



Guía de buenas prácticas para auditar la ciberseguridad



ASOBANCARIA

GUÍA DE BUENAS PRÁCTICAS PARA AUDITAR LA CIBERSEGURIDAD

Autores y colaboradores



Santiago Castro Gómez **Presidente**

Alejandro Vera Sandoval **Vicepresidente Técnico**

Colaboradores:

Grupo Bancolombia
Banco de Bogotá
BBVA
Banco W
Bancamía

Edición:

Liz Marcela Bejarano Castillo Directora Financiera y de Riesgos, Asobancaria.
Laura Sofía Rincón Profesionales Senior, Asobancaria.

Diseño: Babel Group

Este documento, publicado por la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, es producto del trabajo de un equipo interdisciplinario de entidades privadas interesadas en compartir estudios sobre temas bancarios, financieros, económicos, jurídicos y sociales de interés general, dirigidos a fortalecer las áreas de Auditoría Interna de las entidades financieras. El compartir Guías de Buenas Prácticas es una actividad permanente que se realiza entre las entidades agremiadas, entre estas y la Asociación, y entre la Asociación y otros actores como autoridades, centros de estudios, academia y otras agremiaciones. El contenido del presente documento tiene carácter netamente académico e ilustrativo, y, por tal motivo, no debe considerarse como un instrumento vinculante o una hoja de ruta o plan de acción para las entidades agremiadas a Asobancaria o para otros lectores de este.



Índice

01	SIGLAS	PAG. 11
02	GLOSARIO	PAG. 15
03	PRESENTACIÓN	PAG. 19
04	INTRODUCCIÓN	PAG. 23
05	REVISIÓN DE LOS MARCOS INTERNACIONALES DE CIBERSEGURIDAD	PAG. 27
06	MARCO NORMATIVO COLOMBIANO PARA GESTIÓN DEL RIESGO DE CIBERSEGURIDAD	PAG. 61
07	LA POSTURA DE LA AUDITORÍA INTERNA FRENTE AL RIESGO DE CIBERSEGURIDAD	PAG. 67
08	CIBER RESILIENCIA	PAG. 75
09	CONCLUSIONES	PAG. 81

Siglas

- **NIST:** Instituto Nacional de Estándares y Tecnología.
- **SFC:** Superintendencia Financiera de Colombia.
- **IT:** Tecnología de la Información (siglas en inglés).
- **US-CERT:** Equipo de preparación ante emergencias informáticas de Estados Unidos (por sus siglas en inglés).
- **NIIP:** Plan Nacional de Protección de Infraestructura de Estados Unidos (siglas en inglés).
- **CIS:** Centro para la Seguridad en Internet.
- **STIG:** Guías de Implementación Técnica de Seguridad.
- **CVSS:** Sistema de Puntaje de Vulnerabilidades Comunes.
- **IDS:** Sistemas de Detección de Intrusión.
- **DDoS:** Ataque de Denegación del Servicio Distribuido.
- **TIC:** Tecnologías de la Información y la Comunicación.



| **Glosario**

- **Air-gapping:** es una medida de seguridad de la red empleada en uno o más ordenadores para asegurar que una red está físicamente aislada de redes no seguras.
- **Ataque man in the middle:** es un ataque en donde se introduce un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y la fuente.
- **Border router:** es un dispositivo de red que reenvía paquetes de datos entre redes de computadoras.
- **Ciberseguridad:** es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.
- **Diagramas de flujo de los datos:** corresponde a la representación gráfica del flujo de datos a través de un sistema de información.
- **Diagramas de red lógica:** ilustra el flujo de información a través de la red y muestra cómo se comunican los dispositivos entre sí.
- **DMZ:** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.
- **Encriptación end to end:** permite que todo el tráfico de información desde un origen hasta un destino esté totalmente cifrado y autenticado, para que, si alguien captura dicho tráfico, no pueda leer la información que hay en su interior.
- **Ethical Hacking:** es una práctica común que consiste en hackear los sistemas informáticos propios para reforzar su seguridad.
- **Firewalls:** es la parte de un sistema informático o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- **Firmware:** es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.
- **Malware:** es un software malintencionado que realiza acciones dañinas en un sistema informático.
- **Matriz RACI:** es una matriz de asignación de responsabilidad o un gráfico de responsabilidad lineal.
- **Middleware:** es el software que se sitúa entre un sistema operativo y las aplicaciones que se ejecutan en él.
- **Patch management:** es el proceso que ayuda a adquirir, probar e instalar múltiples cambios de código en las aplicaciones y herramientas de software existentes en una computadora, este permite que los sistemas se mantengan actualizados.
- **Seguridad de la Información:** es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.
- **Software:** es el soporte lógico de un sistema informático.
- **VLAN:** es un método para crear redes lógicas independientes dentro de una misma red física.



Presentación

La era digital presenta un importante reto para la gestión de la Auditoría Interna, la cual ha tenido que adaptar sus capacidades a los riesgos emergentes derivados de la ciberseguridad, que se ha exacerbado por las constantes inversiones de las entidades en innovación tecnológica. Lo anterior, no es ajeno al negocio bancario, que ha debido robustecer sus sistemas para afrontar el riesgo cibernético, no solo en materia de identificación de los ataques, sino también en la creación de prácticas para solventar el eslabón más débil de la cadena de ciberseguridad, el recurso humano.

Bajo este contexto, esta Guía de Buenas Prácticas busca ser una ayuda para los auditores internos de las entidades financieras, pues a partir del análisis de un marco internacional y de la normativa local podrán desarrollar políticas para hacer frente al riesgo cibernético. Lo anterior, les permitirá no solo adoptar medidas para auditar su capacidad de reaccionar ante un ataque, sino también la preparación y resiliencia de la organización frente a una situación de riesgo.



Introducción


En la actualidad, el crecimiento en el uso de la tecnología en todos los sectores productivos y el auge de la economía digital, han traído como consecuencia un incremento en el volumen y la sofisticación de los ataques cibernéticos a nivel global. Por esta razón, es fundamental que las organizaciones cuenten con programas formales para auditar las estrategias y procesos asociados a la gestión del riesgo cibernético, usando *frameworks* y mejores prácticas relacionados con la ciberseguridad.

Un punto inicial que es importante tener en cuenta al momento de diseñar un programa de auditoría de ciberseguridad es considerar los siguientes aspectos:

- Frameworks y best practices relacionadas con Ciberseguridad.
- Leyes y regulaciones asociadas con Ciberseguridad.
- Riesgos relevantes relacionados con Ciberseguridad.
- Estrategia de Ciberseguridad de la Organización.
- Políticas, procedimientos y procesos que impactan la Ciberseguridad.
- Sistemas críticos y controles claves de Ciberseguridad.
- Gestión de identidades y accesos.
- Programas de concienciación en Ciberseguridad para la organización y aliados estratégicos.
- Sistemas de Monitoreo de Ciberseguridad.
- Sistemas de respuesta y recuperación ante incidentes de Ciberseguridad.

Esta Guía de Buenas Prácticas desarrolla cuatro apartados. En la primera sección, se encuentra una guía de auditoría en la que se detallan las categorías, objetivos de control y pruebas asociadas a cada una de las funciones del Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), así como las referencias a COBIT 5 y otros marcos de referencia y prácticas internacionales para cada uno de los controles.

En el capítulo siguiente, se presenta un resumen de las disposiciones de la Circular Externa (CE) N°007 de la Superintendencia Financiera de Colombia (SFC) relacionada con los requerimientos mínimos de ciberseguridad que deben cumplir las entidades financieras. En el capítulo tres se explican los diez lineamientos que debe seguir la Auditoría Interna frente a la ciberseguridad; y en el cuarto, las medidas para auditar la resiliencia de la organización ante un evento que atente contra la seguridad informática.

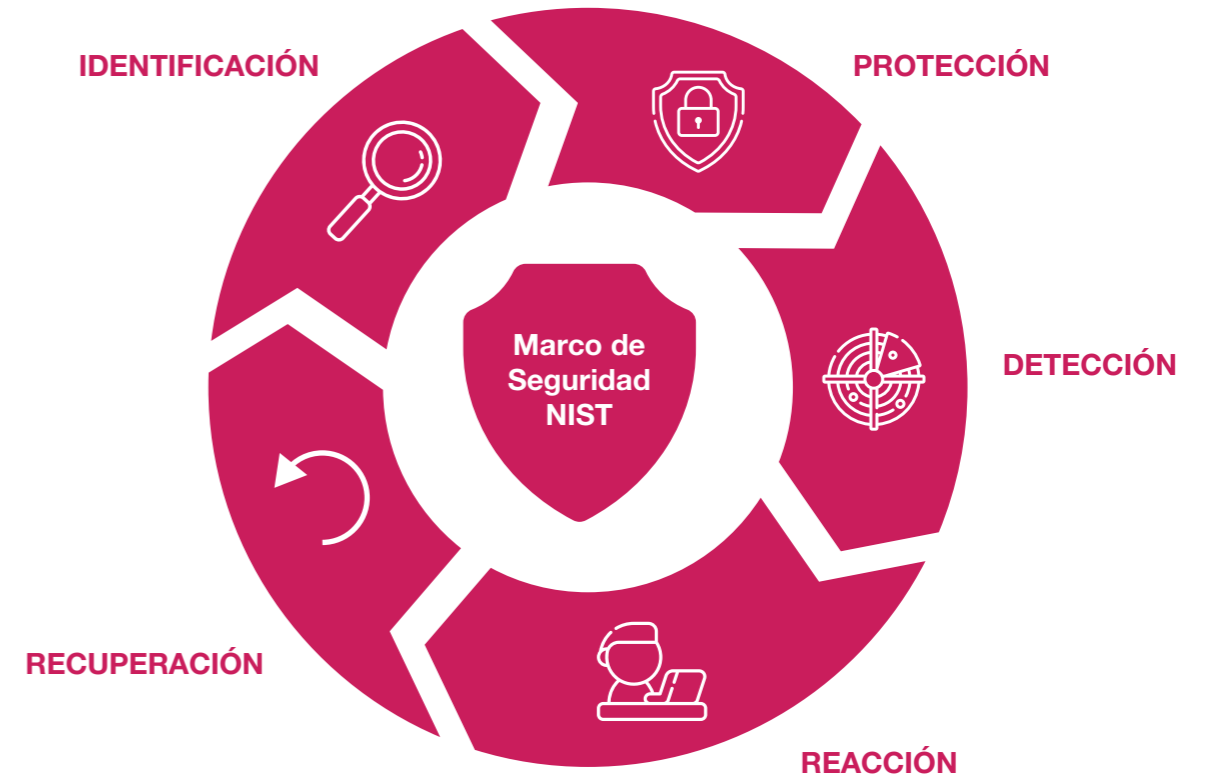


**Revisión de los
marcos
internacionales
de ciberseguridad**

Uno de los frameworks más importantes en relación con la ciberseguridad es el “Marco para la mejora de la seguridad cibernética en infraestructuras críticas”¹ publicado por el NIST el cual propone cinco funciones que ayudan a una organización en la estructuración de su programa de gestión

del riesgo cibernético, lo que facilita la toma de decisiones, identificando y abordando amenazas y mejorando la capacidad de aprendizaje de actividades previas.

Gráfico 1 Funciones definidas en el Cybersecurity Framework - NIST



¹ Instituto Nacional de Estándares y Tecnología (Abril 2018). “Cybersecurity Framework”. Recuperado de: <https://www.nist.gov/cyberframework/framework>

Con base en estas cinco funciones se pueden establecer objetivos de control y una serie de acciones para realizar evaluaciones de auditoría de ciberseguridad, apoyados en las categorías y subcategorías definidas en el Marco:

- **Identificar:** permite desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. Las actividades que engloban esta función son fundamentales para el uso efectivo del marco.
- **Proteger:** describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento que atente a la ciberseguridad.
- **Detectar:** define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo su descubrimiento oportuno. Los ejemplos de categorías de resultados dentro de esta función incluyen: anomalías y eventos, monitoreo continuo de seguridad y procesos de detección.
- **Responder:** incluye actividades necesarias para tomar medidas frente a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial ataque. Algunos ejemplos

de categorías de esta función son: planificación de respuesta, comunicaciones, análisis, mitigación y mejoras.

- **Recuperar:** permite identificar las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado como consecuencia de un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

A continuación, se presenta una guía de auditoría² en la que se detallan las categorías, objetivos de control y pruebas asociadas a cada una de las funciones del Marco de Ciberseguridad de NIST, así como las referencias a COBIT 5 y otros marcos de referencia y prácticas internacionales para cada uno de los controles.

Programa de Auditoría y Ciberseguridad³

IDENTIFICAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Administración de activos	Los datos, el personal, los dispositivos, los sistemas, y las instalaciones que permiten a la organización alcanzar los objetivos empresariales están identificados y gestionados de acuerdo con su importancia relativa para el logro de los objetivos empresariales y de la estrategia de riesgo de la organización.	Los dispositivos y sistemas físicos al interior de la organización están inventariados.	Obtener una copia del inventario de dispositivos y sistemas físicos. Revisar el inventario considerando lo siguiente: a. Alcance de los dispositivos y sistemas físicos con base en el apetito al riesgo de la organización (p.ej., sistemas que contienen información sensible, permiten el acceso a la red, o son críticos para los objetivos empresariales). b. Completitud del inventario (p.ej., ubicación, número del activo, dueño). c. El proceso de recopilación del inventario garantiza que los nuevos dispositivos sean recopilados adecuadamente y a tiempo (p.ej., software automatizado para detectar y/o almacenar el inventario). d. Frecuencia de las revisiones del inventario.
		Las plataformas de software y aplicaciones al interior de la organización están inventariadas.	
		El flujo de la comunicación organizacional y de datos está mapeado.	Garantizar que la organización mantenga copias adecuadas y actuales de los diagramas de flujo de los datos (DFD), diagramas de red lógica (LND), y/u otros diagramas que muestren el flujo de datos y comunicación organizacional.
		Los sistemas de información externos están catalogados.	Si la organización depende de sistemas de información prestados por terceros, obtener una copia del inventario de sistemas externos. Revise el inventario de terceros considerando lo siguiente: a. Alcance de los sistemas externos con base en el apetito al riesgo de la organización. b. Completitud del inventario. c. El proceso de recopilación del inventario garantiza que nuevos sistemas sean recopilados adecuadamente y a tiempo. d. Frecuencia de las revisiones del inventario.
		Los recursos (p.ej., hardware, dispositivos, datos y software) están priorizados de acuerdo a su clasificación, criticidad y valor para el negocio.	1. Obtener una copia del programa de clasificación de datos de la organización (la clasificación también puede ser identificada en la evaluación de riesgos y en el análisis de impacto al negocio). 2. Revisar el programa para determinar si los recursos clave (p.ej., hardware, dispositivos, datos, software) están clasificados y priorizados con base en criticidad y valor comercial.

² Esta guía está basada en la traducción y adaptación libre del documento de ISACA "IS Audit/Assurance Program for Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program" el cual se puede consultar en <https://www.isaca.org/bookstore/cybersecurity-resources/wcsnistf>

³ Marcos de referencia: (i) COBIT 5; (ii) ISO/IEC 27001:2013; (iii) ISO 22301

IDENTIFICAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Están establecidos los roles y responsabilidades de ciberseguridad para todos los empleados y terceros (p.ej., proveedores, clientes, socios).	Revisar las políticas de ciberseguridad, de seguridad de la información, descripciones de trabajo, acuerdos, matriz RACI, acuerdos de nivel de servicios y/o contratos para determinar si incluyen los roles y responsabilidades de ciberseguridad.
Entorno del negocio	La misión, los objetivos, las partes interesadas, y las actividades de la organización se entienden y están priorizados; esta información es usada para informar los roles y responsabilidades de ciberseguridad, y las decisiones de gestión de riesgos.	El rol de la organización en la cadena de abastecimiento está identificado y comunicado.	Obtener la documentación o evidencia (p.ej., estrategia de ciberseguridad, plan de continuidad del negocio, procedimientos de adquisición de sistemas de información, análisis de impacto al negocio, procedimientos de adquisición, revisión de proveedores clave, manejo de las relaciones con proveedores, reportes de debida diligencia de los proveedores) para determinar si la organización ha definido claramente y entiende su papel en la cadena de suministro.
		El lugar de la organización en la infraestructura crítica y su sector industrial está identificado y comunicado.	Obtener la documentación o evidencia (p.ej., estatuto de la misión, política de continuidad del negocio, plan estratégico) para determinar si la organización ha definido claramente y entiende su papel en su sector industrial y su papel dentro de la infraestructura crítica nacional. ⁴
		Las prioridades para la misión, objetivos y actividades de la organización están establecidas y comunicadas.	<ol style="list-style-type: none"> Determinar si la organización tiene un plan estratégico que define los objetivos de la empresa. Se debe asegurar que los objetivos de la empresa están alineados con los intereses de las partes interesadas. Determinar si el estatuto de la misión y los objetivos están claramente publicados, de tal forma que los trabajadores puedan verlos y acceder a ellos fácilmente. Determinar si un plan estratégico de IT está documentado, define funciones y está mapeado a los objetivos de la empresa. Determinar si los trabajadores saben sobre la misión y los objetivos de la organización.
		Las dependencias y funciones críticas para la prestación de servicios críticos están establecidas.	Obtener el plan de continuidad del negocio, el plan de recuperación ante desastres, el análisis del impacto del negocio y las evaluaciones de riesgos, y revisar lo siguiente:

⁴ Tomado de Department of Homeland Security. (<https://www.dhs.gov/what-critical-infrastructure>).

IDENTIFICAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<ol style="list-style-type: none"> Los sistemas de información y software que apoyan funciones críticas del negocio están identificados y priorizados en función del tiempo máximo de inactividad permitido. Los terceros que apoyan funciones críticas del negocio y los sistemas de información/software están identificados y priorizados.
		Los requerimientos de resiliencia para soportar la prestación de servicios críticos están establecidos.	<ol style="list-style-type: none"> Determinar si los planes de continuidad y recuperación ante desastres de la organización (incluyendo el análisis de impacto al negocio) respaldan la capacidad de recuperación de los servicios críticos. Determinar si existe información apropiada para realizar una debida diligencia (p.ej., plan de continuidad del negocio, acuerdos de nivel de servicio, reportes de control de servicio de la organización) y si está revisada para garantizar que los requisitos de recuperación de la organización puedan cumplirse para los servicios críticos de terceros.
Gobierno	Las políticas, procedimientos, y procesos para administrar y monitorear los requisitos reglamentarios, legales, de riesgo, del entorno y operativos de la organización se entienden e informan sobre la gestión de riesgos de ciberseguridad.	La política de seguridad de la información de la organización está establecida.	<ol style="list-style-type: none"> Obtener una copia de la política de seguridad de la información. Determinar si la política está completa y si ha sido aprobada por la estructura de gobierno al interior de la organización. Determinar si la política está comunicada a los empleados.
		Los roles y responsabilidades de seguridad de la información están coordinados y alineados con las funciones internas y socios externos.	<ol style="list-style-type: none"> Determinar si los roles y responsabilidades de seguridad de la información están definidos. Los roles y responsabilidades pueden definirse en políticas, descripciones de trabajo, acuerdos, matriz RACI, cuadros jerárquicos y/o contratos. Determinar si hay suficiente independencia al interior de los roles de seguridad de la información para proporcionar una adecuada separación de las funciones críticas. Revisar contratos, acuerdos de confidencialidad y de nivel de servicio con proveedores críticos para determinar si los controles y la notificación de incidentes de ciberseguridad se abordan adecuadamente.

IDENTIFICAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Los requerimientos legales y reglamentarios relacionados con la ciberseguridad, incluyendo las obligaciones de privacidad y libertades civiles, se comprenden y manejan.	<ol style="list-style-type: none"> 1. Obtener una lista de todos los requisitos legales y reglamentarios para la organización. 2. Determinar si el programa de ciberseguridad está mapeado a los requisitos legales y reglamentarios. 3. Revisar cualquier examen o auditoría reglamentaria reciente de ciberseguridad. Si cualquier excepción fue observada en las auditorías, determinar cómo la organización respondió a las excepciones. 4. Determinar si los contratos críticos con terceros son revisados por un asesor legal previamente a su ejecución. 5. Determinar si existe un proceso formal para monitorear y revisar cambios en las leyes y regulaciones de ciberseguridad.
		Los procesos de Gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.	Determinar la idoneidad de la supervisión ejecutiva o de la junta y la comprensión de ciberseguridad. Considere lo siguiente: <ol style="list-style-type: none"> a. Gestión de riesgos. b. Estructuras de Gobierno. c. Supervisión de seguridad. d. Entrenamiento/formación. e. Responsabilidad. f. Reporte.
Evaluación de riesgos	La organización comprende los riesgos de ciberseguridad de las operaciones, los activos y los individuos.	Las vulnerabilidades de los activos están identificadas y documentadas.	Determinar si las pruebas de vulnerabilidad son conducidas y analizadas en activos organizacionales críticos (p. ej., activos importantes para los objetivos empresariales y la estrategia de riesgo de la organización).
		La información sobre amenazas y vulnerabilidad se recibe de foros y fuentes de intercambio de información.	<ol style="list-style-type: none"> 1. Determinar si la organización es miembro o está suscrita a una organización de intercambio de información sobre amenazas y vulnerabilidad (p.ej., United States Computer Emergency Readiness Team [US-CERT]). 2. Determinar si la organización tiene un proceso formal para difundir información sobre amenazas y vulnerabilidad a individuos con la experticia para revisar la información y la autoridad para mitigar el riesgo que representan para la organización.

IDENTIFICAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Amenazas, tanto internas como externas, están identificadas y documentadas.	<ol style="list-style-type: none"> 1. Revisar las evaluaciones de riesgo para determinar si amenazas internas y externas están identificadas y documentadas. 2. Determinar si la organización ha desarrollado procesos para monitorear y reportar activamente potenciales amenazas.
		Impactos potenciales al negocio y sus probabilidades están identificados.	Revisar las evaluaciones de riesgos y el análisis de impacto al negocio para determinar si impactos probables y potenciales están identificados y analizados en busca de amenazas.
		Las amenazas, vulnerabilidades, probabilidades e impactos son usados para la determinación de riesgos.	<ol style="list-style-type: none"> 1. Determinar si el proceso de evaluación de riesgos identifica amenazas y vulnerabilidades internas y externas razonablemente predecibles, el probable y potencial daño de dichas amenazas, y la suficiencia de los controles para mitigar el riesgo asociado a dichas amenazas. 2. Revisar los resultados relacionados con los tiempos tolerables por la organización para recuperar sus procesos de negocio, productos y servicios críticos.
		Las respuestas a los riesgos están identificadas y priorizadas.	<ol style="list-style-type: none"> 1. Obtener el plan de gestión de riesgos de la organización y/o otra documentación que muestre su respuesta a los niveles de riesgo identificados en la evaluación de riesgos. 2. Determinar si el plan de gestión de riesgos está diseñando para aceptar o reducir el nivel de riesgo de acuerdo con el apetito de riesgo de la organización. 3. Obtener copias de las respuestas de gestión a recientes auditorías y evaluaciones relacionadas con ciberseguridad para determinar si excepciones observadas en auditorías y evaluaciones están identificadas y priorizadas.
Estrategia de gestión de riesgos	Las prioridades, restricciones, tolerancias de riesgo, y suposiciones de la organización se establecen y usan para respaldar las decisiones de riesgo operacional.	Los procesos de gestión de riesgos están establecidos, gestionados y acordados por los terceros o partes interesadas de la organización.	<p>Evaluar el marco o proceso utilizado para la gestión del riesgo. Considere lo siguiente:</p> <ol style="list-style-type: none"> a. ¿Está el proceso formalmente documentado? b. ¿El proceso es actualizado regularmente? c. ¿Es el proceso repetible y medible? d. ¿Tiene dueño el proceso? e. ¿Están las partes interesadas involucradas o informadas sobre el proceso?

IDENTIFICAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		La tolerancia al riesgo organizacional está determinada y claramente expresada.	Determinar si la organización ha definido y aprobado un estatuto de apetito al riesgo cibernético.
		La determinación de la organización frente a la tolerancia al riesgo se basa en su papel en la infraestructura crítica y el análisis de riesgos específicos del sector.	Obtener una copia de la estrategia de gestión de riesgo y estatuto de apetito al riesgo de la organización para determinar si están alineados con su rol en la infraestructura crítica (como está definido por el plan nacional de protección de infraestructura [NIPP] y planes específicos del sector).

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Control de acceso	El acceso a los activos y las instalaciones asociadas está limitado para usuarios, procesos, o dispositivos autorizados, y para actividades y transacciones autorizadas.	Las identidades y credenciales están administradas para dispositivos y usuarios autorizados.	<ol style="list-style-type: none"> Determinar si el acceso a dispositivos de red (p.ej., servidores, estaciones de trabajo, dispositivos móviles, firewalls) está restringido por: <ol style="list-style-type: none"> Único ID de usuario para inicio de sesión. Contraseñas complejas. Autenticación de múltiples factores. Cierre automático si se deja desatendido. Bloqueo automático después de repetidos intentos fallidos de acceso. Cambio de nombre y contraseña predeterminados para cuentas administrativas. Determinar si los parámetros de contraseña cumplen con la política de la organización y/o los requisitos aplicables de la industria. Considere lo siguiente: <ol style="list-style-type: none"> Longitud, complejidad, requisitos de cambio, historia ¿Se suprimen las contraseñas de todos los resultados? ¿Los archivos de contraseña están encriptados y restringidos? Revisar los procedimientos de terminación para garantizar que las credenciales se revocan o cambian cuando un empleado se va. <ol style="list-style-type: none"> Verifique las cuentas para garantizar que el acceso del usuario se revoque después de la terminación y que las cuentas se eliminen de acuerdo con las políticas.

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		El acceso físico a los activos está administrado y protegido.	<ol style="list-style-type: none"> Determinar si el acceso físico a activos clave está físicamente restringido: <ol style="list-style-type: none"> Puertas cerradas. Vigilancia. Cercas o muros. Registros. Acompañamiento al visitante. Determinar si las políticas y procedimientos permiten el acceso únicamente a personal autorizado a áreas sensibles. Revisar los procedimientos de terminación para asegurar que el acceso físico se remueve cuando el empleado se va.
		El acceso remoto está administrado.	<p>Determinar si las políticas y los procedimientos relacionados con las capacidades de acceso de los usuarios remotos están formalizados. Considere lo siguiente:</p> <ol style="list-style-type: none"> Usuarios remotos (p.ej., empleados, contratistas, terceros) con acceso a los sistemas críticos están aprobados y documentados. Conexiones remotas son solo abiertas según sea requerido. Conexiones remotas están registradas y monitoreadas. Conexiones remotas están encriptadas. Existe una autenticación fuerte (p.ej., múltiples factores, parámetros de contraseña fuertes). La capacidad para borrar datos de forma remota en dispositivos móviles cuando faltan datos o son robados está habilitada. Los controles de seguridad de la institución (p.ej., antivirus, patch management) son requeridos en dispositivos remotos que se conectan a la red.
		Los permisos de acceso se manejan, incorporando los principios de mínimos privilegios y separación de deberes.	<ol style="list-style-type: none"> Revisar los derechos y permisos de acceso a la red y a cualquier aplicación crítica. Determinar si los perfiles de acceso del usuario son consistentes con sus funciones de trabajo (con base en el mínimo privilegio). Comparar una muestra de la autoridad de acceso de los usuarios con sus deberes y responsabilidades asignadas. Determinar si el acceso está otorgado para funciones de misión crítica y funciones de soporte de sistemas de información para reducir el riesgo de actividad maliciosa sin conclusión (p.ej. procesos críticos que requieren que dos personas realicen una función).

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			5 Determinar si los usuarios con privilegios de administrador local en estaciones de trabajo requieren este nivel de acceso. 6. Revisar cómo la organización restringe y/o monitorea el acceso a datos sensibles por parte de usuarios con altos privilegios en la red. 7. Determinar si los controles de acceso basados en roles están implementados (p.ej., roles vs. usuarios que tienen asignados derechos de acceso). 8. Determinar si hay revisiones regulares al acceso.
		La integridad de la red es protegida, e incorpora la segregación de la red donde es apropiado.	1. Revisar los diagramas de red y de flujo de datos. 2. Determinar si los sistemas de alto costo/críticos están separados de los sistemas de alto riesgo (p.ej., VLAN, DMZ, copias de seguridad duras, air-gapping) cuando es posible. 3. Determinar si la organización tiene un proceso formal para aprobar el flujo de datos y/o conexiones entre redes y/o sistemas.
Entrenamiento de conciencia	El personal y los socios de la organización están provistos de educación sobre concientización en ciberseguridad, y están capacitados adecuadamente para realizar deberes y responsabilidades relacionados con la seguridad de la información de acuerdo con las políticas, los procedimientos y los acuerdos relacionados.	Todos los usuarios están informados y capacitados.	1. Revisar las políticas de uso aceptable y/o material de capacitación para garantizar que el contenido es adecuado. 2. Revisar los reportes y/o documentación de capacitación del usuario para garantizar que los usuarios son capacitados de acuerdo con la política, orientación, y/o requisito aplicable (p.ej., capacitación anual sobre ciberseguridad de todos los empleados). 3. Determinar si los materiales de capacitación están actualizados con base a cambios en el entorno de amenazas cibernéticas.
		Los usuarios privilegiados entienden sus roles y responsabilidades.	1. Determinar si la organización tiene un procedimiento para identificar usuarios privilegiados. 2. Determinar si los roles de los usuarios privilegiados están bien definidos y si los usuarios privilegiados están capacitados de acuerdo con sus responsabilidades. 3. Revisar el material de capacitación y/o acuerdos de usuario para asegurar que los usuarios con altos privilegios se les ha enseñado sobre los roles y responsabilidades de seguridad asociados a altos privilegios.

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Los terceros (p.ej., proveedores, consumidores, socios) entienden sus roles y responsabilidades.	1. Revisar contratos con terceros, acuerdos con consumidores, y contratos con socios que apliquen para garantizar que los roles y responsabilidades de seguridad están claramente definidos. 2. Revisar el programa de gestión de proveedores de la organización para garantizar que los terceros están cumpliendo con las responsabilidades de ciberseguridad definidos en contratos y acuerdos.
		Los altos ejecutivos entienden sus roles y responsabilidades.	Revisar los programas de capacitación y educación continua para altos ejecutivos. Considerar lo siguiente: a. Los conocimientos de ciberseguridad y niveles de habilidad para realizar sus deberes están definidos. b. Capacitación específica según roles es asignada teniendo en cuenta los roles y responsabilidades de ciberseguridad. c. Existe un método para medir conocimientos y comprensión de la ciberseguridad de los altos ejecutivos con respecto a los requisitos de la organización. d. Materiales de capacitación y educación están actualizados para reflejar los cambios en el entorno de amenaza.
		El personal de seguridad física y de la información entiende sus roles y responsabilidades.	
Seguridad de datos	La información y los registros (datos) son manejados de acuerdo con la estrategia de riesgos de la organización para proteger la confidencialidad, la integridad y la disponibilidad de la información.	Los datos en reposo están protegidos.	1. Determinar si los datos confidenciales o sensibles están identificados en la red de la organización (p.ej., clasificación de datos, evaluación de riesgo). 2. Determinar si la información confidencial está segura (p.ej., encriptación fuerte según está definida por las mejores prácticas de la industria) en reposo. 3. Determinar si los dispositivos móviles (p.ej., laptops, tablets, medios removibles) que son usados para almacenar información confidencial están encriptados. 4. Revisar contratos con terceros que almacenan información confidencial para garantizar que existen controles de seguridad apropiados para datos sensibles en reposo.
		Los datos en tránsito están protegidos.	1. Determinar si los datos sensibles están seguros (p.ej., encriptación fuerte según definida por las mejores prácticas de la industria) cuando son transmitidos a través de redes de acceso público.

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			2. Determinar si existen políticas adecuadas en relación con la transmisión de información confidencial o sensible vía email. 3. Revisar el material de capacitación y/o políticas de uso aceptable para determinar si los empleados están instruidos en las políticas de la organización sobre la transmisión de datos. 4. Revisar contratos con terceros que transmiten información confidencial para garantizar que existen controles de seguridad apropiados para la transmisión de datos sensibles.
		Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	Revisar las políticas y los procedimientos de inventario de activos. Considere lo siguiente: a. Existen procesos formalizados. b. Exactitud en el seguimiento de activos. c. Eliminación o destrucción segura de información confidencial de activos desmantelados.
		Existe una adecuada capacidad para garantizar que la disponibilidad se mantenga.	1. Revisar una muestra de informes de monitoreo de la administración de capacidad usados para monitorear recursos críticos como el ancho de banda, CPU, utilización del disco, disponibilidad de red, intercambio de paquetes, etc. 2. Determinar si los recursos tienen capacidad adecuada (p.ej., espacio en el disco, CPU). 3. Determinar si el riesgo de ataque de denegación de servicio distribuido (DDoS) se ha abordado y está en línea con el apetito de riesgo de la organización.
		Protecciones en contra de la fuga de datos están implementadas.	1. Revisar las evaluaciones de riesgo, las actas de reuniones de seguridad de la información y las estrategias de seguridad de la información para determinar si la prevención al riesgo de pérdida de datos o exfiltración de datos confidenciales se está considerando. 2. Asegurar que existen controles y herramientas (p.ej., prevención de pérdida de datos) para detectar o bloquear una potencial transmisión o eliminación de datos confidenciales (p.ej., email, dispositivos USB).

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Los mecanismos de revisión de integridad son usados para la verificación del software, firmware y de la integridad de la información.	Determinar si la organización emplea herramientas de verificación de la integridad para detectar cambios no autorizados en el software (p.ej., middleware, aplicaciones y sistemas operativos con componentes internos), firmware e información.
		Los entornos de desarrollo y de prueba se encuentran separados del entorno de producción.	Si la organización mantiene un entorno de desarrollo o de prueba de software, revisar los diagramas de red, conexiones de bases de datos y configuraciones de firewall/router que apliquen para determinar la suficiencia en la separación entre estos entornos y la red de producción.
Procesos y procedimientos de protección de la información	Las políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de gestión, y la coordinación entre las entidades de la organización), los procesos, y los procedimientos se mantienen y usan para gestionar la protección de los sistemas de información y los activos.	Una configuración base de los controles de información tecnológica/industrial está creada y en mantenimiento.	1. Determinar si la organización ha creado o adoptado configuraciones base (p.ej., puntos de referencia del centro para la seguridad en Internet [CIS], guías de implementación técnica de seguridad [STIG]) para sistemas (p.ej., servidores, computadores, routers). 2. Muestrear los sistemas contra las configuraciones base de la organización para garantizar que los estándares son seguidos y cumplidos.
		Un ciclo vital del desarrollo de sistemas (SDLC) para el manejo de los sistemas está implementado.	1. Obtener y revisar una copia del ciclo vital del desarrollo de sistemas de la organización. 2. Obtener muestras de documentación y programación de la implementación para garantizar el cumplimiento con las políticas.
		Existen procesos de control para el cambio de la configuración.	Determinar si existen procesos de control de cambio en configuración para sistemas de información. Considere lo siguiente: a. Los cambios propuestos están documentados y aprobados. b. Los cambios están prohibidos hasta que las aprobaciones designadas sean recibidas. c. Los cambios son probados y validados antes de su implementación. d. Los cambios están documentados y reportados al finalizar.

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Las copias de seguridad de la información se realizan, se les hace mantenimiento y se prueban periódicamente.	<ol style="list-style-type: none"> Determinar si existe un plan formal para copias de seguridad y restauración. Revisar los procedimientos de copias de seguridad. Asegurar que se realizan pruebas periódicas de copias de seguridad para verificar que los datos son accesibles y leibles.
		Las políticas y regulaciones respecto al entorno físico de operación para los activos organizacionales se cumplen.	Revisar las políticas, los procedimientos y los planes del entorno operativo de seguridad física. Asegurarse que lo siguiente se aborde: <ol style="list-style-type: none"> Interruptor de emergencia. Iluminación de emergencia. Planta de emergencia. Protección contra el fuego. Control de temperatura y humedad. Protección contra daño por agua. Ubicación de los componentes de sistemas de información (para minimizar daños).
		Los datos son destruidos de acuerdo con las políticas.	<ol style="list-style-type: none"> Revisar las políticas de desinfección de medios (destrucción de datos). Asegurar que las técnicas y procedimientos de desinfección son proporcionales con la categoría o clasificación de seguridad de la información o evaluación, y están de acuerdo con políticas federales y organizacionales y estándares de la organización que apliquen. Verificar basureras, contenedores de basura, basura triturada y/o trituradores para garantizar el cumplimiento de las políticas. Obtener pruebas (p.ej., certificados de destrucción) de que la desinfección de medios ocurre de acuerdo con las políticas.
		Los procesos de protección están en mejoramiento continuo.	Revisar las políticas y los procedimientos de la organización relacionados con el mejoramiento continuo de los procesos de protección. Considere lo siguiente: <ol style="list-style-type: none"> Auditorías, evaluaciones y escaneos de vulnerabilidades en curso son realizados, revisados y respondidos. Los planes, procesos y políticas están actualizados con base a lecciones aprendidas de pruebas (p.ej., continuidad del negocio, recuperación de desastres, respuesta a incidentes).

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<ol style="list-style-type: none"> Posición designada y/o responsable del comité para la evaluación continua de las necesidades y postura de la seguridad de la información de la compañía. Recopilación de la información de amenazas y respuestas a cambios en el entorno de amenaza.
		La efectividad de las tecnologías de protección se comparte con las partes apropiadas.	<ol style="list-style-type: none"> Determinar si la organización participa en grupos de intercambio y análisis de la información. Determinar si la organización facilita el intercambio de información permitiendo la autorización de usuarios para compartir información autorizada con socios de intercambio.
		Los planes de respuesta (respuesta a incidentes y continuidad del negocio) y los planes de recuperación (recuperación ante incidentes y desastres) están en orden y se encuentran administrados.	<ol style="list-style-type: none"> Revisar la respuesta a incidentes y el plan de continuidad del negocio para determinar si la institución tiene documentado cómo responderá a un incidente cibernético. Evaluar los planes para determinar qué tan frecuente se actualizan y aprueban. Validar que la estrategia de ciber resiliencia definida se encuentre alineada a los objetivos del negocio y la estrategia de ciberseguridad. Identificar las soluciones establecidas orientadas a la ciber resiliencia, y cómo estas están incluidas y desarrolladas en las soluciones de ciberseguridad y continuidad del negocio.
		Los planes de respuesta y recuperación están probados.	Determinar si las pruebas de continuidad del negocio y respuesta ante incidentes son realizadas de acuerdo con las políticas y cualquier otra guía que aplique.
		La ciberseguridad está incluida en las prácticas de recursos humanos. (p.ej., desaprovisionamiento, selección de personal).	<ol style="list-style-type: none"> Revisar los procesos de contratación para determinar si la verificación de antecedentes se realiza a todos los empleados. Revisar los procesos de contratación para posiciones con acceso a información sensible para determinar si ellos son proporcionales a un nivel alto de riesgo. Revisar los procesos de terminación para determinar si cuentas/accesos son deshabilitados de manera oportuna.

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Un plan de gestión de vulnerabilidades está desarrollado e implementado.	<ol style="list-style-type: none"> Obtener el plan de gestión de vulnerabilidades de la organización y garantizar que incluya lo siguiente: <ol style="list-style-type: none"> Frecuencia de escaneo de vulnerabilidades. Métodos para medir el impacto de las vulnerabilidades identificadas (p.ej., sistema de puntaje de vulnerabilidades comunes [CVSS]). Incorporación de las vulnerabilidades identificadas en otras evaluaciones de control de seguridad (p.ej., auditorías externas, pruebas de penetración). Procedimientos para el desarrollo de reparación de vulnerabilidades identificadas. Obtener una copia de la evaluación de riesgos de la organización para garantizar que las vulnerabilidades identificadas durante el proceso de gestión de vulnerabilidades están incluidas.
Mantenimiento	El mantenimiento y la reparación de los controles industriales y de los componentes de los sistemas de información se realizan de acuerdo con las políticas y los procedimientos.	El mantenimiento y la reparación de los activos de la organización se realiza y registra de manera oportuna, con herramientas aprobadas y controladas.	<p>Revisar los procesos de mantenimiento controlado. Considere lo siguiente:</p> <ol style="list-style-type: none"> Las actividades de mantenimientos son aprobadas, programadas y documentadas (p.ej., fecha y hora, nombre de los individuos que realizaron el mantenimiento, descripción del mantenimiento realizado, sistemas removidos/remplazados). El personal o los contratistas de mantenimiento son aprobados, autorizados y supervisados (si es requerido). Herramientas y medios de mantenimientos son aprobados e inspeccionados en busca de modificaciones impropias o no autorizadas previas a su uso.
		El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se impide el acceso no autorizado.	<p>Determinar si el mantenimiento remoto en servidores, estaciones de trabajo y otros sistemas es realizado. Considere lo siguiente:</p> <ol style="list-style-type: none"> ¿A quién se le permite conectarse a los sistemas (p.ej. trabajadores internos, terceros)? ¿Qué software/versión o servicios son usados para conectarse? Si los usuarios finales deben realizar alguna acción previa a permitir el control remoto de su estación de trabajo y/o si el acceso se registra y monitorea. Requerimientos de autenticación adecuados (p.ej., autenticación multifactorial).

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Tecnología de protección	Las soluciones de seguridad técnica están gestionadas para garantizar la seguridad y resistencia de los sistemas y los activos, de acuerdo con las políticas, los procedimientos, y los acuerdos relacionados.	Los registros de auditoría están determinados, documentados, implementados y revisados de acuerdo con las políticas.	<ol style="list-style-type: none"> Determinar si los registros de auditoría son mantenidos y revisados de manera oportuna. Verificar la idoneidad de los registros para monitorear y evaluar actividades de IT y eventos de seguridad. Considere lo siguiente: <ol style="list-style-type: none"> Los registros de auditoría contienen contenido apropiado (p.ej., tipo de evento, cuando ocurrió el evento, fuente del evento, resultado del evento, identidad de cualquier individuo o sujeto asociado al evento). Los archivos de registro tienen un tamaño tal que los registros no sean eliminados previamente a su revisión y/o se les haga copia de seguridad. Los registros y las herramientas de auditoría están protegidos de acceso, modificación y eliminación no autorizados. Determinar si los registros para las siguientes partes de la red están monitoreados y revisados: <ol style="list-style-type: none"> Perímetro de la red (p.ej., sistemas de detección de intrusión [IDS], firewalls). Sistemas Microsoft (p.ej., registros de eventos de Windows). Sistemas no Microsoft (p.ej., archivos syslog para servidores Unix/Linux, routers, interruptores).
		Los medios extraíbles están protegidos, y su uso está restringido de acuerdo con las políticas.	<ol style="list-style-type: none"> Obtener una copia de la política de medios removibles. Los controles deben incluir: <ol style="list-style-type: none"> Capacitación al usuario. Encriptación de medios removibles. Acceso restringido a medios removibles (p.ej., restricciones a USB). Procedimientos de desinfección para medios desmantelados. Realización de verificación a sistemas con restricciones de medios removibles para garantizar que las restricciones estén funcionando como se espera y cumplan con las políticas de la organización.
		El acceso a los sistemas y los activos es controlado, incorporando el principio de menor funcionalidad.	<ol style="list-style-type: none"> Revisar los sistemas de información para determinar si las funciones, los puertos, los protocolos y los servicios innecesarios y/o no seguros están deshabilitados. Donde sea factible, la organización limita las funcionalidades de un componente a una sola función por dispositivo (p.ej., servidor dedicado a email).

PROTEGER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			3. Determinar si la organización revisa funciones y servicios prestados por sistemas de información o componentes individuales de sistemas de información para determinar cuáles funciones y servicios son candidatos a ser eliminados.
		Las redes de comunicación y de control están protegidas.	<p>Evaluar los controles relacionados con comunicaciones para garantizar que la red es segura. Considere:</p> <ol style="list-style-type: none"> Existen defensas perimetrales de red (p.ej., border router, firewall). Los controles de seguridad física son usados para prevenir el acceso no autorizado a sistemas de telecomunicaciones, etc. Controles lógicos de acceso a la red (p.ej., VLAN) y controles técnicos (p.ej., encriptar el tráfico) existen para proteger y/o segregar las redes de comunicación (p.ej., wireless, WAN, LAN, VoIP).

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Anomalías y eventos	Las actividades anómalas son detectadas de manera oportuna y el impacto potencial de los eventos es comprendido.	Se establece y maneja una base/referencia para las operaciones de red y el flujo de datos esperado para usuarios y sistemas.	<ol style="list-style-type: none"> Obtener una copia del diagrama lógico de red (LND), los diagramas de flujo de datos, y otros diagramas de red y comunicaciones de la organización. Revisar los diagramas en busca de lo siguiente: <ol style="list-style-type: none"> Frecuencia de actualización de los diagramas. Exactitud y completitud de los diagramas. El alcance de los diagramas es adecuado para identificar ambos dominios de riesgos y niveles de control diferentes (e.d., riesgo alto, porciones públicamente accesibles de una red vs. alto costo, porciones de acceso restringido) y los puntos de control (p.ej., firewalls, routers, sistemas de detección/prevenición de intrusión), entre ellos. Determinar si las herramientas (p.ej., sistemas de gestión de eventos de seguridad y de la información [SIEMs]) son usadas para establecer un tráfico típico (de referencia) y así el tráfico anormal pueda ser detectado.

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Los eventos detectados son analizados para comprender los objetivos y métodos del ataque.	<ol style="list-style-type: none"> Obtener una copia de las políticas y los procedimientos relacionados con el monitoreo de sistemas y de la red. <ol style="list-style-type: none"> Determinar si las políticas y los procedimientos requieren monitoreo de actividad anómala en los puntos de control identificados. Obtener una copia de eventos detectados (p.ej., alertas de IDS) y la respuesta de la organización a ellos. Revisar los eventos y respuestas para asegurar que se realiza un análisis exhaustivo de los eventos detectados.
		Los datos de eventos de múltiples fuentes y sensores están agregados y correlacionados.	<ol style="list-style-type: none"> Obtener un listado de la agregación de eventos y sistemas de monitoreo en uso en la organización (p.ej., SIEMs, sistemas de correlación de registro de eventos). Obtener una lista de las fuentes que proveen datos a cada evento agregado y sistemas de monitoreo (p.ej., firewalls, routers, servidores). Comparar las fuentes para puntos de control identificados entre dominios de riesgos y niveles de control diferentes, y determinar si ellos proveen un cubrimiento de monitoreo adecuado del entorno de la organización.
		El impacto del evento está determinado.	<ol style="list-style-type: none"> Obtener una copia de los eventos detectados y las respuestas de la organización a ellos. Revisar los eventos, tiquetes y respuestas para asegurar que la organización está documentando el impacto de la actividad anómala usando métricas que son aplicables a la organización (p.ej., impacto de cumplimiento, impacto operacional, impacto de reportes exactos).
		Los límites de alertas ante incidentes están establecidos.	<ol style="list-style-type: none"> Obtener una copia de mensajes de alerta, actas de reuniones, reportes y otra documentación donde eventos detectados fueron escalados. Revisar la documentación y determinar lo siguiente: <ol style="list-style-type: none"> Los eventos detectados son reportados de manera oportuna a alguien con el conocimiento y experiencia para resolver o escalar el evento.

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<ul style="list-style-type: none"> b. Los eventos escalados son reportados a individuos o grupos con la autoridad apropiada para tomar decisiones acerca de la respuesta de la organización. c. Los límites están definidos tal que un evento desencadena la respuesta apropiada (p.ej., respuesta de continuidad del negocio, respuesta de recuperación de desastres, respuesta de incidentes, respuesta legal).
Monitoreo continuo de seguridad	Los sistemas de información y los activos son monitoreados en intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	La red está monitoreada para detectar eventos potenciales de ciberseguridad.	<ul style="list-style-type: none"> 1. Obtener una lista del control de monitoreo implementado por la organización a los siguientes niveles: <ul style="list-style-type: none"> a. Red (p.ej., firewall, router, interruptor). b. Sistema operativo (p.ej., plataformas de servidores, plataformas de estaciones de trabajo, electrodomésticos). c. Aplicaciones (p.ej., administración de cuentas, acceso a archivos y bases de datos). 2. Determinar si el monitoreo en cada nivel incluye detección de eventos de ciberseguridad (p.ej., ataques de negación de servicio [DoS], acceso no autorizado a cuentas, acceso no autorizado a archivos/sistemas, ataques de escalada de privilegios, ataques de inyección SQL).
		El entorno físico es monitoreado para detectar eventos potenciales de ciberseguridad.	<ul style="list-style-type: none"> 1. Obtener un inventario de instalaciones críticas (p.ej., centros de datos, armarios de red, centros de operaciones, centros de control crítico). 2. Determinar si los controles de monitoreo de seguridad física están implementados y son apropiados para detectar eventos potenciales de ciberseguridad (p.ej., registros de entrada/salida, detectores de movimiento, cámaras de seguridad, iluminación de seguridad, guardias de seguridad, cerraduras de puertas/ventanas, bloqueo automático del sistema cuando está inactivo, acceso físico restringido a servidores, estaciones de trabajo, dispositivos de red, puertos de red).
		La actividad del personal es monitoreada para detectar eventos potenciales de ciberseguridad.	<ul style="list-style-type: none"> 1. Obtener una lista de los controles de monitoreo implementados por la organización a nivel de aplicación/cuenta de usuario (p.ej., administración de cuentas, roles de acceso de usuarios, monitoreo de actividad de usuarios, acceso a archivos y bases de datos).

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<ul style="list-style-type: none"> 2. Determinar si el monitoreo incluye detección y alertas de eventos de ciberseguridad (p.ej., acceso no autorizado a cuentas, acceso no autorizado a archivos/sistemas, acceso fuera de horario, acceso a datos sensibles, acceso inusual, acceso físico no autorizado, ataques de escalada de privilegios).
		Los códigos maliciosos son detectados.	<ul style="list-style-type: none"> 1. Obtener una copia de los procesos y procedimientos usados para detectar código malicioso en la red y servidores/puestos de trabajo (p.ej., anti-malware software en servidores y estaciones de trabajo, filtros de phishing en sistemas de email, sistemas de prevención/detección de intrusión en la red [IDS/IPS], productos de seguridad de punto final en estaciones de trabajo y/o servidores). 2. Determinar si los controles de código malicioso están: <ul style="list-style-type: none"> a. Instalados en todos los sistemas y puntos de control de la red en los que aplique. b. Actualizados de manera regular. c. Configurados para realizar escaneo en tiempo real o escaneos periódicos en intervalos regulares. 3. Inspeccionar estaciones de trabajo y otros dispositivos de punto final de usuario para verificar lo siguiente: <ul style="list-style-type: none"> a. Los controles de código malicioso están instalados. b. Los controles de código malicioso están actualizados. c. Los controles de código malicioso son capaces de detectar códigos de prueba (p.ej., la prueba de virus EICAR).
		Los códigos móviles no autorizados son detectados.	<ul style="list-style-type: none"> 1. Obtener los procesos y procedimientos documentados usados para detectar un código móvil no autorizado (p.ej., Java, JavaScript, ActiveX, Flash, VBScript) que se corra en los servidores, estaciones de trabajo y dispositivos de la organización. 2. Determinar si los controles de código móvil bloquean un código móvil no autorizado cuando se detecta (p.ej., cuarentena, bloqueo de ejecución, bloqueo de descarga). <p>*Ejemplos de controles de código móvil incluyen:</p> <ul style="list-style-type: none"> a. Detectar y bloquear adjuntos de código móvil en emails (p.ej., archivos .exe, archivos .js).

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<p>b. Detectar y bloquear porciones de código móvil de sitios web.</p> <p>c. Remover la habilidad de correr código móvil en sistemas que no requieren esta funcionalidad (p.ej., desinstalar Java de estaciones de trabajo que no lo requieran).</p> <p>d. Configurar sistemas para generar alertas y bloqueo de ejecución cuando un código móvil que no está firmado con un certificado de firma de código aprobada se intenta ejecutar.</p>
		<p>La actividad de proveedores externos de servicios se monitorea para detectar eventos potenciales de ciberseguridad.</p>	<p>1. Obtener y revisar los contratos ejecutados con proveedores externos de servicios.</p> <p>2. Determinar si los contratos con proveedores externos de servicios requieren que estos:</p> <p>a. Notifiquen a la organización tan pronto como sea posible de cualquier evento conocido o sospechoso de ciberseguridad.</p> <p>b. Notifiquen a la organización tan pronto como sea posible de la terminación de cualquier empleado que posee credenciales para acceder sistemas o instalaciones de la organización.</p> <p>c. Implementen controles de seguridad equivalentes a o que excedan el nivel de seguridad requerido por la organización.</p> <p>3. Obtener una copia del diagrama lógico de red (LND) de la organización para determinar cómo las redes de proveedores externos de servicios están conectadas a la red de la organización, y así a su vez determinar si los controles de monitoreo (p.ej., firewalls, routers, sistemas de detección/prevenición de intrusión) están implementados en estos puntos de conexión.</p> <p>4. Obtener y analizar una copia de las configuraciones del sistema para los controles de monitoreo usados para detectar eventos de ciberseguridad originados en redes de proveedores externos de servicios.</p>

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		<p>Se realiza monitoreo en busca de personal, conexiones, dispositivos y software no autorizados.</p>	<p>1. Obtener una copia de los procesos y procedimientos diseñados para detectar acceso no autorizado a las instalaciones y sistemas de la organización (p.ej., registros de inicio/cierre de sesión o de entrada/salida, videos de vigilancia, alarmas de intrusión, bloqueo de puertos de red, restricciones de dispositivos USB en estaciones de trabajo y dispositivos de usuario, monitoreo de inicios de sesión fallidos excesivos indicando un ataque de adivinación de contraseña).</p> <p>2. Verificación de los controles de acceso no autorizado accediendo a las instalaciones y sistemas con permiso para probar, pero no con autorizaciones estándar. Pedir a la organización que provea las notificaciones de alerta generadas por el acceso no autorizado simulado.</p>
		<p>Se realizan escaneos de vulnerabilidad.</p>	<p>1. Obtener una copia de la programación de la organización para realizar escaneos de vulnerabilidad interna y externa, y los resultados de los escaneos de vulnerabilidad interna y externa más recientes.</p> <p>2. Revisar la programación y los resultados en busca de lo siguiente:</p> <p>a. Frecuencia.</p> <p>b. Finalización exitosa.</p> <p>c. Solución o mitigación documentada de las vulnerabilidades identificadas.</p> <p>d. El alcance de las pruebas incluye a todos los sistemas críticos.</p> <p>3. Determinar si los resultados de los escaneos de vulnerabilidad fueron reportados a individuos o grupos con autoridad apropiada para asegurar su solución.</p>
<p>Procesos de detección</p>	<p>Los procesos y procedimientos de detección están mantenidos y probados para garantizar conciencia oportuna y adecuada ante eventos anómalos.</p>	<p>Los roles y las responsabilidades para la detección están bien definidos, asignando responsabilidades.</p>	<p>1. Obtener una copia de los procesos y procedimientos para monitorear eventos físicos y electrónicos anómalos.</p> <p>2. Determinar si los procesos y procedimientos de la organización asignan responsabilidades clave a individuos o posiciones específicas.</p>

DETECTAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Las actividades de detección cumplen con los requisitos que aplican.	<ol style="list-style-type: none"> Obtener una copia de las leyes, los reglamentos (p.ej., federal, estatal, local), los estándares industriales, los requisitos internos de seguridad y el apetito de riesgo que apliquen a la organización. Determinar si la organización está realizando auditorías/pruebas para asegurar que sus actividades de detección cumplen con estos requisitos.
		Los procesos de detección están probados.	<ol style="list-style-type: none"> Obtener una copia de la programación de la organización para realizar pruebas de respuesta a incidentes, los resultados de pruebas recientes a respuesta a incidentes, y los procesos y procedimientos documentados que requieren pruebas de control de actividad anómala (p.ej., pruebas periódicas de sistemas de detección/prevenición de intrusión, anti-malware software de punto final). Revisar la documentación en busca de lo siguiente: <ol style="list-style-type: none"> Completitud en la prueba de controles implementados de detección de actividad anómala. Frecuencia de la prueba. Solución o mitigación documentada de resultados de prueba negativos.
		La información de detección de eventos es comunicada a las partes apropiadas.	<ol style="list-style-type: none"> Obtener una copia de las actas de reuniones donde las actividades físicas y electrónicas anómalas están reportadas (p.ej., reuniones del comité de seguridad de la información, reuniones de gestión del riesgo). Obtener una copia de las respuestas documentadas a incidentes recientes de actividad física y electrónica anómala. Comparar las actas de reuniones con incidentes documentados y determinar si los eventos detectados están consistentemente reportados y apropiadamente manejados.
		Los procesos de detección están en mejoramiento continuo	<p>Obtener una copia de las respuestas documentadas a incidentes recientes de actividad física y electrónica anómalos. Determinar si las respuestas contienen lo siguiente:</p> <ol style="list-style-type: none"> Lecciones aprendidas y análisis de controles que fallan o son faltantes. Ítems de acción para detectar/prevenir incidentes similares en el futuro.

RESPONDER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Planeación de respuesta	Los procesos y procedimientos de respuesta se realizan y mantienen, para asegurar una respuesta a tiempo a eventos detectados de ciberseguridad.	El plan de respuesta se ejecuta durante o después de un evento.	<ol style="list-style-type: none"> Determinar si la organización ha aprobado respuestas a incidentes y planes de continuidad del negocio. Obtener las copias de reportes de incidentes recientes para validar que los planes son ejecutados. Identificar la estructura establecida para responder ante eventos de ciber resiliencia
Comunicaciones	Las actividades de respuesta son coordinadas con las partes interesadas internas y externas, según corresponda, para incluir el apoyo externo de los organismos encargados de hacer cumplir la ley.	El personal conoce su rol y el orden de las operaciones cuando una respuesta es requerida.	<ol style="list-style-type: none"> Revisar los planes de respuesta ante incidentes para determinar si los roles y responsabilidades están definidas para empleados. Entrevistar a los empleados para determinar si ellos conocen sus roles y responsabilidades según lo definido en el plan. Revisar cualquier prueba de respuesta ante accidentes o capacitación dada a los empleados para determinar si ayudan a educar a los empleados en sus roles y responsabilidades.
		Los eventos son reportados en consistencia con los criterios establecidos.	<ol style="list-style-type: none"> Revisar el plan de respuesta ante incidentes para determinar si la estructura de reporte y los canales de comunicación están claramente definidos. Determinar si los empleados están capacitados para reportar sospechas de incidentes de seguridad. Obtener las copias de reportes de incidentes recientes para validar que el reporte es consistente y sigue el plan.
		La información se comparte consistentemente con los planes de respuesta.	<ol style="list-style-type: none"> Revisar el plan de respuesta ante incidentes para determinar si el intercambio de información está claramente definido dado que relaciona lo siguiente (si corresponde): <ol style="list-style-type: none"> Clientes. Fuerzas del orden público. Reguladores. Medios. Organizaciones de intercambio de información. Obtener las copias de los reportes de incidentes recientes para validar que el intercambio es consistente y sigue el plan.

RESPONDER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		La coordinación con las partes interesadas ocurre en consistencia con los planes de respuesta.	<ol style="list-style-type: none"> 1. Revisar el plan de respuesta ante incidentes para determinar si existe un proceso para comunicarse con las partes interesadas internas y externas durante y/o prosiguiendo a un incidente. 2. Obtener las copias de reportes de incidentes recientes para validar que el reporte es consistente y sigue el plan.
		El intercambio voluntario de información entre las partes interesadas externas.	Revisar el plan de respuesta ante incidentes para determinar si existe un proceso para comunicarse con las partes interesadas externas (p.ej., usuarios finales, proveedores, terceras partes, clientes) prosiguiendo a un incidente.
Análisis	El análisis se realiza para garantizar una respuesta adecuada y apoyar a las actividades de recuperación.	Las notificaciones de sistemas de detección son investigadas.	<ol style="list-style-type: none"> 1. Obtener evidencia de notificaciones de eventos (p.ej., alertas de detección, reportes) de sistemas de información (p.ej., uso de la cuenta, acceso remoto, conectividad wireless, conexión de dispositivos móviles, ajustes de configuración, inventarios de componentes de los sistemas, uso de las herramientas de mantenimiento, acceso físico, temperatura y humedad, actividad anómala, uso de código móvil). 2. Determinar quién recibe las alertas o reportes de los sistemas de detección y qué acciones son tomadas al recibir los reportes. 3. Revisar el plan de respuesta ante incidentes para determinar si las acciones tomadas siguen el plan.
		El impacto del incidente se comprende.	<ol style="list-style-type: none"> 1. Revisar el plan de respuesta ante incidentes para determinar si hay un proceso para analizar y clasificar formalmente los incidentes según su impacto potencial. 2. Revisar el currículum y la capacitación de los miembros del equipo de respuesta a incidentes responsables de determinar su impacto para identificar si ellos tienen el conocimiento y la experiencia para comprender el impacto potencial.
		Se realizan análisis forenses.	Revisar el plan de respuesta ante incidentes en lo que se refiere a análisis forense. Considerar lo siguiente: <ol style="list-style-type: none"> a. Existe un proceso para asegurar que el análisis forense se hará cuando se requiere.

RESPONDER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<ol style="list-style-type: none"> b. Determinar si las investigaciones de seguridad y los análisis forenses están realizados por equipos o terceros cualificados. c. Revisar los procedimientos forenses para garantizar que ellos incluyen controles, como cadena de custodia, para apoyar potenciales acciones legales.
		Los incidentes son categorizados consistentemente con los planes de respuesta.	<ol style="list-style-type: none"> 1. Revisar el plan de respuesta ante incidentes para determinar si está diseñado para priorizarlos, permitiendo una rápida respuesta para incidentes o vulnerabilidades significativas. 2. Obtener copias de los reportes de incidentes recientes para validar que el reporte es consistente y sigue el plan.
Mitigación	Las actividades se realizan para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.	Los incidentes son contenidos.	Revisar el plan de respuesta ante incidentes para determinar si existe pasos adecuados para contener un incidente. Considere lo siguiente: <ol style="list-style-type: none"> a. Pasos para contener y controlar el incidente para prevenir daños adicionales. b. Procedimientos para notificar a terceros potencialmente impactados. c. Estrategias para controlar diferentes tipos de incidentes (p.ej., denegación de servicio distribuido [DDoS], malware).
		Los incidentes son mitigados.	<ol style="list-style-type: none"> 1. Revisar el plan de respuesta ante incidentes para determinar si existen los pasos apropiados para mitigar el impacto de un incidente. Considere lo siguiente: <ol style="list-style-type: none"> a. Pasos para mitigar el incidente para prevenir daños adicionales. b. Procedimientos para notificar a terceros potencialmente impactados. c. Estrategias para mitigar el impacto de diferentes tipos de incidentes (p.ej., denegación de servicio distribuido [DDoS], malware, etc.). 2. Revisar cualquier incidente documentado para determinar si los esfuerzos de mitigación fueron implementados y efectivos.

RESPONDER			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
		Las vulnerabilidades recientemente identificadas son mitigadas o documentadas como un riesgo aceptado.	Determinar si los procesos de monitoreo continuo de la organización (p.ej., evaluación de riesgos, escaneo de vulnerabilidades) facilitan el conocimiento continuo de amenazas, vulnerabilidades y seguridad de la información para respaldar las decisiones de gestión de riesgos organizacionales. Considere lo siguiente: a. ¿Es el proceso continuo (a una frecuencia suficiente para respaldar las decisiones organizacionales relacionadas con los riesgos)? b. Los resultados generan una respuesta apropiada al riesgo (p.ej., estrategia de mitigación, aceptación) con base en el apetito al riesgo de la organización.
Mejoras	Las actividades de respuesta organizacional son mejoradas incorporando lecciones aprendidas de actividades de respuesta/detección actuales o previas.	Los planes de respuesta incorporan las lecciones aprendidas.	1. Revisar los reportes de manejo de incidentes y la documentación de pruebas de incidentes de la organización en busca de ítems de acción y lecciones aprendidas. 2. Evaluar el plan de respuesta ante incidentes para determinar si los resultados (p.ej., ítems de acción, lecciones aprendidas) y pruebas han sido usados para actualizar los procesos, capacitaciones y pruebas de respuesta ante incidentes.
		Las estrategias de respuesta se actualizan.	Revisar la respuesta ante incidentes, y estrategias y planes de continuidad del negocio de la organización. Considere lo siguiente: a. Existe un mecanismo para regularmente revisar, mejorar, aprobar y comunicar los planes. b. La capacidad de respuesta de la organización está informada por incidentes actuales, pruebas y amenazas actuales.

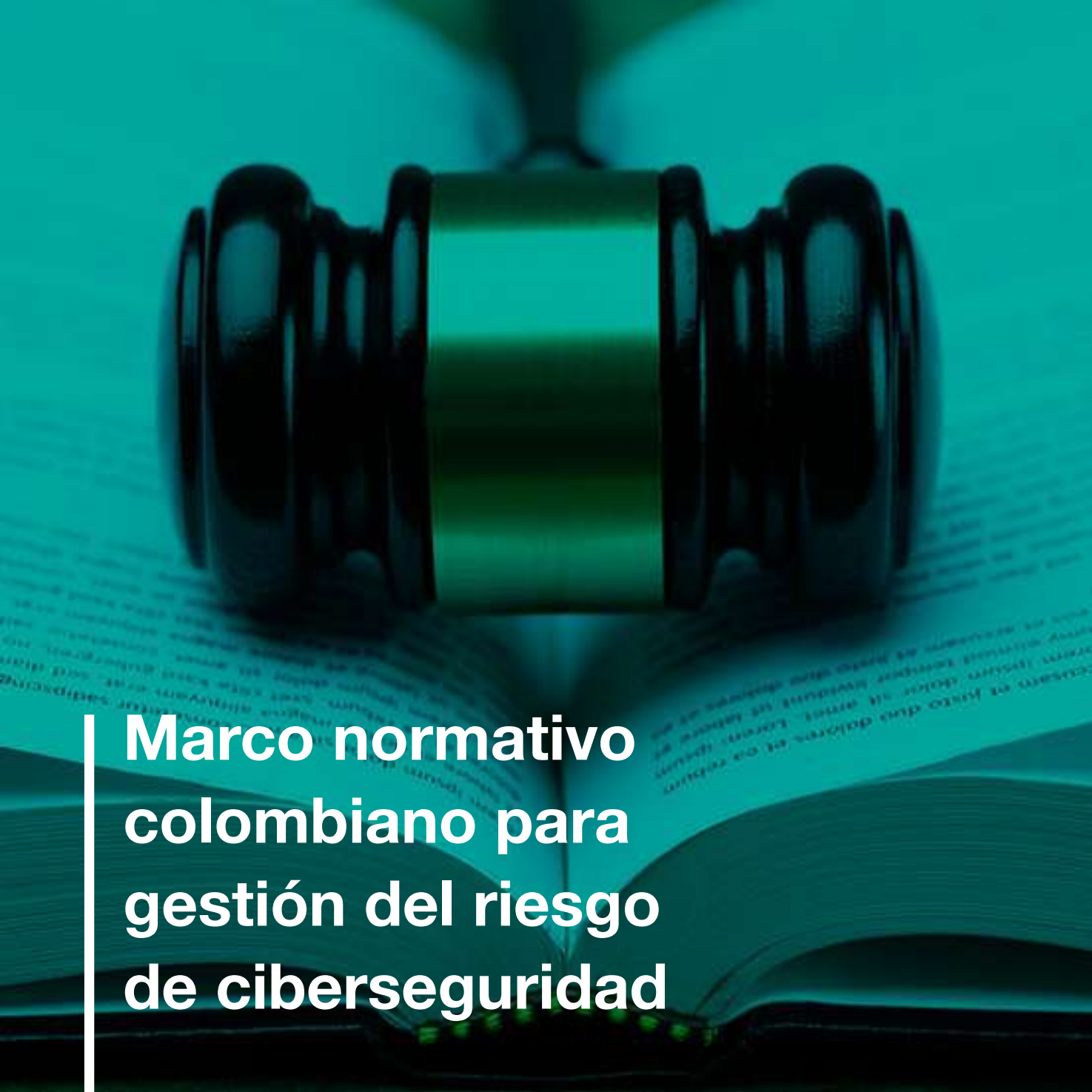
RECUPERAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Planeación de recuperación	Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración a tiempo de sistemas o bienes afectados por eventos de ciberseguridad.	El plan de recuperación se ejecuta durante o después de un evento.	1. Obtener una copia de los planes y procedimientos de recuperación de la organización (p.ej., el plan de continuidad del negocio, el plan de respuesta ante accidentes, el plan de recuperación ante desastres, el plan ante incidentes de ciberseguridad) y los resultados documentados de recientes eventos o pruebas de eventos de ciberseguridad.

RECUPERAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
Mejoras	La planeación y los procesos de recuperación se mejoran incorporando lecciones aprendidas a futuras actividades.		2. Evaluar la documentación en busca de lo siguiente: a. Frecuencia de evaluación. b. Cobertura de las piezas críticas de los planes y procedimientos de recuperación. c. Documentación de incidentes (p.ej. cortes de energía, fallas de comunicación, cortes del sistema, intento y éxito en el acceso o la interrupción no autorizada, maliciosa o descuidada).
		Los planes de recuperación incorporan lecciones aprendidas	1. Obtener una copia de los resultados de recientes eventos o pruebas de eventos de Ciberseguridad. 2. Evaluar la documentación en busca de lo siguiente: a. Lecciones aprendidas y análisis documentados de controles fallidos o faltantes. b. Ítems de acción diseñados para mejorar los planes y procedimientos de recuperación con base en las lecciones aprendidas y los análisis.
		Las estrategias de recuperación están actualizadas.	1. Obtener una copia de los planes y procedimientos de recuperación (p.ej., el plan de continuidad del negocio, el plan de respuesta ante incidentes, el plan de recuperación ante desastres, el plan ante incidentes de ciberseguridad) y los resultados documentados de eventos o pruebas de eventos recientes. 2. Determinar si los planes y procedimientos de recuperación están revisados, actualizados y aprobados regularmente o al hacer cambios a sistemas y controles. 3. Revisar los planes y los procedimientos de recuperación para determinar si los ítems de acción que son el resultado de lecciones aprendidas durante eventos o pruebas de eventos de ciberseguridad han sido implementados.
Comunicaciones	Las actividades de restauración son coordinadas con las partes internas y externas, tales como centros de coordinación, proveedores del servicio de Internet, dueños de sistemas de ataque, víctimas, otros CSIRTs y proveedores.	Las relaciones públicas están gestionadas.	1. Obtener una copia de los planes y procedimientos de recuperación de la organización (p.ej., el plan de continuidad del negocio, el plan de respuesta ante incidentes, el plan de recuperación ante desastres, el plan ante incidentes de ciberseguridad). 2. Determinar si los planes y los procedimientos incluyen lo siguiente: a. Designación de puntos de contacto al interior de la organización con clientes, socios, medios, reguladores y fuerzas del orden público.

RECUPERAR			
Área del Proceso	Objetivos de Control	Controles	Paso de Prueba
			<ul style="list-style-type: none"> b. Capacitación para los empleados acerca de dónde remitir preguntas sobre incidentes de ciberseguridad. c. Orden de la sucesión de los responsables de manejar el riesgo de reputación de la organización durante incidentes de ciberseguridad. d. Notificación responsable y a tiempo a clientes, socios, reguladores y fuerzas del orden público de un incidente de ciberseguridad.
		La reputación después de un evento es reparada.	<p>Obtener los resultados documentados de eventos recientes de ciberseguridad. Determinar si lo siguiente está incluido:</p> <ul style="list-style-type: none"> a. Informar a los clientes, socios, medios, reguladores y fuerzas del orden público, según corresponda, de los esfuerzos en curso para corregir los problemas identificados y su solución final. b. Esfuerzos o planes específicos para abordar la reparación de la reputación.
		Las actividades de recuperación son comunicadas a las partes interesadas internas y los equipos ejecutivos y de gestión.	<ol style="list-style-type: none"> 1. Obtener una copia de las actas de reunión donde estén reportados eventos de ciberseguridad (p.ej. reuniones del Comité de Seguridad de la Información, reuniones de la junta/gerencia, reuniones de gestión del riesgo, reuniones del Comité de Cumplimiento). 2. Obtener una copia de los resultados documentados sobre eventos de ciberseguridad. 3. Comparar las actas de reuniones con los eventos documentados de ciberseguridad y determinar si en las actividades de recuperación se notificaron a las partes interesadas y miembros de la gerencia pertinentes (p.ej. miembros de la junta, accionistas, ejecutivos de nivel C, gerentes de gestión de riesgos, gerentes de departamentos afectados).

Como cada función tiene un alcance importante, se pueden incluir varias evaluaciones para cubrir el ciclo completo y complementarlas con pruebas de Ethical Hacking, que consisten en hackear los sistemas informáticos propios

para reforzar su seguridad, y otro tipo de evaluaciones que complementen y ayuden a tener una visión integral de la gestión del riesgo cibernético en la organización.



**Marco normativo
colombiano para
gestión del riesgo
de ciberseguridad**

Con el fin de hacer frente a las amenazas latentes, en Colombia se han presentado algunas iniciativas regulatorias enfocadas a fortalecer la gestión de ciberseguridad. Dentro de ellas se encuentran: (i) la Ley 1273 de 2009 que creó un nuevo bien jurídico titulado “la protección de la información y los datos”, (ii) la Ley 1581 de 2012 que dispuso mecanismos de protección para salvaguardar los datos personales registrados en cualquier base de datos, (iii) la Ley 1621 de 2013 que fortaleció el marco jurídico que permite a los organismos de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y (iv) el CONPES 3854 de 2016 que actualizó la política de ciberseguridad.

En cuanto al sector financiero, en junio de 2018 la Superintendencia Financiera de Colombia (SFC) publicó la Circular Externa (CE) N°007 por medio de la cual se presentan los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, dentro de sus disposiciones se establece que las entidades vigiladas deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad, para lo cual deben adoptar las siguientes medidas:

- (i) **Política de Ciberseguridad:** esta política debe ser aprobada por la Junta Directiva y documentar las responsabilidades, procesos, etapas y gestión que se realiza frente al riesgo cibernético. Asimismo, debe establecer las funciones de la unidad de seguridad de información y los principios y lineamientos para promover una cultura de la ciberseguridad.
- (ii) **Unidad de gestión de riesgos de seguridad de la información y ciberseguridad:** esta Unidad debe considerar la estructura, el tamaño, el volumen transaccional, el riesgo y los servicios prestados por la entidad, para reportar a la Junta Directiva y a la alta dirección la evaluación de la información, la identificación de amenazas y los resultados de los programas de ciberseguridad. Además, debe actualizarse de manera permanente a las nuevas modalidades de ciberataques, sugerir capacitaciones regulares a los funcionarios de la organización, monitorear y verificar el cumplimiento de

las políticas y procedimientos de ciberseguridad y realizar un análisis de riesgo para determinar la pertinencia de contratar un tercero.

- (iii) **Sistema de gestión para la ciberseguridad:** este puede tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, CIS Critical Security Controls (CSC) o COBIT 5, y sus respectivas actualizaciones.

Adicionalmente, las entidades deben:

- a) Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de la información confidencial, en reposo o en tránsito.
- b) Emplear mecanismos para la adecuada autenticación y segregación de las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.
- c) Establecer procedimientos para la retención y destrucción final de la información.
- d) Establecer una estrategia de comunicación e información que contemple: la información que se debe reportar a la SFC, la información que remitirán a las autoridades que hacen parte del modelo nacional de gestión de incidentes, y la información que se hará de conocimiento público para los consumidores financieros.
- e) Definir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y apps que procesan la información confidencial de la entidad o de los consumidores financieros, aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo.
- f) Incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y

ciberseguridad.

- g) Verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas en contratos con terceros.
- h) Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.
- i) Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.

1. Prevención:

En esta etapa las entidades deben desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad, llevando a cabo las siguientes acciones:

- Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades.
- Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.
- Gestionar y documentar la seguridad de la plataforma tecnológica.
- Garantizar que la unidad de gestión de riesgos de seguridad de la información y ciberseguridad cuente con los recursos necesarios para realizar una adecuada gestión del riesgo cibernético.
- Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes y establecer controles para su mitigación.

- j) Considerar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.

Finalmente, la CE N°007 establece un modelo de cuatro etapas para la gestión de la seguridad de la información y la ciberseguridad:

- Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.
- Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos.
- Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.
- Monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.
- Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad.
- Informar a los consumidores financieros de la entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

2. Protección y detección

Las entidades deben desarrollar e implementar actividades apropiadas para detectar la ocurrencia de un evento de ciberseguridad y de adoptar medidas para protegerse ante los mismos. En este sentido, es necesario:

- Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.

3. Respuesta y comunicación

En esta etapa las entidades deben desarrollar e implementar actividades para responder de manera efectiva a los incidentes relacionados con ciberseguridad, para ello deben:

- Establecer procedimientos de respuesta a incidentes cibernéticos.
- Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados.
- Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o

- Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

- Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.

- Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.
- Preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

4. Recuperación y aprendizaje

En la última etapa, las entidades deben desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a la materialización de un incidente de ciberseguridad, para ello deben:

- Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.
- Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.

A magnifying glass with a gold handle is positioned over a glowing green globe. The globe is set against a background of a complex green circuit board with intricate patterns of lines and components. The overall image has a high-tech, digital aesthetic.

**La visión de la
Auditoría Interna
frente al riesgo de
ciberseguridad**

La Auditoría Interna debe incorporar aproximaciones cada vez más activas al riesgo de ciberseguridad en su plan de revisiones. La ciberseguridad como paradigma que revoluciona la seguridad tradicional necesariamente debe

introducir cambios en la manera en que la Auditoría Interna se aproxima a la misma. A continuación, se propone un enfoque paso a paso que puede ayudar a asumir esta nueva posición.

1. Entendimiento de la organización

Conocer la organización es clave en la definición de una estrategia adecuada de ciberseguridad. El entendimiento de la organización permite establecer aquellos objetivos que

podrían ser de interés para un atacante, determinando los focos de revisión para abordar el riesgo de ciberseguridad de manera paulatina.

2. Análisis y segmentación del riesgo

El perfil de riesgo de las organizaciones cambia muy rápido. La seguridad de la información sigue siendo un factor clave, pero es necesario incorporar y priorizar los paradigmas del mundo de la ciberseguridad. Se deberán tener en cuenta en el análisis al menos los siguientes riesgos:

- Riesgo de disponibilidad y continuidad de las TIC.
- Riesgo de seguridad de las TIC.
- Riesgo de cambio de las TIC.

- Riesgo de integridad de datos TIC.
- Riesgo de la externalización de las TIC.

Dicho análisis debe mapear las interacciones entre los distintos sistemas y la clasificación de los activos de información en cada uno de estos. Todos los sistemas de una organización están de alguna manera interconectados, si bien algunos revisten mayor riesgo que otros, no se deben descuidar las interacciones con sistemas menos relevantes.

3. Aproximación por etapas

Las etapas más comunes de un ciberincidente se pueden simplificar en tres: entrada, movimientos laterales y ataque.

Durante la fase de entrada se logra acceder a la organización empleando técnicas de ingeniería social o por un descuido del usuario final en la navegación a través de Internet, con el fin de ejecutar programas maliciosos y lograr persistencia. Los movimientos laterales se constituyen en la siguiente fase del ataque, y en ella el atacante realiza un *scanning* de la red adyacente para identificar vulnerabilidades con

la elevación de privilegios como objetivo clave. Una vez el atacante los consigue y ha alcanzado su objetivo en la red está listo para lanzar el ataque, estimaciones muestran que entre la infección y el ataque pueden transcurrir entre seis y ocho meses.

Es necesario que el Auditor Interno piense de la misma manera como lo hace el delincuente y así mismo aborde las revisiones a la organización. No se requiere lanzar un ataque *end to end* sobre la organización, basta con demostrar que

cada una de las fases es alcanzable para evidenciar que hay un riesgo importante de ciberseguridad.

La organización puede ser demasiado grande para abordarla en su totalidad. El equipo de auditoría puede plantear una revisión *end to end* de procesos de mayor

4. Manifiesto de pruebas

El Auditor Interno debe establecer dentro de la planeación de su trabajo de auditoría y del alcance de la revisión, el tipo de pruebas que hará en la organización, siempre bajo un enfoque *“one step before the fall”* para no poner en riesgo la operación de servicios críticos o de la organización misma.

En esta planificación se tendrán en cuenta los pasos anteriormente expuestos pues el tipo de pruebas estará asociado al perfil de riesgos de la organización, así

5. Agreement con el blue team

El esquema de trabajo propuesto es un esquema Red Team vs Blue Team. En este caso el equipo de auditoría representará al Red Team o equipo de ataque y el área de la organización que se determine, normalmente el área de seguridad, hará las veces de Blue Team o equipo de defensa.

Se deben establecer acuerdos entre ambos equipos para garantizar la transparencia de la comunicación y las pruebas que de alguna manera la organización está dispuesta a

riesgo o mantener un enfoque por etapas. En este enfoque por etapas se puede, por ejemplo, tomar como referencia el NIST y proporcionar, una a la vez, el aseguramiento de las cinco fases que lo componen (identificación, protección, detección, respuesta y recuperación).

como a los sistemas y a los activos de información más expuestos de acuerdo con el análisis que se haya realizado previamente.

El equipo de trabajo debe establecer acuerdos de comunicación de forma previa al inicio del trabajo para determinar de manera permanente durante la ejecución cuándo una prueba se debe detener o continuar, así como los pasos a seguir.

permitir y las que definitivamente no por temas de riesgo de la operación o consideraciones de políticas internas. Este acuerdo incluye tanto personas como sistemas que serán implicados en el set de pruebas.

Es recomendable que se coordinen ambos equipos al momento de realizar cada prueba, definiendo una hora de inicio y de final, de manera que se pueda distinguir entre un ataque real contra la organización y no se desvíe la atención del Blue Team en caso tal.

6. Árbol de desición de pruebas

El equipo auditor debe tener una batería de pruebas suficiente para abordar la revisión, que contemple el mayor número posible de escenarios de fallo o diferentes caminos para abordar la ejecución.

Se propone un diseño a manera de árbol de decisión, con *flags* o banderas, que determinan el avance al siguiente paso en la medida que un *flag* es marcado como exitoso dentro de una prueba.

El grado de incertidumbre suele ser muy alto en este tipo de revisiones porque se desconoce si los controles

establecidos por la organización van o no a funcionar. Es importante tener en cuenta que el paradigma de la seguridad perimetral se rompe en escenarios ciber porque la puerta de entrada del atacante suele ser el puesto de usuario, el eslabón más débil, y una vez vulnerada el atacante está dentro de la organización como un empleado más.

En este mismo sentido, y dependiendo del tipo de revisión que se quiera realizar y lo exhaustivo de la misma, en las pruebas se puede prescindir de hacer el testing del funcionamiento de los controles de seguridad perimetral.

7. Determinación de acciones

Se deben determinar las acciones a seguir tanto frente a la ejecución como a la organización y ante cada posible escenario, las cuales habrán de depender tanto del acuerdo con el Blue Team como del árbol de decisión de posibles pruebas a realizar. Estas acciones parten de notificar el hallazgo de manera inmediata o no, dependiendo de su relevancia y el posible impacto de un ataque real.

Se ha de establecer un *trade off* entre continuar explotando vulnerabilidades una vez se encuentra una debilidad y el impacto que puede tener para la organización mantenerla abierta para que el equipo de revisión pueda continuar. Lo primero debe ser la seguridad de la organización.

8. Pruebas de concepto

Los siguientes son ejemplos de pruebas de concepto que podrían plantearse y adaptarse a cada organización para valorar posibles escenarios de fuga de información, gestión insuficiente de identidades, credenciales y accesos

Interfaces y APIs inseguras, vulnerabilidades del sistema, hacking de cuentas, intrusión peligrosa, amenazas persistentes avanzadas, entre otros.

9. Pruebas de entrada

- Aplicar técnicas de ingeniería social utilizando el email (con adjunto) para simular malware en el puesto del empleado.
- Aplicar técnicas de ingeniería social utilizando el email y páginas webs maliciosas para simular *malware* en el puesto del empleado.
- Aplicar técnicas de ingeniería social utilizando el email y páginas webs maliciosas para obtener las credenciales del empleado.
- Aplicar técnicas de ingeniería social introduciendo USB malicioso en edificios corporativos para simular *malware* en el puesto del empleado.
- Acceder a la red wi-fi de forma anónima y analizar el tráfico para obtener las credenciales del empleado.
- Acceder a la red wi-fi de forma anónima y analizar el tráfico para identificar sistemas corporativos conectados.
- Acceder a la red wi-fi de forma anónima y realizar un ataque tipo *man in the middle* para obtener las credenciales del empleado.
- Acceder a la red wi-fi de forma anónima y realizar un ataque tipo *man in the middle* para ejecutar *malware* en el puesto del empleado.
- Acceder a la red wi-fi con credenciales válidas y analizar el tráfico para identificar sistemas de la red interna accesibles.

10. Pruebas de movimientos laterales

- Controlar un puesto de usuario desde Internet mediante “*malware*”.
- Controlar un puesto de usuario desde Internet utilizando un dispositivo físico.
- Realizar un reconocimiento del puesto de usuario.
- Realizar un reconocimiento de la red interna desde un puesto de usuario.
- Realizar un reconocimiento de la red interna desde una red de terceros.

11. Pruebas de ataque

- Localizar y acceder a información estratégica.
- Acceder de forma masiva a información de la plataforma bancaria / clientes.
- Extraer información de tipo “señuelo” de la red interna.
- Acceder remotamente a la plataforma bancaria.
- Plantear escenarios de daño a la entidad con enfoque “*one step before the fall*”.
- Consumir servicios digitales.

12. Ejecución iterativa

Se recomienda un enfoque iterativo para la ejecución de manera que el equipo auditor vaya revisando avances y determine próximos pasos con base en el árbol de decisión y en las pruebas de concepto definidas.

En ocasiones una vez logrado un *flag* es posible devolverse en el árbol de decisión y reintentar algunas pruebas dada la nueva información o privilegios obtenidos.

13. Reporting

El informe de auditoría debe contener los hallazgos de la revisión como hechos y describir hasta dónde se ha logrado llegar o qué información o sistemas han logrado ser comprometidos durante la revisión.

redacción del informe de auditoría en este sentido debe ser muy clara, concreta y sencilla de entender e ir a los hechos concretos evitando los juicios de valor.

Uno de los retos que presenta este tipo de auditorías es poder describir en términos no técnicos hallazgos, puesto que normalmente involucran terminología muy específica que la mayoría de los lectores puede desconocer. La

Una de las claves está en la capacidad de mostrar los hallazgos de auditoría con el potencial impacto que tendrían para la organización, bien sea en términos de impacto económico o reputacional dependiendo de si lo que se ha logrado por el Red Team tiene uno u otro, o ambos.



Ciber resiliencia

Acorde con el NIST, la ciber resiliencia es *“la habilidad para anticipar, resistir, recuperarse y adaptarse a condiciones adversas, tensiones, ataques o compromisos en los sistemas que utilizan o están habilitados por los recursos cibernéticos”*,⁵ bajo esta definición la ciber resiliencia se diferencia de la ciberseguridad en la medida en que es la capacidad para responder en caso de que la ciberseguridad haya sido quebrantada, mientras la ciberseguridad es la capacidad de proteger o defender el uso del ciberespacio de los ciberataques.

Una organización es ciber resiliente cuando es capaz de responder y recuperarse de un ciberataque, cuando puede seguir operando durante este y, posteriormente, aprender de lo sucedido para aumentar su capacidad de resistencia ante interrupciones futuras. La ciber resiliencia además involucra la gestión de la continuidad del negocio.

Las estrategias de resiliencia en ciberseguridad siempre deben derivarse de los requisitos generales del gobierno corporativo, riesgo y cumplimiento, establecidos en la

entidad, los cuales incluyen:

- Estrategia de seguridad de la información y estrategia de seguridad corporativa.
- Apetito de riesgo empresarial y tolerancia al riesgo residual.
- Niveles actuales y objetivo de madurez de ciberseguridad.
- Historial de incidentes y ataques.

El concepto de ciber resiliencia incluye una amplia gama de posibles medidas para fortalecer la ciberseguridad, las cuales se deben alinear con las opciones genéricas de tratamiento de riesgos (eliminación, transferencia, mitigación y aceptación).

1. Definición de la estrategia de resiliencia

Fase	Actividades
Definición de alternativas	<ul style="list-style-type: none"> • Identificar alternativas viables. • Evaluar riesgo residual. • Selección de alternativas.
Formulación	<ul style="list-style-type: none"> • Desarrollo de alternativas. • Alineación con procesos.
Implementación	<ul style="list-style-type: none"> • Ejecución de alternativas elegidas. • Definición del mapa de ruta.

⁵ NIST (2019). “Borrador SP 800-160 Volumen 2, Desarrollo de sistemas ciber resilientes: un enfoque de ingeniería de seguridad de sistemas”. Recuperado de: <https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf>

2. Implementando soluciones de resiliencia

Fase	Actividades
Administración de incidentes	<ul style="list-style-type: none"> • Establecer escenarios de incidentes. • Definir la respuesta a incidentes. • Establecer un equipo de incidentes / crisis. • Definir el reporte de incidentes. • Crear un equipo de comunicación con los entes reguladores y medios de comunicación, clientes, entre otros.
Continuidad y recuperación	<ul style="list-style-type: none"> • Definir planes de continuidad y recuperación por cada uno de los posibles escenarios. • Determinar un programa de capacitación al personal clave para atención del ciber ataque. • Identificar procesos claves. • Definir operaciones alternas. • Tener definidos proveedores estratégicos, que apoyen la atención e investigación del ataque.
Retorno a la normalidad	<ul style="list-style-type: none"> • Establecer el gap entre las operaciones alternas versus las normales. • Desarrollar procedimientos de limpieza. • Definir la cadena de custodia. • Realizar la evaluación forense. • Comunicar a clientes, entes reguladores y medio de comunicación. • Cuantificar del impacto económico y reputacional del evento.

3. Mantenimiento y actualización de la estrategia de resiliencia

Fase	Actividades
Entrenamiento y pruebas	<ul style="list-style-type: none"> • Identificar alternativas viables. • Evaluar riesgo residual. • Seleccionar alternativas. • Definir terceros expertos que apoyen la estrategia de la entidad.
Revisiones	<ul style="list-style-type: none"> • Por parte de la gerencia. • De los terceros. • De las áreas de Auditoría y cumplimiento. • Del equipo externo experto en el tema
Mantenimiento	<ul style="list-style-type: none"> • Definir el procedimiento de mejora continua. • Presentar resultados a la Junta Directiva y Comité de Auditoría.

De esta forma, se puede concluir que:

- La ciber resiliencia hace parte integral de la estrategia de ciberseguridad de una empresa.
- Las actividades orientadas a realizar un plan de auditoría para ciber resiliencia hacen parte de las actividades de ciberseguridad.

- La cultura de seguridad, ciberseguridad y ciber resiliencia, es el impulsor principal del nivel de protección que realmente se puede y quiere lograr.
- Dado que los ataques cibernéticos por lo general explotan las debilidades sociales en lugar de las técnicas, la ciber resiliencia es una cuestión de tecnología, pero sobre todo de comportamiento personal.



Conclusiones

El incremento de las amenazas cibernéticas da relevancia a la gestión y administración del riesgo de ciberseguridad, que se impone como uno de los principales retos de las entidades financieras quienes han debido adaptarse rápidamente para satisfacer las necesidades de sus clientes, que requieren cada vez más servicios digitales, a la vez que cumplen con los requerimientos normativos en esta materia.

Las áreas de la auditoría, tercera línea de defensa, han debido transformar sus procesos y adecuar sus capacidades para garantizar un control interno efectivo en materia de ciberseguridad. Si bien se han llevado a cabo esfuerzos significativos por construir políticas internas frente al riesgo cibernético jalonadas por las disposiciones de la CE N°007 de la SFC, es necesario alinear los programas de aseguramiento con los marcos internacionales para garantizar la resiliencia de las organizaciones ante un ciber ataque.

En este sentido, es necesario resaltar la importancia de los estándares internacionales de ciberseguridad del NIST,

COBIT 5 e ISO, y las pruebas propuestas en esta guía para garantizar una adecuada administración del riesgo cibernético. Lo anterior, permitirá a las organizaciones no solo instaurar controles para la identificación de un evento de ciberseguridad, sino también reaccionar de manera efectiva y resiliente a los ciberataques, que se han convertido en una de las principales preocupaciones de las entidades financieras.

De esta forma, el rol del Auditor Interno más allá de proporcionar una revisión y evaluación independiente sobre la eficacia de las líneas de defensa, debe entender y hacer seguimiento al perfil de riesgo de la organización, teniendo en cuenta las nuevas tecnologías y los riesgos emergentes que imponen la sofisticación de los ataques cibernéticos. Para cumplir este objetivo, se requiere una coordinación de todas las áreas de la entidad, desde la alta gerencia hasta los clientes, quienes forman parte del eslabón más débil de la cadena de la ciberseguridad.



ASOBANCARIA