la complejidad y el apetito de riesgo de la institución. MGT.III.C.1: pg27: La alta gerencia debe garantizar que las políticas, estándares y procedimientos estén actualizados, bien documentados e integrados con la estrategia de seguridad de la información de la institución. MGT.WP.4.3: Determine si la institución tiene planes de TI tácticos y operativos adecuados para respaldar los planes estratégicos de TI más grandes ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.SP.B.2 | La institución tiene políticas acordes a su riesgo y complejidad que aborden los conceptos de gestión de riesgos de tecnología de información. (FFIEC seguridad folleto, página 16) | "Fuente: IS-II: pg6: La administración debe desarrollar e implementar un programa de seguridad de la información que haga lo siguiente: Respalda el proceso de gestión de riesgos de TI (ITRM) de la institución al identificar amenazas, medir el riesgo, definir los requisitos de seguridad de la información e implementar controles. IS-WP.3.1: Determine si la institución tiene un programa de seguridad de la información efectivo que respalde el proceso ITRM. MGT.III. C.1: pg27: La administración de la institución debe crear, documentar, mantener y cumplir con las políticas, normas y procedimientos para administrar y controlar el riesgo de TI de la institución. El nivel de detalle depende de la complejidad del entorno de TI, pero debe permitir a la administración monitorear la postura de riesgo identificada. MGT.WP.12.4: Determine si la administración de TI ha desarrollado políticas, estándares y procedimientos adecuados para administrar el riesgo de la tecnología y si están actualizados, documentados y se han comunicado adecuadamente ". | Prácticas de gestión de riesgo de la organización son formalmente aprobadas y expresadas como política. (p. 10) |
| D1.G.SP.B.3 | La institución tiene políticas acordes a su riesgo y complejidad que aborden los conceptos de intercambio de información de amenaza. (FFIEC E - Banking folleto, página 28) | Origen: Es-III. C:pg50: El intercambio de datos de ataque a través de organizaciones como FS-ISAC, también tiene el potencial en beneficio de la industria en general permitiendo a otras instituciones para evaluar mejor y responder a los ataques actuales. Administración debe considerar la posibilidad de incluir tal información compartir como parte de su estrategia para proteger a la institución. ADMINISTRACIÓN III. A:pg22: Participación en un foro de intercambio de información, como el FS-ISAC, debe ser un componente del proceso de identificación de riesgo porque compartir información puede ayudar a la institución identificar y evaluar las vulnerabilidades y las amenazas de ciberseguridad pertinentes. Mgt.WP.10.1.b: Determinar si la gestión se participa en un foro (como FS-ISAC) de intercambio de información. | PR. PT-1: Registros de Auditoría ría son determinados, documentados, implementados y revisados de acuerdo con la política. (p. 29) |
| D1.G.SP.B.4 | La institución tiene políticas aprobado por la Junta Directiva acordes con su complejidad y riesgo seguridad de la información de dirección. (FFIEC seguridad folleto, página 16) | Fuente: IS-I: pg4: gestión también debe hacer lo siguiente: implementar el programa de seguridad de la información aprobada por el Consejo. Establecer políticas apropiadas, normas y procedimientos para apoyar el programa de seguridad de la información. ES-Wp.<br>6.2: determinar si la política de seguridad de la información anualmente es revisada y aprobada por la Junta. | ID. GV-1: Se establece la política de seguridad de la información organizacional. PR (p. 21)<br>PT-2: Medio extraíble está protegido y restringido su uso según una política específica. (p. 29) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.SP.B.5 | La institución tiene políticas acordes a su riesgo y complejidad que aborden los conceptos de dependencia externa o de terceros. (FFIEC Outsourcing folleto, página 2) | Fuente: OT. B.2: Las instituciones financieras deben tener un proceso de gestión de riesgos de Outsourcing integral para regir sus relaciones de CDTAS. | |
| D1.G.SP.B.6 | La institución tiene políticas acordes a su riesgo y complejidad que aborden los conceptos de respuesta a incidentes y recuperación. (FFIEC seguridad folleto, página 83) | "Fuente: IS-II.C.21: pág. 43: La administración debe hacer lo siguiente: ... Establecer y mantener políticas que aborden los conceptos de respuesta y resiliencia de incidentes de seguridad de la información, y probar los escenarios de incidentes de seguridad de la información.<br>IS-Wp.6.34.c: Determine si la administración administra efectivamente las siguientes consideraciones de seguridad de la información relacionadas con la planificación de la continuidad del negocio. Revise la capacidad de la administración para hacer lo siguiente: Desarrollar políticas que aborden los conceptos de respuesta y resiliencia ante incidentes de seguridad de la información y probar los escenarios de incidentes de seguridad de información ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.SP.B.7 | Todos los elementos del programa de seguridad de información se coordinan toda la empresa. (FFIEC seguridad folleto, página 7) | "Fuente IS-Introducción: pg2: Los programas de seguridad de la información deben contar con un sólido respaldo de la junta directiva y la alta gerencia, promover la integración de las actividades y los controles de seguridad en todos los procesos de negocios de la institución y establecer una clara responsabilidad para cumplir con las responsabilidades de seguridad.<br>IS-WP.3.2: Determine si la administración integra adecuadamente el programa de seguridad de la información en las líneas de negocios y funciones de soporte de la institución. Revise si la administración tiene lo siguiente: Políticas de seguridad, estándares y procedimientos diseñados para respaldar y alinearse con las políticas en las líneas de negocios. Programas de respuesta a incidentes que incluyen todas las líneas de negocios y unidades de soporte afectadas. Sensibilización común y mecanismos de cumplimiento entre líneas de negocio y seguridad de la información. Visibilidad para evaluar la probabilidad de amenazas y posibles daños a la institución. La capacidad de identificar e implementar controles sobre las causas raíz de un incidente.<br>MGT.I.B.2: pg10: La institución debe tener un programa integral de seguridad de la información que aborde todos los activos de tecnología e información y que cumpla con las Normas de seguridad de la información. El programa de seguridad de la información debe incluir salvaguardas administrativas, técnicas y físicas apropiadas basadas en el perfil de riesgo inherente y las actividades, productos y servicios individuales de la institución.<br>MGT.III.C.3: pg29: El programa de seguridad de la información debe coordinarse en toda la institución.<br>MGT.WP.8.2: Determine si la gestión de riesgo operacional de la institución incorpora una visión de toda la empresa de los procesos de TI y de negocios que son compatibles con la tecnología ". | ID. GV-2: Roles de seguridad de la información y la responsabilidad son coordinados y alineados con roles internos y externos. (p. 21) |
| D1.G.SP.E.1 | La institución aumentada su estrategia de seguridad de la información para incorporar la seguridad cibernética y la resistencia. | N/A | ID. GV-4: Gobernabilidad y procesos de gestión de riesgo dirección riesgos de ciberseguridad. (p. 22) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.SP.E.2 | La institución tiene un Programa de ciberseguridad formal que se basa en tecnología y estándares de la industria de seguridad o puntos de referencia. | N/A | ID. BE-3: Se establecen prioridades para la misión, objetivos y actividades. (p. 21) |
| D1.G.SP.E.3 | Un proceso formal es en lugar de actualizar políticas como cambios de Perfil de riesgo inherente de la institución. | N/A | Métodos consistentes están en el lugar para responder con eficacia a los cambios en el riesgo. (p. 10) |
| D1.G.SP.Int.1 | La institución cuenta con un conjunto integral de políticas acordes con su riesgo y complejidad que aborden los conceptos de inteligencia de la amenaza. | N/A | |
| D1.G.SP.Int.2 | Gestión periódicamente revisa la estrategia de ciberseguridad a dirección de evolución de las amenazas cibernéticas y cambia al perfil de riesgo inherente de la institución. | N/A | |
| D1.G.SP.Int.3 | La estrategia de ciberseguridad se incorpora, o expresiones cabe dentro, estrategia de gestión de riesgo corporativo de la institución. | N/A | ID. BE-3: Se establecen prioridades para la misión, objetivos y actividades. (p. 21) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.SP.Int.4 | Gestión de enlaces ciberseguridad estratégico objetivos tácticos. | N/A | |
| D1.G.SP.Int.5 | Un proceso formal es para referencia cruzada y actualizar simultáneamente todas las políticas relacionadas con los riesgos cibernéticos a través de líneas de negocio. | N/A | |
| D1.G.SP.A.1 | La estrategia de ciberseguridad describe el estado futuro de la institución de seguridad cibernética con perspectivas a corto y a largo plazo. | N/A | |
| D1.G.SP.A.2 | Normas de ciberseguridad reconocidos en la industria se utilizan como fuentes durante el análisis de brechas de Programa de ciberseguridad. | N/A | |
| D1.G.SP.A.3 | La estrategia de ciberseguridad identifica y comunica el papel de la institución como componente de las infraestructuras críticas en la industria de servicios financieros. | N/A | ID. BE-1: Papel de la organización en la cadena de suministro es identificado y comunicado. (p. 21) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.SP.A.4 | El apetito de riesgo es informado por el papel de la institución en infraestructura crítica. | N/A | ID. RM-3: Determinación de la organización de tolerancia al riesgo es informado por su papel en la crítica infraestructura y sector riesgo específico análisis-(p. 23) |
| D1.G.SP.A.5 | Gestión es la mejora continua el Programa de ciberseguridad existentes para adaptarse como los cambios de estado de ciberseguridad deseado objetivo. | N/A | Continuamente incorpora tecnologías avanzadas y prácticas, adaptación a un cambiante paisaje de ciberseguridad. (p. 11) |
| D1.G.SP.Inn.1 | La estrategia de ciberseguridad identifica y comunica el papel de la institución en relación con otras infraestructuras críticas. | N/A | ID. BE-2: De la organización en las infraestructuras críticas y su ecosistema de industria es identificado y comunicado. (p. 21) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.IT.B.1 | Se mantiene un inventario de activos de la organización (por ejemplo, hardware, software, datos y sistemas alojados externamente). (FFIEC seguridad folleto, página 9) | "Fuente: IS-II.C.5: pg14: La administración debe inventariar y clasificar los activos, incluido el hardware, el software, la información y las conexiones. La gerencia debe mantener y mantener actualizado un inventario de los activos tecnológicos que clasifique la sensibilidad y la criticidad de esos activos., incluyendo hardware, software, información y conexiones.<br>IS-WP.6.6: Determine si la administración mantiene efectivamente un inventario (es) de hardware, software, información y conexiones. Revise si la administración hace lo siguiente: Identifica los activos que requieren protección, como aquellos que almacenan, transmiten o procesan información confidencial del cliente o secretos comerciales. Clasifica los activos adecuadamente. Utiliza la clasificación para determinar la sensibilidad y criticidad de los activos. Utiliza la clasificación para implementar los controles necesarios para salvaguardar los activos de la institución. Actualiza el (los) inventario (es) adecuadamente.<br>MGT.III.A: pg22: La administración debe mantener inventarios de activos (por ejemplo, hardware, software e información), clases de eventos (por ejemplo, desastres naturales, cibernético y abuso o compromiso de información privilegiada), amenazas (por ejemplo, robo, malware, e ingeniería social), y los controles existentes como una parte importante de la identificación efectiva de riesgos " | ID. AM-1: recubrimiento físicos y sistemas dentro de la organización son inventariados. ID. (p. 20) AM-2: Plataformas de Software y aplicaciones dentro de la organización son inventariadas. (p. 20) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.IT.B.2 | Activos de la organización (por ejemplo, hardware, sistemas, datos y aplicaciones) se priorizan para la protección basada en el valor de la clasificación y del negocio de datos. (FFIEC seguridad folleto, página 12) | "Fuente: IS-II.C.5: pg14: La administración debe mantener y mantener actualizado un inventario de activos tecnológicos que clasifique la sensibilidad y criticidad de dichos activos, incluidos el hardware, el software, la información y las conexiones. La gerencia debe tener políticas para gobernar el inventario y la clasificación de los activos tanto al inicio como a lo largo de su ciclo de vida, y dondequiera que se almacenen, transmitan o procesen los activos. Los inventarios permiten a la administración y al personal identificar los activos y sus funciones. La clasificación permite a la institución determinar la sensibilidad y criticidad de activos. La gerencia debe usar esta clasificación para implementar los controles necesarios para salvaguardar los activos físicos y de información de la institución.<br>IS-WP.6.6: Determine si la administración mantiene efectivamente un inventario (es) de hardware, software, información y conexiones. Revise si la administración hace lo siguiente: Identifica los activos que requieren protección, como aquellos que almacenan, transmiten o procesan información confidencial del cliente o secretos comerciales. Clasifica los activos adecuadamente. Utiliza la clasificación para determinar la sensibilidad y criticidad de los activos. Utiliza la clasificación para implementar los controles necesarios para salvaguardar los activos de la institución. Actualiza el (los) inventario (es) adecuadamente. " | ID. AM-5: Recursos se priorizan en base a la clasificación / importancia / valor para el negocio de hardware, dispositivos, datos y software. ID. (p. 20)<br>BE-4: Se establecen las dependencias y funciones críticas para la entrega de servicios críticos. (p. 21) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.IT.B.3 | Gestión asigna responsabilidades para el mantenimiento de un inventario de activos de la organización. (FFIEC seguridad folleto, página 9) | "Fuente: IS-II.C.5: pg14: La administración debe mantener y mantener actualizado un inventario de activos tecnológicos que clasifique la sensibilidad y criticidad de dichos activos, incluidos el hardware, el software, la información y las conexiones. La gerencia debe tener políticas para gobernar el inventario y la clasificación de los activos tanto al inicio como a lo largo de su ciclo de vida, y dondequiera que se almacenen, transmitan o procesen los activos. Los inventarios permiten a la administración y al personal identificar los activos y sus funciones. La clasificación permite a la institución determinar la sensibilidad y criticidad de activos. La gerencia debe usar esta clasificación para implementar los controles necesarios para salvaguardar los activos físicos y de información de la institución.<br>IS-WP.6.6: Determine si la administración mantiene efectivamente un inventario (es) de hardware, software, información y conexiones.<br>MGT.III.A: pg22: La administración debe mantener inventarios de activos (por ejemplo, hardware, software e información), clases de eventos (por ejemplo, desastres naturales, cibernético y abuso o compromiso de información privilegiada), amenazas (por ejemplo, robo, malware, e ingeniería social), y los controles existentes como una parte importante de la identificación efectiva de riesgos. Los inventarios deben incluir sistemas e información alojados o mantenidos externamente ". | |
| D1.G.IT.B.4 | Un proceso de gestión del cambio es para solicitar y aprobar cambios en configuraciones de sistemas, hardware, software, aplicaciones y herramientas de seguridad. (FFIEC seguridad folleto, página 56) | "Fuente: IS-II.C.10: pg21: La administración debe tener un proceso para introducir cambios en el entorno de forma controlada. Los cambios en el entorno de TI incluyen lo siguiente: Gestión de la configuración de los sistemas y aplicaciones de TI. Refuerzo de los sistemas y Aplicaciones. Uso de compilaciones estándar. Administración de parches. El entorno de TI consta de sistemas operativos, middleware, aplicaciones, sistemas de archivos y protocolos de comunicaciones. La institución debe tener un proceso eficaz para introducir cambios en las aplicaciones y el sistema, incluidos hardware, software y red. dispositivos, en el entorno de TI.<br>IS-WP.6.11: Determine si la administración tiene un proceso para introducir cambios en el entorno (por ejemplo, la administración de la configuración de los sistemas y aplicaciones de TI, el fortalecimiento de los sistemas y las aplicaciones, el uso de compilaciones estándar y la administración de parches) de manera controlada ". | SRM IP-3: Procesos de control de cambio de configuración están en el lugar. (p. 27) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.IT.E.1 | El inventario de activos, incluyendo la identificación de activos críticos, se actualiza por lo menos anualmente para hacer frente a activos de nuevo, reubicados y puesta de sol. | N/A | |
| D1.G.IT.E.2 | La institución cuenta con un bien documentado proceso que considera si los activos a ser adquiridos tienen precauciones de seguridad apropiadas de ciclo de vida. | N/A | PR-DS-3: Activos son manejados formalmente a través de la eliminación, las transferencias y disposición. (p. 25) |
| D1.G.IT.E.3 | La institución administra proactivamente sistema EOL (p. ej., reemplazo) para limitar los riesgos de seguridad. | N/A | PR-DS-3: Activos son manejados formalmente a través de la eliminación, las transferencias y disposición. (p. 25) |
| D1.G.IT.E.4 | Cambios son aprobados formalmente por una persona o Comité con autoridad apropiada y con separación de funciones. | N/A | |
| D1.G.IT.Int.1 | Configuraciones de línea de base no se puede modificar sin una solicitud formal, documentado aprobación y una evaluación de las implicaciones de seguridad. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.IT.Int.2 | Cambiar proceso de gestión formal requiere riesgos de ciberseguridad a ser evaluados durante el análisis, aprobación, pruebas y reporte de cambios. | N/A | |
| D1.G.IT.A.1 | Riesgo cadena de suministro es revisado antes de la adquisición de sistemas de información de misión crítica incluyendo componentes del sistema. | N/A | |
| D1.G.IT.A.2 | Herramientas automatizadas permiten el seguimiento, actualización, priorización de activos y reporte personalizado del inventario de activos. | N/A | |
| D1.G.IT.A.3 | Existen procesos automatizados para detectar y bloquear cambios no autorizados al software y hardware. | N/A | |
| D1.G.IT.A.4 | El sistema de gestión de cambio utiliza umbrales para determinar cuándo se requiere una evaluación del riesgo del impacto del cambio. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.IT.Inn.1 | Una función de gestión de cambio formal rige descentralizada o altamente distribuido cambio pide e identifica y mide los riesgos de seguridad que pueden causar la mayor exposición a ataques cibernéticos. | N/A | |
| D1.G.IT.Inn.2 | Herramientas empresa automatizado integral se ejecutan para detectar y bloquear cambios no autorizados al software y hardware. | N/A | |
| D1.RM.RMP.B.1 | Una información seguridad y negocio continuidad riesgo gestión funciones existen dentro de la institución. (FFIEC seguridad folleto, página 68) | "Fuente: IS.II.C.21: pg43: La administración debe hacer lo siguiente: Identificar al personal que desempeñará roles críticos de seguridad de la información durante un desastre, y capacitar al personal en esos roles. Definir las necesidades de seguridad de la información para sitios de respaldo y redes de comunicación alternativas. Establecer y mantener políticas que aborden los conceptos de respuesta y resistencia a incidentes de seguridad de la información y probar los escenarios de incidentes de seguridad de la información.<br>IS.WP.6.34: Determine si la administración administra efectivamente las siguientes consideraciones de seguridad de la información relacionadas con la planificación de la continuidad del negocio.<br>MGT.I.B.4: pg12: la función de continuidad del negocio a menudo reside en la estructura organizativa de la gestión de riesgos. A un miembro específico de la gerencia se le debe asignar la responsabilidad de supervisar la función de continuidad del negocio, y los departamentos de negocios y tecnología deben asignar personal para desarrollar y mantener los planes de las unidades de negocios individuales.<br>MGT.WP.3 .: Como parte de la estructura de ITRM, determine si la administración de la institución financiera ha definido responsabilidades y funciones de TI. Verifique la existencia de responsabilidades y expectativas bien definidas entre la | Gestión de riesgos prácticas son aprobadas por la gerencia, pero no pueden ser establecidas como política de toda la organización. (p. 10) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | | gestión de riesgos y las áreas funcionales de TI, como la seguridad de la información, la gestión de proyectos, la continuidad del negocio y los informes de sistemas de información ". | |
| D1.RM.RMP.E.1 | El Programa de administración de riesgos incorpora riesgo cibernético identificación, medición, mitigación, monitoreo y reporte. | N/A | Riesgo informado, aprobado por la administración de procesos y procedimientos se definen y se implementó, y personal tiene recursos suficientes para realizar sus tareas de ciberseguridad. (p. 10) |
| D1.RM.RMP.E.2 | Gestión de comentarios y utiliza los resultados de las Auditoría para mejorar políticas de ciberseguridad, procedimientos y controles existentes. | N/A | PR.IP-7: Los procesos de protección se mejoran continuamente. (p. 27) |
| D1.RM.RMP.E.3 | Gestión supervisa cuestiones de moderado y alto riesgo residual de la evaluación de riesgos de ciberseguridad hasta artículos se abordan. | N/A | |
| D1.RM.RMP.Int.1 | La función de ciberseguridad tiene una línea de información clara que no presenta un conflicto de intereses. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.RMP.Int.2 | El Programa de administración de riesgos dirige específicamente riesgos cibernéticos más allá de los límites de los impactos tecnológicos (por ejemplo, financiero, estratégico, regulatorio, cumplimiento de normas). | N/A | Administra el riesgo de la seguridad cibernética a través de un enfoque de toda la organización con políticas basadas en el riesgo, los procesos y procedimientos para enfrentar posibles eventos de ciberseguridad. (p. 11) |
| D1.RM.RMP.Int.3 | Puntos de referencia o indicadores de rendimiento objetivo se han establecido para mostrar mejoras o regresiones de la postura de seguridad en el tiempo. | N/A | |
| D1.RM.RMP.Int.4 | Gestión utiliza los resultados de Auditoría independientes y comentarios para mejorar la ciberseguridad. | N/A | |
| D1.RM.RMP.Int.5 | Existe un proceso para analizar y asignar posibles pérdidas y gastos, por centro de costos, asociados con incidentes de seguridad cibernética. | N/A | |
| D1.RM.RMP.A.1 | Métricas de seguridad cibernética se utilizan para facilitar la toma de decisiones estratégica y financiamiento en áreas de necesidad. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.RMP.A.2 | Gestión de riesgos independiente establece y supervisa los límites de riesgo relacionados con el Cibernético para unidades de negocio. | N/A | |
| D1.RM.RMP.A.3 | Personal de administración de riesgo independiente intensifica a la gestión y la Junta o un Comité apropiado discrepancias significativas Comité de evaluaciones de la unidad de negocio de riesgos relacionados con la cibernética. | N/A | |
| D1.RM.RMP.A.4 | Un proceso está en el lugar para analizar el impacto financiero Cibernético incidentes tienen en el capital de la institución. | N/A | DE.AE-4: Se determina el impacto del evento. (p. 30) |
| D1.RM.RMP.A.5 | La agregación de datos de riesgo de Cibernético y capacidades de reporte en tiempo real apoyan necesidades informes de la institución, particularmente durante los incidentes cibernéticos. | N/A | |
| D1.RM.RMP.Inn.1 | La función de administración del riesgo identifica y analiza similitudes en Cibernético eventos que ocurren en la | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | institución y en otros sectores para una administración más predictivo de riesgo. | | |
| D1.RM.RMP.Inn.2 | Un proceso está en el lugar para analizar el impacto financiero que puede tener un incidente de Cibernético en la institución en el sector financiero. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.RA.B.1 | Una evaluación de riesgo enfocada a la protección de información del cliente identifica razonables y previsibles de amenazas internas y externas, el daño probabilidad y potencial de las amenazas y la suficiencia de las políticas, procedimientos y sistemas de información al cliente. (FFIEC seguridad folleto, página 8) | "Fuente: IS.I.B: pág. 4: La administración debe proporcionar un informe al directorio al menos una vez al año que describa el estado general del programa y los asuntos materiales relacionados con el programa, incluidos los siguientes: Proceso de evaluación de riesgos, incluida la identificación y evaluación de amenazas.<br>IS.WP.2.4: Determine si la junta aprueba un programa escrito de seguridad de la información y recibe un informe sobre la efectividad del programa de seguridad de la información al menos una vez al año. Determine si el informe a la junta directiva describe el estado general del programa de seguridad de la información y analiza asuntos importantes relacionados con el programa, como los siguientes:<br>a. Proceso de evaluación de riesgos, incluida la identificación y evaluación de amenazas.<br>MGT.III.A: pg22: La identificación completa de riesgos de TI debe incluir la identificación de los riesgos de ciberseguridad, así como los detalles recopilados durante las evaluaciones de riesgos de seguridad de la información requeridas según las pautas de implementación del GLBA.<br>MGT.WP.7.4: Determine si la institución mantiene un proceso de evaluación de riesgos para realizar lo siguiente:<br>a. Identificar riesgos y amenazas tanto de fuentes internas como externas.<br>segundo. Desarrollar o actualizar políticas dentro de la función de gestión de riesgos para guiar las actividades de medición de riesgos.<br>do. Asegurar la existencia de un proceso para promover una buena comprensión y análisis de amenazas, eventos, activos y controles.<br>re. Mantenga los procesos dentro de la función de gestión de riesgos para ayudar a tomar decisiones de mitigación de riesgos.<br>mi. Determine las entidades que deben participar en ese proceso de toma de decisiones.<br>F. Asegúrese de que el consejo y la gerencia entiendan las categorías de riesgo ". | ID. RA-5: Amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo. (p. 22) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.RA.B.2 | La evaluación de riesgos identifica sistemas basados en internet y las transacciones de alto riesgo que requieren controles de autenticación adicional. (FFIEC seguridad folleto, página 12) | "Fuente: IS.I.B: pág. 4: La administración debe proporcionar un informe al directorio al menos una vez al año que describa el estado general del programa y los asuntos materiales relacionados con el programa, incluidos los siguientes: Proceso de evaluación de riesgos, incluida la identificación y evaluación de amenazas.<br>IS.II.C.17: pg38-39: Las aplicaciones deben proporcionar a la administración la capacidad de hacer lo siguiente:… Proteger las aplicaciones web o de Internet mediante controles adicionales, incluidos los firewalls de aplicaciones web, el análisis regular de vulnerabilidades nuevas o recurrentes, la mitigación o la remediación de las debilidades de seguridad comunes, y la segregación de la red para limitar el acceso o las conexiones inapropiadas a la aplicación u otras áreas de la red.<br>IS.WP.6.27.g: Revise si las aplicaciones en uso ofrecen las siguientes capacidades: Proteja las aplicaciones web o de Internet a través de controles adicionales, que incluyen firewalls de aplicaciones web, análisis regulares de vulnerabilidades nuevas o recurrentes, mitigación o remediación de las debilidades comunes de seguridad. y segregación de red ". | |
| D1.RM.RA.B.3 | La evaluación de riesgos se actualiza a las nuevas tecnologías de dirección, productos, servicios y conexiones antes de la implementación. (FFIEC seguridad folleto, página 13) | "Fuente: IS.II.A: pg7: Los eventos externos que afectan la TI y la capacidad de la institución para cumplir sus objetivos operativos incluyen desastres naturales, ataques cibernéticos, cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías, litigios y nuevas leyes o regulaciones. Estos eventos plantean riesgos y oportunidades, y la institución debería incluirlos en el proceso de identificación de riesgos.<br>IS.II.C: pg11: Además, la administración debe desarrollar, mantener y actualizar un repositorio de información sobre amenazas y vulnerabilidades de seguridad cibernética que se puede usar para realizar evaluaciones de riesgos y brindar actualizaciones a la administración superior y al consejo sobre las tendencias de riesgo cibernético.<br>IS.WP.8.3.d: Determine si la administración tiene procesos efectivos de identificación y evaluación de amenazas, incluidos los siguientes: Uso del conocimiento de amenazas para impulsar la evaluación y respuesta de riesgos ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.RA.E.1 | Las evaluaciones de riesgos se utilizan para identificar los riesgos de ciberseguridad de nuevos productos, servicios o relaciones. | N/A | "ID.RA-5: amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo (p. 22)<br>RS.MI-3: Las vulnerabilidades recientemente identificadas se documentan como riesgos aceptados. (p. 34) " |
| D1.RM.RA.E.2 | El enfoque de la evaluación del riesgo se ha ampliado más allá de la información del cliente para abordar todos los activos de información. | N/A | "ID.RA-1: las vulnerabilidades de los activos están identificadas y documentadas (p. 22)<br>ID.RA-5: Se utilizan amenazas, vulnerabilidades, probabilidades e impactos para determinar el riesgo. (p. 22) " |
| D1.RM.RA.E.3 | La evaluación de riesgos considera que el riesgo de utilizar los componentes de software y hardware EOL. | N/A | |
| D1.RM.RA.Int.1 | La evaluación del riesgo se ajusta para considerar riesgos ampliamente conocidos o las prácticas de gestión de riesgo. | N/A | |
| D1.RM.RA.A.1 | Una función de gestión de riesgo corporativo incorpora análisis de amenazas cibernéticas y la exposición al riesgo específico como parte de la evaluación de riesgo. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.RA.Inn.1 | La evaluación de riesgos se actualiza en tiempo real como se producen cambios en el perfil de riesgo, nuevas normas son lanzadas o actualizadas, y se anticipan nuevas exposiciones. | N/A | |
| D1.RM.RA.Inn.2 | La institución utiliza la información de las evaluaciones de riesgos para predecir amenazas y respuestas en tiempo real en coche. | N/A | |
| D1.RM.RA.Inn.3 | Avanzado o automatizado análisis ofrecen información predictiva y métricas de riesgo en tiempo real. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.G.RM.Au.B.1 | Auditoría o revisión evalúa las políticas, procedimientos y controles en la institución para riesgos y problemas de control asociados a las operaciones de la institución, incluyendo los riesgos de nuevos productos, nuevas tecnologías e información sistemas. (FFIEC Auditoría folleto, página 4) | "Fuente: AUD.B.4: El gerente de auditoría interna debe ser responsable de las evaluaciones de riesgo del control interno, los planes de auditoría, los programas de auditoría y los informes de auditoría asociados con TI.<br>IS.IV.A.2 (d): pg56: Los departamentos internos independientes o terceros suelen realizar auditorías. Las auditorías deben revisar todos los aspectos del programa de seguridad de la información, el entorno en el que se ejecuta el programa y los resultados del programa. Las auditorías deben evaluar si las políticas, estándares y procedimientos son razonables y apropiados y si cumplen con ellas. informar sobre las actividades de seguridad de la información y las deficiencias de control a los tomadores de decisiones; identificar las causas de raíz y las recomendaciones para abordar las deficiencias; y probar la efectividad de los controles dentro del programa.<br>MGT.I.B.7 (b) pg19: Los auditores de TI deben validar que los controles de TI están diseñados de manera adecuada para mitigar el riesgo y que operan según lo previsto por la administración. La auditoría de TI debe ser completamente independiente, no debe tener ningún rol en el diseño o implementación de controles, y no debe tener la responsabilidad principal de hacer cumplir la política.<br>MGT.WP.6.3: Determine si el consejo, o su comité, tiene Vigilancia de auditoría apropiada a través de lo siguiente:<br>a. Auditoría de evaluación de riesgos y plan de auditoría.<br>segundo. Auditoría de actividades de revisión.<br>do. Informes de auditoría con debilidades identificadas.<br>re. Respuestas de la gerencia y acciones correctivas a los problemas de auditoría.<br>mi. Actualizaciones sobre cualquier problema de auditoría y el estado de los problemas " | Hay un enfoque de toda la organización a gestionar los riesgos de la ciberseguridad. Procedimientos, procesos y políticas basadas en el riesgo se define, como previsto y repasa. (p. 10) |
| D1.RM.Au.B.2 | La función de Auditoría independiente valida controles relacionados con el almacenamiento o la transmisión de datos confidenciales. (FFIEC Auditoría folleto, Página 1) | Fuente: AUD. B.1: Una efectiva auditoría programa... debería promover la confidencialidad, integridad y disponibilidad de sistemas de información. | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.Au.B.3 | Prácticas de registro de forma independiente son revisadas periódicamente para garantizar una gestión apropiada del registro (p. ej., controles de acceso, retención y mantenimiento). (FFIEC operaciones folleto, página 29) | "Fuente: OPS.B.29: La administración de operaciones debe revisar periódicamente todos los registros para asegurarse de que no se hayan eliminado, modificado, sobrescrito o comprometido.<br>IS.II.C.22: pg43: las prácticas de registro deben ser revisadas periódicamente por una parte independiente para garantizar una gestión de registro adecuada.<br>IS.WP.6.35 (c): Revise si la administración tiene lo siguiente: Revisión independiente de las prácticas de registro. "s. | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.Au.B.4 | Problemas y acciones correctivas de Auditoría internas y pruebas/evaluaciones independientes formalmente un seguimiento para asegurar los procedimientos y lapsos de control se resuelven de manera oportuna. (FFIEC seguridad folleto, página 6) | "Fuente: IS.IV.A.2 (d): pg56: La auditoría interna debe realizar un seguimiento de los resultados y la remediación de las deficiencias de control informadas en auditorías y revisiones técnicas adicionales, como las pruebas de penetración y las evaluaciones de vulnerabilidad.<br>IS.WP.2.8: Determine la idoneidad de la cobertura de auditoría y el informe del programa de seguridad de la información mediante la revisión de los informes de auditoría apropiados y las actas de la junta o comité de auditoría.<br>AUD.B.8: Un proceso de evaluación de riesgos para describir y analizar los riesgos inherentes a una determinada línea de negocios.<br>AUD.WP.I.7.1: Determine la idoneidad del plan de auditoría general para proporcionar la cobertura adecuada de los riesgos de TI.<br>MGT.I.B.7 (b): pg19: La administración también debe garantizar una respuesta oportuna y precisa a las inquietudes y excepciones de la auditoría, y garantizar una acción correctiva adecuada y oportuna.<br>MGT.WP.1.2: revise la respuesta de la administración a los problemas planteados durante o después del último examen. Considera lo siguiente: a. Adecuación y oportunidad de la acción correctiva. b. Resolución de causas raíz en lugar de problemas específicos. do. Existencia de cuestiones pendientes. re. Si la administración ha tomado medidas positivas para corregir las excepciones informadas en la auditoría y en los informes de examen. mi. Revisión independiente de la resolución y presentación de informes de la resolución al comité de auditoría.<br>MGT.WP.6.1: Consulte con el examinador que revisa la auditoría o la auditoría de TI para determinar la idoneidad de la cobertura de auditoría de TI y la capacidad de respuesta de la administración ante las debilidades identificadas ". | |
| D1.RM.Au.E.1 | La función de Auditoría independiente valida que la función de administración de riesgo es acorde con el riesgo y la complejidad de la institución. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.Au.E.2 | La función de Auditoría independiente valida que amenaza de la institución intercambio de información es acorde con el riesgo y la complejidad de la institución. | N/A | |
| D1.RM.Au.E.3 | La función de Auditoría independiente valida que la función de controles de seguridad cibernética de la institución es acorde con el riesgo y la complejidad de la institución. | N/A | |
| D1.RM.Au.E.4 | La función de Auditoría independiente valida que la gestión de la relación de la tercera parte de la institución es acorde con el riesgo y la complejidad de la institución. | N/A | |
| D1.RM.Au.E.5 | La función de Auditoría independiente valida que Programa de respuesta a incidentes y recuperación de la institución sean proporcionales a los riesgos y complejidad de la institución. | N/A | |
| D1.RM.Au.Int.1 | Un proceso formal es en lugar de la función de Auditoría independiente actualizar sus procedimientos basados en | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | cambios al perfil de riesgo inherente de la institución. | | |
| D1.RM.Au.Int.2 | La función de Auditoría independiente valida que la información sobre amenazas de la institución y la colaboración son acordes con el riesgo y la complejidad de la institución. | N/A | |
| D1.RM.Au.Int.3 | La función de Auditoría independiente regularmente comentarios sobre declaración de apetito de riesgos de gestión Cibernético. | N/A | |
| D1.RM.Au.Int.4 | Auditoría independientes o comentarios se utilizan para identificar las brechas en las capacidades existentes de seguridad y experiencia. | N/A | |
| D1.RM.Au.A.1 | Un proceso formal es en lugar de la función de Auditoría independiente actualizar sus procedimientos basados en cambios en el paisaje cambiante de la amenaza en el sector. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.RM.Au.A.2 | La función de Auditoría independiente regularmente comentarios sobre declaración de apetito de riesgo de la institución Cibernético en comparación con los resultados de la evaluación e incorpora los vacíos en la estrategia de Auditoría. | N/A | |
| D1.RM.Au.A.3 | Auditoría independientes o comentarios se utilizan para identificar las debilidades de la ciberseguridad, causas y el impacto potencial a unidades de negocio. | N/A | |
| D1.RM.Au.Inn.1 | Un proceso formal es en lugar de la función de Auditoría independiente actualizar sus procedimientos basados en cambios en el paisaje cambiante de la amenaza de otros sectores que depende de la institución. | N/A | |
| D1.RM.Au.Inn.2 | La función de Auditoría independiente utiliza herramientas de minería de datos sofisticados para realizar monitoreo continuo de los procesos de la ciberseguridad o controles. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.R.St.B.1 | Responsabilidades y roles de seguridad de la información han sido identificadas. (FFIEC seguridad folleto, página 7) | "Fuente: IS.II.C.1: pg11: Las políticas, normas y procedimientos guían las decisiones y actividades de los usuarios, desarrolladores, administradores y gerentes e informan a esas personas sobre sus responsabilidades de seguridad de la información. Las políticas, normas y procedimientos también deben Especifique los mecanismos a través de los cuales se pueden cumplir las responsabilidades. Las políticas, estándares y procedimientos que abordan el programa de seguridad de la información deben describir los roles del departamento de seguridad de la información, las líneas de negocios y la organización de TI en la administración del programa de seguridad de la información.<br>MGT.I: pg4: La estructura de gobierno especifica las responsabilidades de la junta directiva, gerentes, auditores y otras partes interesadas, y especifica el nivel de autoridad y la responsabilidad para la toma de decisiones.<br>MGT.WP.2.11: Revise la estructura de la institución para determinar si la junta estableció lo siguiente:<br>a. La estructura organizativa proporciona un soporte de TI efectivo en toda la institución, desde la administración de TI hasta la administración superior y la junta directiva.<br>segundo. Funciones y responsabilidades definidas para puestos clave de TI, incluida la administración ejecutiva (CEO y COO, y con frecuencia CIO o CTO) y CISO.<br>mi. Un puesto de CISO o oficial de seguridad de la información responsable de la administración y mitigación de los riesgos de seguridad de la información " | ID. AM-6: Fuerza de trabajo roles y responsabilidades para funciones de negocios, incluyendo la seguridad cibernética, se establecen. (p. 20) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.R.S.B.2 | Existen procesos para identificar los conocimientos adicionales para mejorar las defensas de seguridad de información. (FFIEC información seguridad Programa de trabajo, objetivo I: 2-8) | "Fuente: IS.IC: pág. 5: La financiación, junto con el talento técnico y de gestión, también contribuye a la eficacia del programa de seguridad de la información. La administración debe proporcionar, y el consejo debe supervisar, la financiación adecuada para desarrollar, implementar y mantener un éxito. programa de seguridad de la información. El programa debe contar con personal suficiente que tenga habilidades que estén alineadas con las necesidades técnicas y de gestión de la institución y que se correspondan con su tamaño, complejidad y perfil de riesgo. El conocimiento de los estándares, prácticas y metodologías de tecnología de la tecnología es particularmente importante Al éxito del programa de seguridad de la información.<br>MGT.I.B.7 (a): pg18: Una institución debe tener programas implementados para garantizar que los miembros del personal tengan la experiencia necesaria para realizar sus trabajos y alcanzar las metas y objetivos de la empresa. Es posible que la institución deba buscar externamente para encontrar la experiencia necesaria para áreas especializadas.<br>MGT.WP.5.2.b: Los empleados tienen las calificaciones adecuadas.<br>MGT.WP.5.5: Determine si la institución financiera tiene un proceso para garantizar que el personal tenga la experiencia necesaria para cumplir con sus funciones. Revisar la idoneidad del proceso ". | |
| D1.R.S.E.1 | Se utiliza un proceso formal para identificar ciberseguridad herramientas y conocimientos que se necesiten. | N/A | |
| D1.R.St.E.2 | Gestión con el conocimiento adecuado y experiencia dirige los esfuerzos de ciberseguridad de la institución. | N/A | Personal posee los conocimientos y habilidades para llevar a cabo sus roles designados y responsabilidades. (p. 10) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.R.St.E.3 | Personal con responsabilidades de ciberseguridad tiene las calificaciones necesarias para realizar las tareas necesarias de la posición. | N/A | "El personal posee el conocimiento y las habilidades para desempeñar sus funciones y responsabilidades designadas (p. 10)<br>PR.AT-5: El personal de seguridad física y de la información entiende los roles y las responsabilidades. (p. 25) " |
| D1.R.St.E.4 | Candidatos de empleo, contratistas y terceros están sujetos a verificación de antecedentes proporcional a la confidencialidad de los datos de acceso, requerimientos de negocio y riesgo aceptable. | N/A | PR.IP-11: La ciberseguridad se incluye en las prácticas de recursos humanos (por ejemplo, reaprovisionamiento, selección de personal). (p. 28) |
| D1.R.S.Int.1 | La institución tiene un Programa para la contratación de talento, retención y sucesión planificación para el personal de seguridad cibernética y la resistencia. | N/A | |
| D1.R.S.A.1 | La institución puntos de referencia su ciberseguridad personal contra sus compañeros para identificar si su reclutamiento, retención y planificación de la sucesión | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.R.S.A.2 | Personal de seguridad cibernética dedicada desarrolla o contribuye al desarrollo, seguridad de nivel empresarial integrada y estrategias de defensa cibernética. | N/A | |
| D1.R.S.Inn.1 | La institución se asocia activamente con asociaciones de la industria y la academia para informar los planes de estudio basan en ciberseguridad futuras necesidades de la industria de personal. | N/A | |
| D1.TC.Tr.B.1 | Se proporciona entrenamiento de seguridad de información anual. (FFIEC seguridad folleto, página 66) | "Fuente: IS.B: pgs4-5: La administración también debe hacer lo siguiente: ... Proporcionar a los empleados capacitación en concientización y seguridad de la información y comunicaciones continuas relacionadas con la seguridad para los empleados, y garantizar que los empleados completen dicha capacitación anualmente.<br>IS.WP.2.5.l: Determine si las responsabilidades de la administración son apropiadas e incluyen lo siguiente: Facilitación de la capacitación anual sobre seguridad de la información y concientización y comunicaciones continuas relacionadas con la seguridad para los empleados.<br>MGT.III.C.2: pg28: La institución debe usar descripciones de trabajo, acuerdos de empleo (generalmente para puestos de mayor nivel o mayor sensibilidad), capacitación y programas de concientización para promover la comprensión y aumentar la responsabilidad individual.<br>MGT.WP.12.5.f: Determine si la administración tiene prácticas efectivas de contratación y capacitación que brinden conciencia de seguridad de la información y programas de capacitación ". | Existe una conciencia de riesgo de seguridad cibernética a nivel organizacional, pero no se ha establecido un acercamiento de toda la organización a administrar los riesgos de la ciberseguridad. (p. 10) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.TC.Tr.B.2 | Información anual de capacitación de seguridad incluye respuesta a incidentes, ciber amenazas actual (por ejemplo, phishing, phishing lanza, ingeniería social y seguridad móvil) y los problemas emergentes. (FFIEC seguridad folleto, página 66) | "Fuente: IS.II.C.7 (e): pg17: Los materiales de capacitación para la mayoría de los usuarios se centran en temas como la seguridad del punto final, los requisitos de inicio de sesión y las pautas de administración de contraseñas. Los programas de capacitación deben incluir escenarios que capturen áreas de importancia y una creciente preocupación, como intentos de phishing e ingeniería social, pérdida de datos a través de correo electrónico o medios extraíbles, o publicación no intencional de información confidencial o de propiedad exclusiva en las redes sociales.<br>IS.WP.6.8.f: Determine si la administración mitiga efectivamente los riesgos planteados por los usuarios. Revise si la administración hace lo siguiente: Brinda capacitación para respaldar el conocimiento y el cumplimiento de políticas " | PR. AT-1: Todos los usuarios son informados y capacitados. (p. 24) |
| D1.TC.Tr.B.3 | Materiales de conocimiento de la situación a disposición a los empleados cuando se le solicite por eventos Cibernético visibles o por avisos reglamentarios. (FFIEC seguridad folleto, página 7) | "Fuente: IS.II.C.7 (e): pg17 :: Los materiales de capacitación para la mayoría de los usuarios se centran en temas como la seguridad del punto final, los requisitos de inicio de sesión y las pautas de administración de contraseñas.<br>Los programas de capacitación deben incluir escenarios que capturen áreas de preocupación significativa y creciente, como intentos de phishing e ingeniería social, pérdida de datos a través de correo electrónico o medios extraíbles, o publicación no intencional de información confidencial o patentada en las redes sociales. A medida que el entorno de riesgo cambia, también debería hacerlo la capacitación.<br>IS.WP.6.8.f: Determine si la administración mitiga efectivamente los riesgos planteados por los usuarios. Revise si la administración hace lo siguiente: Brinda capacitación para respaldar el conocimiento y el cumplimiento de políticas " | Información de seguridad cibernética se comparte dentro de la organización de manera informal. (p. 10) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.TC.Tr.B.4 | Materiales de conocimiento de cliente están disponibles (por ejemplo, materiales del mes de concientización sobre seguridad cibernética DHS). (Programa de trabajo de E-Banking FFIEC, objetivo 6-3) | "Fuente: IS.II.C.16: pg36: Más allá de la autenticación, los controles de acceso remoto deben incluir controles de seguridad en capas adicionales y pueden incluir alguna combinación de lo siguiente: Educación del cliente para aumentar el conocimiento del riesgo de fraude y técnicas efectivas que los clientes pueden usar para mitigar el riesgo.<br>IS.II.C.16 (a): pág. 37: los esfuerzos de concienciación y educación de los clientes de la institución deben tener en cuenta a los titulares de cuentas comerciales y minoristas.<br>IS.WP.6.26: Determine si la gerencia desarrolla el conocimiento del cliente y los esfuerzos educativos que abordan tanto a los titulares de cuentas minoristas (consumidores) como comerciales. | PR. AT-3: Actores de terceros (proveedores, clientes, socios) comprenden roles y responsabilidades. (p. 24) |
| D1.TC.Tr.E.1 | La institución tiene un Programa de ciberseguridad formación continua y desarrollo de habilidades para el personal de seguridad cibernética. | N/A | |
| D1.TC.Tr.E.2 | Gestión se proporciona entrenamiento de ciberseguridad pertinente a sus responsabilidades de trabajo. | N/A | "Existe una conciencia del riesgo de ciberseguridad a nivel organizativo, pero no se ha establecido un enfoque de toda la organización para gestionar el riesgo de ciberseguridad (p. 10)<br><br>PR.AT-4: Los ejecutivos senior entienden los roles y responsabilidades. (p. 24) " |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.TC.Tr.E.3 | Empleados con permisos de la cuenta privilegiada reciben capacitación adicional sobre ciberseguridad acorde con sus niveles de responsabilidad. | N/A | "PR.AT-2: Los usuarios privilegiados entienden los roles y las responsabilidades. (Pág. 24)<br>PR.AT-5: El personal de seguridad física y de la información entiende los roles y las responsabilidades. (p. 25) " |
| D1.TC.Tr.E.4 | Unidades de negocios disponen de ciberseguridad formación pertinente a los riesgos de su negocio particular. | N/A | |
| D1.TC.Tr.E.5 | La institución valida la efectividad de la capacitación (por ejemplo, ingeniería social o pruebas de phishing). | N/A | |
| D1.TC.Tr.Int.1 | Gestión incorpora lecciones de ingeniería social y phishing ejercicios para mejorar los Programas de sensibilización de empleados. | N/A | Adaptar las prácticas de seguridad cibernética basadas en lecciones aprendidas e indicadores predictivos derivan de las actividades anteriores y actuales de la ciberseguridad. (p. 11) |
| D1.TC.Tr.Int.2 | Ciberseguridad conciencia información se proporciona a los clientes minoristas y clientes comerciales por lo menos anualmente. | N/A | PR.AT-3: Las partes interesadas de terceros (proveedores, clientes, socios) entienden los roles y las responsabilidades. (p. 24) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.TC.Tr.Int.3 | Unidades de negocios disponen de ciberseguridad formación pertinente para los riesgos de negocio particular, más allá de lo que se requiere de la institución como un todo. | N/A | |
| D1.TC.Tr.Int.4 | La institución actualiza regularmente su entrenamiento al personal de seguridad para adaptarse a las nuevas amenazas. | N/A | |
| D1.TC.Tr.A.1 | Directores independientes cuentan con formación de ciberseguridad que se ocupa de complejos productos, servicios y líneas de negocio afectan el riesgo de Cibernético de la institución. | N/A | |
| D1.TC.Tr.Inn.1 | Indicadores clave de rendimiento se utilizan para determinar si los Programas de formación y sensibilización positivamente influyen en el comportamiento. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.TC.Cu.B.1 | Gestión tiene a empleados responsables de cumplir con el Programa de seguridad de la información. (FFIEC seguridad folleto, página 7) | "Fuente: IS.II.C.7 (e): pg17: La gerencia debe responsabilizar a todos los empleados, funcionarios y contratistas por el cumplimiento de las políticas de seguridad y uso aceptable, y debe garantizar que la información de la institución y otros activos estén protegidos.<br>MGT.III.C.2: pg28: La administración debe requerir el reconocimiento periódico de las políticas de uso aceptable para la red, aplicaciones de software, Internet, correo electrónico, datos confidenciales y redes sociales. Los programas de concientización y capacitación sobre seguridad de la información ayudan a respaldar la seguridad de la información y otras políticas de gestión.<br>MGT.WP.12.5: Determine si la administración tiene prácticas efectivas de contratación y capacitación que incluyen lo siguiente:<br>re. Requerir el reconocimiento periódico de las políticas de uso aceptable.<br>mi. Obtención de acuerdos firmados de confidencialidad y no divulgación.<br>F. Proporcionar programas de sensibilización y capacitación en seguridad de la información. | ID. AM-6: Fuerza de trabajo roles y responsabilidades para funciones de negocios, incluyendo la seguridad cibernética, se establecen. (p. 20) |
| D1.TC.Cu.E.1 | La institución cuenta con normas formales de conducta que responsabilizar a todos los empleados para cumplir con los procedimientos y las políticas de seguridad cibernética. | N/A | Administra el riesgo de la seguridad cibernética a través de un enfoque de toda la organización con políticas basadas en el riesgo, los procesos y procedimientos para enfrentar posibles eventos de ciberseguridad. (p. 11) |
| D1.TC.Cu.E.2 | Riesgos cibernéticos se discuten activamente en las reuniones de unidad de negocio. | N/A | |
| D1.TC.Cu.E.3 | Los empleados tienen una clara comprensión de cómo identificar y escalar potenciales cuestiones de ciberseguridad. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D1.TC.Cu.Int.1 | Gestión asegura planes de rendimiento están vinculados al cumplimiento de normas y políticas de seguridad cibernética con el fin de responsabilizar a los empleados. | N/A | |
| D1.TC.Cu.Int.2 | La cultura de riesgo requiere consideración formal de riesgos cibernéticos en todas las decisiones de negocios. | N/A | Fomentar la gestión de riesgos de ciberseguridad como parte de la cultura. (p. 11) |
| D1.TC.Cu.Int.3 | Informes de riesgo de Cibernético es presentado y discutido en las reuniones de gestión de riesgo independiente. | N/A | |
| D1.TC.Cu.A.1 | Gestión asegura la mejora continua de la conciencia cultural de riesgo cibernético. | N/A | Fomentar la gestión de riesgos de ciberseguridad como parte de la cultura. (p. 11) |
| D1.TC.Cu.Inn.1 | La institución dirige los esfuerzos para promover la cultura de seguridad cibernética en todo el sector y otros sectores que dependen de ellos. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.TI.Ti.B.1 | La institución pertenece o se suscribe a una fuente que proporciona información sobre las amenazas (por ejemplo, intercambio de información de servicios financieros y el centro de análisis [FS-ISAC], [[US Computer Emergency Readiness Team de intercambio de información amenaza y vulnerabilidad US-CERT]). (FFIEC E - Banking Programa de trabajo, página 28) | "Fuente: IS.II.C: pg11: La administración también debe obtener, analizar y responder a la información de varias fuentes (por ejemplo, Centro de Análisis e Intercambio de Información de Servicios Financieros [FS-ISAC]) sobre amenazas cibernéticas y vulnerabilidades que pueden afectar la institución.<br>IS.WP.8.3.f: Determine si la administración tiene procesos efectivos de identificación y evaluación de amenazas, incluidos los siguientes: Desarrollar procesos apropiados para evaluar y responder a la información de vulnerabilidad de grupos externos o individuos.<br>MGT.III.A: pg22: La participación en un foro de intercambio de información, como FS-ISAC, debe ser un componente del proceso de identificación de riesgos porque compartir información puede ayudar a la institución a identificar y evaluar amenazas y vulnerabilidades de seguridad cibernética relevantes.<br>MGT.WP.10.1.b: Determine si la administración participa en un foro de intercambio de información (como FS-ISAC) ". | La organización entiende sus dependencias y socios y recibe información de los socios que permite la colaboración y las decisiones de gestión de riesgo dentro de la organización en respuesta a eventos. ID. (p. 10) RA-2: Se recibe información de amenaza y la vulnerabilidad de fuentes y foros de intercambio de información. (p. 22) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.TI.Ti.B.2 | Información de la amenaza se utiliza para controlar las amenazas y vulnerabilidades. (FFIEC seguridad folleto, página 83) | "Fuente: IS.III.A: pg47: La gerencia debe desarrollar procedimientos para obtener, monitorear, evaluar y responder a la evolución de la información sobre amenazas y vulnerabilidades. La identificación de amenazas involucra las fuentes de amenazas, sus capacidades y sus objetivos. Información sobre las amenazas generalmente provienen del gobierno (por ejemplo, US-CERT), organizaciones de intercambio de información (por ejemplo, FS-ISAC), fuentes de la industria, la institución y terceros. IS.WP.8.3.f: Determine si la administración tiene procesos efectivos de identificación y evaluación de amenazas, incluidos los siguientes: Desarrollar procesos apropiados para evaluar y responder a la información de vulnerabilidad de grupos externos o individuos. MGT.I.A.2: pg6: Establezca un proceso formal para obtener, analizar y responder a la información sobre amenazas y vulnerabilidades mediante el desarrollo de un programa repetible de inteligencia y colaboración sobre amenazas. MGT.WP.2.8.f: establece un proceso formal para obtener, analizar y responder a la información sobre amenazas y vulnerabilidades mediante el desarrollo de un programa de colaboración e inteligencia de amenazas repetible. MGT.III.C.3: pg29: La administración de la institución debe: Desarrollar e implementar un proceso de inteligencia y colaboración sobre amenazas para identificar y responder a la información sobre amenazas y vulnerabilidades. MGT.WP.12.8.c: Determine si la estructura de control incluye: Usar un proceso de colaboración e inteligencia de amenazas para identificar y responder a la información sobre amenazas y vulnerabilidades ". | ID. RA-1: Activos vulnerabilidades son identificadas y documentadas. (p. 22) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.TI.Th.B.3 | Información de la amenaza se utiliza para mejorar los controles e interno Gestión de riesgos. (FFIEC seguridad folleto, página 4) | Fuente: es. III. A:PG48: Una vez se identifica una amenaza y se evalúan las vulnerabilidades potenciales, la importancia de la amenaza debe provocar una respuesta. La respuesta debe ser acorde con el riesgo que plantea la amenaza y debe incluir las opciones de remediación. Administración debe diseñar políticas para permitir amenazas inmediatas y emergentes para tratarse rápidamente, mientras que las amenazas menos importantes se tratan como parte de un proceso más amplio de gestión de riesgo. Cuando gestión recibe información sobre la vulnerabilidad de grupos o individuos externos, gestión debería tener procesos adecuados y procedimientos para evaluar la credibilidad de la información para abordarlo adecuadamente. ES. WP.8.3.a.d: Determinar si la gestión tiene procesos identificación y evaluación de la amenaza efectiva, incluyendo las siguientes: mantener los procedimientos para obtención, supervisión, evaluación y respuesta a la evolución de la amenaza y la vulnerabilidad de la información .. . Uso conocimiento de amenaza a la evaluación de riesgos de la unidad un. | Priorización de las actividades de la ciberseguridad es informada directamente por objetivos de riesgo organizacional, el ambiente de amenaza o requisitos de misión de negocios. (p. 10) |
| D2.TI.Ti.E.1 | Información de la amenaza recibida por la institución incluye análisis de tácticas, pautas y recomendaciones de mitigación de riesgo. | N/A | |
| D2.TI.Th.Int.1 | Un Programa de inteligencia de amenaza formal se lleva a cabo y cuenta con suscripción a los feeds de la amenaza de los proveedores externos y fuentes internas. | N/A | La organización entiende sus dependencias y socios y recibe información de los socios que permite la colaboración y las decisiones de gestión de riesgo dentro de la organización en respuesta a eventos. (p. 10) |
| D2.TI.Ti.Int.2 | Se implementan protocolos de recogida de información de colegas del sector y del gobierno. | N/A | |
| D2.TI.Ti.Int.3 | Se mantiene un repositorio central, de sólo lectura de la inteligencia de amenazas | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.TI.Ti.A.1 | Un modelo de inteligencia cibernética se utiliza para recopilar información sobre una amenaza. | N/A | |
| D2.TI.Ti.A.2 | Información sobre amenazas automáticamente se recibe de múltiples fuentes en tiempo real. | N/A | |
| D2.TI.Ti.A.3 | Información sobre amenazas de la institución incluye información relacionada a eventos geopolíticos que podrían aumentar los niveles de amenazas de ciberseguridad. | N/A | |
| D2.TI.Ti.Inn.1 | Un sistema de análisis de amenaza correlaciona automáticamente datos de amenazas a riesgos específicos y luego toma acciones automatizadas basadas en riesgo y gestión de alertas. | N/A | |
| D2.TI.Ti.Inn.2 | La institución invierte en el desarrollo de nuevos amenaza de inteligencia y colaboración mecanismos (por ejemplo, tecnologías, procesos de negocio) que va a transformar cómo información es reunida y compartida. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.MA.Ma.B.1 | Registros de Auditoría y otros registros de sucesos de seguridad se revisan y conservan de forma segura. (FFIEC seguridad folleto, página 79) | "Fuente: IS.II.C.22: pg44: La administración debe tener políticas efectivas de retención de registros que aborden la importancia de mantener registros para las necesidades de respuesta y análisis de incidentes ... Además, las prácticas de registro deben ser revisadas periódicamente por una parte independiente para asegurar que sean apropiadas gestión de registros ... Independientemente del método de administración de registros, la administración debe desarrollar procesos para recopilar, agregar, analizar y correlacionar información de seguridad. IS.WP.6.35: Determine si la administración tiene un proceso de administración de registro efectivo que involucre un repositorio de registro central, la transmisión oportuna de archivos de registro y un análisis de registro efectivo " | PR. PT-1: Registros de Auditoría son determinados, documentados, implementados y revisados de acuerdo con la política. (p. 29) |
| D2.MA.Ma.B.2 | Registros de eventos de ordenador sirven para investigaciones una vez ha ocurrido un evento. (FFIEC seguridad folleto, página 83) | "Fuente: IS.II.C.22: pg44: los archivos de registro son críticos para la investigación y el procesamiento de incidentes de seguridad y pueden potencialmente contener información confidencial ... Los sistemas de gestión de eventos e información de seguridad (SIEM) pueden proporcionar un método para que la administración los recopile, agregue, analice y correlacione información de sistemas y aplicaciones discretas. La administración puede utilizar los sistemas SIEM para discernir tendencias e identificar posibles incidentes de seguridad de la información. IS.WP.6.35: Determine si la administración tiene un proceso de administración de registro efectivo que involucre un repositorio de registro central, la transmisión oportuna de archivos de registro y un análisis de registro efectivo. Revise si la administración tiene lo siguiente: (d) Procesos para recopilar, agregar, analizar y correlacionar efectivamente la información de eventos de seguridad de sistemas y aplicaciones discretas ". | PR. PT-1: Registros de Auditoría son determinados, documentados, implementados y revisados de acuerdo con la política. (p. 29) |
| D2.MA.Ma.E.1 | Se implementa un proceso para monitorear información de amenaza para descubrir amenazas emergentes. | N/A | ID.RA-3: Se identifican y documentan las amenazas a los activos de la organización. (p. 22) |
| D2.MA.Ma.E.2 | El proceso de información y análisis de amenaza se asigna a un grupo específico o individuo. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.MA.Ma.E.3 | Tecnología y procesos de seguridad centralizadas y coordinadas en un centro de operaciones de seguridad (SOC) o equivalente. | N/A | |
| D2.MA.Ma.E.4 | Sistemas de vigilancia funcionan continuamente con un soporte adecuado para la eficiente gestión de incidentes. | N/A | ID.RA-3: Se identifican y documentan las amenazas a los activos de la organización. (p. 22) |
| D2.MA.Ma.Int.1 | Un equipo de inteligencia de amenaza está en el lugar que evalúa la inteligencia de la amenaza de múltiples fuentes de credibilidad, relevancia y exposición. | N/A | |
| D2.MA.Ma.Int.2 | Se crea un perfil para cada amenaza que identifica la probable intención, capacidad y objetivo de la amenaza. | N/A | ID.RA-3: Se identifican y documentan las amenazas a los activos de la organización. (p. 22) |
| D2.MA.Ma.Int.3 | Fuentes de información sobre una amenaza que abordan todos los componentes del perfil de amenaza son priorizados y monitoreados. | N/A | |
| D2.MA.Ma.Int.4 | Inteligencia de amenaza se analiza para elaborar resúmenes de la amenaza de Cibernético incluyendo riesgos para la institución y | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | acciones específicas para la institución a tener en cuenta. | | |
| D2.MA.Ma.A.1 | Existe un Comité de identificación y análisis de amenaza cibernética dedicada o equipo para centralizar y coordinar las iniciativas y las comunicaciones. | N/A | |
| D2.MA.Ma.A.2 | Se han definido procesos formales para resolver posibles conflictos en la información recibida de los centros de intercambio y análisis u otras fuentes. | N/A | |
| D2.MA.Ma.A.3 | Surgiendo la amenaza interna y externa de inteligencia y análisis de correlación de logs sirven para predecir futuros ataques. | N/A | |
| D2.MA.Ma.A.4 | Información sobre amenazas es visto dentro del contexto del perfil de riesgo y apetito por el riesgo para priorizar acciones de mitigación en previsión de amenazas de la institución. | N/A | |
| D2.MA.Ma.A.5 | Información sobre amenazas se utiliza para actualizar normas de arquitectura y | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | configuración. | | |
| D2.MA.Ma.Inn.1 | La institución utiliza múltiples fuentes de inteligencia, análisis de correlación de logs, alertas, flujos de tráfico interno y eventos geopolíticos para predecir posibles futuros ataques y atacar a las tendencias. | N/A | |
| D2.MA.Ma.Inn.2 | Escenarios de riesgo más alto se utilizan para predecir las amenazas contra los objetivos específicos del negocio. | N/A | |
| D2.MA.Ma.Inn.3 | Sistemas automáticamente detectan debilidades de configuración basadas en la gestión de inteligencia y alerta de amenaza así que acciones pueden priorizarse. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.IS.Is.B.1 | Las amenazas de seguridad de la información y se comparte con empleados internos aplicables. (FFIEC seguridad folleto, página 83) | "Fuente: IS.II.D: pg45: El informe de riesgos es un proceso que produce informes de sistemas de información que abordan amenazas, capacidades, vulnerabilidades y cambios de riesgos inherentes. Los informes de riesgos deben describir los eventos de seguridad de la información que enfrenta la institución y la efectividad de La respuesta de la administración y la resistencia a esos eventos. El proceso de presentación de informes debe proporcionar un método para difundir esos informes a los miembros apropiados de la administración. El contenido de los informes debe impulsar la acción, si es necesario, de manera oportuna para mantener niveles adecuados de riesgo.<br>IS.WP.7.1: Determine si la institución tiene procesos de monitoreo y reporte de riesgos que abordan las condiciones cambiantes de amenaza tanto en la institución como en la industria financiera en general. Determine si estos procesos abordan los eventos de seguridad de la información que enfrenta la institución, la efectividad de la respuesta de la administración y la resistencia de la institución a esos eventos. Revise si el proceso de informes incluye un método para difundir esos informes a los miembros apropiados de la gerencia ". | PR. IP-8: Eficacia de las tecnologías de protección es compartida con personas apropiadas. (p. 28) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.IS.Is.B.2 | Información de contacto de la aplicación de la ley y el regulador se mantiene y actualiza periódicamente. (FFIEC continuidad del negocio planificación de Programa de trabajo, objetivo I: 5 - 1) | "Fuente: BCP.WP.I.5.1: Incluye (s) planes de preparación para emergencias y manejo de crisis que ... Incluyen un árbol de contactos preciso, así como información de contacto principal y de emergencia, para comunicarse con los empleados, proveedores de servicios, proveedores, reguladores, Autoridades municipales, y personal de respuesta a emergencias.<br>IS.III.D: pg.51: Las consideraciones principales para la respuesta a incidentes incluyen lo siguiente: Protocolos para definir cuándo y bajo qué circunstancias notificar e involucrar a los reguladores, clientes y autoridades policiales, incluidos los nombres y la información de contacto de cada grupo.<br>MGT.III.C.3: pg29: Desarrolle una política para escalar e informar los incidentes de seguridad a la junta, a las agencias gubernamentales, a las autoridades policiales y al principal regulador federal y estatal de la institución según los umbrales definidos por la institución financiera y los requisitos legales aplicables. Los umbrales relevantes podrían incluir un impacto financiero significativo, un tiempo de inactividad operacional significativo, una falla operativa o del sistema, o la pérdida de infraestructura crítica.<br>MGT.WP.12.8.i: Desarrollar una política para escalar e informar los incidentes de seguridad a la junta, a las agencias gubernamentales, a las autoridades policiales y a los reguladores primarios federales y estatales de la institución según los umbrales definidos por la institución financiera ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.IS.Is.B.3 | Información sobre amenazas es compartida con la aplicación de la ley y reguladores cuando lo requiera o se le solicite. (FFIEC seguridad folleto, Página 84) | "Fuente: IS.III.D: pg.51: Las consideraciones principales para la respuesta a incidentes incluyen lo siguiente: Cómo, cuándo y qué comunicar fuera de la institución, ya sea a la policía, las agencias reguladoras, las organizaciones de intercambio de información, los clientes, Proveedores de servicios de terceros, víctimas potenciales u otros.<br>MGT.III.C.3: pg29: Desarrolle una política para escalar e informar los incidentes de seguridad a la junta, a las agencias gubernamentales, a las autoridades policiales y al principal regulador federal y estatal de la institución según los umbrales definidos por la institución financiera y los requisitos legales aplicables. Los umbrales relevantes podrían incluir un impacto financiero significativo, un tiempo de inactividad operacional significativo, una falla operativa o del sistema, o la pérdida de infraestructura crítica.<br>MGT.WP.12.8.i: Desarrollar una política para escalar e informar los incidentes de seguridad a la junta, a las agencias gubernamentales, a las autoridades policiales y a los reguladores primarios federales y estatales de la institución según los umbrales definidos por la institución financiera ". | |
| D2.IS.Is.E.1 | Un proceso formal y seguro está en el lugar para compartir información de amenaza y vulnerabilidad con otras entidades. | N/A | |
| D2.IS.Is.E.2 | Un representante de la institución participa en la aplicación de la ley o el intercambio de información organización reuniones. | N/A | PR.IP-8: La efectividad de las tecnologías de protección se comparte con las partes apropiadas. (p. 28) |
| D2.IS.Is.Int.1 | Es un protocolo formal para compartir la amenaza, la vulnerabilidad y el incidente de información a empleados basados en su función específica. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.IS.Is.Int.2 | Acuerdos de intercambio de información se utilizan según sea necesario o requeridos para facilitar compartir información amenaza con otros organismos del sector financiero o de terceros. | N/A | "ID.GV-3: los requisitos legales y reglamentarios relacionados con la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles, se comprenden y gestionan (pág. 21)<br>DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables. (p. 32)<br>Perfil del marco: identifique y aborde las implicaciones de la privacidad individual y las libertades civiles que pueden resultar de las operaciones de ciberseguridad (p. 15)<br>Gobernanza del riesgo de ciberseguridad. Identificación y autorización de acceso.<br>Medidas de sensibilización y formación.<br>Detección de actividad anómala revisada por cuestiones de privacidad.<br>Revisión del intercambio de información personal dentro y fuera de la organización ". |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.IS.Is.Int.3 | Información se comparte de forma proactiva con la industria, aplicación de la ley, los reguladores y foros de intercambio de información. | N/A | Compartir activamente información con socios para asegurar que la información precisa y actual está siendo distribuido y consumido para mejorar la ciberseguridad antes de que ocurra un evento de seguridad cibernética. (p. 11) |
| D2.IS.Is.Int.4 | Un proceso es para comunicarse y colaborar con el sector público con respecto a las amenazas cibernéticas. | N/A | |
| D2.IS.Is.A.1 | Gestión comunica información sobre amenazas con contexto de riesgo empresarial y recomendaciones de manejo de riesgo específico para las unidades de negocio. | N/A | |
| D2.IS.Is.A.2 | Existen relaciones con los empleados de las instituciones pares para compartir información sobre amenazas cibernética. | N/A | |
| D2.IS.Is.A.3 | Se ha establecido una red de relaciones de confianza (formales o informales) para evaluar la información sobre las amenazas cibernéticas. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D2.IS.Is.Inn.1 | Un mecanismo está en el lugar para compartir información sobre amenazas Cibernético con unidades de negocio en tiempo real, incluyendo el posible impacto financiero y operativo de la inacción. | N/A | |
| D2.IS.Is.Inn.2 | Un sistema informa automáticamente la gestión de nivel de riesgo del negocio específico de la institución y el avance de pasos recomendados para mitigar los riesgos. | N/A | |
| D2.IS.Is.Inn.3 | La institución es líder en esfuerzos para crear nueva información sectorial - compartir canales vacíos de dirección en los mecanismos de intercambio de información exteriores. | N/A | |
| D3.PC.Im.B.1 | Se utilizan herramientas de defensa de perímetro de red (por ejemplo, frontera router y firewall). (FFIEC seguridad folleto, página 33) | "Fuente: IS.II.C.9: pg19: Las herramientas utilizadas para imponer y detectar la protección perimetral incluyen enrutadores, cortafuegos, sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos, proxis, pasarelas, cajas de salto, zonas desmilitarizadas, redes privadas virtuales (VPN), LAN virtuales (VLAN), sistemas de monitoreo de registro e inspección de tráfico de red, sistemas de prevención de pérdida de datos (DLP) y listas de control de acceso.<br>IS.WP.8.1.a: Determine si las actividades de operaciones de seguridad de la institución incluyen lo siguiente: Software de seguridad y administración de dispositivos (por ejemplo, mantenimiento de firmas en dispositivos basados en firmas y reglas de firewall). " | PR. AC-5: Integridad de la red está protegida, incorporando la segregación de la red en su caso. PR (p. 24) PT-4: Redes de comunicaciones están aseguradas. (p. 29) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.B.2 | Sistemas que son accesibles desde Internet o por partes externas están protegidos por firewalls o dispositivos similares. (FFIEC seguridad folleto, página 46) | "Fuente: IS.II.C.17: pg39: Proteja las aplicaciones web o de Internet a través de controles adicionales, incluidos los firewalls de aplicaciones web, el análisis regular de vulnerabilidades nuevas o recurrentes, la mitigación o la remediación de las debilidades de seguridad comunes y la segregación de la red para limitar Acceso inapropiado o conexiones a la aplicación u otras áreas de la red.<br>IS.WP.6.27 (g): revise si las aplicaciones en uso ofrecen las siguientes capacidades: Proteja las aplicaciones web o de Internet a través de controles adicionales, que incluyen firewalls de aplicaciones web, análisis regulares de vulnerabilidades nuevas o recurrentes, mitigación o remediación de las debilidades comunes de seguridad , y segregación de la red.<br>OPS.B.23: Los controles de transmisión deben abordar tanto los riesgos físicos como los lógicos. En instituciones grandes y complejas, la administración debe considerar segregar los segmentos de redes de área amplia (WAN) y redes de área local (LAN) con firewalls que restringen el acceso, así como el contenido del tráfico entrante y saliente.<br>OPS.WP.8.1: Determine si la administración ha implementado controles y procesos operativos diarios apropiados que incluyan ... la alineación de la arquitectura y el proceso de telecomunicaciones con el plan estratégico.<br>MGT.III.C.3: pg29: realizar la diligencia debida inicial y el monitoreo continuo para comprender completamente los tipos de conexiones y los controles de mitigación existentes entre la institución financiera y sus proveedores externos ". | |
| D3.PC.Im.B.3 | Todos los puertos son monitoreados. (FFIEC seguridad folleto, página 50) | Fuente IS.II.C.12: pg26: Monitoreo de puertos para identificar conexiones de red no autorizadas.<br>IS.II.C.16: pg37: Para prevenir o minimizar la exposición a estos incidentes, la administración debe hacer lo siguiente: Limitar el tráfico (por ejemplo, permitir el tráfico válido y bloquear el tráfico mal conocido por puerto o dirección IP) | |
| D3.PC.Im.B.4 | Hasta la fecha se utilizan herramientas antivirus y anti-malware. (FFIEC seguridad folleto, página 78) | "Fuente: IS.II.C.12: pg26: La administración debe implementar la defensa en profundidad para proteger, detectar y responder al malware. La institución puede usar muchas herramientas para bloquear el malware antes de que entre al entorno y para detectar y detectar Responde si no está bloqueado.<br>IS.WP.6.17: Determine si la administración ha implementado la defensa en profundidad para proteger, detectar y responder al malware ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.B.5 | Configuraciones de sistemas (para servidores, computadoras, routers, etc.) siguen las normas de la industria y se aplican. (FFIEC seguridad folleto, página 56) | "Fuente: IS.II.C.10 (c): pg23: La institución debe usar compilaciones estándar, que permiten que una configuración documentada se aplique a múltiples computadoras de manera controlada.<br>IS.WP.6.14: Determine si la administración utiliza compilaciones estándar, permitiendo que una configuración documentada se aplique a múltiples computadoras de manera controlada, para crear inventarios de hardware y software, actualizar o parchar sistemas, restaurar sistemas, investigar anomalías y auditar configuraciones. " | PR. IP-1: Una configuración Base tecnología industrial control de sistemas de información es creada y mantenida. (p. 26) |
| D3.PC.Im.B.6 | Puertos, funciones, protocolos y servicios están prohibidos si ya no es necesario para fines comerciales. (FFIEC seguridad folleto, página 50) | "Fuente: IS.II.C.10 (b): pg23: El endurecimiento puede incluir las siguientes acciones: ... Determinar el propósito de las aplicaciones y sistemas y documentar los requisitos y servicios mínimos de software y hardware que se incluirán. Instalación del hardware mínimo, software y servicios necesarios para cumplir los requisitos mediante un procedimiento de instalación documentado.<br>IS.B.6.13: Determine si la administración tiene procesos para fortalecer las aplicaciones y los sistemas (por ejemplo, instalando servicios mínimos, instalando los parches necesarios, configurando las configuraciones de seguridad adecuadas, aplicando el principio de privilegios mínimos, cambiando las contraseñas predeterminadas y habilitando el registro} ". | |
| D3.PC.Im.B.7 | Acceso a realizar cambios en configuraciones de sistemas (incluyendo máquinas virtuales y los hipervisores) es controlado y supervisado. (FFIEC seguridad folleto, página 56) | "Fuente: IS.II.C.10: pg21: La institución debe tener un proceso eficaz para introducir cambios en las aplicaciones y el sistema, incluidos los dispositivos de hardware, software y red, en el entorno de TI ... Consideraciones de control de la aplicación y del sistema para introducir cambios en el entorno de TI antes de la implementación debe incluir lo siguiente ... Restricción de cambios a usuarios autorizados.<br>IS.WP.6.11: Determine si la administración tiene un proceso para introducir cambios en el entorno (por ejemplo, la administración de la configuración de los sistemas y aplicaciones de TI, el fortalecimiento de los sistemas y las aplicaciones, el uso de compilaciones estándar y la administración de parches) de manera controlada ". | PR. AC-1: Identidades y credenciales son gestionadas por los usuarios y los dispositivos autorizados. PR (p. 23) MA-2: Mantenimiento remoto de activos de la organización es aprobado, registrado y realizado de una manera que impide el acceso no autorizado (p. 28) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.B.8 | Programas que pueden reemplazar el sistema objeto, red, máquina virtual y controles de aplicación están restringidos. (FFIEC seguridad folleto, página 41) | "Fuente: IS.II.C.15 (a): pg32: Los administradores de sistemas y seguridad deben restringir y monitorear el acceso privilegiado a los sistemas operativos y utilidades del sistema.<br>IS.WP.6.21: Como parte del proceso de la administración para asegurar el sistema operativo y todos los componentes del sistema, determine si la administración hace lo siguiente: Limita el número de empleados con acceso al sistema operativo y las utilidades del sistema y otorga solo el nivel mínimo de acceso requerido para desempeñar responsabilidades de trabajo ". | |
| D3.PC.Im.B.9 | Sesiones del sistema están bloqueadas después de un período predefinido de inactividad y se terminaron después de que se cumplan las condiciones previamente definidas. (FFIEC seguridad folleto, página 23) | Fuente: IS.II.C.16: pg36: Más allá de la autenticación, los controles de acceso remoto deben incluir controles de seguridad en capas adicionales y pueden incluir alguna combinación de lo siguiente: Tiempos de espera de la aplicación con re-autenticación obligatoria. | |
| D3.PC.Im.B.10 | Entornos de red inalámbricos requieren configuración de seguridad con cifrado fuerte para la autenticación y transmisión. (* N/A si hay no hay redes inalámbricas.) (FFIEC seguridad folleto, página 40) | "Fuente: IS.II.C.9 (a): pg20: La gerencia debe utilizar un nivel de cifrado aceptado por la industria con una fortaleza acorde con el perfil de riesgo de la institución en las redes inalámbricas de la institución.<br>IS.II.C.9 (a): pg21: las instituciones a menudo proporcionan conectividad de red remota para empleados o proveedores de servicios externos que no están ubicados dentro o alrededor de las instalaciones de la institución. Esta conectividad presenta ventajas operativas, pero se deben tomar medidas para garantizar que la conexión esté cifrada y segura. "Las conexiones VPN deben usarse tanto para redes de banda ancha como para conexiones inalámbricas de tarjeta de aire para aislar y cifrar el tráfico remoto a las redes de la institución". | |
| D3.PC.Im.E.1 | Hay un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y redes internas. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.E.2 | Sistemas de detección/prevención de intrusiones y antivirus (IDS/IPS) detectan y bloquean ataques reales e intentados o intrusiones. | N/A | |
| D3.PC.Im.E.3 | Controles técnicos evitar que dispositivos no autorizados, incluyendo red inalámbrica a dispositivos y medios extraíbles, conectarse a las redes internas. | N/A | PR.PT-2: Los medios extraíbles están protegidos y su uso está restringido de acuerdo con una política específica. (p. 29) |
| D3.PC.Im.E.4 | Una solución basada en el riesgo está en su lugar en la institución o proveedor de hosting de Internet para mitigar ciberataques disruptivo (p. ej., ataques de DDoS). | N/A | PR.DS-4: Capacidad adecuada para asegurar que se mantenga la disponibilidad. (p. 25) |
| D3.PC.Im.E.5 | Redes inalámbricas huésped son completamente separadas de las redes internas. (* N/A si hay no hay redes inalámbricas.) | N/A | |
| D3.PC.Im.E.6 | Dominio nombre sistema Security Extensiones (DNSSEC) es desplegado en toda la empresa. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.E.7 | Sistemas críticos soportados por tecnologías heredadas son revisados regularmente para identificar vulnerabilidades potenciales, oportunidades de actualización o nuevas capas de defensa. | N/A | |
| D3.PC.Im.E.8 | Controles para los sistemas son implementados y probados. | N/A | |
| D3.PC.Im.Int.1 | La red empresarial está segmentada en múltiples, zonas de confianza y de seguridad separada con estrategias de defensa en profundidad (por ejemplo, segmentación de la red lógica, duro copias de seguridad, separaciones de aire) para mitigar ataques. | N/A | "PR.AC-5: La integridad de la red está protegida, incorporando segregación de red cuando sea apropiado. (P. 24)<br>PR.PT-4: Redes de comunicaciones seguras. (p. 29) " |
| D3.PC.Im.Int.2 | Controles de seguridad se utilizan para el acceso remoto a todas las consolas administrativas, incluidos los sistemas virtuales restringidos. | N/A | PR.AC-3: Se gestiona el acceso remoto. (p. 23) |
| D3.PC.Im.Int.3 | Entornos de red inalámbricos tienen firewalls perimetrales que son puesto en ejecución y configurados para restringir el tráfico no autorizado. (* N/A si hay | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | no hay redes inalámbricas.) | | |
| D3.PC.Im.Int.4 | Las redes inalámbricas utilizan el cifrado fuerte con claves de encriptación que cambian con frecuencia. (* N/A si hay no hay redes inalámbricas.) | N/A | |
| D3.PC.Im.Int.5 | La gama de difusión de las redes inalámbricas se limita a límites controlados por la institución. (* N/A si hay no hay redes inalámbricas.) | N/A | |
| D3.PC.Im.Int.6 | Las medidas técnicas son para prevenir la ejecución de código no autorizado de la institución de propiedad o administrados de dispositivos, infraestructura de red y componentes de los sistemas. | N/A | |
| D3.PC.Im.A.1 | Instancias virtuales y entornos de red diseñadas y configuradas para restringir y controlar el tráfico entre las zonas de confianza y sin confianza. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.A.2 | Se permite solamente una función primaria por servidor para evitar funciones que requieran niveles de seguridad diferentes de coexistencia en el mismo servidor. | N/A | |
| D3.PC.Im.A.3 | Medidas anti-spoofing son para detectar y bloquear direcciones IP de fuente falsificados entren en la red. | N/A | |
| D3.PC.Im.Inn.1 | Las puntuaciones de riesgo institución todos sus activos de infraestructura y actualizaciones en tiempo real basados en las amenazas, vulnerabilidades o cambios operativos. | N/A | |
| D3.PC.Im.Inn.2 | Controles automáticos se ponen en práctica basado en puntajes de riesgo a los activos de infraestructura, incluyendo automáticamente desconectar activos afectados. | N/A | |
| D3.PC.Im.Inn.3 | La institución busca proactivamente identificar las brechas de control que pueden ser utilizadas como parte de un ataque de día cero. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Im.Inn.4 | Servidores público habitualmente se rotan y restaurados a un estado limpio conocido para limitar la ventana de tiempo que un sistema está expuesto a amenazas potenciales. | N/A | |
| D3.PC.Am.B.1 | Se concede el acceso de empleados a los sistemas y datos confidenciales basados en responsabilidades de trabajo y los principios de privilegio mínimo. (FFIEC seguridad folleto, página 19) | "Fuente: IS.II.C.7: pg15: Los usuarios deben tener acceso a los sistemas, aplicaciones y bases de datos en función de sus responsabilidades laborales.<br>IS.II.C.10 (b): pg23: El endurecimiento puede incluir las siguientes acciones: ... Configurar los privilegios y los controles de acceso al denegar todo, luego devolver el mínimo necesario a cada usuario (es decir, hacer cumplir el principio de privilegio mínimo) .<br>IS.WP.6.13: Determine si la administración tiene procesos para fortalecer las aplicaciones y los sistemas (por ejemplo, instalando los servicios mínimos, instalando los parches necesarios, configurando las configuraciones de seguridad adecuadas, aplicando el principio de privilegio mínimo, cambiando las contraseñas predeterminadas y habilitando el registro).<br>MGT.III.C.2: pg28: La gerencia debe documentar y confirmar los privilegios de acceso para cada miembro del personal según su descripción de trabajo. " | PR. AC-4: Se manejan permisos de acceso, incorporando los principios de privilegio mínimo y la separación de funciones. (p. 24) |
| D3.PC.Am.B.2 | Acceso de los empleados a los sistemas y datos confidenciales se proporciona para la separación de funciones. (FFIEC seguridad folleto, página 19) | "Fuente: IS.II.C.7: pg15: La administración debe mitigar los riesgos que plantean los usuarios al hacer lo siguiente: Emplear la separación de funciones.<br>IS.WP.2.5.g: Determine si las responsabilidades de la administración son apropiadas e incluyen lo siguiente: ... Establecimiento de una adecuada segregación de funciones ". | PR. AC-4: Se manejan permisos de acceso, incorporando los principios de privilegio mínimo y la separación de funciones. (p. 24) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.B.3 | Privilegios elevados (por ejemplo, privilegios de administrador) son limitados y bien controladas (por ejemplo, asignado a los individuos, no compartidos y requieren controles de contraseña más fuerte). (FFIEC seguridad folleto, página 19) | "Fuente: IS.II.C.15: pg31: La autorización para el acceso privilegiado debe controlarse estrictamente.<br>IS.WP.6.20: Determine si la administración tiene un proceso efectivo para administrar derechos de acceso de seguridad lógicos para la red, sistemas operativos, aplicaciones, bases de datos y dispositivos de red. Revise si la administración tiene lo siguiente: Un proceso para controlar el acceso privilegiado ". | PR. PT-3: Acceso a los sistemas y activos es controlado, incorporando el principio de funcionalidad por lo menos. (p. 29) |
| D3.PC.Am.B.4 | Opiniones de acceso se realizan periódicamente para todos los sistemas y aplicaciones basadas en el riesgo en la aplicación o sistema. (FFIEC seguridad folleto, página 18) | "Fuente: IS.II.C.15: pg31: Como parte del proceso de monitoreo de los derechos de acceso de los usuarios, la administración debe realizar revisiones periódicas para validar el acceso de los usuarios. Las revisiones deben probar si los derechos de acceso siguen siendo apropiados o si deben modificarse o no. eliminado. La gerencia debe revisar los derechos de acceso en un horario acorde con el riesgo.<br>IS.Wp.6.8.c: Determine si la administración mitiga efectivamente los riesgos planteados por los usuarios. Revise si la administración hace lo siguiente: ... Establece y administra adecuadamente un programa de acceso de usuario para el acceso físico y lógico.<br>MGT.III.C.2: pg28: La administración debe establecer un proceso oportuno para revisar, actualizar y eliminar los privilegios de acceso asociados con cualquier parte cuando sea apropiado. La falta de tal proceso puede resultar en una actividad no autorizada o inapropiada. Si no se eliminan los privilegios de acceso cuando es apropiado, especialmente para aquellas personas con altos niveles de privilegios, representa un riesgo significativo ". | PR. PT-3: Acceso a los sistemas y activos es controlado, incorporando el principio de funcionalidad por lo menos. (p. 29) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.B.5 | Cambios de acceso físicos y lógicos del usuario, incluyendo aquellos que resultan de las terminaciones voluntarias e involuntarias, son sometidos a y aprobados por personal adecuado. (FFIEC seguridad folleto, página 18) | "Fuente: IS.II.C.7 (b): pg16: La gerencia debe desarrollar un programa de acceso de usuarios para implementar y administrar controles de acceso físicos y lógicos para salvaguardar los activos de información y la tecnología de la institución. Este programa debe incluir los siguientes elementos: ... Revisiones continuas por parte de los propietarios de la línea comercial y de la aplicación para verificar el acceso apropiado en función de los roles de los puestos de trabajo, con cambios informados oportunamente al personal de administración de seguridad. Notificación oportuna de recursos humanos a administradores de seguridad para ajustar el acceso de los usuarios según los cambios de trabajo, incluidas las terminaciones.<br>IS.WP.6.8: Determine si la administración mitiga efectivamente los riesgos planteados por los usuarios. Revise si la administración hace lo siguiente: Desarrolla y mantiene una cultura que fomenta el acceso responsable y controlado de los usuarios. Establece y administra adecuadamente un programa de acceso de usuario para el acceso físico y lógico ". | PR. AC-4: Se manejan permisos de acceso, incorporando los principios de privilegio mínimo y la separación de funciones. (p. 24) |
| D3.PC.Am.B.6 | Identificación y autenticación son requeridos y administrados para acceder a sistemas, aplicaciones y hardware. (FFIEC seguridad folleto, página 21) | Fuente: ISIS.II. C.15 (b): pg33: gestión debe implementar controles de acceso de la aplicación efectiva de la siguiente: aplicación de un método de autenticación robusto consistente con la importancia y la sensibilidad de la aplicación. ES. WP.6.22: Determinar si gestión controla el acceso a aplicaciones. Revisar si la administración hace lo siguiente: implementa un método de autenticación robusto consistente con la importancia y la sensibilidad de la aplicación. | PR. AC-1: Identidades y credenciales son gestionadas por los usuarios y los dispositivos autorizados. (p. 23) |
| D3.PC.Am.B.7 | Controles de acceso incluyen la complejidad de contraseña y límites a los intentos de contraseña y la reutilización. (FFIEC seguridad folleto, página 66) | "Fuente: IS.II.C.7: pg15: Los derechos de acceso deben otorgarse de acuerdo con las políticas de control de acceso lógico y físico de la institución.<br>IS.WP.8.1.k: Determine si las actividades de operaciones de seguridad de la institución incluyen lo siguiente: Cumplimiento de los controles de acceso y políticas de control de acceso lógico ".. | PR. PT-3: Acceso a los sistemas y activos es controlado, incorporando el principio de funcionalidad por lo menos. (p. 29) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.B.8 | Todas las contraseñas por defecto y por defecto innecesarias cuentas se cambian antes de la implementación del sistema. (FFIEC seguridad folleto, Página 61) | "Fuente: IS.II.C.15: pg31: Los derechos de acceso al nuevo software y hardware presentan un problema diferente. Por lo general, el hardware y el software se envían con usuarios predeterminados y al menos un usuario predeterminado tiene acceso privilegiado. Las listas de cuentas predeterminadas y Las contraseñas están disponibles y pueden permitir que cualquier persona con acceso al sistema obtenga acceso privilegiado. Estas contraseñas se deben cambiar y las cuentas se deben desactivar.<br>IS.WP.6.20: Determine si la administración tiene un proceso efectivo para administrar derechos de acceso de seguridad lógicos para la red, sistemas operativos, aplicaciones, bases de datos y dispositivos de red. Revise si la administración tiene lo siguiente: Un proceso para cambiar o deshabilitar cuentas de usuario y contraseñas predeterminadas ". | |
| D3.PC.Am.B.9 | Acceso del cliente a través de Internet productos o servicios requiere autenticación controles (por ejemplo, capas, multifactorial) que sean proporcionales al riesgo. (FFIEC seguridad folleto, página 21) | "Fuente: IS.II.C.16: pg36: las instituciones ofrecen cada vez más servicios a los clientes a través de tecnología de acceso remoto, como Internet y servicios financieros móviles. Si la institución ofrece dichos servicios, la administración debe implementar técnicas de autenticación apropiadas acordes con el riesgo de actividades bancarias remotas.<br>IS.WP.6.22: Determine si la administración controla el acceso a las aplicaciones. Revise si la administración hace lo siguiente: Implementa un método de autenticación robusto consistente con la criticidad y la sensibilidad de la aplicación " | |
| D3.PC.Am.B.10 | Entornos de producción y no producción están segregados para evitar acceso no autorizado o cambios a los activos de información. (* N/A si no entorno de producción existe en la institución o de terceros de la institución.) (FFIEC seguridad folleto, página 64) | Fuente: IS.II. C.9:pg19: Gestión debe asegurar el acceso a las redes informáticas a través de varias capas de controles de acceso haciendo lo siguiente: establecimiento de zonas (por ejemplo, de confianza y no es de confianza) según el perfil de riesgo y la criticidad de los activos dentro de las zonas y requisitos de acceso apropiados dentro de y entre cada zona de seguridad. ES. WP.6. 10.a: Determinar si la gestión asegura el acceso a sus redes informáticas a través de varias capas de controles de acceso. Revisar si la administración hace lo siguiente: establece zonas (por ejemplo, de confianza y no es de confianza) según el riesgo con requerimientos de acceso apropiados dentro de y entre cada zona. | PR. DS-7: El desarrollo y entornos de prueba están separados desde el entorno de producción. (p. 26) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.B.11 | Controles de seguridad física se utilizan para prevenir acceso no autorizado a sistemas de información y sistemas de telecomunicaciones. (FFIEC seguridad folleto, página 47) | "Fuente: IS.II.C.8: pg18: La administración debe implementar controles preventivos, de detección y correctivos apropiados para la seguridad física. El acceso físico y el daño o la destrucción de los componentes físicos pueden afectar la confidencialidad, la integridad y la disponibilidad de la información. Administración debe implementar controles preventivos, de detección y correctivos apropiados para mitigar los riesgos inherentes a esas zonas de seguridad física.<br>IS.WP.6.9: Determine si la administración aplica controles de seguridad física apropiados para proteger sus instalaciones y áreas más sensibles, como sus centros de datos ". | PR. AC-2: El acceso físico a los bienes es administrado y protegido. PR (p. 23) IP-5: Políticas y regulaciones en relación con el ambiente físico de la operación de activos de la organización se cumplan. PR (p. 27) PT-4: Redes de comunicaciones están aseguradas. (p. 29) |
| D3.PC.Am.B.12 | Todas las contraseñas están cifradas en el almacenamiento y el tránsito. (FFIEC seguridad folleto, página 21) | "Fuente: IS.II.C.19: pg41: El cifrado se utiliza para proteger las comunicaciones y el almacenamiento de datos, en particular las credenciales de autenticación y la transmisión de información confidencial ... Las contraseñas deben estar cifradas o cifradas en el almacenamiento.<br>IS.WP.6.30: Determine cómo y dónde la administración utiliza el cifrado y si el tipo y la solidez son suficientes para proteger la información de manera adecuada ". | |
| D3.PC.Am.B.13 | Datos confidenciales se cifran cuando se transmiten a través de las redes públicas o no confiables (por ejemplo, Internet). (FFIEC seguridad folleto, página 51) | "Fuente: IS.II.C.13 (b): pg28: Cuando se transmite información confidencial a través de una red pública, la información debe estar cifrada para protegerla de la interceptación o la interceptación.<br>IS.WP.6.30: Determine cómo y dónde la administración utiliza el cifrado y si el tipo y la solidez son suficientes para proteger la información de manera adecuada ". | PR. DS-2: Datos en tránsito está protegido. (p. 25) |
| D3.PC.Am.B.14 | Dispositivos móviles (por ejemplo, ordenadores portátiles, tabletas y extraíbles) están encriptados si se utiliza para almacenar datos confidenciales. (* N/A si no se utilizan dispositivos móviles.) (FFIEC seguridad folleto, página 51) | "Fuente: IS.II.C.13 (a): pg27: El almacenamiento de datos en dispositivos portátiles, como computadoras portátiles, teléfonos inteligentes y tabletas, plantea problemas únicos ... La mitigación de riesgos generalmente implica el cifrado de datos.<br>IS.WP.6.30: Determine cómo y dónde la administración utiliza el cifrado y si el tipo y la solidez son suficientes para proteger la información de manera adecuada " | PR. DS-1: Datos en reposo está protegido. (p. 25) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.B.15 | Acceso remoto a sistemas críticos por los empleados, contratistas y terceros utiliza conexiones encriptadas y autenticación de múltiples factores. (FFIEC seguridad folleto, página 45) | "Fuente: IS.II.C.15 (c): pg33: La administración debe desarrollar políticas para garantizar que el acceso remoto de los empleados, ya sea utilizando la institución o los dispositivos de propiedad personal, se proporcione de manera segura y sólida ... La administración debe emplear lo siguiente Medidas: Utilice métodos de autenticación robustos para el acceso y el cifrado para asegurar las comunicaciones.<br>IS.WP.6.23: Revise si la administración hace lo siguiente: Proporciona acceso remoto de manera segura y sólida. Implementa los controles necesarios para ofrecer un acceso remoto de forma segura (por ejemplo, deshabilita el acceso remoto innecesario, obtiene aprobaciones y realiza auditorías de acceso remoto, mantiene configuraciones sólidas, permite el registro y la supervisión, protege los dispositivos, restringe el acceso remoto durante momentos específicos, controla las aplicaciones, habilita autenticación fuerte, y utiliza cifrado) ". | PR. AC-3: Acceso Remoto es administrado. PR (p. 23) DS-5: Protección contra pérdidas de datos se implementa. (p. 26) |
| D3.PC.Am.B.16 | Controles administrativos, físicos o técnicos son para evitar que usuarios sin responsabilidades administrativas instalar software no autorizado. (FFIEC seguridad folleto, página 25) | "Fuente: IS.II.C.12: pág. 26: Los métodos o sistemas que la administración debe considerar incluyen los siguientes: ... Monitoreo de software no autorizado y no permitir la instalación de software no autorizado.<br>IS.WP.6.11: Determine si la administración tiene un proceso para introducir cambios en el entorno (por ejemplo, la administración de la configuración de los sistemas y aplicaciones de TI, el fortalecimiento de los sistemas y las aplicaciones, el uso de compilaciones estándar y la administración de parches) de manera controlada ". | PR. AC-2: El acceso físico a los bienes es administrado y protegido. (p. 23) |
| D3.PC.Am.B.17 | Servicio al cliente (por ejemplo, el centro de llamadas) utiliza procedimientos formales para autenticar a clientes acordes con el riesgo de la transacción o petición. (FFIEC seguridad folleto, página 19) | "Fuente: IS.II.C.16: pg36: Más allá de la autenticación, los controles de acceso remoto deben incluir controles de seguridad en capas adicionales y pueden incluir alguna combinación de lo siguiente: Controles sobre los cambios en las actividades de mantenimiento de la cuenta (por ejemplo, cambios de dirección o contraseña) realizados por los clientes, ya sea en línea o a través de los canales de servicio al cliente.<br>IS.WP.6.22.a: Determine si la administración controla el acceso a las aplicaciones. Revise si la administración hace lo siguiente: Implementa un método de autenticación robusto consistente con la criticidad y la sensibilidad de la aplicación ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.B.18 | Datos eliminados o destruidos según requisitos documentados y plazos previstos. (FFIEC seguridad folleto, página 66) | "Fuente: IS.II.C.13 (c): pg28: La institución debe basar sus políticas de eliminación en la confidencialidad de la información. Las políticas, los procedimientos y la capacitación deben informar a los empleados sobre las acciones que deben tomarse para eliminar la computadora de manera segura Basados en medios y protegen los datos de los riesgos de reconstrucción.<br>IS.WP.6.18.e: Determine si la administración mantiene políticas y efectivamente controla y protege el acceso y la transmisión de información para evitar pérdidas o daños. Revise si la administración hace lo siguiente: ... Tiene procedimientos de eliminación apropiados para información tanto electrónica como en papel ". | PR. IP-6: Los datos se destruyen según política. (p. 27) |
| D3.PC.Am.E.1 | Cambios en permisos de acceso de usuario activan avisos automáticos a personal adecuado. | N/A | |
| D3.PC.Am.E.2 | Los administradores tienen dos cuentas: una para uso administrativo y otra para uso general, las tareas no administrativas. | N/A | |
| D3.PC.Am.E.3 | Uso de datos de clientes en entornos de producción no cumple con los requisitos legales, reglamentarios e interna política para ocultar o eliminación de elementos de datos sensibles. | N/A | |
| D3.PC.Am.E.4 | Acceso físico a los sistemas de alto riesgo o confidencial es restringido, registrado, y se bloquea el acceso no autorizado. | N/A | |
| D3.PC.Am.E.5 | Existen controles para prevenir acceso no autorizado a las claves | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | criptográficas. | | |
| D3.PC.Am.Int.1 | La institución ha implementado herramientas para prevenir el acceso no autorizado a o perdida de datos confidenciales. | N/A | PR.DS-5: Se implementan protecciones contra fugas de datos. (p. 26) |
| D3.PC.Am.Int.2 | Los controles son para evitar no autorizado escalada de privilegios de usuario. | N/A | |
| D3.PC.Am.Int.3 | Existen controles de acceso para administradores de base de datos para evitar que la descarga no autorizada o la transmisión de datos confidenciales. | N/A | |
| D3.PC.Am.Int.4 | Todos los accesos físicos y lógicos se quita inmediatamente tras la notificación de terminación automática y dentro de 24 horas de la salida voluntaria de un empleado. | N/A | |
| D3.PC.Am.Int.5 | Autenticación de múltiples factores o capas los controles han sido implementados para asegurar todos los accesos de terceros a la institución red o sistemas y aplicaciones. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.Int.6 | Técnicas de autenticación de múltiples factores (p. ej., tokens, certificados digitales) se utilizan para el acceso de los empleados a los sistemas de alto riesgo identificados en las evaluaciones de riesgo. (* N/A si no sistemas de alto riesgo.) | N/A | |
| D3.PC.Am.Int.7 | Datos confidenciales se cifran en tránsito a través de conexiones privadas (por ejemplo, frame relay y T1) y dentro de zonas de confianza de la institución. | N/A | |
| D3.PC.Am.Int.8 | Existen controles para prevenir el acceso no autorizado a dispositivos informáticos de colaboración y aplicaciones (por ejemplo, pizarras en red, cámaras, micrófonos, aplicaciones en línea como mensajería instantánea y compartir documentos). (* N/A si no se utilizan dispositivos de computación colaborativos.) | N/A | |
| D3.PC.Am.A.1 | Cifrado de datos seleccionados en reposo se determina por evaluación de clasificación y riesgo de | N/A | PR.DS-1: Los datos en reposo están protegidos. (p. 25) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | datos de la institución. | | |
| D3.PC.Am.A.2 | Autenticación de cliente para transacciones de alto riesgo incluye métodos para prevenir el malware y los ataques de man in the middle (por ejemplo, mediante firma de transacción visual). | N/A | |
| D3.PC.Am.Inn.1 | Controles de acceso adaptable de provisión o aislar a un empleado, terceros o credenciales de cliente para minimizar los posibles daños si se sospecha de un comportamiento malintencionado. | N/A | |
| D3.PC.Am.Inn.2 | Datos confidenciales no estructurados son rastreados y asegurados a través de un sistema de identidad consciente, multiplataforma que protege contra amenazas internas, controla el acceso de los usuarios y seguimiento de los cambios. | N/A | |
| D3.PC.Am.Inn.3 | Tokenización es utilizado para sustituir valores únicos para información confidencial (por ejemplo, tarjeta de crédito virtual). | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Am.Inn.4 | La institución es líder en esfuerzos para crear nuevas tecnologías y procesos para la gestión de clientes, empleados y terceros autenticación y acceso. | N/A | |
| D3.PC.Am.Inn.5 | Mitigación de riesgos en tiempo real se toma en base a puntuación de riesgo automatizado de las credenciales de usuario. | N/A | |
| D3.PC.De.B.1 | Los controles son en su lugar para restringir el uso de medios extraíbles al personal autorizado. (Programa de trabajo de seguridad de información de FFIEC, I: objetivo 4 - 1) | "Fuente: IS.II.C.13 (a): pg27: La administración debe implementar los controles apropiados (como el uso de un programa DLP) sobre los dispositivos portátiles y la información confidencial que contienen.<br>IS.II.C.13 (d): pg29: La administración debe implementar políticas para mantener la seguridad de los medios físicos (incluidas las cintas de copia de seguridad) que contienen información confidencial durante el tránsito, incluido el almacenamiento fuera del sitio, o cuando se comparte con terceros ... . Uso de encriptación adecuada de información sensible grabada en medios que se está transportando físicamente.<br>IS.WP.6.18: Determine si la administración mantiene políticas y controla y protege efectivamente el acceso y la transmisión de información para evitar pérdidas o daños. Revise si la administración hace lo siguiente: Requiere el almacenamiento seguro de todo tipo de información confidencial, ya sea en sistemas informáticos, dispositivos portátiles, medios físicos o documentos impresos ". | PR. PT-2: Medio extraíble está protegido y restringido su uso según una política especifica. (p. 29) |
| D3.PC.De.E.1 | Herramientas automáticamente bloquean el intento acceso de empleado sin parchear y dispositivos de terceros. | N/A | |
| D3.PC.De.E.2 | Herramientas automáticamente bloquean el acceso intento | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | por dispositivos no registrados para redes internas. | | |
| D3.PC.De.E.3 | La institución tiene controles para evitar que la incorporación no autorizada de nuevas conexiones. | N/A | |
| D3.PC.De.E.4 | Los controles son para evitar que a personas no autorizadas copien datos confidenciales en medios extraíbles. | N/A | |
| D3.PC.De.E.5 | Herramientas antivirus y anti-malware se implementan en los dispositivos de punto final (por ejemplo, estaciones de trabajo, portátiles y dispositivos móviles). | N/A | DE.CM-5: Se detectó un código móvil no autorizado. (p. 31) |
| D3.PC.De.E.6 | Dispositivos móviles con acceso a los datos de la institución son administrados de forma centralizada para antivirus y despliegue de parches. (* N/A si no se utilizan dispositivos móviles.) | N/A | |
| D3.PC.De.E.7 | La institución limpia remotamente datos en dispositivos móviles cuando un dispositivo es robado o desaparecido. (* N/A si no se utilizan | N/A | PR.AC-3: Se gestiona el acceso remoto. (p. 23) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | dispositivos móviles.) | | |
| D3.PC.De.Int.1 | Se implementan controles de prevención de pérdida de datos o dispositivos para comunicaciones entrantes y salientes (por ejemplo, correo electrónico, FTP, Telnet, prevención de la transferencia de grandes archivos). | N/A | PR.DS-5: Se implementan protecciones contra fugas de datos. (p. 26) |
| D3.PC.De.Int.2 | Administración de dispositivos móviles incluye análisis de integridad (p. ej., detección de jailbreak/raíces). (* N/A si no se utilizan dispositivos móviles.) | N/A | PR.DS-6: los mecanismos de comprobación de integridad se utilizan para verificar el software, el firmware y la integridad de la información. (p. 26) |
| D3.PC.De.Int.3 | Dispositivos móviles de conexión a la red corporativa para almacenar y acceder a información de la empresa permiten validación de la versión/parche de software remoto. (* N/A si no se utilizan dispositivos móviles.) | N/A | |
| D3.PC.De.A.1 | Dispositivos empleados y terceras partes (incluyendo móviles) sin los últimos parches de seguridad son puestos en cuarentena y parcheados antes de que el | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | dispositivo se concede acceso a la red. | | |
| D3.PC.De.A.2 | Datos confidenciales y aplicaciones en dispositivos móviles sólo son accesibles a través de un recinto seguro, aislado o un contenedor seguro. | N/A | |
| D3.PC.De.Inn.1 | Una herramienta de gestión centralizada de punto final proporciona administración completamente integrado de parche, configuración y la vulnerabilidad, mientras que también siendo capaz de detectar malware a su llegada para evitar un ataque. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Se.B.1 | Los desarrolladores que trabajan para la institución seguir seguro Programa codificación de prácticas, como parte de un ciclo de vida de desarrollo de sistema (SDLC), que cumplen estándares de la industria. (FFIEC seguridad folleto, página 56) | "Fuente: IS.II.C.17: pg38: Un ciclo de vida de desarrollo de software seguro garantiza que las aplicaciones orientadas a Internet y al cliente tengan los controles de seguridad necesarios. La institución debe garantizar que todas las aplicaciones se desarrollen de manera segura ... En las instituciones que emplean terceros para desarrollar aplicaciones, la administración debe garantizar que los terceros cumplan con los mismos controles.<br>IS.WP.6.27: Determine si la administración usa aplicaciones que se desarrollaron siguiendo prácticas de desarrollo seguras y que cumplen con un nivel de seguridad prudente.<br>MGT.III.C.5: pg31: La administración debe guiar el desarrollo o la adquisición de software mediante el uso de un ciclo de vida de desarrollo del sistema (SDLC) o una metodología similar adecuada para el entorno de TI específico. La extensión o el uso del SDLC depende del tamaño y la complejidad de la institución y del tipo de actividades de desarrollo realizadas. Si la institución adquiere software principalmente, la administración debe verificar el uso efectivo de un SDLC por parte del proveedor externo.<br>MGT.WP.12.10. Determine si la administración evalúa y mitiga los riesgos operacionales asociados con el desarrollo o la adquisición de software. La gestión adecuada de los riesgos debe incluir lo siguiente:<br>a. Políticas que documentan los controles de gestión de riesgos para el desarrollo y adquisición de sistemas.<br>segundo. "Ciclo de vida del desarrollo del sistema o metodología similar basada en la complejidad y el tipo de desarrollo realizado". | PR. IP-2: Se implementa un ciclo de vida de desarrollo de sistema para administrar sistemas. (p. 26) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Se.B.2 | Los controles de seguridad de software desarrollado internamente periódicamente son revisados y probados. (* N/A si no hay software desarrollo.) (FFIEC seguridad folleto, página 59) | "Fuente: IS.II.C.10: pg21: El proceso para introducir software debe abarcar el desarrollo, la implementación y la prueba segura de los cambios tanto en el software desarrollado internamente como en el adquirido.<br>IS.WP.6.15: Determine si la administración tiene un proceso para actualizar y parchear sistemas operativos, dispositivos de red y aplicaciones de software, incluido el software desarrollado internamente que se proporciona a los clientes, para las vulnerabilidades recién descubiertas.<br>MGT.III.C.5: pg31: Las pruebas, que deberían incluir pruebas de seguridad, validan que los equipos y sistemas funcionan correctamente y producen los resultados deseados. Como parte del proceso de prueba, la administración debe verificar si los nuevos sistemas de tecnología funcionan de manera efectiva con otros componentes de tecnología, incluida la tecnología suministrada por el proveedor. La gerencia debe realizar reevaluaciones periódicamente para ayudar a administrar la exposición al riesgo de manera continua.<br>MGT.WP.12.10. Determine si la administración evalúa y mitiga los riesgos operacionales asociados con el desarrollo o la adquisición de software. La gestión adecuada de los riesgos debe incluir lo siguiente:<br>a. Políticas que documentan los controles de gestión de riesgos para el desarrollo y adquisición de sistemas.<br>segundo. Ciclo de vida del desarrollo del sistema o metodología similar basada en la complejidad y el tipo de desarrollo realizado.<br>do. "Pruebas de nueva tecnología, sistemas y productos antes de la implementación para validar la funcionalidad, los controles y la interoperabilidad". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Se.B.3 | Los controles de seguridad en el código de software internamente desarrollado independientemente se revisan antes de migrar el código a producción. (* N/A si no hay software desarrollo.) (FFIEC desarrollo y adquisición de folleto, página 2) | "Fuente: IS.II.C.10: pg21: El proceso para introducir software debe abarcar el desarrollo, la implementación y la prueba segura de los cambios tanto en el software desarrollado internamente como en el adquirido.<br>IS.WP.6.15: Determine si la administración tiene un proceso para actualizar y parchear sistemas operativos, dispositivos de red y aplicaciones de software, incluido el software desarrollado internamente que se proporciona a los clientes, para las vulnerabilidades recién descubiertas.<br>MGT.III.C.5: pg31: Las pruebas, que deberían incluir pruebas de seguridad, validan que los equipos y sistemas funcionan correctamente y producen los resultados deseados. Como parte del proceso de prueba, la administración debe verificar si los nuevos sistemas de tecnología funcionan de manera efectiva con otros componentes de tecnología, incluida la tecnología suministrada por el proveedor. La gerencia debe realizar reevaluaciones periódicamente para ayudar a administrar la exposición al riesgo de manera continua.<br>MGT.WP.12.10. Determine si la administración evalúa y mitiga los riesgos operacionales asociados con el desarrollo o la adquisición de software. La gestión adecuada de los riesgos debe incluir lo siguiente:<br>a. Políticas que documentan los controles de gestión de riesgos para el desarrollo y adquisición de sistemas.<br>segundo. Ciclo de vida del desarrollo del sistema o metodología similar basada en la complejidad y el tipo de desarrollo realizado. "Pruebas de nueva tecnología, sistemas y productos antes de la implementación para validar la funcionalidad, los controles y la interoperabilidad". | |
| D3.PC.Se.B.4 | Código de propiedad y producción intelectual se mantienen en fideicomiso. (* N/A si no existe ningún código de la producción para mantener en fideicomiso.) (FFIEC desarrollo y adquisición de folleto, página 39) | "Fuente: D & A.B.39: Además de garantizar el acceso a la documentación actual, las organizaciones deben considerar proteger sus derechos de depósito en garantía al exigir a los proveedores de software que informen a la organización si el proveedor de software se compromete con el software como garantía del préstamo.<br><br>D & A.WP.6.1: Evalúe la idoneidad de las actividades de adquisición mediante la evaluación ... La adecuación de las disposiciones contractuales y de licencia que abordan ... Accesibilidad de código fuente / aseveraciones de custodia ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Se.E.1 | Pruebas de seguridad produce en todo post-diseño fases de la SDLC para todas las aplicaciones, incluyendo aplicaciones móviles. (* N/A si no hay software desarrollo.) | N/A | PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para administrar sistemas. (p. 26) |
| D3.PC.Se.Int.1 | Existen procesos para mitigar las vulnerabilidades identificadas como parte del desarrollo seguro de aplicaciones y sistemas. | N/A | |
| D3.PC.Se.Int.2 | La seguridad de aplicaciones, incluyendo aplicaciones basadas en Web conectadas a Internet, se prueba contra tipos conocidos de ataques cibernéticos (por ejemplo, inyección SQL, intercambio scripting, desbordamiento de búfer) antes de la aplicación o después de cambios significativos. | N/A | |
| D3.PC.Se.Int.3 | Scripts y software código ejecutables están firmados digitalmente para confirmar al autor de software y garantizar que el código no se altera o corrompido. | N/A | PR.DS-6: los mecanismos de comprobación de integridad se utilizan para verificar el software, el firmware y la integridad de la información. (p. 26) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.PC.Se.Int.4 | Una función de aseguramiento de la información basado en el riesgo, independiente evalúa la seguridad de aplicaciones internas. | N/A | |
| D3.PC.Se.A.1 | Vulnerabilidades identificadas a través de un análisis estático del código son remediadas antes de aplicar recién desarrollado o cambia aplicaciones en producción. | N/A | |
| D3.PC.Se.A.2 | Se han identificado todas las interdependencias entre las aplicaciones y servicios. | N/A | |
| D3.PC.Se.A.3 | Revisiones de código independiente se lleven internamente desarrolladas o proporcionado por el proveedor de aplicaciones personalizadas para asegurar que sin lagunas de seguridad. | N/A | |
| D3.PC.Se.Inn.1 | Código de software se explora activamente herramientas automatizadas en el entorno de desarrollo para que las debilidades de seguridad pueden resolver inmediatamente durante la | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | fase de diseño. | | |
| D3.DC.Th.B.1 | Pruebas independientes (incluyendo pruebas de penetración y análisis de vulnerabilidad) se lleva a cabo según la evaluación del riesgo para instalaciones exteriores y la red interna. (FFIEC seguridad folleto, Página 61) | "Fuente: ISIS.II.C.17: pg38: Para verificar que los controles se hayan desarrollado e implementado adecuadamente, la administración debe realizar las pruebas apropiadas (por ejemplo, pruebas de penetración, evaluaciones de vulnerabilidad y pruebas de seguridad de la aplicación) antes de iniciar o realizar cambios significativos en Aplicaciones orientadas al exterior.<br>IS.WP.4.2.d: Revise si la administración tiene lo siguiente: Una validación del proceso de identificación de riesgos a través de auditorías, autoevaluaciones, pruebas de penetración y evaluaciones de vulnerabilidad.<br>MGT.III.C.3: pg29: realice pruebas de penetración antes de lanzar o realizar cambios significativos en los sistemas críticos, incluidas las aplicaciones orientadas a Internet y al cliente. La gerencia debe revisar todos los hallazgos y desarrollar procesos para asegurar la reparación oportuna de los problemas identificados por las pruebas.<br>MGT.WP.12.8.f: Determine si, como parte del programa de seguridad de la información de la institución, el consejo de administración supervisa y la administración establece una estructura de control que pretende abordar específicamente los riesgos de seguridad cibernética e incluye lo siguiente: Realizar pruebas de penetración antes de lanzar nuevos o realizar cambios significativos en las aplicaciones existentes de Internet y de clientes y remediar los hallazgos de las pruebas ". | ID. RA-1: Activos vulnerabilidades son identificadas y documentadas. (p. 22) |
| D3.DC.Th.B.2 | Se utilizan herramientas antivirus y anti-malware para detectar ataques. (FFIEC seguridad folleto, página 55) | "Fuente: IS.II.C.12: pg26: La administración debe implementar la defensa en profundidad para proteger, detectar y responder al malware. La institución puede usar muchas herramientas para bloquear el malware antes de que entre al entorno y para detectar y detectar Responde si no está bloqueado.<br>IS.WP.6.17: Determine si la administración ha implementado la defensa en profundidad para proteger, detectar y responder al malware " | DE. CM-4: Código malicioso es detectado. (p. 31 |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.Th.B.3 | Reglas de firewall son Auditoría o verificadas por lo menos trimestralmente. (FFIEC seguridad folleto, página 82) | "Fuente: IS.III: pg46: Las actividades de operaciones de seguridad pueden incluir lo siguiente: Software de seguridad y administración de dispositivos (por ejemplo, mantener las firmas en dispositivos basados en firmas y reglas de firewall). IS.WP.8.1.a: Determine si las actividades de operaciones de seguridad de la institución incluyen lo siguiente: Software de seguridad y administración de dispositivos (por ejemplo, mantenimiento de firmas en dispositivos basados en firmas y reglas de firewall). " | |
| D3.DC.Th.B.4 | Mecanismos de protección de correo electrónico se utilizan para filtrar las amenazas cibernéticas común (por ejemplo, malware adjunto o enlaces maliciosos). (FFIEC seguridad folleto, página 39) | "Fuente: IS.II.C.12: pg26: La administración debe implementar la defensa en profundidad para proteger, detectar y responder al malware. La institución puede usar muchas herramientas para bloquear el malware antes de que entre al entorno y para detectar y detectar Responde si no está bloqueado. IS.WP.6.17: Determine si la administración ha implementado la defensa en profundidad para proteger, detectar y responder al malware ". | |
| D3.DC.Th.E.1 | Pruebas de penetración independiente del límite de la red y aplicaciones Web críticas se realizan rutinariamente para identificar brechas de control de seguridad. | N/A | |
| D3.DC.Th.E.2 | Pruebas de penetración independiente se realizan en aplicaciones de conexión a Internet o sistemas antes de que se inician o experimentan un cambio significativo. | N/A | |
| D3.DC.Th.E.3 | Herramientas antivirus y anti-malware se actualizan automáticamente. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.Th.E.4 | Las reglas del firewall se actualizan habitualmente. | N/A | |
| D3.DC.Th.E.5 | Análisis de vulnerabilidad es realizado y analizado antes de despliegue y redespliegue de dispositivos nuevos/existentes. | N/A | "ID.RA-1: las vulnerabilidades de los activos están identificadas y documentadas (p. 22)<br>DE.CM-8: Se realizan exploraciones de vulnerabilidad. (p. 31) " |
| D3.DC.Th.E.6 | Procesos están en el lugar para supervisar la actividad potencial de la información privilegiada que podría conducir a robo de datos o destrucción. | N/A | |
| D3.DC.Th.Int.1 | Auditoría o riesgo gestión recursos revisión la penetración pruebas de alcance y los resultados para ayudar a determinar la necesidad de rotación de empresas basadas en la calidad de la obra. | N/A | |
| D3.DC.Th.Int.2 | E-mails y archivos adjuntos son escaneados automáticamente para detectar malware y están bloqueados cuando el malware está presente. | N/A | |
| D3.DC.Th.A.1 | Análisis de vulnerabilidad semanal se gira entre entornos para explorar todos los ambientes durante todo el año. | N/A | ID.RA-1: Se identifican y documentan las vulnerabilidades de los activos. (p. 22)) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.Th.A.2 | Pruebas de penetración incluyen simulaciones de ataque cibernético o tácticas reales y técnicas como el equipo rojo de la prueba para detectar deficiencias de control en el comportamiento del empleado, las defensas de seguridad, políticas y recursos. | N/A | |
| D3.DC.Th.A.3 | Herramienta automatizada identifica proactivamente comportamiento de alto riesgo un empleado que puede plantear una amenaza por una persona enterada y de señalización. | N/A | |
| D3.DC.Th.Inn.1 | Tareas de usuario y el contenido (por ejemplo, abrir un archivo adjunto de correo electrónico) son automáticamente aislado en un contenedor seguro o entorno virtual para que el malware puede ser analizado pero no puede acceder a datos vitales, punto final los sistemas operativos o aplicaciones en la institución red. | N/A | |
| D3.DC.Th.Inn.2 | Análisis de vulnerabilidad se realizan sobre una base semanal a través de todos | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | los ambientes. | | |
| D3.DC.An.B.1 | La institución es capaz de detectar actividades anómalas a través del monitoreo en el entorno. (FFIEC seguridad folleto, página 32) | "Fuente: IS.II.C.12: pg26: La administración debe implementar la defensa en profundidad para proteger, detectar y responder al malware. La institución puede usar muchas herramientas para bloquear el malware antes de que entre al entorno y para detectar y detectar responda si no está bloqueado. Los métodos o sistemas que la administración debe considerar incluyen los siguientes… Monitoreo de actividad anómala para malware y código polimórfico.<br>IS.WP.6.17: Determine si la administración ha implementado la defensa en profundidad para proteger, detectar y responder al malware ". | ID. RA-3: Amenazas a activos de la organización son identificadas y documentadas. (p. 22) |
| D3.DC.An.B.2 | Transacciones del cliente generando alertas de actividad anómala son monitoreadas y revisadas. (FFIEC venta por mayor los pagos folleto, página 12) | "Fuente: WPS.B.12: Supervisar y registrar el acceso a los sistemas de transferencia de fondos, manteniendo una pista de auditoría de todas las transacciones secuenciales.<br>WPS.WP.II.1.3: Requiere que su alta gerencia reciba y revise los informes de actividad y control de calidad que revelen actividades inusuales o no autorizadas e intentos de acceso ". | |
| D3.DC.An.B.3 | Registros de acceso físico o lógico se revisan después de acontecimientos. (FFIEC seguridad folleto, página 73) | "Fuente: IS.III.C.22: pg44: Las instituciones mantienen registros de eventos para comprender un incidente o un evento cibernético después de que ocurra. La supervisión de los registros de eventos para detectar anomalías y la relación de esa información con otras fuentes de información amplía la capacidad de la institución para comprender las tendencias. reaccionar a las amenazas y mejorar los informes a la gerencia y al consejo.<br>IS.WP.6.21 (f): como parte del proceso de la administración para asegurar el sistema operativo y todos los componentes del sistema, determine si la administración hace lo siguiente: Filtra y revisa los registros para detectar posibles eventos de seguridad y proporciona informes y alertas adecuados ". | |
| D3.DC.An.B.4 | Acceso a sistemas críticos por parte de terceros es monitoreado para actividades no autorizadas o inusual. (FFIEC Outsourcing folleto, página 26) | Fuente: OT.B.26: Deben existir controles de acceso y monitoreo apropiados entre los sistemas del proveedor de servicios y la institución. | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.An.B.5 | Se vigilan los privilegios elevados. (FFIEC seguridad folleto, página 19) | "Fuente: IS.II.C.15: pg31: La autorización para el acceso privilegiado debe controlarse estrictamente.<br>IS.WP.8.4.f: Determine si la administración tiene procesos efectivos de monitoreo de amenazas, que incluyen lo siguiente: Establecer y documentar un proceso para monitorear de forma independiente a los administradores y otros usuarios con privilegios más altos ". | |
| D3.DC.An.E.1 | Existen sistemas para detectar el comportamiento anómalo automáticamente en clientes, empleados y terceros autenticación. | N/A | |
| D3.DC.An.E.2 | Registros de seguridad se revisan regularmente. | N/A | |
| D3.DC.An.E.3 | Los registros proporcionan trazabilidad para todo sistema de acceso por usuarios individuales. | N/A | |
| D3.DC.An.E.4 | Los umbrales se han establecido para determinar actividad dentro de los registros que se merecen una respuesta de la administración. | N/A | |
| D3.DC.An.Int.1 | Las transacciones en línea de clientes son supervisadas activamente por comportamiento anómalo. | N/A | |
| D3.DC.An.Int.2 | Se utilizan herramientas para detectar la minería de datos no autorizados. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.An.Int.3 | Herramientas activamente monitorear registros de seguridad de alerta dentro de parámetros establecidos y comportamiento anómalo. | N/A | |
| D3.DC.An.Int.4 | Registros de Auditoría están respaldados en un servidor de registro centralizado o los medios de comunicación que es difícil de alterar. | N/A | |
| D3.DC.An.Int.5 | Los umbrales para el registro de seguridad son evaluados periódicamente. | N/A | |
| D3.DC.An.Int.6 | Actividad anómala y otras alertas de red y sistema están correlacionados a través de unidades de negocio para detectar y prevenir ataques múltiples (por ejemplo, toma cuenta simultánea y DDoS ataque). | N/A | |
| D3.DC.An.A.1 | Una herramienta automatizada desencadena alertas de sistema o fraude cuando inicios de sesión de cliente en un período corto de tiempo sino de lugares físicamente distantes de IP. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.An.A.2 | Traslados externos de cuentas de clientes generan alertas y requieren revisión y autorización, si se detecta el comportamiento anómalo. | N/A | |
| D3.DC.An.A.3 | Es un sistema para supervisar y analizar el comportamiento del empleado (patrones de uso de red, horas de trabajo y dispositivos conocidos) para alertar sobre las actividades anómalas. | N/A | DE.CM-3: La actividad del personal se monitorea para detectar posibles eventos de ciberseguridad. (p. 31) |
| D3.DC.An.A.4 | Es una herramienta automatizada para detectar y evitar la extracción de datos de amenazas internas. | N/A | |
| D3.DC.An.A.5 | Etiquetas en ficticios datos confidenciales o archivos se utilizan para proporcionar Avanzado alertas de autoría doloso cuando se accede a los datos. | N/A | |
| D3.DC.An.Inn.1 | La institución cuenta con un mecanismo de puntuación de riesgo automatizado en tiempo real de amenazas. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.An.Inn.2 | La institución está desarrollando nuevas tecnologías que detecta posibles amenazas internas y bloquear la actividad en tiempo real. | N/A | |
| D3.DC.Ev.B.1 | Se establece una Base de la actividad de red normal. (FFIEC seguridad folleto, página 77) | "Fuente: IS.III.C: pg49: La identificación de incidentes involucra indicadores y análisis ... Los ejemplos de sistemas y herramientas de identificación de intrusos basados en tecnología incluyen lo siguiente: ... Sistemas de análisis de comportamiento de redes.<br>IS.WP.8.4.e: Determine si la administración tiene procesos efectivos de monitoreo de amenazas, incluidos los siguientes: Monitoreo del tráfico de red entrante y saliente para identificar actividad maliciosa y perdida de datos ". | DE. AE-1: Una Base de operaciones de red y flujos de datos esperados para los usuarios y sistemas es establecida y administrada. (p. 30) |
| D3.DC.Ev.B.2 | Mecanismos (por ejemplo, alertas de antivirus, alertas de eventos de registro) están en el lugar de administración de alertas a posibles ataques. (FFIEC seguridad folleto, página 78) | "Fuente: IS.III.B: pg48: Las políticas de monitoreo de amenazas deben proporcionar un monitoreo continuo y ad hoc de las comunicaciones y sistemas de inteligencia de amenazas, la detección y respuesta efectiva de incidentes, y el uso de informes de monitoreo en procedimientos legales subsiguientes ... El monitoreo de amenazas debe abordar los indicadores de vulnerabilidades, ataques, sistemas comprometidos y usuarios sospechosos, como aquellos que no cumplen o buscan evadir las políticas de seguridad.<br>IS.WP.8.5: Determine si la administración tiene procesos efectivos de identificación y evaluación de incidentes para hacer lo siguiente:<br>mi. Escala el evento consistente con la clasificación.<br>F. Informe interno y externo según corresponda ". | DE. DP-4: Detección de eventos información es comunicada a las partes apropiadas. (p. 32) |
| D3.DC.Ev.B.3 | Procesos están en el lugar para supervisar la presencia de usuarios no autorizados, dispositivos, conexiones y software. (Programa de trabajo de seguridad de información de FFIEC, II objetivo: M-9) | Fuente: IS. Introducción: pg2: Alinea el programa de seguridad de la información con el programa de gestión de riesgos de la empresa e identifica, mide, mitiga y monitorea el riesgo ... La administración debe poder identificar y caracterizar las amenazas, evaluar los riesgos, tomar decisiones con respecto al implementación de controles apropiados, y proporcionar un monitoreo y reporte apropiado. | DE. CM-7: Seguimiento por personal no autorizado, se realiza las conexiones, dispositivos y software. (p. 31) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.Ev.B.4 | Responsabilidades de monitoreo y reportan de actividad de sistemas sospechosos han sido asignados. (FFIEC seguridad folleto, página 83) | "Fuente: IS.III.B: pg48: La administración debe establecer la responsabilidad y la autoridad del personal de seguridad y los administradores de sistemas para el monitoreo. El monitoreo de amenazas debe abordar los indicadores de vulnerabilidades, ataques, sistemas comprometidos y usuarios sospechosos, como aquellos que no lo hacen. Cumplir o buscar evadir las políticas de seguridad. IS.WP.8.4.b: Determine si la administración tiene procesos efectivos de monitoreo de amenazas, incluyendo lo siguiente: Establecer responsabilidad y responsabilidad para el personal de seguridad y los administradores de sistemas para el monitoreo ". | DE. DP-1: Funciones y responsabilidades para la detección están bien definidos para asegurar la rendición de cuentas. (p. 31) |
| D3.DC.Ev.B.5 | El ambiente físico es monitoreado para detectar posibles accesos no autorizados. (FFIEC seguridad folleto, página 47) | "Fuente: IS.II.C.8: pg18: La gerencia debe implementar controles preventivos, de detección y correctivos apropiados para la seguridad física. IS.WP.6.9: Determine si la administración aplica controles de seguridad física apropiados para proteger sus instalaciones y áreas más sensibles, como sus centros de datos ".. | |
| D3.DC.Ev.E.1 | Un proceso está en su lugar para correlacionar información sobre procedente de múltiples fuentes (por ejemplo, red, aplicación o firewall). | N/A | DE.AE-3: Los datos de eventos se agregan y se correlacionan de múltiples fuentes y sensores. (p. 30) |
| D3.DC.Ev.Int.1 | Los controles o herramientas (por ejemplo, prevención de pérdida de datos) están en lugar para detectar potenciales transmisión no autorizada o accidental de datos confidenciales. | N/A | PR.DS-5: Se implementan protecciones contra fugas de datos. (p. 26) |
| D3.DC.Ev.Int.2 | Procesos de detección de evento se prueban confiables. | N/A | DE.DP-3: Se prueban los procesos de detección. (p. 32) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.DC.Ev.Int.3 | Supervisión de seguridad especializado se utiliza para activos críticos a lo largo de la infraestructura. | N/A | |
| D3.DC.Ev.A.1 | Herramientas automatizadas detectan cambios no autorizados a los archivos críticos del sistema, firewalls, IPS, IDS u otros dispositivos de seguridad. | N/A | |
| D3.DC.Ev.A.2 | Detección y monitoreo de red en tiempo real se implementa e incorpora información de evento en todo el sector. | N/A | |
| D3.DC.Ev.A.3 | Alertas en tiempo real se envían automáticamente cuando no autorizada software, hardware o cambios se producen. | N/A | |
| D3.DC.Ev.A.4 | Las herramientas son para correlacionar información sobre procedente de múltiples fuentes activamente y enviar alertas basadas en parámetros establecidos. | N/A | |
| D3.DC.Ev.Inn.1 | La institución es líder en los esfuerzos para desarrollar sistemas de detección de eventos que se correlacionan en tiempo real cuando eventos van a | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | ocurrir. | | |
| D3.DC.Ev.Inn.2 | La institución está liderando el esfuerzo de desarrollo para el diseño de nuevas tecnologías que detectan posibles amenazas internas y actividad de bloqueo en tiempo real. | N/A | |
| D3.CC.Pa.B.1 | Un Programa de gestión de parches se implementa y garantiza que el software y parches de firmware se aplican de manera oportuna. (FFIEC seguridad folleto, página 62) | "Fuente: IS.II.C.10 (d): pg24: La administración debe implementar sistemas y software de administración de parches para garantizar que todos los componentes de la red (máquinas virtuales, enrutadores, conmutadores, dispositivos móviles, cortafuegos, etc.) se actualicen adecuadamente.<br>IS.WP.6.15: Determine si la administración tiene un proceso para actualizar y parchear sistemas operativos, dispositivos de red y aplicaciones de software, incluido el software desarrollado internamente que se proporciona a los clientes, para las vulnerabilidades recién descubiertas.<br>OPS.B.22: La administración debe establecer procedimientos para mantenerse al tanto de los parches, probarlos en un entorno segregado e instalarlos cuando sea apropiado.<br>OPS.WP.5.1: Determine si la administración ha implementado y utiliza efectivamente los programas, procesos y herramientas de control operacional, como ... Gestión de proyectos, cambios y parches ". | |
| D3.CC.Pa.B.2 | Los parches son probados antes de ser aplicados a sistemas o software. (FFIEC operaciones folleto, página 22) | "Fuente: OPS.B.22: La gerencia debe establecer procedimientos para mantenerse al tanto de los parches, probarlos en un entorno segregado e instalarlos cuando sea apropiado.<br>OPS.WP.5.1: Determine si la administración ha implementado y utiliza efectivamente los programas, procesos y herramientas de control operacional, como ... Gestión de proyectos, cambios y parches ". | |
| D3.CC.Pa.B.3 | Revisión de informes de gestión son revisados y reflejan falta de parches de seguridad. (FFIEC desarrollo y adquisición de | Fuente: D & A.B.50: Los estándares de administración de parches deben incluir procedimientos para identificar, evaluar, aprobar, probar, instalar y documentar parches ... Las organizaciones deben contar con procedimientos para identificar los parches disponibles y adquirirlos de fuentes confiables. | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | folleto, página 50) | | |
| D3.CC.Pa.E.1 | Un proceso formal es en el lugar para adquirir, probar e instalar los parches de software basados en la criticidad. | N/A | |
| D3.CC.Pa.E.2 | Sistemas están configurados para obtener automáticamente los parches. | N/A | |
| D3.CC.Pa.E.3 | Impacto en las operaciones se evalúa antes de despliegue de parches de seguridad. | N/A | |
| D3.CC.Pa.E.4 | Una herramienta automatizada se utiliza para identificar revisiones de seguridad que faltan, así como el número de días puesto que cada parche se convirtió disponible. | N/A | |
| D3.CC.Pa.E.5 | Revisiones que faltan en todos los ambientes son prioridad y seguimiento. | N/A | |
| D3.CC.Pa.Int.1 | Parches para vulnerabilidades de alto riesgo son probados y aplicados cuando se libera o se acepta el riesgo y responsabilidad asignada. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.CC.Pa.A.1 | Parche de software de monitoreo está instalado en todos los servidores para identificar cualquier falta parches para el software de sistema operativo, middleware, bases de datos y otro software clave. | N/A | |
| D3.CC.Pa.A.2 | La institución supervisa la revisión de informes de gestión para parches de seguridad están probados e implementados plazos agresivos (p. ej., 0-30 días). | N/A | |
| D3.CC.Pa.Inn.1 | La institución desarrolla parches de seguridad o corrección de errores o contribuye para abrir desarrollo de código fuente para sistemas de usa. | N/A | |
| D3.CC.Pa.Inn.2 | Sistemas segregados o separados son en el lugar que espejo permitiendo la prueba rápida y aplicación de los parches de los sistemas de producción y para respaldo rápido cuando sea necesario. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.CC.Re.B.1 | Problemas identificados en las evaluaciones son priorizadas y resuelto en base a la criticidad y dentro de los plazos establecidos en la respuesta al informe de evaluación del. (FFIEC seguridad folleto, Página 87) | "Fuente: IS.IV.A.4: pg56: Los informes deben priorizar los riesgos y los hallazgos en el orden de importancia, sugerir opciones para la remediación y resaltar los problemas de repetición. Además, los informes deben abordar las causas principales. Procedimientos oportunos y confiables de escalamiento y respuesta. IS.WP.1.2.a: revise la respuesta de la administración a los problemas planteados en, o desde, el último examen. Considere lo siguiente: Adecuación y tiempo de acción correctiva ". | |
| D3.CC.Re.E.1 | Datos es destruidos o borrados en medios portátiles móviles y hardware cuando un dispositivo es perdido, robados, o ya no es necesario. | N/A | |
| D3.CC.Re.E.2 | Existen procesos formales para resolver debilidades identificadas durante las pruebas de penetración. | N/A | PR.IP12: Se desarrolla e implementar un plan de gestión de vulnerabilidades. (p. 28) |
| D3.CC.Re.Int.1 | Esfuerzos de remediación son confirmados mediante la realización de un análisis de seguimiento de la vulnerabilidad. | N/A | |
| D3.CC.Re.Int.2 | Pruebas de penetración se repitieron para confirmar eso medio - y las vulnerabilidades de alto riesgo, explotación han sido resueltas. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D3.CC.Re.Int.3 | Investigaciones de seguridad, análisis forense y rehabilitación son realizadas por personal cualificado o de terceros. | N/A | |
| D3.CC.Re.Int.4 | Generalmente aceptados y apropiados procedimientos forenses, incluyendo la cadena de custodia, se utilizan para reunir y presentar pruebas para apoyar posibles acciones legales. | N/A | |
| D3.CC.Re.Int.5 | El mantenimiento y reparación de activos de la organización son realizadas por personas autorizadas con herramientas aprobadas y controladas. | N/A | PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y se registran de manera oportuna, con herramientas aprobadas y controladas (pág. 28) |
| D3.CC.Re.Int.6 | El mantenimiento y reparación de activos de la organización se registran en tiempo y forma. | N/A | PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y se registran de manera oportuna, con herramientas aprobadas y controladas (pág. 28) |
| D3.CC.Re.A.1 | Todos los problemas de mediano y alto riesgo identifican en pruebas, análisis de vulnerabilidad de penetración y otras pruebas independientes comunicado a la Junta o un | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | Comité apropiado de aceptación de riesgo si no resuelve en tiempo y forma. | | |
| D3.CC.Re.Inn.1 | La institución está desarrollando tecnologías que se corregir sistemas dañados por ataques de día cero para mantener los actuales objetivos de tiempo de recuperación. | N/A | |
| D4.C.Co.B.1 | Se han identificado los procesos críticos de negocio que dependen de la conectividad externa. (FFIEC seguridad folleto, página 9) | "Fuente: IS.II.C.6: pg14-15: Para mitigar el riesgo de interconectividad, la administración debe hacer lo siguiente: Identificar conexiones con terceros, incluidas otras instituciones financieras, instituciones financieras. IS.WP.6.7: Determine si la administración identifica, mide, mitiga, monitorea e informa de manera integral y efectiva el riesgo de interconectividad ". | La organización entiende sus dependencias y socios y recibe información de los socios que permite la colaboración y las decisiones de gestión de riesgo dentro de la organización en respuesta a eventos. ID. (p. 10) BE-4: Se establecen las dependencias y funciones críticas para la entrega de servicios críticos. (p. 21) |
| D4.C.Co.B.2 | La institución asegura que las conexiones de terceros están autorizadas. (FFIEC seguridad folleto, página 17) | "Fuente: IS.II.C.6: pg14-15: Para mitigar el riesgo de interconectividad, la administración debe hacer lo siguiente: Identificar conexiones con terceros, incluidas otras instituciones financieras, intermediarios de instituciones financieras y proveedores de servicios de terceros ... Evaluación todas las conexiones con terceros que proporcionan capacidad de acceso remoto o control sobre los sistemas internos. IS.WP.6.7: Determine si la administración identifica, mide, mitiga, monitorea e informa de manera integral y efectiva el riesgo de interconectividad. Revise si la administración hace lo siguiente: Identifica conexiones con terceros. … Mide el riesgo asociado a las conexiones con terceros con acceso remoto. Implementa y evalúa la idoneidad de los controles apropiados para garantizar la seguridad de las conexiones ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.C.Co.B.3 | Un diagrama de red es en el lugar e identifica todas las conexiones externas. (FFIEC seguridad folleto, página 9) | "Fuente: IS.II.C.9: pg20: Para garantizar la seguridad adecuada de la red, la administración debe mantener la red y los diagramas de flujo de datos precisos, y almacenarlos de manera segura, brindando acceso solo al personal esencial. Estos diagramas deben identificar el hardware, software y Componentes de la red, conexiones internas y externas, y tipos de información que pasan entre los sistemas para facilitar el desarrollo de una arquitectura de seguridad de defensa en profundidad.<br>IS.WP.6.10.b: Determine si la administración asegura el acceso a sus redes de computadoras a través de múltiples capas de controles de acceso. Revise si la administración hace lo siguiente: Mantiene diagramas de red precisos y diagramas de flujo de datos ". | ID. AM-4: Sistemas de información externos son asignados y catalogados. (p. 20) |
| D4.C.Co.B.4 | Diagramas de flujo de datos están en su lugar y documentar el flujo de información a terceros. (FFIEC seguridad folleto, página 10) | "Fuente: IS.II.C.9: pg20: Para garantizar la seguridad adecuada de la red, la administración debe mantener la red y los diagramas de flujo de datos precisos, y almacenarlos de manera segura, brindando acceso solo al personal esencial. Estos diagramas deben identificar el hardware, software y Componentes de la red, conexiones internas y externas, y tipos de información que pasan entre los sistemas para facilitar el desarrollo de una arquitectura de seguridad de defensa en profundidad.<br>IS.WP.6.10.b: Determine si la administración asegura el acceso a sus redes de computadoras a través de múltiples capas de controles de acceso. Revise si la administración hace lo siguiente: Mantiene diagramas de red precisos y diagramas de flujo de datos ". | ID. AM-3: Se asigna el flujo de datos y comunicación organizacional. DE (p. 20). AE-1: Una Base de operaciones de red y flujos de datos esperados para los usuarios y sistemas es establecida y administrada. (p. 30) |
| D4.C.Co.E.1 | Procesos críticos del negocio se ha valor a las conexiones externas de apoyo. | N/A | |
| D4.C.Co.E.2 | El diagrama de red se actualiza cuando conexiones con terceras partes cambiar o al menos anualmente. | N/A | |
| D4.C.Co.E.3 | Diagramas de red y los sistemas se almacenan de forma segura con las | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | restricciones adecuadas de acceso. | | |
| D4.C.Co.E.4 | Controles para conexiones de terceros de primarias y de respaldo son supervisados y probados de manera regular. | N/A | |
| D4.C.Co.Int.1 | Un inventario de activos validado se utiliza para crear esquemas integrales con repositorios de datos, flujo de datos, infraestructura y conectividad. | N/A | ID.AM-3: Se mapea la comunicación organizacional y el flujo de datos. (p. 20) |
| D4.C.Co.Int.2 | Controles de seguridad están diseñados y verificados para detectar y prevenir intrusiones de conexiones de terceros. | N/A | |
| D4.C.Co.Int.3 | Controles de seguimiento cubren todas las conexiones externas (por ejemplo, los proveedores de servicios de terceros, socios, clientes). | N/A | |
| D4.C.Co.Int.4 | Controles de seguimiento cubren todas las conexiones de red a la red internas. | N/A | |
| D4.C.Co.A.1 | La arquitectura de seguridad es validada y documentada antes de los cambios de infraestructura | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | de conexión de red. | | |
| D4.C.Co.A.2 | La institución trabaja en estrecha colaboración con los proveedores de servicios de terceros para mantener y mejorar la seguridad de las conexiones externas. | N/A | |
| D4.C.Co.Inn.1 | Esquemas de conexiones externas son interactivo, muestran en tiempo real cambios en la infraestructura de conexión de red, nuevas conexiones y las fluctuaciones de volumen y avisa cuando los riesgos se presentan. | N/A | |
| D4.C.Co.Inn.2 | Las conexiones de la institución pueden ser segmentadas o cortadas instantáneamente para evitar contagio de ataques cibernéticos. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Dd.B.1 | Basado en el riesgo debida diligencia se realiza en terceros potenciales antes de que los contratos están firmados, incluidas revisiones de sus antecedentes, reputación, situación financiera, estabilidad y controles de seguridad. (FFIEC seguridad folleto, página 69) | "Fuente: IS.II.C.20: pg42: La administración debe supervisar las operaciones subcontratadas a través de lo siguiente: Diligencia debida apropiada en la investigación, selección y gestión de relaciones con terceros.<br>IS.WP.6.31: Determine si la administración supervisa adecuadamente la efectividad de los controles de seguridad de la información sobre las operaciones subcontratadas y es responsable de la mitigación de los riesgos relacionados con el uso de proveedores de servicios de terceros. Revise la diligencia debida involucrada, los controles de seguridad para mitigar el riesgo y las capacidades de monitoreo sobre los terceros de la institución.<br>MGT.III.C.8: pg34: Un programa de administración de terceros efectivo debe proporcionar el marco para que la administración identifique, mida, mitigue, monitoree e informe los riesgos asociados con el uso de proveedores externos. La gerencia debe desarrollar e implementar políticas y procedimientos para toda la empresa que rijan el programa de administración de terceros, incluido el establecimiento de objetivos y estrategias, la selección de un proveedor, la negociación del contrato y el monitoreo de la relación subcontratada.<br>MGT.WP.12.14.d: Un programa efectivo de gestión de terceros debe incorporar: Evaluación de posibles proveedores de terceros según el alcance y la criticidad de los servicios prestados ". | |
| D4.RM.Dd.B.2 | Se mantiene una lista de proveedores de servicios de terceros. (FFIEC Outsourcing folleto, página 19) | "Fuente: OT.B.19: Para aumentar la efectividad del monitoreo, la administración debe clasificar periódicamente las relaciones de los proveedores de servicios según el riesgo para determinar qué proveedores de servicios requieren un monitoreo más cercano.<br>OT.WP.I.1.3: Entreviste a la administración y revise la información de la institución para identificar ... las relaciones actuales de subcontratación, incluidas las relaciones de computación en la nube, y los cambios en esas relaciones desde el último examen. Identificar a cualquier proveedor de servicios de material subcontratistas; proveedores de servicios afiliados; proveedores externos con sede en el extranjero; volumen de transacciones actual en cada función subcontratada; Cualquier problema material experimentado con el servicio prestado; y proveedores de servicios con debilidades financieras o de control significativas ". | ID. AM-4: Sistemas de información externos son asignados y catalogados. (p. 20) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Dd.B.3 | Una evaluación del riesgo se realiza para identificar la criticidad de los proveedores de servicios. (FFIEC Outsourcing folleto, página 6) | "Fuente: OT.B.6: La gerencia debe considerar los siguientes factores al evaluar la cantidad de riesgo al inicio de una decisión de subcontratación, [incluidos] ... Los riesgos relacionados con la función subcontratada incluyen ... [y] Los riesgos relacionados con la tecnología utilizada .<br>OT.B.23: Las instituciones financieras también deben considerar cuáles de sus servicios financieros críticos dependen de los servicios de TSP, incluidos los principales proveedores de servicios de telecomunicaciones y redes.<br>MGT.III.C.8: pg34: La gerencia debe evaluar la calidad del servicio, el entorno de control y la condición financiera de los terceros que proporcionan a la institución servicios de TI críticos.<br>MGT.III.C.8: pg35: Algunos factores que la administración debe considerar o abordar con respecto a un programa efectivo de administración de terceros incluyen lo siguiente: Adaptación del programa de administración de la institución en base a una evaluación de riesgos inicial y continua del tercero de la institución. partes y los servicios que prestan.<br>MGT.WP.12.14: Un programa de administración de terceros efectivo debe incorporar lo siguiente:<br>Reevaluación de posibles proveedores externos en función del alcance y la criticidad de los servicios prestados.<br>mi. Adecuación del programa de monitoreo basado en la evaluación de riesgos inicial y continua de la tercera parte y los servicios prestados ". | |
| D4.RM.Dd.E.1 | Un proceso formal existe para analizar las evaluaciones de los controles de seguridad cibernética de terceros. | N/A | |
| D4.RM.Dd.E.2 | La Junta Directiva o un Comité apropiado los comentarios sobre un resumen de por resultados de diligencia, incluyendo las recomendaciones de manejo para uso de terceros que afectan el | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | perfil de riesgo inherente de la institución. | | |
| D4.RM.Dd.Int.1 | Es un proceso en el lugar para confirmar que los proveedores de servicios de terceros de la institución realización debido diligencia de sus terceras partes (por ejemplo, subcontratistas). | N/A | |
| D4.RM.Dd.Int.2 | Precontrato, física visitas de proveedores de alto riesgo se llevan a cabo por la institución o por un tercero calificado. | N/A | |
| D4.RM.Dd.A.1 | Un Programa de mejora de proceso continuo está en lugar para terceros por la actividad de la diligencia. | N/A | |
| D4.RM.Dd.A.2 | Auditorías de proveedores de alto riesgo se llevan a cabo sobre una base anual. | N/A | |
| D4.RM.Dd.Inn.1 | La institución promueve los esfuerzos sectoriales para construir por mecanismos de diligencia que conducen a fondo y eficiente seguridad y resistencia Comentarios. | N/A | |
| D4.RM.Dd.Inn.2 | La institución lidera esfuerzos para desarrollar nuevos procesos Auditables y para realización de Debida | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | diligencia y seguimiento de los riesgos de ciberseguridad planteadas por terceros. | | |
| D4.RM.Co.B.1 | Formal los contratos esa dirección requisitos relevantes de seguridad y privacidad están en lugar para todas las terceras partes que procesan, almacenan, o transmitir datos confidenciales o servicios críticos. (FFIEC seguridad folleto, página 7) | "Fuente: IS.II.C.20: pg42: Si el proveedor de servicios de terceros almacena, transmite, procesa o dispone la información del cliente, la administración debe exigir a los proveedores de servicios de terceros por contrato que implementen las medidas apropiadas diseñadas para cumplir con los requisitos. Normas de seguridad de la información.<br>IS.WP.6.31 (c): Determine si la administración supervisa adecuadamente la efectividad de los controles de seguridad de la información sobre las operaciones subcontratadas y es responsable de la mitigación de los riesgos relacionados con el uso de proveedores de servicios externos. Revise la diligencia debida involucrada, los controles de seguridad para mitigar el riesgo y las capacidades de monitoreo sobre los terceros de la institución. Revise las políticas, normas y procedimientos de la institución relacionados con el uso de los siguientes:<br>... Garantías contractuales de proveedores de servicios de terceros para responsabilidades de seguridad, controles e informes.<br>MGT.III.C.8: pág. 35: Los terceros deben respaldar las responsabilidades de los clientes de sus instituciones financieras para cumplir con todas las leyes, regulaciones y guías de supervisión aplicables.<br>MGT.III.C.8: pg35: Cuando la administración de la institución financiera contrata con proveedores externos para algunos o todos los servicios de TI, debe garantizar que los controles sobre las actividades subcontratadas proporcionen a la institución el mismo nivel de seguridad que los controles sobre las actividades realizadas en la casa ". | Comunicar requisitos Ciberseguridad con los actores interdependientes responsables para la entrega de servicios de infraestructura críticos esenciales. (p. 15) identificar y dirección individual privacidad y libertades civiles consecuencias que resulten del Ciberseguridad riesgo de Gobierno de Ciberseguridad de operaciones (p. 15). Identificar y autorizar el acceso. Medidas de sensibilización y Formación. Detección de actividad anómala revisado por cuestiones de privacidad. Informe sobre el intercambio de información personal dentro y fuera de la organización. PR. DS-1: Datos en reposo está protegido. (p. 25) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Co.B.2 | Contratos reconocen que el tercero es responsable por la seguridad de la información confidencial de la institución que lo posee, almacena, procesa o transmite. (FFIEC seguridad folleto, página 12) | "Fuente: IS.II.C.20: pg42: La gerencia debe supervisar las operaciones subcontratadas a través de lo siguiente: Garantías contractuales para responsabilidades de seguridad, controles e informes.<br>IS.WP.6.31 (c): Determine si la administración supervisa adecuadamente la efectividad de los controles de seguridad de la información sobre las operaciones subcontratadas y es responsable de la mitigación de los riesgos relacionados con el uso de proveedores de servicios externos. … Revise las políticas, estándares y procedimientos de la institución relacionados con el uso de lo siguiente: Garantías contractuales de proveedores de servicios de terceros para responsabilidades de seguridad, controles e informes ". | ID. GV-2: Roles de seguridad de la información y la responsabilidad son coordinados y alineados con roles internos y externos. (p. 21) |
| D4.RM.Co.B.3 | Los contratos estipulan que los controles de seguridad de terceros son regularmente revisados y validados por un partido independiente. (FFIEC seguridad folleto, página 12) | "Fuente: IS.II.C.20: pg42: La gerencia debe verificar que los proveedores de servicios externos implementen y mantengan controles suficientes para mitigar los riesgos de manera adecuada. Los contratos de la institución deben hacer lo siguiente: ... Especificar que la institución o un auditor independiente tiene acceso al proveedor de servicios para realizar evaluaciones del desempeño del proveedor de servicios en relación con los Estándares de seguridad de la información.<br><br>IS.WP.6.31.e: Determine si la administración supervisa adecuadamente la efectividad de los controles de seguridad de la información sobre las operaciones subcontratadas y es responsable de la mitigación de los riesgos relacionados con el uso de proveedores de servicios de terceros. … Revise las políticas, estándares y procedimientos de la institución relacionados con el uso de lo siguiente: Revisión independiente de la seguridad del proveedor de servicios de terceros a través de informes apropiados de auditorías y pruebas ". | |
| D4.RM.Co.B.4 | Contratos identifican el recurso disponible a la institución debe los terceros no cumplen con requisitos de seguridad definidos. (FFIEC Outsourcing folleto, página 12) | "Fuente: OT.B.12: Las instituciones deben incluir estándares de desempeño que definan los requisitos de nivel de servicio mínimo y soluciones para el incumplimiento de los estándares en el contrato.<br><br>OT.WP.I.3.4: Evalúe el proceso para celebrar un contrato con un proveedor de servicios. Considere si el contrato contiene acuerdos de nivel de servicio adecuados y medibles ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Co.B.5 | Contratos establecen responsabilidades para responder a incidentes de seguridad. (FFIEC E-Banking folleto, página 22) | "Fuente: IS.II.C.20: pg42: La gerencia debe supervisar las operaciones subcontratadas a través de lo siguiente:<br>• Garantías contractuales para las responsabilidades de seguridad, controles e informes.<br>• Coordinación de políticas de respuesta a incidentes y requisitos contractuales de notificación.<br>• Verificación de que la información y los riesgos de ciberseguridad se identifican, miden, mitigan, monitorean y reportan adecuadamente.<br>IS.WP.6.31 (f) & (g): revise las políticas, normas y procedimientos de la institución relacionados con el uso de los siguientes:<br>F. Coordinación de políticas de respuesta a incidentes y requisitos contractuales de notificación.<br>sol. Verificación de que la información y los riesgos de ciberseguridad se identifican, miden, mitigan, monitorean y reportan de manera apropiada ". | ID. GV-2: Roles de seguridad de la información y la responsabilidad son coordinados y alineados con roles internos y externos. (p. 21) |
| D4.RM.Co.B.6 | Los contratos especifican los requisitos de seguridad para la devolución o destrucción de datos en caso de terminación de contrato. (FFIEC Outsourcing folleto, página 15) | Fuente: OT.B.15: El contrato debe establecer requisitos de notificación y marco de tiempo y prever la devolución oportuna de los datos y recursos de la institución en un formato legible por máquina al momento de la terminación. Cualquier costo asociado con la asistencia de conversión también debe indicarse claramente. | |
| D4.RM.Co.E.1 | Responsabilidades para la gestión de dispositivos (por ejemplo, firewalls, routers) que aseguran las conexiones con terceras partes están documentadas formalmente en el contrato. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Co.E.2 | Responsabilidad para la notificación de incidentes de seguridad directas e indirectas y las vulnerabilidades se documenta en los contratos o acuerdos de nivel de servicio (SLAs). | N/A | "La organización entiende sus dependencias y socios y recibe información de estos socios que permite la colaboración y las decisiones de gestión basadas en el riesgo dentro de la organización en respuesta a los eventos (pág. 10) Comunicar los requisitos de ciberseguridad con las partes interesadas interdependientes responsables de la prestación de servicios esenciales de infraestructura crítica. (p. 15) " |
| D4.RM.Co.E.3 | Los contratos estipulan límites geográficos en donde los datos pueden ser almacenados o transmitidos. | N/A | |
| D4.RM.Co.Int.1 | Terceros SLAs o medios similares están en lugar que requieren notificación oportuna de eventos de seguridad. | N/A | |
| D4.RM.Co.A.1 | Contratos requieren de políticas de seguridad del proveedor de servicios de terceros cumplen o superan los de la institución. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Co.A.2 | Una estrategia de terminación o salida de terceros ha sido establecida y validado con la administración. | N/A | |
| D4.RM.Co.Inn.1 | La institución promueve un esfuerzo sectorial para influir en requisitos contractuales crítica por parte de terceros a la industria. | N/A | |
| D4.RM.Om.B.1 | La evaluación de riesgos de terceros se actualiza regularmente. (FFIEC Outsourcing folleto, página 3) | Fuente: OT.B.3: Los factores que las instituciones deberían considerar incluyen ... adaptar el programa de monitoreo de proveedores de servicios a nivel de toda la empresa basado en evaluaciones de riesgo iniciales y continuas de servicios subcontratados. | |
| D4.RM.Om.B.2 | Auditorías, evaluaciones e informes de desempeño se obtienen y revisaron regularmente validando controles de seguridad crítica por parte de terceros. (FFIEC seguridad folleto, página 86) | "Fuente: IS.II.C.20: pg42: La gerencia debe supervisar las operaciones subcontratadas a través de lo siguiente: ... Revisión independiente de la seguridad del tercero a través de informes apropiados de auditorías y pruebas.<br>IS.WP.6.31.e: Determine si la administración supervisa adecuadamente la efectividad de los controles de seguridad de la información sobre las operaciones subcontratadas y es responsable de la mitigación de los riesgos relacionados con el uso de proveedores de servicios de terceros ... Revise las políticas, estándares y procedimientos de la institución relacionados con el uso de lo siguiente: ... Revisión independiente de la seguridad del proveedor de servicios de terceros a través de informes apropiados de auditorías y pruebas.<br>MGT.III.C.8: pág. 34 Como parte del programa de administración de terceros de una institución financiera, la administración debe garantizar que los proveedores de terceros brinden apoyo de manera efectiva al hacer lo siguiente: Revisar los resultados de las auditorías independientes de los controles de TI de los proveedores de terceros .<br>MGT.WP.12.18: Al revisar la información provista por los proveedores externos de la institución, determine la calidad del seguimiento y la resolución de las preocupaciones de los clientes y los problemas con sus proveedores externos ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Om.B.3 | Prácticas de monitoreo permanentes incluyen revisión de planes de recuperación crítica de terceros. (FFIEC Outsourcing folleto, página 19) | "Fuente: OT.B.19: El programa debe supervisar el entorno del proveedor del servicio, incluidos sus controles de seguridad, fortaleza financiera y el impacto de cualquier evento externo.<br>OT.WP.I.3.6: Evaluar el proceso de la institución para monitorear el riesgo presentado por la relación del proveedor de servicios. Asegúrese de que el monitoreo aborde el entorno de control general del proveedor de servicios a través de la recepción y revisión de los informes de auditoría y reglamentarios apropiados; programa de recuperación ante desastres del proveedor de servicios y pruebas; seguridad de información.<br>MGT.WP.4.7.c: Determine si la administración tiene un proceso de monitoreo continuo efectivo de sus proveedores externos ". | |
| D4.RM.Om.E.1 | Un proceso para identificar nuevas relaciones de terceros está en lugar, incluyendo la identificación de nuevas relaciones que se establecieron sin la aprobación formal. | N/A | |
| D4.RM.Om.E.2 | Un Programa formal de asigna la responsabilidad de la Vigilancia continua de acceso de terceros. | N/A | |
| D4.RM.Om.E.3 | Supervisión de terceros se ajusta, en términos de profundidad y frecuencia, según el riesgo de terceros. | N/A | |
| D4.RM.Om.E.4 | Recordatorios automatizados o ticklers existen para identificar cuando se requiera información de terceros debe ser obtenida o analizado. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D4.RM.Om.Int.1 | Acceso de los empleados de terceros a datos confidenciales de la institución se realiza un seguimiento activamente basado en los principios de menor privilegio. | N/A | "PR.PT-3: El acceso a los sistemas y activos está controlado, incorporando el principio de funcionalidad mínima (p. 29)<br>DE.CM-6: La actividad del proveedor de servicios externo se monitorea para detectar posibles eventos de ciberseguridad. (p. 31) " |
| D4.RM.Om.Int.2 | Se llevan a cabo evaluaciones periódicas in situ de proveedores de alto riesgo para asegurar los controles de seguridad adecuados. | N/A | |
| D4.RM.Om.A.1 | Acceso de los empleados de terceros a datos confidenciales en sistemas host de terceros se realiza un seguimiento activamente a través de alertas e informes automatizados. | N/A | |
| D4.RM.Om.Inn.1 | La institución es líder en los esfuerzos para desarrollar nuevos procesos auditables para realizar monitoreo de riesgos de seguridad cibernética por parte de terceros. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Pl.B.1 | La institución ha documentado cómo reaccionar y responder a incidentes cibernéticos. (FFIEC negocio continuidad planificación folleto, página 4) | "Fuente: BCP.B.4: la planificación de la continuidad empresarial implica el desarrollo de un plan de continuidad empresarial (BCP) y la priorización de los objetivos empresariales y las operaciones críticas que son esenciales para la recuperación ... enfocados en el impacto de diversas amenazas que podrían potencialmente interrumpir las operaciones en lugar de en eventos específicos. BCP.WP.7.5: Determine la existencia de un BCP apropiado para toda la empresa. BCP.WP.10: Determine si las estrategias de gestión de riesgos de la institución financiera y TSP están diseñadas para lograr resiliencia, como la capacidad de responder de manera efectiva a las interrupciones a gran escala, incluidos los ataques cibernéticos y los ataques a múltiples sectores de infraestructura crítica. MGT.III.C.3: pg29: La administración de la institución debe desarrollar, implementar y probar periódicamente los procedimientos de respuesta a incidentes, que deben abordar la escalada, la remediación y la notificación de eventos e incidentes. MGT.III.C.3 (b): pg30: Para abordar el riesgo de ciberseguridad, el programa de seguridad de la información debe considerar lo siguiente: Gestión de incidentes cibernéticos y resiliencia. MGT.WP.12.8.a: Determine si una estructura de control incluye: Desarrollar e implementar procesos para identificar, proteger, detectar, responder y recuperar eventos e incidentes de seguridad ". | Administra el riesgo de Cibernético a través de un enfoque de toda la organización con políticas basadas en el riesgo, los procesos y procedimientos para enfrentar posibles eventos de Ciberseguridad y. ID. (p. 11) RA-6: Respuestas de riesgo identificadas y priorizadas. PR (p. 22) IP-9: Planes de respuesta (respuesta a incidentes y continuidad del negocio) y planes de recuperación (incidente de recuperación y recuperación ante desastres) están en su lugar y manejados. RS (p. 28). PL-1: Plan de respuesta se ejecuta durante o después de un evento. (p. 33) |
| D5.IR.Pl.B.2 | Canales de comunicación existen para proporcionar a empleados un medio para reportar eventos de seguridad de la información de manera oportuna. (FFIEC seguridad folleto, página 83) | "Fuente: IS.III: pg46: La gerencia debe establecer procesos definidos y una gobernanza adecuada para facilitar el desempeño de las operaciones de seguridad. Las políticas deben abordar el tiempo y el alcance de las actividades de las operaciones de seguridad, los informes, los activadores de escalamiento y las acciones de respuesta. IS.WP.2.7: Determine si los oficiales de seguridad y los empleados saben, comprenden y son responsables de cumplir con sus responsabilidades de seguridad ". | RS. CO-2: Eventos divulgan consistente con criterios establecidos. (p. 33) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Pl.B.3 | Se definen roles y responsabilidades para los miembros del equipo de respuesta a incidentes. (FFIEC seguridad folleto, Página 84) | "Fuente: IS.III.D: pg51: La preparación determina el éxito de cualquier respuesta de intrusión. Dicha preparación implica la definición de las políticas y procedimientos que guían la respuesta; la asignación de responsabilidades a los individuos ... IS.WP.8.6.e: Determine si la administración tiene procesos efectivos de respuesta a incidentes, incluidos los siguientes: ... Políticas y procedimientos para guiar la respuesta, asignando responsabilidades a los individuos; ... " | RS. CO-1: Personal conoce sus funciones y el orden de las operaciones cuando se necesita una respuesta. (p. 33) |
| D5.IR.Pl.B.4 | El equipo de respuesta incluye a individuos con una amplia gama de antecedentes y conocimientos de muchas áreas diferentes dentro de la institución (p. ej., administración, legal, relaciones públicas, así como tecnología de la información). (FFIEC seguridad folleto, Página 84) | "Fuente: IS.III.D: pg52: Debido a la amplia gama de problemas técnicos y no técnicos planteados por una intrusión, la membresía típica de SIRT incluye personas con una amplia gama de antecedentes y experiencia en diferentes áreas dentro de la institución. Estas áreas incluyen la administración, legal, y relaciones públicas, así como personal de TI. IS.WP.8.6.c: Determine si la administración tiene procesos efectivos de respuesta a incidentes, incluidos los siguientes: ... Equilibrio adecuado de personas y tecnologías adecuadas en la respuesta ". | PR. DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad. RC (p. 25). RP-1: Plan de recuperación es ejecutada durante o después de un evento. (p. 34) |
| D5.IR.Pl.B.5 | Un plan de backup y recuperación formal existe para todas las líneas de negocio. (FFIEC negocio continuidad planificación folleto, página 4) | "Fuente: BCP.B.4: El proceso de planificación de la continuidad del negocio debe incluir la recuperación, reanudación y mantenimiento de todos los aspectos del negocio, no solo la recuperación de los componentes tecnológicos. BCP.WP.3.1: Determine si el análisis de flujo de trabajo se realizó para garantizar que todos los departamentos y procesos de negocios estén cubiertos ". | ID. BE-5: Se establecen requisitos de resistencia para apoyar la prestación de los servicios críticos. PR (p. 21) DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad. PR (p. 25) IP-4: Copias de seguridad de la información se llevó a cabo, mantenidos y comprobarse periódicamente. (p. 27) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Pl.B.6 | Los planes de la institución para utilizar datos, recuperación ante desastres y continuidad del negocio de copia de seguridad Programas para recuperar las operaciones tras un incidente. (FFIEC seguridad folleto, página 71) | "Fuente: IS.II.C.21: pg43: los planes de continuidad de negocios deben revisarse como parte integral del proceso de seguridad. Las estrategias deben considerar los diferentes entornos de riesgo y el grado de mitigación de riesgo necesario para proteger a la institución si los planes de continuidad deben La gerencia debe capacitar al personal con respecto a sus roles de seguridad durante un desastre. Además, la gerencia debe actualizar las tecnologías y los planes para los sitios de respaldo y las redes de comunicaciones.<br>IS.WP.6.34: Determine si la administración administra efectivamente las siguientes consideraciones de seguridad de la información relacionadas con la planificación de la continuidad del negocio.<br>BCP.B.8: la evaluación de riesgos es el segundo paso en el proceso de planificación de la continuidad del negocio. Debe incluir: evaluar los supuestos del análisis de impacto en el negocio (BIA) utilizando varios escenarios de amenazas.<br>BCP.WP.I.4: Determine si la administración de riesgos adecuada sobre el proceso de continuidad del negocio está implementada y si las estrategias de administración de riesgos de la institución financiera y de TSP consideran escenarios de recuperación a gran escala diseñados para lograr resiliencia en toda la industria ". | PR. DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad. RC (p. 25). RP-1: Plan de recuperación es ejecutada durante o después de un evento. (p. 34) |
| D5.IR.Pl.E.1 | El plan de remediación y proceso describe las acciones atenuantes, los recursos y parámetros de tiempo. | N/A | ID.RA-6: Se identifican y priorizan las respuestas de riesgo. (p. 22) |
| D5.IR.Pl.E.2 | La recuperación corporativa ante desastres, continuidad del negocio y planes de manejo de crisis han integrado cuenta de incidentes cibernéticos. | N/A | |
| D5.IR.Pl.E.3 | Se han establecido procesos alternativos para continuar actividad crítica dentro de un período de tiempo razonable. | N/A | "ID.BE-5: Se han establecido los requisitos de resiliencia para respaldar la entrega de servicios críticos. (Pág. 21)<br>PR.DS-4: Capacidad adecuada |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | | | para asegurar que se mantenga la disponibilidad. (p. 25) " |
| D5.IR.Pl.E.4 | Análisis de impacto de negocios se han actualizado para incluir la seguridad cibernética. | N/A | |
| D5.IR.Pl.E.5 | Debida diligencia ha sido realizada en fuentes técnicas, consultores o empresas de servicio forense que podrían ser llamadas para asistir a la institución durante o después de un incidente. | N/A | |
| D5.IR.Pl.Int.1 | Es una estrategia para coordinar y comunicarse con las partes interesadas internas y externas durante o después de un ataque cibernético. | N/A | "RC.CO-2: Reputación después de reparar un evento. (P. 35)<br>RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y los equipos ejecutivos y de gestión. (p. 35) " |
| D5.IR.Pl.Int.2 | Los planes son para cambio de ruta o sustituir funciones vitales y/o servicios que pueden ser afectados por un ataque exitoso en los sistemas de conexión a Internet. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Pl.Int.3 | Un contrato cooperativo o contractual directa está en su lugar con una organización de respuesta a incidentes o proveedor (es) para ayudar a rápidamente con esfuerzos de mitigación. | N/A | |
| D5.IR.Pl.Int.4 | Lecciones aprendidas de la vida real ciber incidentes y ataques a la institución y otras organizaciones se utilizan para mejorar las capacidades de mitigación de riesgo y plan de respuesta de la institución. | N/A | "Adaptar las prácticas de ciberseguridad basadas en las lecciones aprendidas e indicadores predictivos derivados de actividades de ciberseguridad anteriores y actuales. (P. 11)<br>DE.AE-2: los eventos detectados se analizan para comprender los objetivos y los métodos de ataque. (p. 30)<br>RC.IM-1: Los planes de recuperación incorporan las lecciones aprendidas. (p. 35)<br>RC.IM-2: Se actualizan las estrategias de recuperación. (p. 35)<br>RS.IM-1: Los planes de respuesta incorporan las lecciones aprendidas. (p. 34)<br>DE.DP-5: los procesos de detección se mejoran continuamente. (p. 32)<br>RS.IM-2: Se actualizan las estrategias de respuesta. (p. 34) " |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Pl.A.1 | Métodos para responder a y recuperarse de incidentes cibernéticos son tejidos a lo largo de las unidades de negocio recuperación ante desastres, continuidad del negocio y planes de gestión de crisis. | N/A | |
| D5.IR.Pl.A.2 | Múltiples sistemas, Programas o procesos se ejecutan en un Programa de resistencia de Cibernético completo para mantener, minimizar y recuperar las operaciones de una amplia gama de incidentes cibernéticos potencialmente disruptivos y destructivos. | N/A | Responde a las amenazas evolutivas y sofisticadas de manera oportuna. (p. 11) |
| D5.IR.Pl.A.3 | Un proceso está en su lugar a mejorar continuamente el plan de resistencia. | N/A | |
| D5.IR.Pl.Inn.1 | El plan de respuesta a incidentes está diseñado para garantizar la recuperación de la interrupción de servicios, aseguramiento de la integridad de los datos y recuperación de datos perdidos o dañados tras un incidente de seguridad cibernética. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Pl.Inn.2 | El proceso de respuesta a incidentes incluye acciones detalladas y regla-basado en disparadores de respuesta automatizada. | N/A | |
| D5.IR.Te.B.1 | Escenarios se utilizan para mejorar la respuesta y la detección de incidentes. (FFIEC seguridad folleto, página 71) | "Fuente: IS.II.C.21: pg43: La administración debe hacer lo siguiente: ... Establecer y mantener políticas que aborden los conceptos de respuesta y resiliencia de incidentes de seguridad de la información, y probar los escenarios de incidentes de seguridad de la información.<br>BCP.B.J-13: Las amenazas cibernéticas continuarán desafiando la preparación para la continuidad del negocio. Las instituciones financieras deben permanecer conscientes de las amenazas y escenarios cibernéticos emergentes y considerar su impacto potencial en la resiliencia operativa.<br>BCP.WP.II.1.1: Determine si la estrategia de prueba aborda varios escenarios de eventos, incluidos los problemas potenciales encontrados durante una interrupción a gran escala ". | PR. IP-10: Planes de recuperación y respuesta son probados. (p. 28) |
| D5.IR.Te.B.2 | Pruebas de continuidad de negocio consiste en colaboración con la crítica de terceros. (FFIEC negocio continuidad planificación folleto, página J-6) | "Fuente: BCP.B.J-6: Las pruebas con terceros deben revelar la idoneidad de la capacidad de ambas organizaciones para recuperar, restaurar, reanudar y mantener las operaciones después de interrupciones, de conformidad con los requisitos comerciales y contractuales.<br>BCP.WP.I.9.3: Evaluar si el contrato de terceros TSP proporciona los siguientes elementos para garantizar la capacidad de recuperación del negocio ... Requisitos de prueba con el TSP ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Te.B.3 | Recuperación de sistemas, aplicaciones y datos se prueba por lo menos anualmente. (FFIEC negocio continuidad planificación folleto, página J-7) | "Fuente: BCP.BJ-7: Para servicios críticos, se requieren pruebas anuales o más frecuentes del plan de contingencia. Al igual que con todas las pruebas de BCP, la frecuencia debe ser impulsada por la evaluación de riesgos, la calificación de riesgos y cualquier cambio significativo de la institución financiera. Al entorno operativo.<br>BCP.WP.I.11.4: Determine si la estrategia de prueba incluye pautas para la frecuencia de las pruebas que son consistentes con la criticidad de las funciones empresariales, los objetivos de tiempo de recuperación (RTO), los objetivos de punto de recuperación (RPO) y la recuperación de la ruta crítica, como se define en el análisis de impacto empresarial (BIA) y la evaluación de riesgos, la política corporativa y las pautas regulatorias ". | PR. IP-10: Planes de recuperación y respuesta son probados. (p. 28) |
| D5.IR.Te.E.1 | Escenarios de recuperación incluyen planes para recuperarse de la destrucción de datos y el impacto a la integridad de los datos, pérdida de datos y la disponibilidad de datos y sistema. | N/A | DE.AE-4: Se determina el impacto del evento. (p. 30) |
| D5.IR.Te.E.2 | Los eventos informados ampliamente se utilizan para evaluar y mejorar la respuesta de la institución. | N/A | |
| D5.IR.Te.E.3 | Copias de seguridad de información se prueban periódicamente para verificar que sean accesibles y legibles. | N/A | PR.IP-4: Las copias de seguridad de la información se llevan a cabo, se mantienen y se prueban periódicamente. (p. 27) |
| D5.IR.Te.Int.1 | Escenarios de ataque cibernético se analizan para determinar el potencial impacto en | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | procesos críticos del negocio. | | |
| D5.IR.Te.Int.2 | La institución participa en ejercicios sectoriales Cibernético o escenarios (por ejemplo, FS-ISAC ataque cibernético (contra) los procesadores de pago (CAPP)). | N/A | |
| D5.IR.Te.Int.3 | Pruebas de resistencia se basan en el análisis e identificación de las amenazas realistas y muy probables, así como la institución de amenazas nuevas y emergentes. | N/A | |
| D5.IR.Te.Int.4 | Los procesos y sistemas en línea crítica se prueban para soportar las tensiones durante períodos prolongados (por ejemplo, DDoS). | N/A | |
| D5.IR.Te.Int.5 | Los resultados del ejercicio cibernético se utilizan para mejorar el plan de respuesta a incidentes y disparadores automatizados. | N/A | "RS.IM-2: Las estrategias de respuesta se actualizan (pág. 34)<br><br>RC.IM-2: Se actualizan las estrategias de recuperación. (p. 35) " |
| D5.IR.Te.A.1 | Prueba de resistencia es integral y coordinada en todas las funciones críticas del negocio. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.IR.Te.A.2 | La institución valida que es capaz de recuperarse de eventos cibernéticos similares a ataques sofisticados y conocidos de otras organizaciones. | N/A | |
| D5.IR.Te.A.3 | Pruebas de respuesta a incidentes evalúa la institución desde la perspectiva de un atacante para determinar cómo pueden orientarse hacia la institución o sus activos a la crítica de terceros. | N/A | |
| D5.IR.Te.A.4 | La institución corrige causas raíz de problemas descubiertos durante las pruebas de resistencia de ciberseguridad. | N/A | |
| D5.IR.Te.A.5 | Ciberseguridad se utilizan escenarios de incidentes que implican una pérdida financiera significativa al estrés prueba de gestión del riesgo de la institución. | N/A | |
| D5.IR.Te.Inn.1 | La institución las pruebas de la capacidad de cambiar procesos de negocio o funciones entre centros de procesamiento de diferentes sistemas o de tecnología para incidentes cibernéticos sin interrupción al negocio o la | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | pérdida de productividad o los datos. | | |
| D5.IR.Te.Inn.2 | La institución ha validado que es capaz de corregir sistemas dañados por ataques de día cero para mantener los actuales objetivos de tiempo de recuperación. | N/A | |
| D5.IR.Te.Inn.3 | La institución está liderando el desarrollo de entornos de pruebas más realistas. | N/A | |
| D5.IR.Te.Inn.4 | Escenarios de incidentes cibernéticos sirven para prueba de tensión posibles pérdidas financieras en el sector. | N/A | |
| D5.DR.De.B.1 | Se establecen parámetros de alerta para detectar incidentes de seguridad de la información que solicitan acciones de mitigación. (FFIEC seguridad folleto, página 43) | "Fuente: IS.II.C.15 (a): pg32: Para evitar el acceso no autorizado o una actividad inapropiada en el sistema operativo y las utilidades del sistema, la administración debe hacer lo siguiente:… Filtrar y revisar los registros para detectar posibles eventos de seguridad y proporcionar Informes y alertas.<br>IS.II.C.15 (b): pg33: La administración debe implementar controles efectivos de acceso a las aplicaciones al hacer lo siguiente:… Registrar el acceso y los eventos, definir alertas para eventos significativos y desarrollar procesos para monitorear y responder a anomalías y alertas.<br>IS.WP.6.21.f: Como parte del proceso de la administración para asegurar el sistema operativo y todos los componentes del sistema, determine si la administración hace lo siguiente: ... Filtra y revisa los registros para detectar posibles eventos de seguridad y proporciona informes y alertas adecuados.<br>IS.WP.6.22.f: Determine si la administración controla el acceso a las aplicaciones. Revise si la administración hace lo siguiente: ... Registra el acceso y los eventos, define alertas para eventos significativos y desarrolla procesos para monitorear y responder a anomalías y alertas ". | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.DR.De.B.2 | Informes de rendimiento del sistema contienen información que puede utilizarse como un indicador de riesgo para detectar incidentes de seguridad de la información. (FFIEC seguridad folleto, página 86) | "IS.II.D: pg45: El informe de riesgo es un proceso que produce informes de sistemas de información que abordan amenazas, capacidades, vulnerabilidades y cambios de riesgo inherentes. El informe de riesgo debe describir cualquier evento de seguridad de la información que enfrenta la institución y la efectividad de la respuesta de la administración. y resiliencia a esos eventos.<br>IS.WP.7.1: Determine si la institución tiene procesos de monitoreo y reporte de riesgos que abordan las condiciones cambiantes de amenaza tanto en la institución como en la industria financiera en general. Determine si estos procesos abordan los eventos de seguridad de la información que enfrenta la institución, la efectividad de la respuesta de la administración y la resistencia de la institución a esos eventos ". | |
| D5.DR.De.B.3 | Herramientas y procesos están en lugar para detectar, alertar y activar el Programa de respuesta a incidentes. (FFIEC seguridad folleto, Página 84) | "Fuente: IS.III.D: pg50: El programa de la institución debe tener protocolos definidos para declarar y responder a un incidente identificado.<br>IS.WP.8.6.a: Determine si la administración tiene procesos efectivos de respuesta a incidentes, incluidos los siguientes: Protocolos definidos en la política de respuesta a incidentes para declarar y responder a un incidente una vez identificado. " | |
| D5.DR.De.E.1 | La institución cuenta con procesos para la detección y alerta al equipo de respuesta a incidentes cuando actividad potencial información privilegiada manifiesta podría conducir a robo de datos o destrucción. | N/A | |
| D5.DR.De.Int.1 | El Programa de respuesta a incidentes se desencadena cuando se detectan comportamientos anómalos y ataque patrones o firmas. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.DR.De.Int.2 | La institución tiene la capacidad para descubrir la infiltración, antes de que el atacante atraviesa a través de sistemas, establece un equilibrio, roba información o causa daño a datos y sistemas. | N/A | |
| D5.DR.De.Int.3 | Los incidentes son detectados en tiempo real a través de procesos automatizados que incluyen alertas instantáneas al personal adecuado que pueda responder. | N/A | RS.CO-2: Los eventos se reportan de acuerdo con los criterios establecidos. (p. 33) |
| D5.DR.De.Int.4 | Alertas de red y sistema están correlacionados a través de unidades de negocio para mejor detectar y prevenir ataques multifacéticos (p. ej., simultánea DDoS ataque y cuenta de toma de posesión). | N/A | |
| D5.DR.De.Int.5 | Procesos de detección de incidentes son capaces de correlacionar eventos en toda la empresa. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.DR.De.A.1 | Se implementan tecnologías sofisticadas y adaptables que puede detectar y alertar al equipo de respuesta a incidentes de tareas específicas cuando indicadores de amenaza en toda la empresa indican potenciales amenazas externas e internas. | N/A | |
| D5.DR.De.A.2 | Herramientas automáticas se ejecutan para proporcionar supervisión de seguridad especializado basado en el riesgo de los activos para detectar y alertar a los equipos de respuesta a incidentes en tiempo real. | N/A | |
| D5.DR.De.Inn.1 | La institución es capaz de detectar y bloquear los intentos de día cero e informar a la gerencia y el equipo de respuesta a incidentes en tiempo real. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.DR.Re.B.1 | Apropiadas medidas para contener y controlar un incidente para prevenir el acceso no autorizado o uso de información del cliente. (FFIEC seguridad folleto, Página 84) | "Fuente: IS.III.D: pg52: Si bien las estrategias de contención entre instituciones pueden variar, por lo general incluyen los siguientes elementos generales: aislamiento de sistemas comprometidos o monitoreo mejorado de actividades de intrusos. Búsqueda de sistemas comprometidos adicionales. Recopilación y preservación de evidencia. Comunicación con las partes afectadas y, a menudo, con el regulador principal, las organizaciones de intercambio de información (por ejemplo, FS-ISAC) o la aplicación de la ley.<br>IS.WP.8.6.b: Determine si la administración tiene procesos efectivos de respuesta a incidentes, incluidos los siguientes: Procedimientos para minimizar el daño a través de la contención del incidente, restauración de sistemas, preservación de datos y pruebas, y notificación, según corresponda, a los clientes y otros según sea necesario " | ID. RA-4: Se analizan los impactos potenciales. (p. 22) |
| D5.DR.Re.E.1 | El plan de respuesta a incidentes está diseñado para dar prioridad a los incidentes, lo que permite una respuesta rápida para ciberseguridad importantes incidentes o vulnerabilidades. | N/A | ID.RA-6: Se identifican y priorizan las respuestas de riesgo. (p. 22) |
| D5.DR.Re.E.2 | Un proceso está en su lugar para ayudar a contener los incidentes y restaurar las operaciones con una interrupción mínima del servicio. | N/A | |
| D5.DR.Re.E.3 | Se desarrollan estrategias de contención y mitigación de varios tipos de incidente (por ejemplo, DDoS, malware). | N/A | |
| D5.DR.Re.E.4 | Los procedimientos incluyen estrategias de contención y notificar a | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | potencialmente afectadas terceras personas. | | |
| D5.DR.Re.E.5 | Procesos están en lugar para activar el Programa de respuesta a incidentes, cuando un incidente ocurre en una tercera parte. | N/A | |
| D5.DR.Re.E.6 | Registros son generados para apoyar la mitigación e investigación de incidentes. | N/A | RS.CO-2: Los eventos se reportan de acuerdo con los criterios establecidos. (p. 33) |
| D5.DR.Re.E.7 | La institución pide a terceros, según sea necesario, para proporcionar servicios de mitigación | N/A | |
| D5.DR.Re.E.8 | Análisis de eventos se utilizan para mejorar las políticas y medidas de seguridad de la institución. | N/A | Adapte las prácticas de ciberseguridad basadas en lecciones aprendidas e indicadores predictivos derivados de actividades de ciberseguridad anteriores y actuales. (p. 11) |
| D5.DR.Re.Int.1 | Análisis de incidentes de seguridad se realizan en las primeras etapas de una intrusión para minimizar el impacto del incidente. | N/A | |
| D5.DR.Re.Int.2 | Modificaciones a sistemas y aplicaciones o para acceder a los derechos necesarios para la gestión de incidencias son revisados por la gerencia | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | para su aprobación formal antes de la implementación. | | |
| D5.DR.Re.Int.3 | Procesos están en lugar para asegurar los activos afectados por un incidente de seguridad que no puede ser devueltos al estado de funcionamiento son en cuarentena, eliminados, eliminados o reemplazados. | N/A | |
| D5.DR.Re.Int.4 | Los procesos son para asegurar que los activos son restaurados apropiadamente reconfigurados y probados a fondo antes de ponerlos en funcionamiento. | N/A | |
| D5.DR.Re.A.1 | La función de gestión de incidencias colabora eficazmente con la función de inteligencia cibernética amenaza durante un incidente. | N/A | |
| D5.DR.Re.A.2 | Vínculos entre la inteligencia de amenaza, de operaciones y respuesta a incidentes permiten proactiva ante posibles labores. | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.DR.Re.A.3 | Las medidas técnicas aplican técnicas de defensa en profundidad como la inspección profunda de paquetes y agujerear negro para la detección y oportuna respuesta a los ataques basados en red relacionados con entrada anómala o patrones de tráfico de salida o ataques DDoS. | N/A | |
| D5.DR.Re.Inn.1 | Gestión del riesgo de la institución de los resultados de incidentes significativos Cibernético en limitarse a sin interrupciones a los servicios críticos. | N/A | |
| D5.DR.Re.Inn.2 | La infraestructura de la tecnología se ha diseñado para limitar los efectos de un ataque cibernético en el entorno de producción de migrar al entorno de backup (por ejemplo, con huecos de aire ambiente y procesos). | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.ER.Es.B.1 | Un proceso existe para personal que se encargan de analizar y responder a un incidente. (FFIEC seguridad folleto, página 83) | "Fuente: IS.III.C: pg50: Las políticas de escalamiento deben abordar cuándo se contactará con el personal diferente dentro de la organización y la responsabilidad que dicho personal tiene en el análisis y respuesta a incidentes.<br>IS.WP.8.5.h: Determine si la administración tiene procesos efectivos de identificación y evaluación de incidentes para hacer lo siguiente: Desarrollar procedimientos para probar la escalada de incidentes, la respuesta y los procesos de informes.<br>MGT.WP.2.8.f: Determine si la administración establece un proceso formal para obtener, analizar y responder a la información sobre amenazas y vulnerabilidades mediante el desarrollo de un programa de colaboración y de inteligencia de amenazas repetible ". | DE. DP-4: Detección de eventos información es comunicada a las partes apropiadas. RC (p. 32). CO-3: Actividades de recuperación serán comunicadas a los interesados internos y ejecutivo y gestión de equipos. (p. 35) |
| D5.ER.Es.B.2 | Existen los procedimientos para notificar a los clientes, reguladores y aplicación de la ley sea requerido o necesario, cuando la institución tenga conocimiento de un incidente que involucre el acceso no autorizado o uso de información confidencial de clientes. (FFIEC seguridad folleto, Página 84) | "Fuente: IS.III.D: pg51: Además, la administración debe definir umbrales para reportar incidentes de seguridad significativos, y considerar procesos de desarrollo para cuando la institución debe notificar a sus reguladores de incidentes que puedan afectar las operaciones, la reputación o la información confidencial de los clientes. .<br>IS.III.D: pg51: Protocolos para definir cuándo y en qué circunstancias notificar e involucrar a los reguladores, clientes y autoridades, incluidos los nombres y la información de contacto de cada grupo.<br>IS.WP.8.6.f: Determine si la administración tiene procesos efectivos de respuesta a incidentes, incluidos los siguientes: Umbrales para reportar incidentes de seguridad significativos y procesos para notificar, según corresponda, a los reguladores de la institución de aquellos incidentes que puedan afectar a la institución o al sistema financiero .<br>MGT.III.C.3: pg29: Desarrolle una política para escalar e informar los incidentes de seguridad a la junta, a las agencias gubernamentales, a las autoridades policiales y al principal regulador federal y estatal de la institución según los umbrales definidos por la institución financiera y los requisitos legales aplicables. Los umbrales relevantes podrían incluir un impacto financiero significativo, un tiempo de inactividad operacional significativo, una falla operativa o del sistema, o la pérdida de infraestructura crítica.<br>MGT.WP.2.2.f: Revise si la junta directiva aprueba una política para escalar e informar los incidentes de seguridad significativos a la junta directiva, al comité directivo, a las agencias gubernamentales y a la policía, según corresponda ". | RS. CO-3: La información es compartida consistente con criterios establecidos. (p. 33) |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| D5.ER.Es.B.3 | La institución Prepárate un informe anual de incidentes de seguridad o violaciones de la Junta o un Comité apropiado. (FFIEC seguridad peligros, página 5) | Fuente: es. I.B:PG4: Gestión debe presentar un informe a la Junta por lo menos anualmente que describe el estado general de las cuestiones de programa y material relacionado con el programa, incluyendo las siguientes: ... Las brechas de seguridad o violaciones de la ley o regulación y las respuestas de la administración a esos incidentes. ES. WP.2.4.e:... Determinar si el informe a la Junta Directiva describe el estado general del seguridad del programa de información y discute asuntos materiales relacionadas con el programa como los siguientes:... Las brechas de seguridad o las violaciones y las respuestas de la gerencia. | |
| D5.ER.Es.B.4 | Incidentes son clasificados, registrados y seguimiento. (FFIEC operaciones folleto, página 28) | "Fuente: IS.IB: pág. 4: La administración debe proporcionar un informe a la junta directiva al menos una vez al año que describa el estado general del programa y los asuntos materiales relacionados con el programa, incluidos los siguientes: ... Infracciones de seguridad o violaciones de la ley o reglamento y Las respuestas de la gerencia a tales incidentes.<br>IS.WP.2.4.e: ... Determine si el informe a la junta directiva describe el estado general del programa de seguridad de la información y analiza asuntos importantes relacionados con el programa, como los siguientes: ... Infracciones o violaciones de seguridad y las respuestas de la administración ". | RS. CO-2: Eventos divulgan consistente con criterios establecidos. (p. 33) |
| D5.ER.Es.E.1 | Se han establecido criterios para escalada de incidentes cibernéticos o vulnerabilidades a la Junta y senior gestión basada en el impacto y criticidad de los riesgos potenciales. | N/A | "ID.RA-4: Se analizan los impactos potenciales (p. 22)<br>DE.DP-4: La información de detección de eventos se comunica a las partes apropiadas. (p. 32)<br>DE.AE-4: Se determina el impacto del evento. (p. 30) " |
| D5.ER.Es.E.2 | Reguladores, aplicación de la ley y proveedores de servicios, según corresponda, se notificaron cuando la institución es consciente de cualquier acceso no autorizado a sistemas o que ocurra un incidente de Cibernético | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | podría resultar en la degradación de los servicios. | | |
| D5.ER.Es.E.3 | Incidentes cibernéticos orugas están correlacionados para análisis de tendencias e informes. | N/A | |
| D5.ER.Es.Int.1 | Empleados que son esenciales para mitigar el riesgo (por ejemplo, fraude, resistencia del negocio) conocen su papel en la escalada de incidentes. | N/A | |
| D5.ER.Es.Int.2 | Un plan de comunicación se utiliza para notificar a otras organizaciones, incluyendo terceros, de incidentes que puedan afectar a ellos o sus clientes. | N/A | |
| D5.ER.Es.Int.3 | Un plan de comunicación externa se utiliza para notificar a los medios de comunicación acerca de incidentes cuando sea aplicable. | N/A | RC.CO-1: Se gestionan las relaciones públicas. (p. 35) |
| D5.ER.Es.A.1 | La institución ha establecido indicadores cualitativos y cuantitativos para el proceso de respuesta a incidentes de | N/A | |

| Número de mapeo | Declaración | Aprendiz A Base Mapeo | FFIEC declarado Mapeo a Subcategorías NIST |
|---|---|---|---|
| | seguridad cibernética. | | |
| D5.ER.Es.A.2 | Métricas detalladas, pantallas de información y cartas de indicadores de que Cibernético incidentes y eventos se proporcionan a la gerencia y son parte del paquete de reunión de Junta Directiva. | N/A | |
| D5.ER.Es.Inn.1 | Un mecanismo está en lugar para proporcionar notificación instantánea de incidentes a gerencia y empleados esenciales a través de múltiples canales de comunicación con el seguimiento y verificación de la recepción. | N/A | |

## 10.4. Anexo 4. Resultados del Nivel de Madurez.

| Dominio | Madurez del dominio | Facto de evaluación | Factor de madurez de dominio | Componente | Base | Evolucionando | Intermedio | Avanzado | Innovador | Nivel de madurez estimado |
|---|---|---|---|---|---|---|---|---|---|---|
| 1: Gestión y supervisión del riesgo cibernético | Incompleto | 1: Gobierno | Incompleto | 1: Vigilancia | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Estrategia / Políticas | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 3: Gestión de activos de TI | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 2: Gestión de riesgos | Incompleto | 1: Gestión de riesgos Programa | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Evaluación de riesgos | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 3: Auditoria | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 3: Recursos | Incompleto | 1: Dotación de personal | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 4: Entrenamiento y Cultura | Incompleto | 1: Formación | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Cultura | 0% | 0% | 0% | 0% | 0% | Incompleto |
| 2: Inteligencia de amenazas y colaboración | Incompleto | 1: Inteligencia de amenazas | Incompleto | 1: Inteligencia de amenazas e información. | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 2: Monitoreo y análisis | Incompleto | 1: Monitoreo y análisis | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 3: Intercambio de información | Incompleto | 1: Intercambio de información | 0% | 0% | 0% | 0% | 0% | Incompleto |
| 3: Controles de ciberseguridad | Incompleto | 1: Controles Preventivos | Incompleto | 1: Gestión de infraestructura | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Acceso y gestión de datos | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 3: Dispositivo / seguridad de punto final | 0% | 0% | 0% | 0% | 0% | Incompleto |

| Dominio | Madurez del dominio | Facto de evaluación | Factor de madurez de dominio | Componente | Base | Evolucionando | Intermedio | Avanzado | Innovador | Nivel de madurez estimado |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 4: Codificación segura | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 2: Controles Detectivos | Incompleto | 1: Detección de amenazas y vulnerabilidad | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Detección de actividad anómala | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 3: Detección de eventos | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 3: Controles correctivos | Incompleto | 1: Gestión de parches | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Remediación | 0% | 0% | 0% | 0% | 0% | Incompleto |
| 4: Gestión de la dependencia externa | Incompleto | 1: Conexiones | Incompleto | 1: Conexiones | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | 2: Gestión de relaciones | Incompleto | 1: Debida Diligencia | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Contractos | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 3: Monitoreo continuo | 0% | 0% | 0% | 0% | 0% | Incompleto |
| 5: Gestión de incidentes cibernéticos y resiliencia | Incompleto | 1: Planificación y Estrategia de Resiliencia de Incidentes | Incompleto | 1: Planificación | 0% | 0% | 0% | 0% | 0% | Incompleto |
| | | | | 2: Pruebas | 0% | 0% | 0% | 0% | 0% | Incompleto |