Guía de buenas prácticas para auditar la ciberseguridad

ASOBANCARIA

GUÍA DE BUENAS PRÁCTICAS PARA AUDITAR LA CIBERSEGURIDAD

Autores y colaboradores

Hernando José Gómez **Presidente**

Alejandro Vera Sandoval **Vicepresidente Técnico**

Colaboradores:

Grupo Bancolombia
Banco de Bogotá
BBVA
Banco W
Bancamía
Banco Davivienda
Banco Caja Social
Scotiabank Colpatria.

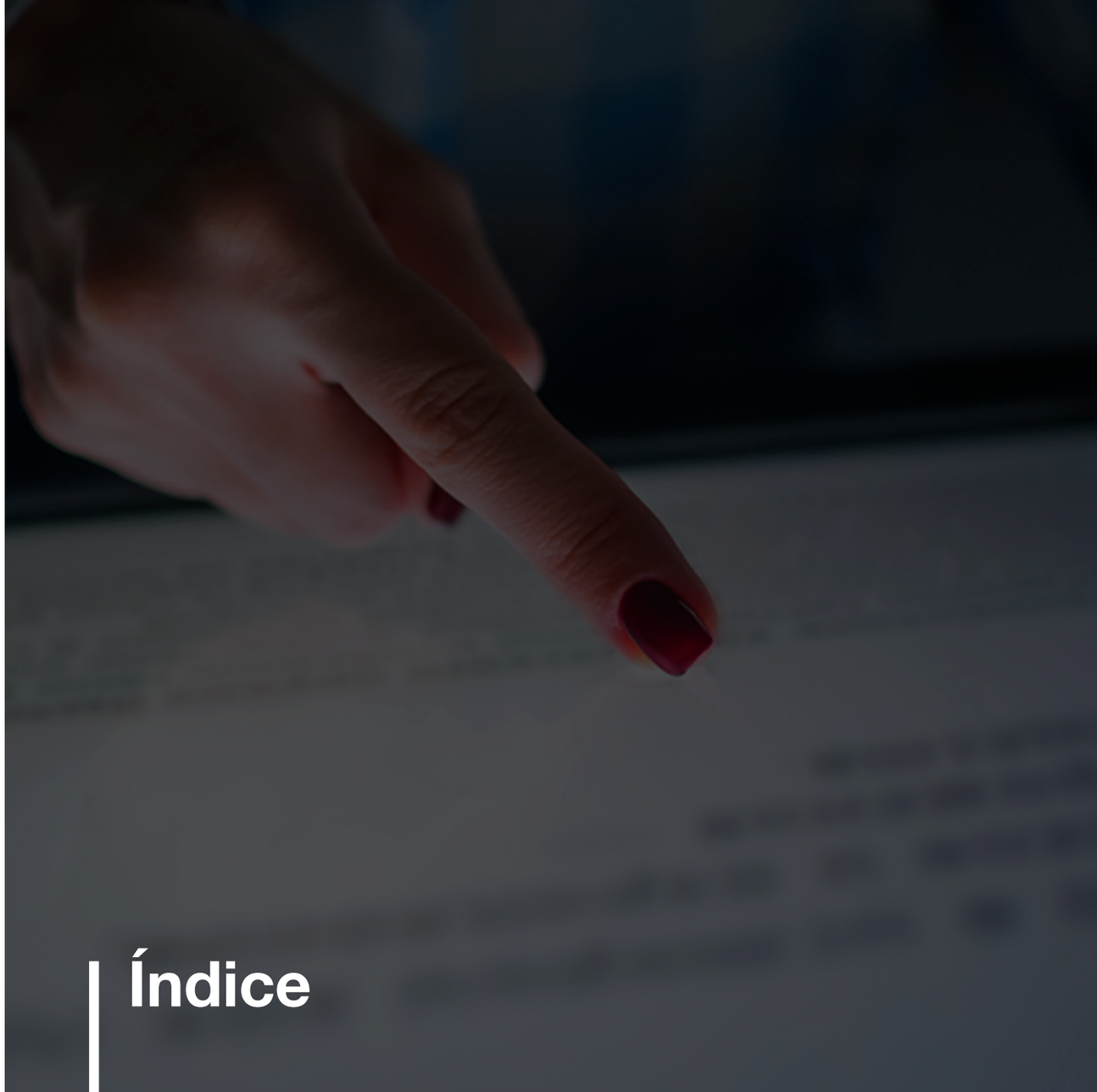
Edición:

Liz Marcela Bejarano Castillo — Directora Financiera y de Riesgos, Asobancaria.
Laura Sofía Rincon Coronado — Profesional Master, Asobancaria
Valentina Beltrán Lizarazo — Profesional Junior, Asobancaria.

Diseño: Babel Group
Camilo Andrés Grillo Velásquez

Junio de 2022

Este documento, publicado por la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, es producto del trabajo de un equipo interdisciplinario de entidades bancarias interesadas en compartir las mejores prácticas en materia de auditoría de ciberseguridad. 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, una hoja de ruta o plan de acción para las entidades agremiadas a Asobancaria o para otros lectores de este. Es importante aclarar que esta Guía no pretende reemplazar el detalle, la formalidad ni la rigurosidad de un libro de texto especializado, sino más bien, es un complemento a contenidos ya existentes de este tipo, enfocado en usuarios del mercado colombiano. Por este motivo, dejamos a consideración del lector la consulta de textos especializados en la sección de referencias.



Índice

Siglas

- **BYODt:** Usar su propio dispositivo.
- **CIS:** Centro para la Seguridad en Internet.
- **CVSS:** Sistema de Puntaje de Vulnerabilidades Comunes.
- **DDoS:** Ataque de Denegación del Servicio Distribuido.
- **IDS:** Sistemas de Detección de Intrusión.
- **IT:** Tecnología de la Información (siglas en inglés).
- **LAN:** Red de área local.
- **LDAP:** Protocolo ligero de acceso a directorios.
- **NIIP:** Plan Nacional de Protección de Infraestructura de Estados Unidos (siglas en inglés).
- **NIST:** Instituto Nacional de Estándares y Tecnología.
- **RDP:** Acceso de escritorio remoto.
- **SFC:** Superintendencia Financiera de Colombia.
- **STIG:** Guías de Implementación Técnica de Seguridad.
- **TIC:** Tecnologías de la Información y la Comunicación.
- **US-CERT:** Equipo de preparación ante emergencias informáticas de Estados Unidos (por sus siglas en inglés).
- **VDI:** Infraestructura de escritorio virtual.
- **VMI:** Infraestructura móvil virtual.
- **VPN:** Red privada virtual.
- **WAN:** Red de área amplia.
- **WLAN:** Red de área local inalámbricas.
- **WMAN:** Red de área metropolitana inalámbricas.
- **WPAN:** Red de área personal inalámbricas.

Glosario

- **Acceso remoto:** También conocida como host-to-gateway, esta arquitectura protege comunicaciones entre uno o más hosts individuales y una red específica que pertenece a una organización. La arquitectura de acceso remoto se utiliza con mayor frecuencia para permitir que los hosts en redes no seguras, como empleados que viajan y teletrabajadores, para obtener acceso a servicios organizativos internos, como el correo electrónico y los servidores web de la organización.

- **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.

- **BOTS:** Es un programa malicioso, que permite hacerse con el control de un equipo infectado. Generalmente, los bots que también son denominados robots web son parte de una red de máquinas infectadas, llamadas botnets, que, a su vez, está compuesta por máquinas víctimas de todo el mundo. Debido a que un equipo infectado por bots cumple las órdenes que se le dan, muchas personas tienden a referirse a estos equipos como zombies.

- **BYOD:** se puede definir como la práctica en la que se alienta a los trabajadores al uso de los dispositivos que tienen en casa para acceder a los sistemas y datos empresariales.

- **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.

- **Dirección IP:** es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice internet.

- **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.

- **Gusano:** Un virus informático o gusano informático es un programa de software malicioso que puede replicarse a sí mismo en ordenadores o a través de redes de ordenadores sin darse cuenta de que el equipo está infectado. Como cada copia del virus o gusano informático también puede reproducirse, las infecciones pueden propagarse de forma muy rápida.

- **LDAP:** hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

- **LAN:** es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

- **Malware:** es un programa malicioso que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

- **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.

- **RPD:** es un protocolo propietario desarrollado por Microsoft que permite la comunicación entre una terminal y un servidor Windows en la ejecución de aplicaciones, es decir, permite acceder de forma remota a equipos de cómputo sin estar físicamente delante de estos.

- **ROOTKITS:** es un término que se aplica a un tipo de malware, diseñado para infectar un PC, el cual permite al hacker instalar diferentes herramientas que le dan acceso remoto al ordenador. El rootkit contiene diferentes herramientas maliciosas como un keylogger, un módulo para robar los números de tarjeta o cuentas bancarias, un bot para ataques DDoS y otras funciones que pueden desactivar el software de seguridad.

- **Sandboxing:** Técnica que proporciona un entorno de prueba potente y aislado, que permite ejecutar un programa/dispositivo sospechoso para observar y analizar su comportamiento antes de conectarlo a la red.

- **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.

- **Servicio de directorio:** es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.

- **Shadow IT:** Dispositivos, software y servicios de TI utilizados dentro de las organizaciones y los cuales se encuentran fuera de su propiedad o control.

- **Software:** es el soporte lógico de un sistema informático.

- **SPYWARE:** es un tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue las actividades en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que se escribe, carga, descarga y almacena. Algunas cepas de spyware también son capaces de activar cámaras y micrófonos para verlo y escucharlo sin que el usuario se dé cuenta.

- **TROYANOS:** es un tipo de malware que a menudo se disfraza de software legítimo. Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios. Generalmente, los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, los troyanos permiten a los cibercriminales espiar, robar información confidencial y obtener acceso de puerta trasera del sistema.

- **VDI:** es una tecnología que consiste en virtualizar los entornos de trabajo de los empleados y alojarlos en una ubicación controlada por la empresa.

- **VMI:** es una infraestructura que permite acceder a aplicaciones móviles remotas desde un dispositivo móvil.

- **VLAN:** es un método para crear redes lógicas independientes dentro de una misma red física.

- **VPN:** es una red virtual, un túnel seguro construido sobre redes físicas existentes, que puede proporcionar un mecanismo de comunicaciones seguro para los datos y otra información transmitida entre dos puntos finales. La VPN da acceso al trabajador remoto a diferentes recursos corporativos tales como aplicaciones, servidores de archivos e impresoras.

- **VPN de sitio a sitio:** es un puente virtual entre las redes de oficinas geográficamente distantes, que les permite conectarse a través de internet para mantener una comunicación segura y privada entre las redes.

- **WAN:** es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación 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 mayor 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. Así mismo, es importante considerar aspectos adicionales como:

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

Adicionalmente, la contingencia sanitaria originada por el COVID-19, los acelerados cambios tecnológicos y la transformación de los modelos de negocio de la industria bancaria, han generado importantes retos para las entidades del sector financiero, quienes han debido adaptarse para garantizar la continuidad de sus operaciones en un contexto limitado por las restricciones derivadas del distanciamiento social y el autocuidado, factores críticos para superar la pandemia.

Bajo este panorama, uno de los riesgos emergentes a los que se ve expuesta la banca es el relacionado con el esquema masivo de trabajo en casa o teletrabajo[1]. Si bien estos modelos de trabajo son diferentes desde la óptica de la legislación laboral, son semejantes en lo operativo y lo técnico, con las ventajas y amenazas que conlleva desarrollar actividades remotas por los funcionarios de las entidades.

Bajo este contexto, esta Guía de Buenas Prácticas busca ser un apoyo en el desarrollo de políticas frente al riesgo cibernético que permitan la preparación, reacción y resiliencia de la organización ante este tipo de situaciones. Con este propósito, el presente documento se desarrolla en doce capítulos. En el quinto 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 sexto, 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. Posteriormente, en el séptimo se explican los diez lineamientos que debe seguir

[1] Según la “Guía para empleadores sobre el trabajo desde casa en respuesta al brote del COVID-19” de la Organización Internacional del Trabajo (OIT), se considera que el trabajo desde casa es una modalidad de teletrabajo o trabajo remoto en el hogar, con la diferencia de que el teletrabajo puede desempeñarse en diversos lugares alejados del lugar de trabajo principal o de los locales del empleador (como el trabajo itinerante). Para el propósito de esta guía, se asumirá el concepto de teletrabajo o trabajo remoto para que las prácticas recomendadas puedan ser aplicables a las distintas modalidades de teletrabajo de manera generalizada.

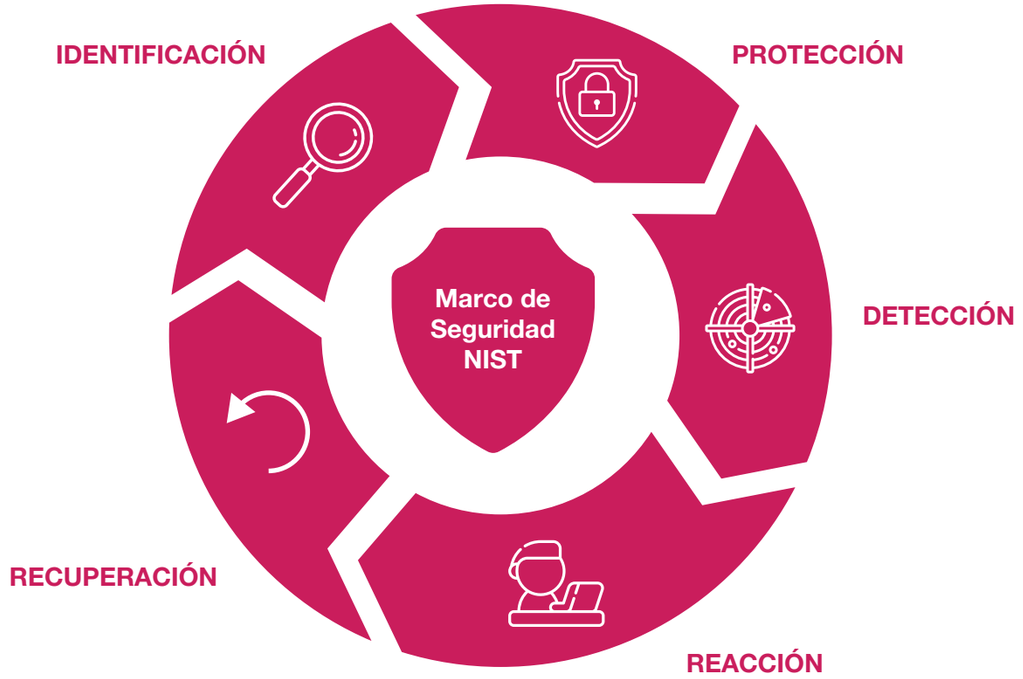
la auditoría Interna frente a la ciberseguridad y en el octavo, las medidas para auditar la resiliencia de la organización ante un evento que atente contra la seguridad informática.

En el noveno capítulo se exponen las principales características de las conexiones remotas en el teletrabajo, así como los marcos de referencia relacionados (NIST y Normas ISO) y la Guía para el Teletrabajo de Entidades Vigiladas por la SFC. Por último, en el décimo se presenta una guía de pruebas a los controles para trabajo remoto y algunas herramientas enfocadas en el aseguramiento técnico de conexiones remotas.

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"*[2] 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 Cibersecurity Framework - NIST**



[2] Instituto Nacional de Estándares y Tecnología (Abril 2018). "Cibersecurity Framework". Recuperado de: https://www.nist.gov/cyberframeworkframework

Con base en estas cinco funciones se pueden establecer objetivos de control y una serie de acciones para realizar evaluaciones de auditoria 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 auditoria[3] 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.

[3] 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

Programa de Auditoría y Ciberseguridad[4]

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.

[4] 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 las 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.[5]
		Las prioridades para la misión, objetivos y actividades de la organización están establecidas y comunicadas.	1. 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. 2. 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. 3. Determinar si un plan estratégico de IT está documentado, define funciones y está mapeado a los objetivos de la empresa. 4. 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:

[5] Tomado de Department of Homeland Security. (https://www.dhs.gov/what-critical-infrastructure).

IDENTIFICAR			
Área del Proceso	**Objetivos de Control**	**Controles**	**Paso de Prueba**
			a. Los sistemas de información y software que apoyan funciones críticas del negocio están identificados y priorizados en función del tiempo máximo de inactividad permitido. b. 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.	1. 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. 2. 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.	1. Obtener una copia de la política de seguridad de la información. 2. Determinar si la política está completa y si ha sido aprobada por la estructura de gobierno al interior de la organización. 3. 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.	1. 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. 2. Determinar si hay suficiente independencia al interior de los roles de seguridad de la información para proporcionar una adecuada separación de las funciones críticas. 3. 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.	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: 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 fórums y fuentes de intercambio de información.	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.	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.	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.	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 riegos están establecidos, gestionados y acordados por los terceros o partes interesadas de la organización.	Evaluar el marco o proceso utilizado para la gestión del riesgo. Considere lo siguiente: a. ¿Está el proceso formalmente documentado? b. ¿El proceso es actualizado regularmente? b. ¿Es el proceso repetible y medible? c. ¿Tiene dueño el proceso? d. ¿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.	1. Determinar si el acceso a dispositivos de red (p.ej., servidores, estaciones de trabajo, dispositivos móviles, firewalls) está restringido por: a. Único ID de usuario para inicio de sesión. b. Contraseñas complejas. c. Autenticación de múltiples factores. d. Cierre automático si se deja desatendido. e. Bloqueo automático después de repetidos intentos fallidos de acceso. f. Cambio de nombre y contraseña predeterminados para cuentas administrativas. 2. Determinar si los parámetros de contraseña cumplen con la política de la organización y/o los requisitos aplicables de la industria. Considere lo siguiente: a. Longitud, complejidad, requisitos de cambio, historia b. ¿Se suprimen las contraseñas de todos los resultados? c. ¿Los archivos de contraseña están encriptados y restringidos? 3. Revisar los procedimientos de terminación para garantizar que las credenciales se revoquen o cambien cuando un empleado se va. a. 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.	1. Determinar si el acceso físico a activos clave está físicamente restringido: a. Puertas cerradas. b. Vigilancia. c. Cercas o muros. d. Registros. e. Acompañamiento al visitante. 2. Determinar si las políticas y procedimientos permiten el acceso únicamente a personal autorizado a áreas sensibles. 3. Revisar los procedimientos de terminación para asegurar que el acceso físico se remueve cuando el empleado se va.
		El acceso remoto está administrado.	Determinar si las políticas y los procedimientos relacionados con las capacidades de acceso de los usuarios remotos están formalizados. Considere lo siguiente: a. Usuarios remotos (p.ej., empleados, contratistas, terceros) con acceso a los sistemas críticos están aprobados y documentados. b. Conexiones remotas son solo abiertas según sea requerido. c. Conexiones remotas están registradas y monitoreadas. d. Conexiones remotas están encriptadas. e. Existe una autenticación fuerte (p.ej., múltiples factores, parámetros de contraseña fuertes). f. La capacidad para borrar datos de forma remota en dispositivos móviles cuando faltan datos o son robados está habilitada. g. 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.	1. Revisar los derechos y permisos de acceso a la red y a cualquier aplicación crítica. 2. Determinar si los perfiles de acceso del usuario son consistentes con sus funciones de trabajo (con base en el mínimo privilegio). 3. Comparar una muestra de la autoridad de acceso de los usuarios con sus deberes y responsabilidades asignadas. 4. 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.	1. Determinar si existe un plan formal para copias de seguridad y restauración. 2. 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 leíbles.
		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: a. Interruptor de emergencia. b. Iluminación de emergencia. c. Planta de emergencia. d. Protección contra el fuego. e. Control de temperatura y humedad. f. Protección contra daño por agua. g. Ubicación de los componentes de sistemas de información (para minimizar daños).
		Los datos son destruidos de acuerdo con las políticas.	1. Revisar las políticas de desinfección de medios (destrucción de datos). 2. 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. 3. Verificar basureras, contenedores de basura, basura triturada y/o trituradores para garantizar el cumplimento de las políticas. 4. 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: a. Auditorías, evaluaciones y escaneos de vulnerabilidades en curso son realizados, revisados y respondidos. b. 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**
			c. 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. d. 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.	1. Determinar si la organización participa en grupos de intercambio y análisis de la información. 2. 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.	1. 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. 2. Evaluar los planes para determinar qué tan frecuente se actualizan y aprueban. 3. Validar que la estrategia de ciber resiliencia definida se encuentre alineada a los objetivos del negocio y la estrategia de ciberseguridad. 4. 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).	1. Revisar los procesos de contratación para determinar si la verificación de antecedentes se realiza a todos los empleados. 2. Revisar los procesos de contratación para posiciones con acceso a información sensible para determinar si ellos son proporcionales a un nivel alto de riesgo. 3. 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.	1. Obtener el plan de gestión de vulnerabilidades de la organización y garantizar que incluya lo siguiente: a. Frecuencia de escaneo de vulnerabilidades. b. Métodos para medir el impacto de las vulnerabilidades identificadas (p.ej., sistema de puntaje de vulnerabilidades comunes [CVSS]). c. Incorporación de las vulnerabilidades identificadas en otras evaluaciones de control de seguridad (p.ej., auditorías externas, pruebas de penetración). d. Procedimientos para el desarrollo de reparación de vulnerabilidades identificadas. 2. 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.	Revisar los procesos de mantenimiento controlado. Considere lo siguiente: a. 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). b. El personal o los contratistas de mantenimiento son aprobados, autorizados y supervisados (si es requerido). c. 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.	Determinar si el mantenimiento remoto en servidores, estaciones de trabajo y otros sistemas es realizado. Considere lo siguiente: a. ¿A quién se le permite conectarse a los sistemas (p.ej. trabajadores internos, terceros)? b. ¿Qué software/versión o servicios son usados para conectarse? c. 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. d. Requerimientos de autentificación adecuados (p.ej., autentificación 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.	1. Determinar si los registros de auditoría son mantenidos y revisados de manera oportuna. 2. Verificar la idoneidad de los registros para monitorear y evaluar actividades de IT y eventos de seguridad. Considere lo siguiente: a. 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). b. 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. c. Los registros y las herramientas de auditoría están protegidos de acceso, modificación y eliminación no autorizados. 3. Determinar si los registros para las siguientes partes de la red están monitoreados y revisados: a. Perímetro de la red (p.ej., sistemas de detección de intrusión [IDS], firewalls). b. Sistemas Microsoft (p.ej., registros de eventos de Windows). c. 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.	1. Obtener una copia de la política de medios removibles. Los controles deben incluir: a. Capacitación al usuario. b. Encriptación de medios removibles. c. Acceso restringido a medios removibles (p.ej., restricciones a USB). d. Procedimientos de desinfección para medios desmantelados. 2. 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.	1. Revisar los sistemas de información para determinar si las funciones, los puertos, los protocolos y los servicios innecesarios y/o no seguros están deshabilitados. 2. 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.	Evaluar los controles relacionados con comunicaciones para garantizar que la red es segura. Considere: a. Existen defensas perimetrales de red (p.ej., border router, firewall). b. Los controles de seguridad física son usados para prevenir el acceso no autorizado a sistemas de telecomunicaciones, etc. c. 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.	1. 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. 2. Revisar los diagramas en busca de lo siguiente: a. Frecuencia de actualización de los diagramas. b. Exactitud y completitud de los diagramas. c. 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/prevención de intrusión), entre ellos. 3. 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.	1. Obtener una copia de las políticas y los procedimientos relacionados con el monitoreo de sistemas y de la red. a. Determinar si las políticas y los procedimientos requieren monitoreo de actividad anómala en los puntos de control identificados. 2. 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.	1. 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). 2. Obtener una lista de las fuentes que proveen datos a cada evento agregado y sistemas de monitoreo (p.ej., firewalls, routers, servidores). 3. 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.	1. Obtener una copia de los eventos detectados y las respuestas de la organización a ellos. 2. 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 cumplimientos, impacto operacional, impacto de reportes exactos).
		Los límites de alertas ante incidentes están establecidos.	1. Obtener una copia de mensajes de alerta, actas de reuniones, reportes y otra documentación donde eventos detectados fueron escalados. 2. Revisar la documentación y determinar lo siguiente: a. Los eventos detectados son reportados de manera oportuna a alguien con el conocimiento y experticia para resolver o escalar el evento.

DETECTAR			
Área del Proceso	**Objetivos de Control**	**Controles**	**Paso de Prueba**
			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.	1. Obtener una lista del control de monitoreo implementado por la organización a los siguientes niveles: 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.	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.	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**
			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.	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: 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: 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.	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 detective de código móvil bloquean un código móvil no autorizado cuando se detecta (p.ej., cuarentena, bloqueo de ejecución, bloqueo de descarga). *Ejemplos de controles de código móvil incluyen: 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**
			b. Detectar y bloquear porciones de código móvil de sitios web. c. Remover la habilidad de correr código móvil en sistemas que no requieren está funcionalidad (p.ej., desinstalar Java de estaciones de trabajo que no lo requieran). 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.
		La actividad de proveedores externos de servicios se monitorea para detectar eventos potenciales de ciberseguridad.	1. Obtener y revisar los contratos ejecutados con proveedores externos de servicios. 2. Determinar si los contratos con proveedores externos de servicios requieren que estos: a. Notifiquen a la organización tan pronto como sea posible de cualquier evento conocido o sospechoso de ciberseguridad. 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. c. Implementen controles de seguridad equivalentes a o que excedan el nivel de seguridad requerido por la organización. 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/prevención de intrusión) están implementados en estos puntos de conexión. 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.

DETECTAR			
Área del Proceso	**Objetivos de Control**	**Controles**	**Paso de Prueba**
		Se realiza monitoreo en busca de personal, conexiones, dispositivos y software no autorizados.	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). 2. Verificación de los controles de acceso no autorizado accediendo a las instalaciones y sistemas con permiso para probar, pero no con autorización estándar. Pedir a la organización que provea las notificaciones de alerta generadas por el acceso no autorizado simulado.
		Se realizan escaneos de vulnerabilidad.	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. 2. Revisar la programación y los resultados en busca de lo siguiente: a. Frecuencia. b. Finalización exitosa. c. Solución o mitigación documentada de las vulnerabilidades identificadas. d. El alcance de las pruebas incluye a todos los sistemas críticos. 3. Determinar si los resultados de los escaneos de vulnerabilidad fueron reportados a individuos o grupos con autoridad apropiada para asegurar su solución.
Procesos de detección	Los procesos y procedimientos de detección están mantenidos y probados para garantizar conciencia oportuna y adecuada ante eventos anómalos.	Los roles y las responsabilidades para la detección están bien definidos, asignando responsabilidades.	1. Obtener una copia de los procesos y procedimientos para monitorear eventos físicos y electrónicos anómalos. 2. Determinar si los procesos y procedimientos de la organización asignan responsabilidades clave a individuos o posiciones específicas.

DETECTAR			
Área del Proceso	**Objetivos de Control**	**Controles**	**Paso de Prueba**
		Las actividades de detección cumplen con los requisitos que aplican.	1. 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. 2. 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.	1. 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/prevención de intrusión, anti-malware software de punto final). 2. Revisar la documentación en busca de lo siguiente: a. Completitud en la prueba de controles implementados de detección de actividad anómala. b. Frecuencia de la prueba. c. Solución o mitigación documentada de resultados de prueba negativos.
		La información de detección de eventos es comunicada a las partes apropiadas.	1. 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 la junta/gerencia, reuniones de gestión del riesgo). 2. Obtener una copia de las respuestas documentadas a incidentes recientes de actividad física y electrónica anómala. 3. 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	Obtener una copia de las respuestas documentadas a incidentes recientes de actividad física y electrónica anómalos. Determinar si las respuestas contienen lo siguiente: a. Lecciones aprendidas y análisis de controles que fallan o son faltantes. b. 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.	1. Determinar si la organización ha aprobado respuestas a incidentes y planes de continuidad del negocio. 2. Obtener las copias de reportes de incidentes recientes para validar que los planes son ejecutados. 3. 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.	1. Revisar los planes de respuesta ante incidentes para determinar si los roles y responsabilidades están definidas para empleados. 2. Entrevistar a los empleados para determinar si ellos conocen sus roles y responsabilidades según lo definido en el plan. 3. 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.	1. Revisar el plan de respuesta ante incidentes para determinar si la estructura de reporte y los canales de comunicación están claramente definidos. 2. Determinar si los empleados están capacitados para reportar sospechas de incidentes de seguridad. 3. 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.	1. Revisar el plan de respuesta ante incidentes para determinar si el intercambio de información está claramente definido dado que relaciona lo siguiente (si corresponde): a. Clientes. b. Fuerzas del orden público. c. Reguladores. d. Medios. e. Organizaciones de intercambio de información. 2. 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.	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.	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.	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: 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**
			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.	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: 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.	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: 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.

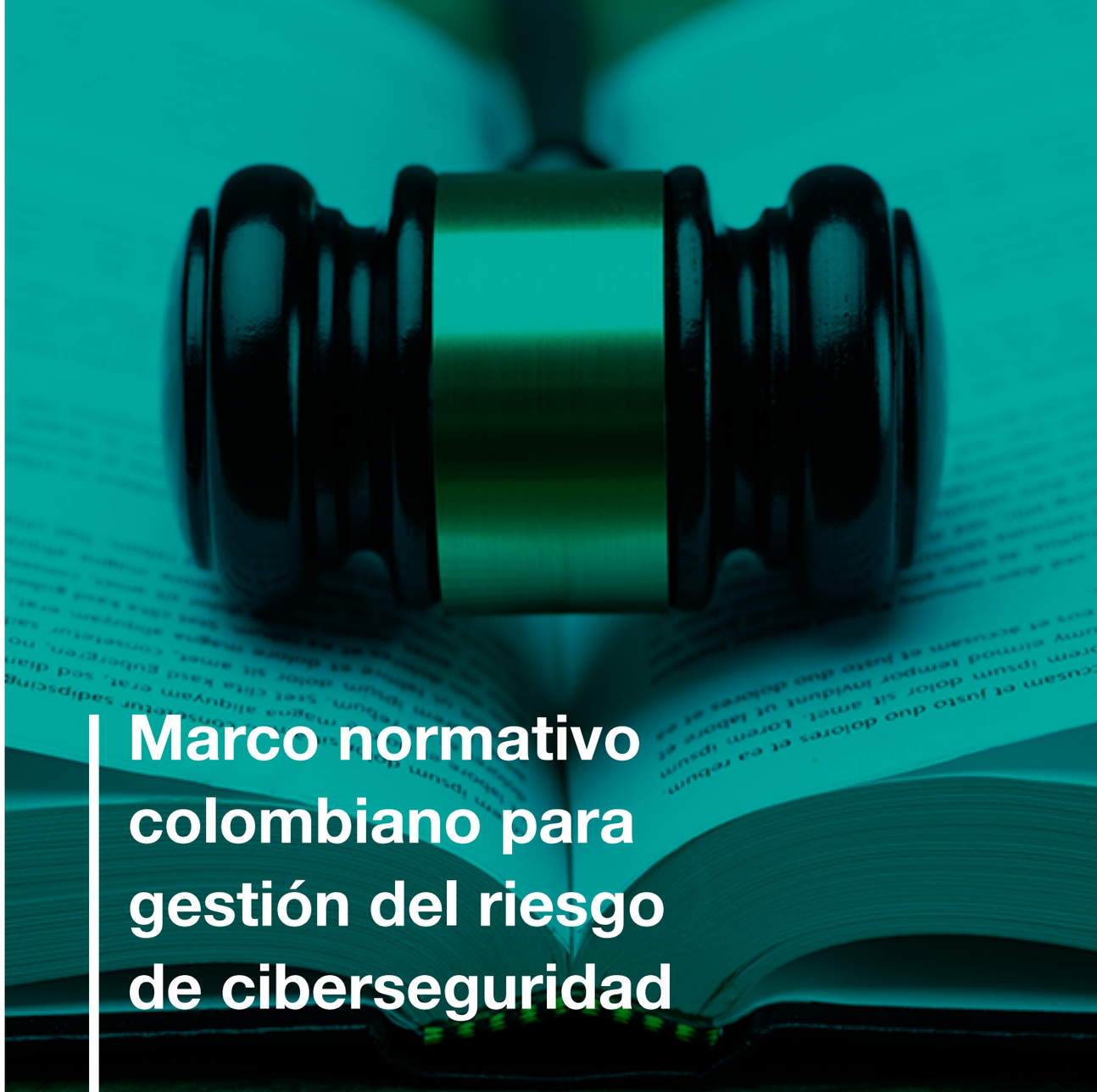
RESPONDER			
Área del Proceso	**Objetivos de Control**	**Controles**	**Paso de Prueba**
		Las vulnerabilidades recientemente identificadas son mitigadas o documentadas como un riesgo aceptado.	Determinar si los procesos de monitoreo continuo de la organización (p.ej., evaluación de riesgos, escaneo de 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 disrupción 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**
			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.	Obtener los resultados documentados de eventos recientes de ciberseguridad. Determinar si lo siguiente está incluido: 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.	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 Cumplimento). 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 Directica 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 segregar 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.

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:

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.
- 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.
- 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.

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 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.

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 auditoria puede plantear una revisión *end to end* de procesos de mayor 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).

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 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.

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 auditoria 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 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.

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 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.

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"*,[6] 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	• Identificar alternativas viables. • Evaluar riesgo residual. • Selección de alternativas.
Formulación	• Desarrollo de alternativas. • Alineación con procesos.
Implementación	• Ejecución de alternativas elegidas. • Definición del mapa de ruta.

[6] 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	• 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	• 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	• 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	• Identificar alternativas viables. • Evaluar riesgo residual. • Seleccionar alternativas. • Definir terceros expertos que apoyen la estrategia de la entidad.
Revisiones	• Por parte de la gerencia. • De los terceros. • De las áreas de Auditoría y cumplimiento. • Del equipo externo experto en el tema
Mantenimiento	• 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.

Aseguramiento de seguridad perimetral y conexiones remotas

9.1 Características principales de las conexiones remotas en el teletrabajo

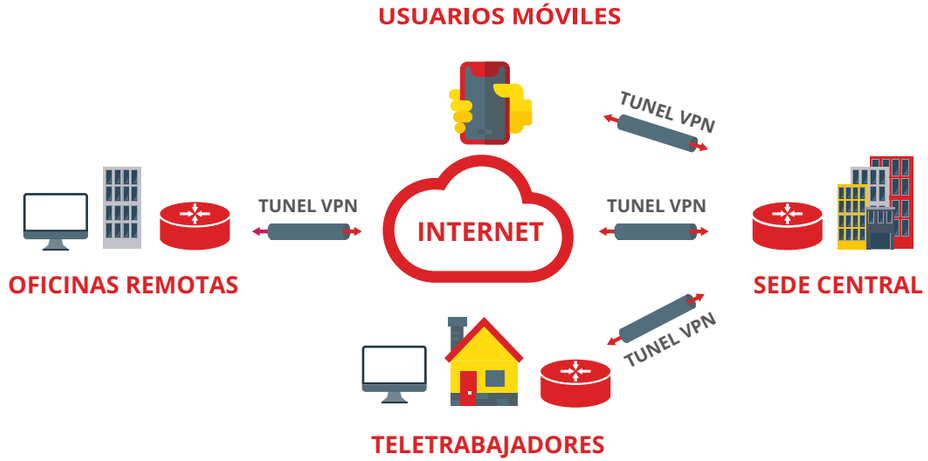
La mayoría de los “teletrabajadores” utilizan el acceso remoto (VPN, VDI -Virtual desktop infrastructure, escritorio remoto, portales de aplicaciones y conexión directa a las aplicaciones), lo que permite que los usuarios de una organización puedan acceder a los recursos informáticos de la empresa desde ubicaciones externas distintas de las instalaciones de la compañía.

A continuación, se describen algunos de estos métodos y sus principales características

9.1.1 VPN

Una red privada virtual (VPN, por sus siglas en inglés) es una tecnología de red que permite una extensión segura de una red local (LAN, por sus siglas en inglés)[7] sobre una red pública o no controlada como Internet.

Gráfico 2 **Estructura de una VPN para una empresa**



Fuente: *Gráfico tomado de INCIBE - Instituto Nacional de Ciberseguridad, 2020*

[7] Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadorasque abarca un área reducida a una casa, un departamento o un edificio.

Las conexiones establecidas que utilizan VPN protegen la información que se intercambia, ya que establecen un "túnel" o canal cifrado de comunicación entre el dispositivo y el lugar de trabajo por donde viajan los datos confidenciales de manera segura. El *software* VPN cifra la información enviada por los dispositivos, lo que significa que no se puede interceptar el tráfico que se está transmitiendo a través de Internet. Este sistema funciona aplicando una clave de cifrado a los datos para transformarlos de forma tal que la información sólo puede ser descifrada por un sistema que también tenga la clave utilizada para cifrar los datos (clave secreta previamente compartida).

Además de proteger la confidencialidad y la integridad las VPN proporcionan:

- **Autenticación mutua:** proceso por el cual dos partes de una comunicación se identifican y autentican una a la otra simultáneamente, garantizando la legitimidad de los participantes en la comunicación.
- **Protección frente a reenvíos:** asegurando que los datos solo se entregan una vez, evitando la posibilidad de que sean interceptados por un ciberdelincuente o que este inserte paquetes maliciosos en la comunicación.
- **La protección frente al análisis de tráfico:** impidiendo que se pueda extraer información a través del análisis de la comunicación (los datos que se transmiten entre los dos extremos, la cantidad de datos transmitidos, etc.).

Arquitecturas VPN

En términos simples, una VPN crea un "túnel de comunicación" que une cliente y servidor para mantener una comunicación segura y privada entre ellos. Posibilita la ampliación de la red de la empresa haciendo que los recursos informáticos de una ubicación estén disponibles para los empleados de otras ubicaciones.

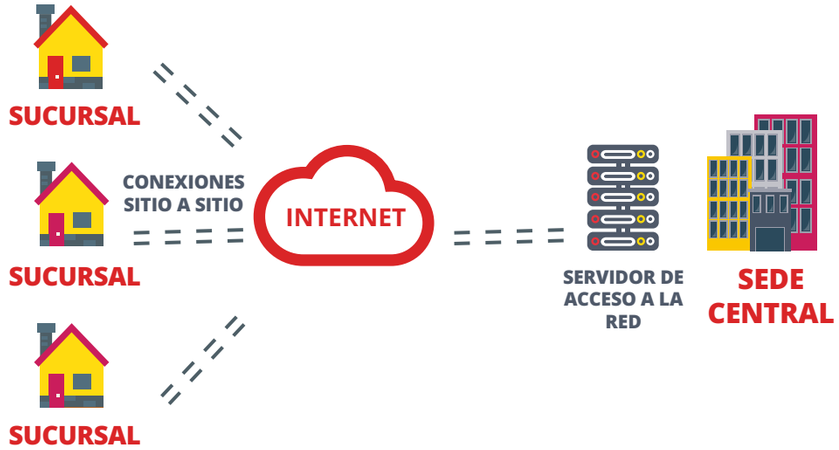
Los escenarios de VPN más comunes y sus principales características técnicas son:

VPN de sitio a sitio

También conocida como VPN *Site-To-Site* (por su denominación en inglés). Esta implementación se utiliza principalmente para comunicar un sitio con uno o más sitios remotos (por ejemplo, la sede principal de la empresa y una sede secundaria) a través de una red pública como Internet, estableciendo una conexión segura.

En este escenario, los dispositivos cliente (terminales) no necesitan ningún *software* VPN, ni precisan ningún tipo de configuración adaptada para el uso de esta. Requiere de dos dispositivos servidores VPN, uno en cada sitio que se quiera conectar.

Gráfico 3 **VPN de sitio a sitio basada en Intranet**



Fuente: *Gráfico tomado de INCIBE - Instituto Nacional de Ciberseguridad, 2020*

Existen dos tipos de implementaciones VPN de sitio a sitio:

- **Basada en intranet:** si una empresa tiene una o más ubicaciones remotas a las que desea unirse en una sola red privada puede crear una VPN de intranet para conectar cada LAN separada a una sola WAN[8].
- **Basada en extranet:** cuando una compañía tiene una relación cercana con otra compañía (como un socio, proveedor o cliente), puede construir una extranet VPN que conecte las LAN de esas compañías. Esta extranet VPN permite a las empresas trabajar juntas en un entorno de red seguro y compartido, a la vez que impide el acceso a sus intranets independientes.

VPN de acceso remoto

Se utiliza principalmente para salvaguardar las comunicaciones entre el dispositivo del teletrabajador y la red interna de la empresa. Se puede utilizar este tipo de VPN para hacer que una red de oficina esté disponible de forma remota para los usuarios autorizados, como por ejemplo los empleados que trabajan desde casa o en el transcurso de un viaje, y por tanto necesitan acceder de forma remota a las aplicaciones y a la información corporativas utilizando Internet como vínculo de acceso.

[8] Una red de área amplia, o WAN (Wide Area Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

Gráfico 4 VPN de acceso remoto

Fuente: *Gráfico tomado de INCIBE - Instituto Nacional de Ciberseguridad, 2020*

Esta configuración requiere de dos dispositivos:

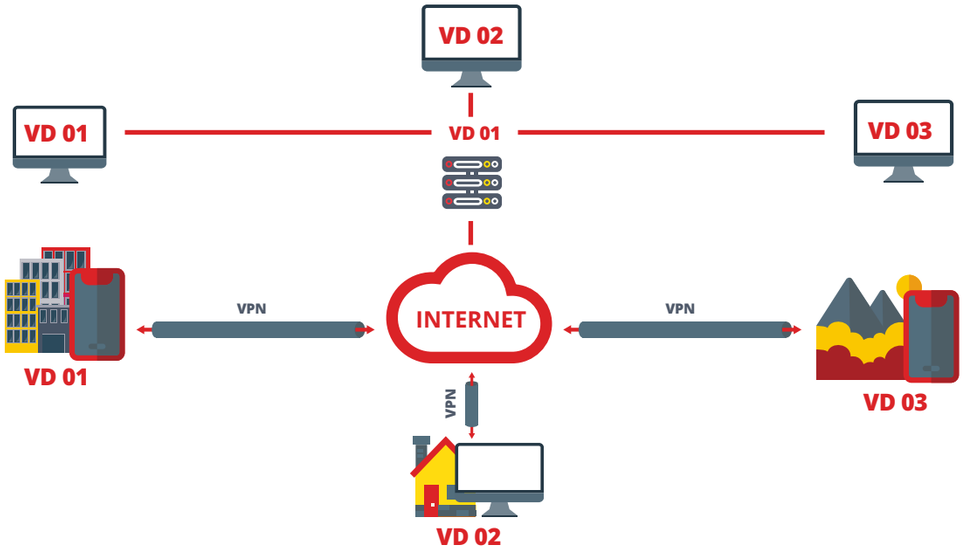
- Un dispositivo *hardware* instalado en la red de la organización, denominado concentrador de VPN o VPN *Gateway*, que conecta la red de la organización con los clientes VPN de forma segura.
- Un dispositivo *software* o cliente VPN en el lado del usuario que conecta de forma segura a los dispositivos cliente, como por ejemplo ordenadores o *smartphones* de empleados que trabajan en remoto, con las redes de la organización.

9.1.2 Infraestructura de escritorio virtual

Una infraestructura de escritorio virtual (VDI, por sus siglas en ingles), es una tecnología que consiste en virtualizar los entornos de trabajo de los empleados y alojarlos en una ubicación controlada por la empresa. Este tipo de solución encaja tanto para situaciones de teletrabajo en las que gran parte de la plantilla está fuera de la oficina, como también cuando habitualmente hay trabajadores con una elevada movilidad, como comerciales, flotas de reparto, soporte in situ, etc.

Para el empleado es muy similar a trabajar desde su puesto en la oficina ya que puede disponer del mismo sistema operativo y aplicaciones con las que ya trabajaba, pero desde cualquier dispositivo: ordenadores portátiles, *smartphones* o tablets, accediendo a su entorno de trabajo personal generalmente a través de un navegador web.

Gráfico 5 Infraestructura de escritorio virtual o VDI



Fuente: *Gráfico tomado de INCIBE - Instituto Nacional de Ciberseguridad, 2020*

9.1.3 VDI propio o como servicio «DaaS»

Los entornos de trabajo de los empleados son gestionados por la empresa mediante la solución VDI elegida, pudiendo estar alojada en un servidor propio o en los servidores de una empresa contratada según las necesidades de la organización.

Instalar VDI en un servidor propio: su principal ventaja es el control sobre la administración del sistema evitando depender de terceros a los que se les traslade los requisitos de seguridad. No obstante, hay que contar con personal técnico que realice la implementación, así como considerar el tiempo de despliegue y el gasto económico que conlleva la adquisición de *hardware*.

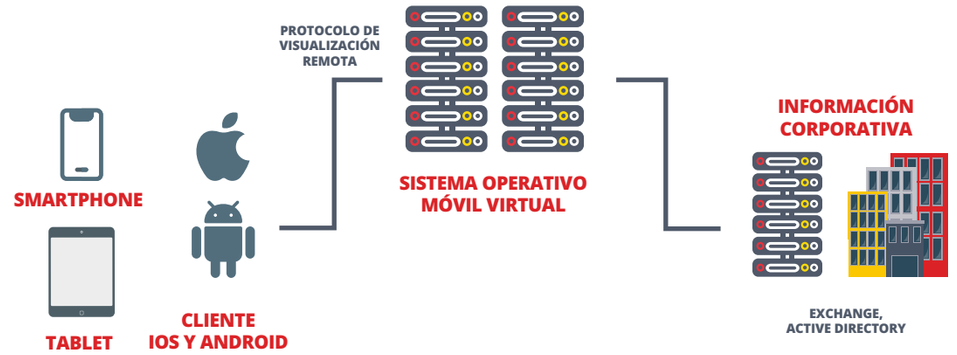
VDI como servicio o DaaS (Desktop as a Service): Consiste en contratar a una empresa externa todo lo relacionado con la puesta en marcha y mantenimiento del sistema VDI. Los escritorios virtuales de los empleados pueden seguir siendo gestionados internamente y así aplicar las mismas medidas y políticas de seguridad que si el VDI estuviera ubicado en un servidor propio.

El principal inconveniente de este modelo es que la privacidad de la información gestionada puede verse comprometida. Para evitarlo, además de leer detenidamente la política de privacidad y seguridad del servicio contratado, tendremos que detallar los requisitos de seguridad y privacidad y firmar un acuerdo de nivel de servicio.

9.1.4 Infraestructura Móvil Virtual

Ya que las tecnologías móviles están cada vez más presentes en el entorno empresarial, la infraestructura móvil virtual (VMI, por sus siglas en inglés) es una muy buena opción a considerar a la hora de mejorar la seguridad de las organizaciones. Una infraestructura móvil virtual permite acceder a aplicaciones móviles remotas desde un dispositivo móvil. Como las aplicaciones se ejecutan en servidores corporativos, no es posible perder sus datos o que los roben, incluso si se pierde el dispositivo o es sustraído. Resulta muy útil para separar entornos de trabajo y personales en un mismo dispositivo.

Gráfico 6 Infraestructura VMI



Fuente: *Gráfico tomado de INCIBE - Instituto Nacional de Ciberseguridad, 2020*

Es además muy práctico si un empleado deja su puesto de trabajo ya que la empresa sólo tiene que bloquearle el acceso al sistema remoto y toda la información corporativa deja de ser accesible para ese usuario.

9.1.5 Aplicaciones de escritorio remoto

Las aplicaciones de acceso de escritorio remoto (RPD, por sus siglas en inglés) proporcionan al teletrabajador la posibilidad de controlar remotamente un equipo, siendo habitual conectarse al equipo del que se es usuario en la oficina de la organización, desde un dispositivo cliente de teletrabajo.

En este modelo de conexión, el teletrabajador tiene control de teclado y ratón sobre el ordenador remoto y ve la pantalla de ese equipo en la pantalla del dispositivo con el que está trabajando. Uno de los escritorios remotos más conocido es RDP, ya que se encuentra integrado en el sistema operativo Windows, aunque existen otras muchas opciones.

El acceso remoto al escritorio permite al usuario acceder a todas las aplicaciones, datos y otros recursos como si utilizara su ordenador en la oficina. El funcionamiento se basa en que un programa cliente de acceso de escritorio remoto o *plug-in* de navegador web está instalado en cada dispositivo cliente de teletrabajo, y se conecta directamente con la correspondiente estación de trabajo interna del empleado en la red interna de la organización.

Gráfico 7 **Modelo de acceso remoto**

Fuente: *Gráfico tomado de INCIBE - Instituto Nacional de Ciberseguridad, 2020*

A simple vista puede parecer un buen método para conectarse remotamente, ya que la instalación de estas aplicaciones es muy sencilla y no requiere de altos conocimientos técnicos para su implantación. La parte negativa es que estas herramientas pueden crear puertas traseras (backdoors) a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos.

Otro problema grave de seguridad con el *software* de escritorio remoto es que está descentralizado; es decir, en lugar de que la organización tenga que proteger un único servidor de puerta de enlace VPN, es necesario proteger cada estación de trabajo interna a la que se puede acceder a través del acceso de escritorio remoto.

Debido a que se puede acceder a estas estaciones de trabajo internas desde Internet, por lo general necesitan estar protegidas con el mismo rigor que los servidores de acceso remoto. Elevar la seguridad a un nivel aceptable requeriría una cantidad significativa de tiempo y recursos, así como la implementación de controles de seguridad adicionales.

9.1.6 Soluciones en la nube

Las soluciones en la nube ofrecen gran versatilidad y un modelo diferente a la hora de compartir y almacenar información cuando se teletrabaja. Algunos esquemas son:

Portales para aplicaciones

Otra de las opciones para implementar soluciones de acceso remoto en la organización son los portales para aplicaciones. Un portal es un servidor que proporciona el acceso a una o más aplicaciones corporativas a través de una interfaz única centralizada. La mayoría de estos portales están basados en web, por lo que el teletrabajador solo necesita utilizar un navegador como cliente para acceder a las aplicaciones de la empresa y poder realizar las funciones relativas a su trabajo. Cada empleado tendrá un perfil configurado en el que se le dará acceso solo a aquellas aplicaciones necesarias para desempeñar su trabajo.

En términos de seguridad, los portales protegen la información que se intercambia entre los dispositivos cliente y el portal, proporcionando control de acceso y autenticación entre otros servicios de seguridad.

Los portales y las VPN comparten características de seguridad y se diferencian en la ubicación del *software* cliente de la aplicación y de los datos asociados. En la VPN, el *software* y los datos están en el dispositivo cliente y en un portal se encuentran en el servidor del portal, aunque estos se pueden configurar para permitir la descarga de contenido del portal y almacenarlo en el dispositivo cliente o en otros dispositivos fuera del entorno seguro.

Herramientas colaborativas

Las tecnologías colaborativas mantienen en contacto al equipo de trabajo cuando desempeña tareas fuera de la organización: paquetes ofimáticos, videoconferencias, pizarras virtuales, intercambio de documentos y ficheros, chats, etc. Al utilizar estas herramientas se debe proporcionar la seguridad necesaria a la información que se intercambia y por ello establecer una serie de pautas básicas de seguridad.

9.2 Marcos de referencia relacionados

9.2.1 Norma ISO / IEC 27033

La serie de normas ISO/IEC 27033[10] consta de seis partes diseñadas para garantizar la seguridad de la red de dispositivos, aplicaciones, servicios y usuarios finales[11]. Estos apartados tratan sobre la seguridad de las comunicaciones entre redes mediante puertas de enlace de seguridad, VPN y acceso inalámbrico a redes IP, así:

- ISO/IEC 27033-1 es un mapeo hacia las otras partes. Proporciona una visión general de los conceptos y orientación de la gestión de seguridad de la red al ayudar a las organizaciones a identificar y analizar los riesgos y los requisitos de seguridad de la red.

- ISO/IEC 27033-2 proporciona directrices sobre la planificación, el diseño, la implementación y la documentación de la seguridad de la red. Presenta la arquitectura de seguridad de la red, sus requisitos y los principios de diseño.

- ISO/IEC 27033-3 muestra escenarios de red y sus amenazas relacionadas, técnicas de diseño y problemas de control. Ayuda a las organizaciones a revisar la arquitectura de seguridad técnica, el diseño y los controles de seguridad.

- ISO/IEC 27033-4 proporciona directrices sobre riesgos, técnicas de diseño y controles de puertas de enlace de seguridad. Presenta puertas de enlace de seguridad para proteger los flujos de información entre redes.

- ISO/IEC 27033-5 proporciona directrices sobre riesgos, técnicas de diseño y controles de VPN. Ayuda a las organizaciones a seleccionar, implementar y supervisar los controles técnicos necesarios para conectar usuarios remotos a redes.

- ISO/IEC 27033-6 proporciona directrices sobre riesgos, técnicas de diseño y controles de redes inalámbricas IP. Ayuda a las organizaciones a seleccionar, implementar y supervisar los controles técnicos necesarios para asegurar la comunicación entre redes inalámbricas. Esta parte presenta las redes de área personal inalámbricas (WPAN), las redes de área local inalámbricas (WLAN) y las redes de área metropolitana inalámbricas (WMAN).

9.2..2 Norma NIST 800-113

Este documento busca ayudar a las organizaciones a comprender las tecnologías SSL VPN. La publicación también hace recomendaciones para diseñar, implementar, configurar, asegurar, monitorear y mantener soluciones VPN SSL[12]. Incluye una comparación con otras tecnologías similares, como las VPN de seguridad de protocolo de Internet (IPsec) y otras soluciones de VPN (NIST, 2021), y analiza las tecnologías y características fundamentales de las VPN SSL y cómo encaja en el contexto de la seguridad de red en capas.

[10] ISO (2017). “Protección de las comunicaciones a través de redes mediante redes privadas virtuales (VPN)”.
[11] Seguridad de red aplica a la seguridad de los dispositivos, la seguridad de actividades de gestión relacionadas con los dispositivos, aplicaciones/servicios, y usuarios finales; sumada a la seguridad de la información siendo transferida a través de los enlaces de comunicación.
[12] Una VPN SSL consta de una o más VPN dispositivos a los que los usuarios se conectan mediante sus navegadores web. El tráfico entre el navegador web y el dispositivo SSL VPN está encriptado con el protocolo SSL. (Norma NIST 800-113)

El documento está organizado en seis secciones principales que buscan:

- Proporcionar una introducción general a la seguridad de la capa de red y transporte.
- Describir los fundamentos de las VPN SSL y sus servicios y características.
- Explotar en profundidad cada una de las fases de planificación e implementación de VPN SSL.
- Proporcionar una lista consolidada de prácticas recomendadas para la implementación de VPN SSL en términos del enfoque del ciclo de vida del desarrollo del sistema.
- Describir varios protocolos VPN que se utilizan como alternativas a las VPN SSL en diferentes escenarios.
- Presentar un caso de estudio de implementación y planificación de una solución VPN SSL.

En la siguiente tabla se relacionan las principales temáticas que recoge cada una de las secciones mencionadas:

Resumen de los contenidos de las temáticas de la norma NIST 800-113

Sección	Temáticas abordadas

Seguridad de la capa de transporte y red	• La necesidad de seguridad en la red y la capa de transporte.
	• VPN
	  ◦ VPN del portal SSL
	  ◦ VPN de túnel SSL
	  ◦ Administración de VPN SSL

Fundamentos de las VPN SSL y sus servicios y características	• Arquitectura VPN
	• Funciones VPN
	• Funciones y servicios de seguridad de SSL
	  ◦ Manejabilidad
	  ◦ Alta disponibilidad y escalabilidad
	  ◦ Personalización del portal
	  ◦ Autenticación
	  ◦ Protección de integridad y cifrado
	  ◦ Control de acceso
	  ◦ Controles de seguridad de terminales
	  ◦ Prevención de intrusiones
	• Conceptos básicos del protocolo SSL
	  ◦ Versiones de SSL
	  ◦ Criptografía utilizada en sesiones SSL
	  ◦ Autenticación utilizada para identificar servidores SSL
	• Desafíos de SSL VPN

Fase	Actividades

Planificación e implementación de SSL VPN	• Identificar requisitos
	• Aprobación de SSL VPN y FIPS (Federal Información Processing Standard) 140-2
	  ◦ Versiones de SSL
	  ◦ Establecimiento de claves utilizado por SSL
	  ◦ Funciones hash utilizadas por SSL
	  ◦ Cifrado SSL
	  ◦ Certificados utilizados durante las negociaciones SSL
	• Diseñar la solución
	  ◦ Diseñar la Política de Control de Acceso
	  ◦ Diseñar la política de seguridad de end points
	  ◦ Seleccione los métodos de autenticación
	  ◦ Diseñar la Arquitectura
	  ◦ Política de criptografía y cumplimiento de FIPS
	  ◦ Otras decisiones de diseño
	• Implementar y probar el prototipo
	  ◦ Interoperabilidad de aplicaciones y clientes
	• Implementar la solución
	• Gestionar la solución

Prácticas recomendadas para la implementación de VPN SSL.	• Presenta las prácticas recomendadas correspondientes a las fases del ciclo de vida
	  ◦ Iniciación
	  ◦ Adquisición y desarrollo
	  ◦ Implementación
	  ◦ Mantenimiento

Alternativas a las VPN SSL.	• Protocolos VPN de la capa de enlace de datos • Protocolos VPN de capa de red • Capa de aplicación “VPN”
Caso de estudio	• Se presenta un caso de estudio de implementación y planificación de una solución VPN SSL.

Fuente: *Construcción propia con base en la norma NIST 800-113*

9.3 Guía para el teletrabajo de entidades vigiladas de la Superintendencia Financiera de Colombia

La Delegatura de Riesgo Operacional y Ciberseguridad de la Superintendencia Financiera de Colombia, emitió el 17 de marzo de 2020 un documento denominado “Guía para el teletrabajo de entidades vigiladas”, el cual contiene los siguientes apartados:

Para las entidades vigiladas:

- Recomendaciones para el teletrabajo.
- Uso de laptops personales para el trabajo.
- Gestión de información confidencial.
- Contactos y canales de emergencia.
- Monitoreo.
- Medios de comunicación y redes sociales.
- *Malware* y aplicaciones móviles.

Para los empleados de las entidades:

- Monitoreo sobre correos electrónicos y ataques de *phishing*.
- Higiene cibernética.
- Uso de redes Wifi Seguras.
- Reporte dispositivos perdidos o robados.

Entre las recomendaciones realizadas a las entidades, se resaltan las siguientes:

- Establecer una política o directriz que sea conocida y aprobada por la Junta Directiva y la Alta Gerencia.

- Revisar los procesos y procedimientos de seguridad relacionados con el acceso remoto a los sistemas corporativos.

- Contar con la capacidad de recursos humanos y de infraestructura para la adopción de mecanismos de trabajo remoto.

- Disponer de los mecanismos y protocolos para la asistencia al personal que realice las operaciones de forma remota, contando con una clara identificación de roles y responsabilidades dentro del personal de TI de la entidad.

- Establecer, como mínimo, canales y árboles de comunicación para el soporte y mantenimiento.

- Contemplar herramientas para la gestión remota de equipos.

- Considerar y aprovisionar los recursos necesarios para garantizar una conectividad VPN mayor a lo habitual, realizando un análisis de riesgos y costos asociados.

- Preparar a los funcionarios que prestan el soporte para la instalación y la configuración de los equipos para trabajo remoto.

- Realizar mesas de trabajo para tener una comunicación constante de la situación y el estado de aquellos empleados que se encuentran trabajando de manera remota.

9.4 Otros aspectos a tener en cuenta

9.4.1 Riesgos y amenazas

Los cambios que genera el trabajo remoto traen consigo nuevos riesgos y situaciones que hacen relajar los controles de ciberseguridad, tal como lo plantea (Deloitte, 2020) en su artículo "Covid-19- Ataques cibernéticos ante la oficina remota".

Gráfico 8 **Amenazas Cibernéticas relacionadas con la oficina remota**

Fuente: *Deloitte, 2020. "Covid-19- Ataques Cibernéticos ante la oficina remota"*

Según el INCIBE[13], actualmente existen muchas amenazas que afectan a la seguridad de los dispositivos cliente de teletrabajo, que al materializarse por ciberdelincuentes tienen diferentes motivaciones, incluyendo causar daño material y reputacional a la organización, robar propiedad intelectual, cometer robo de identidad y otras formas de fraude.

La principal amenaza contra la mayoría de los dispositivos cliente de teletrabajo es el *malware*, incluyendo virus, gusanos, troyanos, rootkits, spyware y bots, que pueden infectar los dispositivos a través de muchos medios, como el correo electrónico, los sitios web, las descargas y el uso compartido de archivos, la mensajería instantánea y las redes sociales. El uso de medios o dispositivos extraíbles no autorizados, como las memorias flash, es otro mecanismo muy común de transmisión del *malware*.

Una amenaza a destacar contra los dispositivos cliente de teletrabajo es la pérdida o el robo del dispositivo, ya que alguien con acceso físico a un dispositivo tiene muchas opciones para intentar ver o copiar la información almacenada en él. Un atacante con acceso físico también podría infectar con *malware* el dispositivo y así conseguir que le proporcione acceso a los datos a los que se accede o se introducen en dicho dispositivo, como por ejemplo las contraseñas de los usuarios que se escriben en el teclado de un ordenador portátil (keylogger). Entre las amenazas identificadas por el INCIBE también se incluyen:

- **Falta de controles de seguridad física:** en ciertas ocasiones los dispositivos destinados al teletrabajo se utilizan en lugares fuera de la organización como por ejemplo en hoteles, cafeterías, en salas de conferencias, etc. Esta condición aumenta el riesgo de que los dispositivos se pierdan o sean robados, lo que lo convierte a su vez en una posible pérdida de datos corporativos si no están convenientemente protegidos. Es muy importante tener en cuenta este tipo de situaciones a la hora de aplicar las medidas de seguridad necesarias para este tipo de dispositivos y proteger la información de accesos no deseados.

- **Errores de configuración:** para asegurar una configuración óptima en los equipos es aconsejable que únicamente el personal técnico autorizado pueda instalar, actualizar y eliminar *software*.

- **Redes no seguras:** las organizaciones no tienen control sobre las redes que usan sus empleados para teletrabajar. Es una práctica habitual utilizar redes abiertas e inseguras (aeropuertos, cafeterías, etc.) que un ciberdelincuente podría aprovechar para acceder a la información que contiene el dispositivo utilizado para el trabajo en remoto.

- **Dispositivos infectados en redes corporativas:** la inclusión del BYOD[14] en el ámbito empresarial ha sumado factores de riesgo, como el uso de dispositivos que están infectados con algún tipo de *malware* a consecuencia del uso personal. El problema surge cuando una vez infectados se conectan a la red de la empresa, pudiendo propagar el *malware* a otros dispositivos.

- **Acceso remoto a los recursos internos:** permitir el acceso externo a los recursos corporativos implica su exposición a nuevas amenazas, aumentando la posibilidad de que estos se vean comprometidos. Por este motivo, es necesario otorgar acceso a estos recursos solo a los empleados que lo necesiten para el desempeño de su trabajo.

- **Falta de formación:** es habitual que la falta de formación o de conocimiento de las políticas de seguridad de la empresa por parte de los empleados pongan en riesgo la seguridad de la información.

[13] INCIBE (2020). "Ciberseguridad en el teletrabajo - Una guía de aproximación al empresario"
[14] De sus siglas en inglés Bring Your Own Device, en español trae tu propio dispositivo, se puede definir como la práctica en la que se alienta a los trabajadores al uso de los dispositivos que tienen en casa para acceder a los sistemas y datos empresariales

Otra variable adicional que se incorpora al ecosistema del teletrabajo es la conexión que hacen los usuarios desde su red doméstica de Internet, servicio prestado generalmente por un proveedor de telefonía. Dada esta condición el INCIBE resalta como principales riesgos de las redes inalámbricas, las siguientes:

- **Denegación de servicio (DoS):** se trata de incapacitar la infraestructura inalámbrica a través de peticiones de servicio masivas a los puntos de acceso, provocando que los sistemas se vean incapaces de atender a tantas peticiones. Mediante este ataque se busca sobrecargar el punto de acceso o el *router* e impedir que los usuarios legítimos hagan uso de los servicios que este presta.

- ***Man-in-the-middle:*** se basa en que el atacante pueda situarse entre el emisor y el receptor, suplantando una de las partes y haciendo creer a la otra que está hablando con el legítimo destinatario de la comunicación, o incluso suplantando al punto de acceso.

- **Ataques por fuerza bruta:** método consistente en hacer uso de todas las contraseñas posibles cuya finalidad es averiguar las claves criptográficas de la comunicación o de las que dan acceso a la red wifi. A pesar de que parezca poco probable conseguirlas, en Internet existen multitud de herramientas gratuitas que permiten hacerse con las claves de redes que no cuenten con algoritmos criptográficos o claves robustas.

- **Eavesdropping:** captura de tráfico de red no autorizado realizado a través de alguna herramienta como antenas de gran alcance. El objetivo es capturar la información que transmitimos, que podría ser completa si no se encuentra cifrada o, en caso contrario, hacerse con patrones de comportamiento para intentar un descifrado.

- **MAC Spoofing:** se trata de suplantar la dirección MAC[15] de un dispositivo permitido cuando el punto de acceso tenga configurada una lista de este tipo de direcciones permitidas.

9.4.2 Recomendaciones generales de seguridad

El primer paso será establecer una política organizativa en la que se definan las normas a cumplir en los distintos escenarios o respecto al uso de los distintos sistemas y métodos de acceso. Esta política deberá contemplar distintos aspectos, como los siguientes:

- Relación de usuarios que disponen de la opción de trabajar en remoto. Será necesario llevar un control de las personas que por su perfil dentro de la empresa o las características de su trabajo tienen la opción de teletrabajar.

- Procedimientos para la solicitud y autorización del teletrabajo.

- Aplicaciones y recursos a los que tiene acceso cada usuario. Cada usuario tendrá acceso solo a las aplicaciones y recursos que requiera para realizar su trabajo, dependiendo del rol que desempeñe en la empresa. Se detallarán las aplicaciones colaborativas y de teleconferencia permitidas, así como sus condiciones de uso evitando utilizar programas no controlados por la empresa, práctica conocida como Shadow IT[16].

[15] De sus siglas en inglés Media Access Control, la dirección MAC es un identificador único e irrepetible que identifica todo dispositivo conectado a una red. También es conocida como dirección física.
[16] El término Shadow IT engloba dispositivos, *software* y servicios de TI utilizados dentro de las organizaciones y los cuales se encuentran fuera de su propiedad o control.

- Mecanismos de acceso seguro mediante contraseña. Para las credenciales de acceso se utilizarán siempre contraseñas robustas y el doble factor de autenticación siempre que sea posible, y forzando su cambio periódico. Este mecanismo puede estar ligado a la gestión de cuentas de usuario y control de accesos a través de servicios de directorio[17] LDAP[18].

- Configuración que deberán tener los dispositivos desde los que se establezcan las conexiones remotas: sistema operativo, antivirus, control de actualizaciones, etc., tanto si son corporativos como si son aportados por el trabajador. En este caso se puede controlar su configuración a través del *fingerprinting* de dispositivos, es decir, registrando una huella digital del dispositivo autorizado generada con datos de uso: navegador y *plugins* instalados, operador de telefonía, ubicación, horarios, etc.).

- Procedimiento y tecnología para cifrar los soportes de información para proteger los datos de la empresa de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

- Definición de la política de almacenamiento en los equipos de trabajo[19] así como de almacenamiento en la red corporativa[20].

- Procedimiento y planificación de las copias de seguridad periódicas de todos los soportes y comprobar regularmente que pueden restaurarse.

- Uso de conexiones seguras a través de una red privada virtual, en lugar de las aplicaciones de escritorio remoto.

- Virtualización de entornos de trabajo para eliminar los riesgos asociados al uso de un dispositivo propio.

- En el caso de utilizar dispositivos móviles para teletrabajar, la política debe incluir la utilización de aplicaciones de administración remota. Definir los criterios para evitar el uso de redes wifi-públicas y utilizar las conexiones 4 G/5G en su lugar.

- Formar a los empleados antes de empezar a teletrabajar.

[17] Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.
[18] El protocolo ligero de acceso a directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas de LDAP) hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
[19] Incibe. "Políticas de seguridad para la pyme – Almacenamiento en los equipos de trabajo". Recuperado de: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-en-los-equipos-trabajo.pdf
[20] Incibe. "Políticas de seguridad para la pyme – Almacenamiento en la red corporativa". Recuperado de: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-red-corporativa.pdf

9.5 Ciclo de Vida de un Ataque

Según la organización que establece la base de conocimientos mundial de tácticas y técnicas de adversarios para ataques a infraestructura (MITRE ATT&CK), relaciona en su matriz las siguientes etapas que se dan en un ataque.

9.5.1 Reconocimiento

Es el paso donde el adversario intenta ganar conocimiento acerca del objetivo y que utilizará en el plan de ataque.

- Escaneo activo: Se ejecutan procesos como escaneo de IP y vulnerabilidades para obtener información acerca de la infraestructura.

- Información de los equipos: Se obtiene información del *Hardware, Software, Firmware*, Versión del Sistema Operativo, Tipo de virtualización, Arquitectura, Lenguaje, Zona horaria, entre otros.

- Información de Identidad: Durante la recolección de información se puede evidenciar datos de empleados, contacto de técnicos, correos electrónicos y en algunas ocasiones se pueden encontrar contraseñas.

- Información de la Red: Es esencial encontrar información acerca de los segmentos de red asignados a la víctima, nombres de los dominios, números de teléfono y correos electrónicos de los administradores, DNS, Topología como la identificación de los Appliances de seguridad, *Firewalls*, IPS entre otros.

- Información de la organización: En este paso se busca información acerca de la estructura organizacional, operaciones claves de negocio como los nombres de las personas a cargo de los mismos. La ubicación física, los horarios de oficina y atención al público como las personas que están a cargo de los principales proyectos de tecnología.

- *Phishing*: Teniendo la anterior información se realiza un ataque de *Phishing* masivo y dirigido (*Spear*) con el fin de obtener acceso a cuentas.

- Bases en venta: Se puede comprar información acerca de la víctima en fuentes confiables que han recolectado datos relevantes como los especialistas de Inteligencia de amenazas.

- Fuentes abiertas: Existe información pública que puede servir para el ataque en sitios como administradores de DNS, WHOIS, Certificados digitales, CDN y bases de encuestas. Así como en redes sociales, motores de búsqueda y en la misma página web de la víctima.

9.5.2 Recursos para el ataque

El adversario establece con cuales recursos cuenta y determina la estrategia para realizar el ataque. Desarrolla las técnicas que utilizaría a través de la creación, compra o robo de las mismas.

- Adquirir la Infraestructura: El adversario puede comprar, alquilar o rentar la infraestructura como dominios, servidores DNS, Virtualizaciones, *Botnets* o el registro de servicios web en páginas como Google o Twitter.

- Compromiso de cuentas: A través de Ingeniería Social se determina que cuentas se van a comprometer que serían de utilidad para el ataque. Cuentas de aplicación, redes sociales o de correos electrónicos.

- Compromiso de Infraestructura: Se puede atacar infraestructura de terceros para obtener acceso a recursos como dominios, Servidores DNS, Sitios Web y otros necesarios para el ataque.

- Desarrollo de herramientas: Otra forma de realizar el ataque es desarrollar las propias herramientas para realizar el ataque entre las cuales se encuentra la elaboración de *Malware*, Certificados Digitales, Exploits o la automatización de herramientas libres.

9.5.3 Acceso Inicial

Se utilizan varios vectores para ganar el acceso inicial dentro de la red. Dentro de las técnicas utilizadas para esto se encuentra el *Phishing* dirigido y la explotación de vulnerabilidades en servidores Web.

- Explotación de vulnerabilidades: El adversario puede ingresar al sitio Web donde ejecuta comandos para hacer que el sistema se comporte diferente. Esta debilidad en el sistema puede ser originada por un Bug o por una vulnerabilidad en el diseño. Esto aplica para sitios Web pero también para base de datos, al igual que protocolos de comunicación.

- Acceso Remoto: Se pueden iniciar servicios de forma remota para generar la vulnerabilidad como VPN, Citrix y otros mecanismos de acceso que permiten conexión a los recursos internos de la empresa.

- Equipos espías: El adversario puede conectar *hardware* especializado a los equipos de cómputo así como equipos de comunicación y que permiten un acceso remoto.

- *Phishing*: Se puede enviar mensajes a través de correos dirigidos que contengan archivos, enlaces o SMS de terceros para obtener la información de credenciales y obtener acceso a los recursos de las víctimas.

- Unidades de almacenamiento externo: Se puede distribuir un *Malware* a través de memorias USB, discos duros externos o cualquier medio removible en sistemas que tienen la característica de ejecutar “Autorun”

- Compromiso en Cadena de Abastecimiento: Se puede comprometer los sistemas de terceros a través de *software* o *hardware* ya que tendrían acceso a los recursos de las víctimas.

- Cuentas de usuario: Teniendo credenciales comprometidas el adversario puede ingresar a servicios como VPN, correo electrónico o escrito remoto. Existen cuentas por defecto que puede traer el fabricante y que no han sido configuradas de forma correcta. Cuentas de usuario del domino así como las locales y cuentas de servicios de nube.

9.5.4 Ejecución del ataque

Se ejecuta los códigos maliciosos o las herramientas seleccionadas con el objetivo de explorar o robar información de una red.

- Interpretador de comandos y Scripts: Se puede ejecutar comandos o Scripts en los sistemas operativos o plataformas donde se ha tenido acceso. Dentro de los interpretadores se tiene PowerShell, Applescript, Windows Shell, Unix Shell, Visual Basic, Python, Java Script y consola de los dispositivos de Red.

- Contenedores: Se puede hacer ejecución utilizando comandos dentro de un contenedor como Docker, Kubernets o Kubelet. También se pueden distribuir estos contenedores dentro del sistema comprometido.

- Comandos en aplicaciones: Las aplicaciones comprometidas pueden permitir la ejecución de código del sistema para ganar acceso o robar información.

- Comunicación entre procesos: Pueden utilizar los protocolos de comunicación entre dos dispositivos (IPC) para inyectar comandos o alterar procesos que se encuentran en ejecución (COM).

- API Nativas: Se puede interactuar con las API nativas para obtener el control sobre el Kernel del sistema operativo. Estas API son llamadas durante el Boot del sistema.

- Tareas programadas: El adversario programa tareas programadas en el sistema operativo que les permitirá la ejecución de comandos a través del Shell.

- Módulos compartidos: Se puede ejecutar Payload usando librerías del sistema o de aplicaciones (DLL) para crear procesos específicos que permitirán el acceso al sistema.

- Herramientas de distribución de *Software*: Se puede tener acceso a la aplicación a través de terceros que se encargan de la distribución de *software* en los cuales pueden incorporar Malware a los equipos.

- Servicios del Sistema: Los servicios o Daemon pueden ser comprometidos y ejecutar códigos maliciosos para crear más servicios como puertas traseras.

- Compromiso del usuario: El usuario puede ejecutar código malicioso a través de un enlace o al abrir documentos o ejecutables comprometidos.

9.5.5 Persistencia

El adversario mantiene su acceso a los sistemas cambiando contraseñas, creando servicios y otras herramientas que le permitan mantenerse conectado.

- Manipulación de cuentas de usuario: Consiste en modificar los permisos en grupos o contraseñas para mantener el acceso y así saltar las políticas de seguridad. Estas aplican para cuentas de dominio, nube, correo electrónico como en llaves de protocolo SSH.

- Boot o Login inicial: Se programa tareas que cada vez que se inicie la sesión o se inicie el sistema puedan ejecutar códigos que permitan el acceso del adversario. Estos programaciones se pueden hacer en el Windows Registry, Carpeta Startup, paquetes de autenticación (LSA), Proveedores de Tiempo, módulos del Kernel y extensiones, controladores, modificaciones en atajos de aplicaciones, monitoreo de puertos, Procesos de impresión, entre otros.

- Extensiones del navegador: Se modifican las extensiones del navegador o plug-ins para crear puertos y mantener el acceso.

- Creación de cuentas: Ya teniendo acceso al Directorio Activo, se crean cuentas especiales que mantengan el acceso con suficientes privilegios. Las cuentas pueden ser de Dominio o locales.

9.5.6 Escalamiento de privilegios

Cuando ya se está dentro del sistema, se debe ganar privilegios para tener mayor cobertura del ataque y a los recursos. Estos privilegios pueden ser como administrador local o del dominio.

- Mecanismos de escalamiento: Se utiliza las herramientas que traen los sistemas para permitir cambiar de rol y así elevar los niveles de autorización. En Unix se utilizan los comandos Setuid y Setgid para modificar los permisos del usuario sobre los objetos del sistema. SUDO es otro comando muy utilizado para obtener los privilegios de administración.

- Manipulación a los Token: Mediante robo de credenciales o Token se pueden tener acceso a diferentes niveles de acceso y que permitirán crear procesos para obtener más credenciales y seguir escalando.

- Boot o Logon inicial: Modificando estos registros para usuarios privilegiados se puede ejecutar procesos con el suficiente nivel de jerarquía para crear cuentas, modificar parámetros del sistema o ejecutar *Malware* que mantengan el acceso.

- Modificación de Políticas: En el dominio se modifican los parámetros para evadir las defensas o escalar privilegios. Esto se realiza en las políticas de grupo o modificando los dominios de confianza.

9.5.7 Evasión de la defensa

El adversario se esconde para no ser detectado mediante la deshabilitación o desinstalación de herramientas de seguridad u ofuscando sus códigos maliciosos.

- Mecanismos de escalamiento: Los sistemas limitan el acceso a cuentas privilegiadas y alertan sobre cambios en parámetros de seguridad.

- Modificación de Políticas: Cuando se presentan cambios en las políticas se alertan sobre todo cuando cambian los servicios de confianza.

- Explotación para la defensa: Las aplicaciones de seguridad también poseen vulnerabilidades que pueden ser aprovechadas por el atacante para ejecutar comandos que deshabiliten o no alerten sobre eventos.

- Ocultar artefactos: Se pueden ocultar archivos de sistema infectados o tareas programadas que no sean identificados por los programas de seguridad y que se activen una vez se requieran para continuar con el ataque.

- Afectación a la defensa: Se modifican los componentes del entorno de la víctima para deshabilitar los mecanismos de defensa. También bloquea el registro de eventos en los principales Logs del sistema o aplicaciones. Dentro de las herramientas afectadas están el Firewall, Antivirus, Antimalware y herramientas para nube.

9.5.8 Acceso a las credenciales

En esta etapa el adversario intenta robar cuentas y contraseñas claves de los sistemas para tener accesos validos con el fin de no ser detectado ya que pasa por comportamiento real.

- Fuerza bruta: Para obtener las contraseñas o los hash de las mismas, el adversario utiliza técnicas como la de adivinar la contraseña con las palabras comunes, romper la contraseña utilizando una lista de palabras claves y sus combinaciones.

- Contraseñas almacenadas: Se buscan contraseñas almacenadas en archivos de usuario y del sistema, Scripts o tareas programadas o en los códigos de programa.

- Credenciales Web: El acceso se puede tomar a través de las cookies que o Tokens de sesiones SAML en las cuales roban la sesión.

- *Keylogging*: Se instala aplicaciones que capturan las pulsaciones del teclado en un archivo de texto que es enviado al adversario para analizar e identificar usuarios y contraseñas.

- *Man-in-the-Middle*: Interceptan las comunicaciones entre dos sistemas utilizando técnicas como el *sniffing* y luego ganan acceso al sistema víctima con el fin de ejecutar comandos o modificar parámetros.

9.5.9 Descubrimiento

Obtener conocimiento sobre la infraestructura y Red interna y decidir cómo atacar los sistemas.

- Descubrimiento de cuentas: Obtener la lista de cuentas sobre el sistema o del entorno como Dominio, local, correos electrónicos, nube, entre otras.
- Aplicaciones: Se obtiene la lista de las aplicaciones instaladas y en ejecución que corren sobre el sistema ya sea Windows o Unix.
- Infraestructura Nube: Identificar la infraestructura disponible (IaaS) donde se listen las virtualizaciones, servicios disponibles (SaaS), direcciones IP públicas, contenedores, entre otros.
- Navegador: Listar las marcaciones como favoritos dentro del navegador ya que indica cuales son los sitios Web principales que utiliza la víctima y que puede ser aprovechado.
- Directorios y Archivos: Enumerar los archivos claves del usuario como los directorios de más uso y determinar el comportamiento de la víctima. Revisar también la papelera. Esto ayuda para saber si se compromete todo el sistema o solo un parte de este.
- Escaneo Servicios de Red: Identificar los servicios que están disponibles en todos los equipos de la red y determinar cuáles son los más vulnerables.

9.5.10 Movimiento Lateral

Consiste en comprometer más sistemas de información y equipos que están a la mano del objetivo ya alcanzado.

- Explotación de Servicios Remotos: Obtener acceso a través de la explotación de vulnerabilidades de los servicios expuestos en la Red interna, así se comprometen más sistemas.
- *Phishing* interno: Se envía *Phishing* desde el correo interno comprometido por lo que gana mayor credibilidad y se obtiene más información de las cuentas de la compañía.
- Transferencias de herramientas: Se puede transferir las herramientas utilizadas para comprometer el sistema y usarlas para el compromiso de otros sistemas. Esta transferencia se puede hacer a través de protocolos FTP, RDP, entre otros.
- Herramientas de distribución de *Software*: Se puede distribuir los códigos o *Malware* a través de la distribución de *software* en los cuales se llegan a más equipos de la Red.

9.5.11 Recolección

Cuando se tienen identificadas las fuentes de información, el siguiente paso es el robo o exfiltración de esta data. En la información objetivo se encuentra archivos de vídeo o audio, bases de datos de clientes como información estratégica.

- Archivos: Se comprime y agrupa la data que se desea extraer de los sistemas. También permite ocultar para que las aplicaciones de seguridad no puedan detectarla.
- Captura de audio y video: El adversario puede aprovechar los periféricos de los sistemas de cómputo para grabar conversaciones, tomar capturas de pantalla y fotos del entorno.
- Información almacenada en Nube: Los usuarios utilizan estos servicios para almacenar archivos y datos importantes como Dropbox, Onedrive, entre otros, los cuales pueden ser accedidos y poder descargar en cualquier equipo conectado a la red.
- Recursos compartidos: Buscar los recursos compartidos en red y descargar los archivos almacenados en estos repositorios.
- Correo electrónico: Revisar los adjuntos que contengan información clave y que sirva para continuar el ataque. También se programa los reenvíos a cuentas de correo externas sin que el usuario se dé cuenta.

9.5.12 Comando y Control

Después de tener comprometido el sistema, el adversario puede tener acceso remoto a la consola de comandos y de ahí tener el control de todos los recursos y sin ser detectado por los elementos de seguridad.

- Capa de Aplicación: La comunicación entre el servidor y el sistema comprometido se realiza a través de este protocolo para evitar ser detectado por los mecanismos de seguridad. Tanto los comandos como los resultados son embebidos en este protocolo. Los protocolos utilizados son Web, FTP, Correo, DNS, entre otros.
- Codificación: Para evitar ser detectado el tráfico entre los dos sistemas (servidor y sistema comprometido) es codificado o cifrado. Los protocolos utilizados van desde estándares conocidos como propietarios.
- Ofuscación: Utiliza esta técnica de camuflaje para utilizar las comunicaciones de aplicaciones comunes para enviar los comandos y recibir respuesta sin que sean detectados. Los procesos utilizados son colocar la data en los espacios no utilizados por el protocolo, Esteganografía y mezclas entre protocolos.
- Canal cifrado: Se crea una VPN entre los dos sistemas (servidor y sistema comprometido) utilizando los protocolos de cifrado comunes.
- Proxy: El adversario puede utilizar un proxy para evitar conectar directamente su infraestructura con el sistema comprometido. Se puede utilizar herramientas como HTRAN, ZXProxy, and ZXPortMap. Estos proxies pueden ser internos, externos, multi-hop.
- *Software* de Acceso Remoto: También se utiliza aplicaciones comerciales para el acceso remoto como Team Viewer, LogMein, VNC, entre otros.

9.5.13 Exfiltración

Uno de los objetivos del adversario es el robo de información por lo que aplicará todas las técnicas para recolectar, empaquetar y extraer los datos relevantes de la víctima.

- Automatización: Creación de procesos para que recolecten, compacten y envíen los archivos requeridos. Un aspecto importante es el tamaño de los paquetes que son enviados para evitar que el monitoreo de trafico de red pueda ser detectado.

- Protocolos seguros: Otra forma de transferir la información es a través de una VPN donde se cifra los datos de punta a punta. Los adversarios envía la información a servidores diferentes a los utilizados para el comando y control.

- Redes diferentes: También la información extraída puede ser enviada por infraestructuras diferentes, es decir, si el comando y control se realiza por cableado, la exfiltración se hace por WiFi, Modem o Celular.

- Medios extraíbles: Cuando se tiene acceso físico a las instalaciones o equipos otra forma es a través de memorias USB, discos duros extraíbles, celulares y otros medios extraíbles.

- Servicios Web: Se utilizan sitios populares de servicios Web de almacenamiento para almacenar la información que es extraída. Una forma de automatizar el proceso es sincronizar un directorio con el de nube.

9.5.14 Impacto

El adversario no solo intentará extraer información clave sino que impactará los sistemas en su disponibilidad e integridad.

- Bloquear acceso a los usuarios: Se eliminara, cambiara contraseña o cualquier otro parámetro que afecta la disponibilidad de los usuarios. También se puede afectar todo el dominio para que el impacto sea mayor.

- Destrucción de la data: Eliminar la información o cifrarla (Ransomware) para que los usuarios no tengan acceso. Estos procesos utilizan técnicas antiforenses con el fin de que no se pueda recuperar.

- Manipulación: Otro aspecto es modificar la información para beneficio de terceros y que afectan los objetivos de la víctima. Las modificaciones se realizan sobre la información almacenada como en la que es transmitida. También pueden modificar la información que es presentada en informes o cuadros de control para sabotear las decisiones que se toman basadas en ellas.

- *Defacement*: Esta técnica cambia algunos valores de la información con el fin de crear pánico al interior de la organización de la víctima.

- Borrado de disco: Se utilizan técnicas de sobreescritura en el disco para evitar que la información eliminada sea recuperada.

- Ataque de negación de servicio: Se puede realizar un ataque DDOS a un sistema o servicios internos para afectar la disponibilidad de los recursos.

- Daños del Firmware: Se sobrescribe o daña la memoria flash que contiene el sistema BIOS afectando la disponibilidad del *hardware*. También se pueden afectar la tarjeta madre, discos duros y tarjetas de vídeo.

- Afectar el sistema de Recuperación: Los sistemas de cómputo tienen un espacio donde almacenan el *Software* de recuperación del sistema operativo en caso de fallo critico el cual puede ser modificado o alterado para que no se tenga forma de recuperación rápida.

9.6 Guía de pruebas a los controles para Trabajo Remoto

Los esquemas de trabajo remoto habilitan a los empleados, contratistas, proveedores y otros usuarios para realizar trabajo desde su casa, apartamento, lugar de residencia o cualquier otra locación externa a las facilidades de la empresa. En marzo del año 2020 Colombia confirmó su primer caso de COVID-19 en el territorio nacional, a partir de ese momento y como parte de las medidas tomadas por el gobierno se propició una nueva dinámica laboral que ha llevado a las empresas a movilizar a sus empleados hacia esquema de trabajo en casa y trabajo remoto. Estas medidas no han sido ajenas para los Bancos, para quienes el número de empleados trabajando desde casa ha aumentado de manera importante, permitiéndoles acceder a los recursos, sistemas empresariales e información de todo tipo desde diferentes dispositivos y locaciones, siendo ahora la forma más común para trabajar dentro del marco de resiliencia organizacional por muchas compañías para dar continuidad a su negocio dentro de la situación global de emergencia sanitaria.

Para habilitar estos esquemas de trabajo, las organizaciones se han basado en tecnologías de conexión remota existentes como la virtualización, la conexión mediante redes privadas (VPN) o la habilitación de protocolos de escritorios remotos, si bien suplen las necesidades de conexión, también traen consigo riesgos que representan una creciente preocupación sobre las áreas de control y seguridad en las organizaciones. Cuando un dispositivo utiliza su acceso remoto, se convierte en una extensión lógica de la red de la entidad. En ese sentido si no existe un adecuado aseguramiento de estos dispositivos se generan riesgos adicionales, no solo sobre la información a la que el trabajador remoto tenga acceso, sino también a los sistemas y redes de la organización.

Ante este nuevo contexto de operación, desde el grupo de trabajo de Ciberseguridad de las entidades agremiadas a Asobancaria se genera esta guía de pruebas a los controles para Trabajo Remoto, que compila recomendaciones de aspectos de control basados en buenas prácticas y estudios recientes que podrán ser considerados por las áreas de auditoría con el objetivo de brindar aseguramiento sobre estos nuevos y crecientes esquemas de trabajo.

GUÍA DE PRUEBAS A LOS CONTROLES PARA TRABAJO REMOTO

Componente	Riesgo(s) asociado	Objetivo de control	Alto nivel enfoque de pruebas sugerido
Políticas y procedimientos	Perdida de la confidencialidad, integridad y disponibilidad de la información por accesos remotos no autorizados o configurados inapropiadamente.	Se han establecido formalmente políticas y procedimientos de conexión remota y aseguramiento de dispositivos que son difundidos y aplicados de manera consistente por los empleados, contratistas, proveedores y otros usuarios que realicen trabajo remoto.	Para empleados, contratistas, proveedores y otros usuarios que realizan trabajo remoto, verificar que: • Se cuenta con políticas y procedimientos formalizados, aprobados y difundidos en cuanto al trabajo remoto que formalicen la posición de la organización, responsabilidades y gestión de los riesgos asociados con este tipo de conexiones, proceso de autorización y aprovisionamiento de las conexiones, actividades de control/monitoreo de la operación (incluyendo controles mínimos a asegurar para provisionar este tipo de conexiones), entre otros. • La entidad cuenta con procedimientos documentados y difundidos a los diferentes actores en cuando a la identificación, reporte y gestión de los incidentes de seguridad. Los usuarios finales deben tener claridad de los canales y procedimientos a seguir para reportar cualquier actividad sospechosa o incidente materializado asociado con seguridad de la información/ciberseguridad. • Se han realizado diferentes actividades de concientización en cuanto a la responsabilidad en el aseguramiento de sus redes caseras, equipos conectados a la red, manejo de la información, controles de seguridad física en su lugar de trabajo, copias de respaldo, manejo de tokens, gestión de contraseñas, acciones a tomar frente a los ataques cibernéticos. Sobre estos aspectos se deben liberan guías específicas a los funcionarios que les permitan tener lineamientos mínimos a seguir para el aseguramiento de sus redes caseras y trabajo en casa, así como establecer mecanismos de verificación que permitan certificar la aplicación de las guías por parte de los usuarios finales.

Componente	Riesgo(s) asociado	Objetivo de control	Alto nivel enfoque de pruebas sugerido
Control de acceso en conexiones remotas.	Perdida de la confidencialidad, integridad y disponibilidad de la información por accesos remotos no autorizados o configurados inapropiadamente.	Se han establecido controles para gestionar la solicitud, creación, suspensión oportuna, modificación de cuentas de usuario y cuentas privilegiadas en las conexiones remotas.	Identifique y evalúe los procedimientos de control de acceso para conexiones remotas y las consideraciones que deban aplicarse a todos los usuarios, incluidos los administradores (usuarios privilegiados), los usuarios internos y externos (Incluyendo terceras partes) considerando los controles asociados con: • Mecanismos de autenticación y acceso mediante agentes VPN y de conexión remota, uso de doble factor de autenticación, aprovisionamiento de Tokens (lógicos o físicos). • Proceso de autenticación mediante LDAP, Directorio Activo, uso de certificados digitales, entre otros mecanismos. • Aseguramiento de usuarios privilegiados, custodia de contraseñas. • Parámetros robustos de seguridad en contraseñas, incluyendo parámetros de bloqueo por intentos fallidos de conexión, desbloqueo del acceso por administrador, cambio periódico de la contraseña. • Parámetros especiales de aseguramiento y custodia de contraseñas para los administradores de las VPNs y otros sistemas de administración de accesos remotos (pej: Virtualización, escritorios remotos) Procedimientos de acceso mediante VPN • Se cuenta con procedimientos o controles para la solicitud, aprobación, monitoreo y eliminación del acceso mediante VPN a los empleados basado en roles, acceso a sistemas críticos de información y/o privilegios y se han considerado los respectivos flujos de aprobación para tal acceso. • Se cuenta con procedimientos formales para la revisión periódica de los permisos de acceso a través de VPN dentro del cual se incluyan las actividades para validar la necesidad de contar con el acceso y la remoción de este en los casos donde sea no sea necesario contar más con los permisos. • El proceso de aprovisionamiento de conexiones remotas debe incluir la evaluación de riesgos asociada con la identificación de accesos a información sensible y la definición de controles adicionales alineados con los niveles de clasificación de la información y de los datos a los que el funcionario tenga acceso.

Componente	Riesgo(s) asociado	Objetivo de control	Alto nivel enfoque de pruebas sugerido
Aseguramiento de dispositivos.	Materialización de ataques cibernéticos o explotación de vulnerabilidades sobre la red de la entidad debido a clientes inseguros accediendo a través de conexiones remotas.	Se implementan mecanismos para asegurar que los dispositivos que se utilizan para realizar conexiones remotas se encuentra debidamente asegurados en alineación con los estándares y políticas de la Entidad.	La entidad ha puesto en operación controles para asegurar que los dispositivos que se utilizan para realizar accesos remotos (por ejemplo, computadores de escritorio, celulares, portátiles, tabletas, etc.) cuentan con características mínimas de seguridad alineadas con los estándares corporativos y que dicha seguridad se mantiene en el tiempo de manera sostenible. Ejemplo de estas condiciones mínimas de seguridad son: - Instalación de agente antivirus y su actualización. - Uso de clave y contraseña - Cifrado de disco duro. - Instalación de actualizaciones de parches. - Aplicación de controles de navegación, bloqueo de puertos USB, lectores de memoria SD, y otro tipo de restricciones. - Aplicación de configuraciones seguras de red. - Restricciones en la instalación de software. - Restricciones en el uso de equipos móviles desbloqueados o "rooteados" para funciones corporativas. - En dispositivos móviles: Solicitud de PIN o inicio de sesión seguro en dispositivos móviles, uso de partición aislada, protegida y encriptada para gestionar información de la organización, capacidades de borrado remoto, entre otros.
Gestión de conexiones remotas.	Perdida de la confidencialidad, integridad y disponibilidad de la información por accesos remotos no autorizados o configurados inapropiadamente.	Se han implementado controles de monitoreo sobre conexiones remotas.	• Se cuenta con controles para asegurar que la configuración de herramientas de acceso remoto se realiza únicamente en equipos autorizados y que cumplan con las condiciones de seguridad establecidas por la Entidad. • Se han establecido controles de tipo "sanboxing" para las conexiones que no sean autorizadas o que no sea posible determinar su identidad. • Existen lineamientos establecidos para el borrado de conexiones previas, contraseñas, historiales de conexión, borrado de memoria caches, cookies en los equipos clientes de las conexiones remotas. • Se han implementado controles de configuración para cerrar la sesión remota por inactividad o evitar múltiples conexiones activas. • Los logs de eventos que se generan de la solución VPN son almacenados y analizados a través de herramientas de monitoreo de seguridad para la detección de actividades anómalas.

Componente	Riesgo(s) asociado	Objetivo de control	Alto nivel enfoque de pruebas sugerido
Arquitectura de conexiones remotas.	Fallas en la disponibilidad de los servicios o errores de procesamiento de las aplicaciones por incompatibilidades en la arquitectura de conexiones remotas.	Se han realizado análisis de riesgos para determinar la arquitectura apropiada para conexiones remotas. Se monitorea la capacidad de estas conexiones para garantizar la disponibilidad.	El diseño de la arquitectura de la implementación de conexiones remotas incluye como mínimo las siguientes consideraciones: • Selección del hardware, ubicación de los dispositivos, consideraciones de firewall y enrutamiento, selección de software del cliente, alta disponibilidad de la conexión, consola de administración, soporte y mantenimiento por parte del proveedor, proceso de licenciamiento, compatibilidad con los sistemas operativos con los que cuenta la organización. • La arquitectura empleada cubre las necesidades de la organización de acuerdo con la demanda del servicio, el número de empleados conectados, la dimensión o crecimiento de acuerdo con la situación de pandemia. • Se ha realizado un análisis de riesgos formal sobre las tipologías de conexión implementadas, considerando aspectos como: Ubicación de los dispositivos, filtrado de tráfico, ubicación del firewall, fuga de información, gestión de accesos privilegiados, implementación de controles de monitoreo. • La arquitectura de conexiones remotas se revisa periódicamente para garantizar que la solución esté actualizada y aborde los problemas de riesgo y vulnerabilidad identificados en las evaluaciones de riesgo. Los procesos se encuentran documentados y formalizados y se realizan actualizaciones periódicas.
Administración de la solución de conexión remota.	Fallas en los algoritmos de cifrado y protocolos de conexión segura podrían permitir a los atacantes descifrar el tráfico o la información sensible mediante métodos de interceptación.	Se han implementado protocolos adecuados de conexión.	Para las conexiones remotas se ha considerado conexiones seguras a los sistemas y servicios de la entidad, teniendo en cuenta como mínimo: • Selección e implementación de protocolos de conexión seguros considerando el tipo de arquitectura definida. Para los protocolos seleccionados se han considerado posibles debilidades de seguridad y el despliegue de controles mitigantes. • Controles de restricción de tráfico mediante VPN- Gateways: Se han considerado controles adicionales al cifrado del tráfico, controles para el enrutamiento a los servicios y a la información dependiendo el perfil y las necesidades de acceso del empleado. Para este caso considerar los controles a nivel de VPN Gateway usados luego de la autenticación del empleado en la VPN.

Componente	Riesgo(s) asociado	Objetivo de control	Alto nivel enfoque de pruebas sugerido
Acceso a los servicios mediante la VPN y mecanismos de virtualización/ acceso remoto	Infección de los sistemas internos o fuga de información crítica (PII, PCI, Estratégica) expuesta en las redes públicas..	Se cuenta con un análisis sobre los riesgos y controles de exponer información y servicios críticos de la organización mediante acceso remoto	Revisar si se ha realizado un análisis de cómo se debe acceder a cada recurso tecnológico disponible a través de conexión remota. Para el caso de VPN identificar si se han listado los recursos o servicios qué deban estar disponibles, los requisitos generales y específicos de las aplicaciones, servidores, bases de datos, versiones, sistemas operativos a los que se desea acceder, teniendo presente aspectos como compatibilidad, el rendimiento del servicio, aplicaciones legadas y si la conexión es escalable o soporta la demanda de la operación. Verificar si la Entidad ha realizado un análisis de los accesos asignados a los funcionarios que se encuentran en trabajo remoto, con el fin de asegurar que los permisos que se tenían asignados durante el esquema de trabajo en sitio se encuentran alineados con los permisos que se asignan para el trabajo remoto. De igual manera identifique el mecanismo de acceso a los servicios que se habilita en la VPN, considere que por lo menos se hayan implementado restricciones en las extensiones de la red (No todos los usuarios acceden a todos los servicios), se tienen puertos asegurados para las conexiones exclusivas de la VPN (ciertos puertos TCP o UDP en lugar de todos los puertos en una vez)

Esta guía de controles parte de la definición de políticas y procedimientos para la capacitación a los usuarios, así como la gestión de la arquitectura y seguridad de las conexiones remotas. Este apartado, no pretende hacer una revisión exhaustiva de todos los controles existentes para asegurar los nuevos esquemas de trabajo remoto. Sin embargo, se comparte con el objetivo de que pueda proveer a las entidades una base de controles que pueda ser utilizada para guiar los procesos de planeación y ejecución de auditorías asociadas con estos nuevos esquemas de trabajo.

9.7 Aseguramiento técnico de conexiones remotas

Las recomendaciones para realizar una auditoría de VPN de Acceso Remoto, es decir, una VPN que necesite de conexión remota a un equipo de cómputo que esté dentro de la organización son las siguientes:

9.7.1 Intercepción de datos

Lo primero que tenemos que realizar es la conexión de un Sniffer en la red hogar del funcionario, existen dos tipos, uno de *software* y otro a nivel físico. Para este punto utilizaremos uno físico llamado Plunder Bug.

Gráfico 9 **Conexiones para la captura de datos**

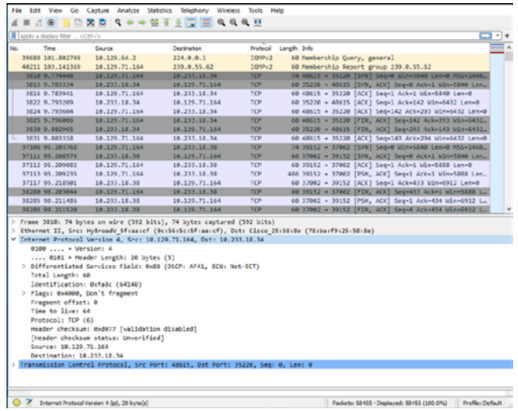
Fuente: *Hak5*

Fuente: *elaboración propia*

De esta manera podemos capturar los datos entre la red del funcionario y el destino de la conexión VPN. Garantizando el enmascaramiento de datos sensible del cliente.

Después de realizar la captura de los paquetes que viajan dentro de la red, es necesario verificar que estos estén ofuscados una de muchas herramientas que se puede realizar esta comprobación es llamada *Wireshark*, una herramienta multiplataforma utilizada para realizar análisis sobre paquetes de red

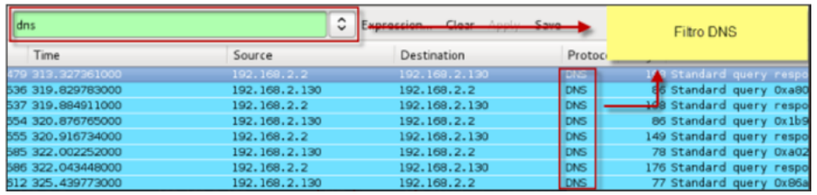
Gráfico 10 Wireshark análisis de paquetes



Fuente: *Captura software Wireshark*

Tenemos que revisar todos los paquetes que fueron capturados, analizarlos mediante filtros y poder determinar si los datos están ofuscados. Ejemplo de alguno de los filtros que podemos realizar:

Gráfico 11 Wireshark análisis de paquetes

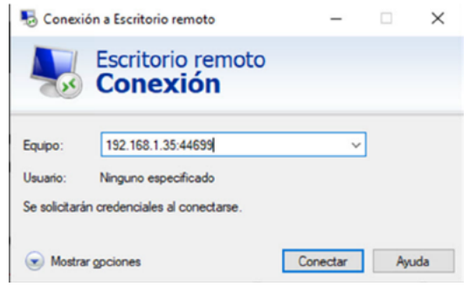


Fuente: *Gráfico tomado de We live security*[21]

9.7.2 Análisis de puertos RDP

Una de las condiciones principales para realizar una conexión VPN de acceso remoto es que los equipos cuenten con el escritorio remoto habilitado para conexión, para esto es necesario que esté habilitado el puerto RDP 3389:

Gráfico 12 Demostración conexión remota Windows



Fuente: *Captura conexión escritorio remoto*

[21] We Live Security (2013). "Uso de filtros wireshark para detectar actividad maliciosa". Recuperado de: https://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/

Para auditar este puerto lo podemos realizar de la siguiente manera, con ayuda de la herramienta NMAP: “Nmap -p 3389 --script RDP-enum ---Dirección Ip----“

- -P: especificar el puerto
- --script Nmap
- --dirección IP destino

Gráfico 13 **NMAP RDP**

```
C:\Users\hang5jebat>nmap -p 3389 --script rdp-enum-encryption [redacted]

Starting Nmap 6.25 ( http://nmap.org ) at 2013-08-06 23:49 Malay Peninsula Stand
ard Time
Nmap scan report for [redacted] ([redacted])
Host is up (0.35s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP: SUCCESS
|     Native RDP: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
|     128-bit RC4: SUCCESS
|_    FIPS 140-1: SUCCESS

Nmap done: 1 IP address (1 host up) scanned in 10.26 seconds
```

Fuente: *NMAP.org*[22]

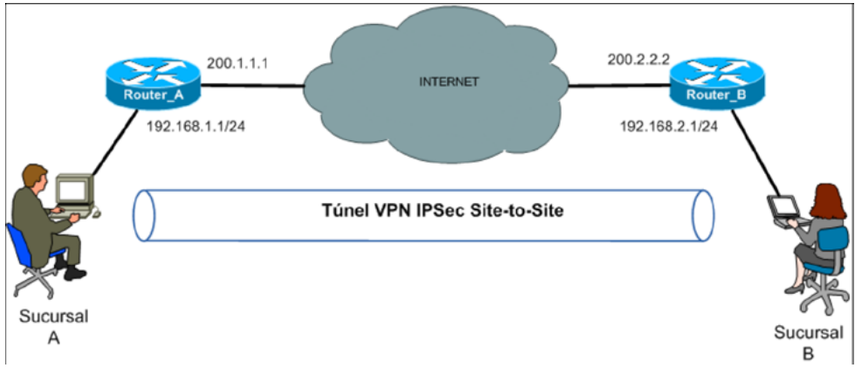
Según el resultado obtenido podemos identificar si existen vulnerabilidades asociadas a este puerto, poder realizar las actualizaciones y el *hardening* necesario para mitigar estas posibles vulnerabilidades.

[22] NMAP.org. “¿Qué es lo que tu sistema operativo le permite hacer a otros?”. Recuperado de: https://nmap.org/nsedoc/scripts/rdp-ntlm-info.htmlsa/

9.7.3 VPN Punto a Punto

Una VPN punto a punto (en inglés, Point-to-Point Tunneling Protocol). Es una VPN que crea un túnel y captura los datos, estas son empleadas por usuarios remotos para conectarse a la red LAN mediante su VPN.

Gráfico 14 **VPN punto a punto**



Fuente: *Elaboración propia*

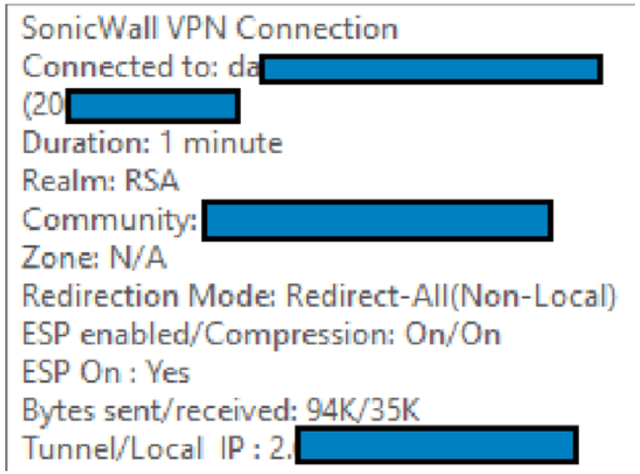
Las recomendaciones para realizar una auditoría a este tipo de VPN son los siguientes:

- Datos de conexión VPN

Lo primero que tenemos que realizar es la identificación de información tal como la dirección IP destino de nuestra VPN información proporcionada por los administradores. Después de encontrar esta información podemos auditar las IP correspondientes con ayuda del *software* NMAP.

Otra manera en que podemos encontrar esta información es realizando una conexión VPN, y luego dentro de la aplicación observar a donde se está conectando, cómo se puede ver en la siguiente imagen:

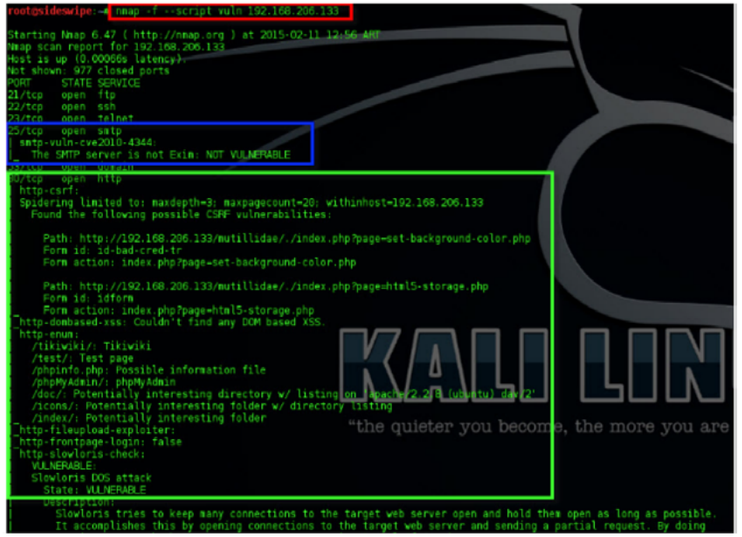
Gráfico 15 **SONICWALL ejemplo conexión**



Fuente: *Conexión propia*

Con scripts de NMAP se pueden determinar si se encuentra algún tipo de vulnerabilidad reconocida. NMAP incorpora sistemas de scripts conocido como NSE (NMAP Scripting Engine) que permite a los usuarios extender las capacidades de NMAP usando los diversos scripts, como se puede ver en el próximo ejemplo:

Gráfico 16 **Ejemplo vulnerabilidades con NMAP**



Fuente: *NMAP.org*[23]

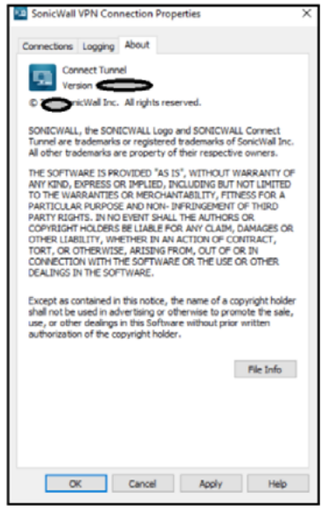
De esta manera podemos determinar si el servicio que se encuentra alojado es posiblemente vulnerable.

- Verificación versiones de VPN

Se realiza la verificación de las versiones instaladas de las VPNs, con el objetivo de búsqueda de vulnerabilidades. Para identificar el tipo de versión de la VPN, la mayoría de los *software* contienen esta información en las características.

[23] NMAP.org. "¿Qué es lo que tu sistema operativo le permite hacer a otros?". Recuperado de https://nmap.org/nsedoc/scripts/rdp-ntlm-info.html

Gráfico 17 Ejemplo versionamiento VPN



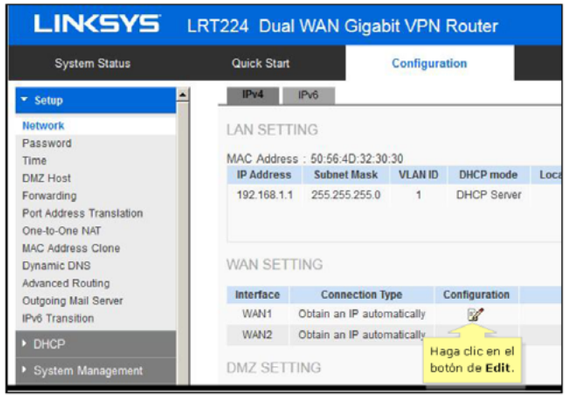
Fuente: *Software /www.sonicwall.com*

Las actualizaciones son modificaciones realizadas sobre las aplicaciones, cuyo objetivo es mejorar tanto aspectos de funcionalidad como de seguridad. Por eso es la importancia de la revisión de estas versiones.

- Vulnerabilidades sobre router público

Al momento de realizar configuraciones de VPNs una mala configuración los routers de la organización, dejando la dirección IP pública del mismo con acceso permitido para cualquier individuo.

Gráfico 18 Ejemplo VPN en router

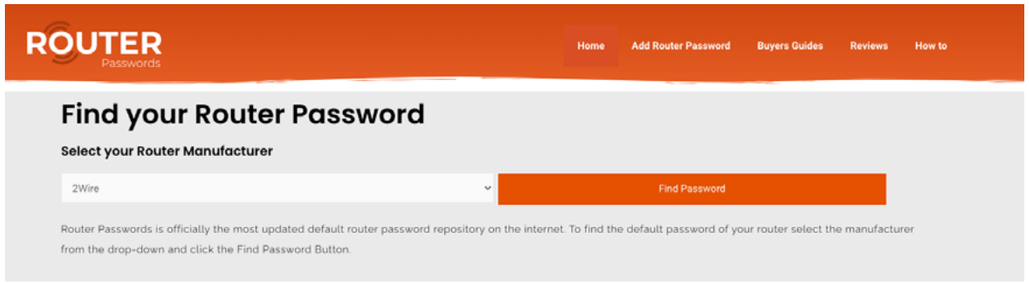


Fuente: *SLinksys*[24]

Al momento de auditar este tipo de routers es indispensable realizar la verificación de las contraseñas por defecto. Para poder comprobar esta configuración nos ayudamos de la aplicación web Router Password, la cual contiene todas las contraseñas por defecto de los fabricantes:

[24] NMAP.org. "¿Qué es lo que tu sistema operativo le permite hacer a otros?". Recuperado de https://nmap.org/nsedoc/scripts/rdp-ntlm-info.html

Gráfico 19 **Contraseñas router por defecto**



Fuente: *Router Passwords*[25]

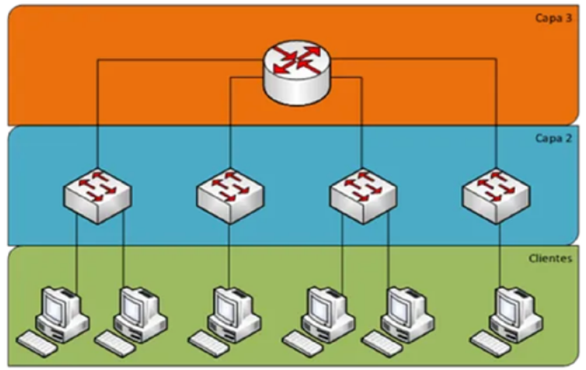
Si esto llegase a materializarse un ciberdelincuente tiene acceso a toda la administración del router incluso configuraciones VPN, y datos de nuestros usuarios finales.

[25] NMAP.org. "¿Qué es lo que tu sistema operativo le permite hacer a otros?". Recuperado de https://nmap.org/nsedoc/scripts/rdp-ntlm-info.html

9.7.4 Segmentación de Redes

Una estrategia de *hardening* sobre sistemas de redes informáticas es dividir o segmentar los clientes de la red. Esto se considera una forma eficaz a la hora de contener amenazas:

Gráfico 20 **Ejemplo segmentación redes**



Fuente: *https://www.gb-advisors.com/*

Buenas prácticas para la segmentación de redes:

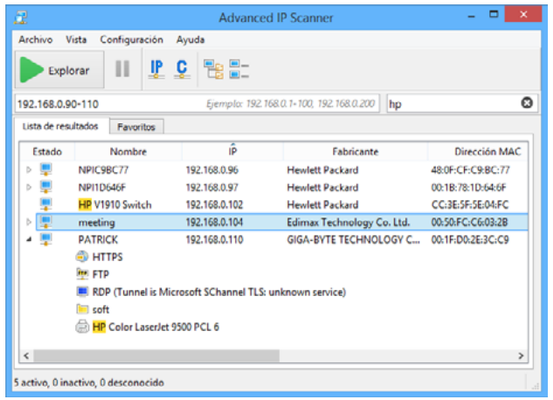
- Utilizar infraestructuras PKI, WPA2/infraestructura Enterprise y RADIUS/TACACS (parámetros de seguridad en redes inalámbricas al momento de realizar segmentaciones) Esto proporciona un depósito centralizado de usuarios o dispositivos autorizados para acceder a la red al utilizar certificados para autenticar el servidor y el dispositivo.

- Crear y configurar segmentos VLAN: Una VLAN permitirá agrupar dispositivos.

- Procurar que cada segmento tenga su propia configuración de direccionamiento IP, así como su modo de enrutamiento, control de acceso e interfaces (grupos Wifi SSID, Ethernet y VLAN(Tipos de segmentación de redes)).

Para realizar la identificación de dispositivos conectados a la misma red, se puede realizar reconocimiento sobre dispositivos en la misma red con ayuda del aplicativo IP SCANNER.

Gráfico 21 **Demostración escaneo red interna**



Fuente: *Advance IP Scanner*[26]

De esta manera se puede realizar la identificación de los equipos que estén conectados dentro de la red, y comprobar si en verdad existe una segmentación de redes. Esta garantiza la protección absoluta ante alguna propagación de algún *malware*.

Para equipos Linux que quisiéramos auditar para confirmar la segmentación de redes lo podemos realizar con este script realizado en BASH:

Gráfico 22 **Escaneo red interna**

```
for i in $(seq 2 254); do
timeout 1 bash -c "ping -c 1 192.168.1.$i > /dev/null 2>&1" && echo
"host 192.168.1.$i - active" &
done; wait
```

Fuente: *Elaboración propia.*

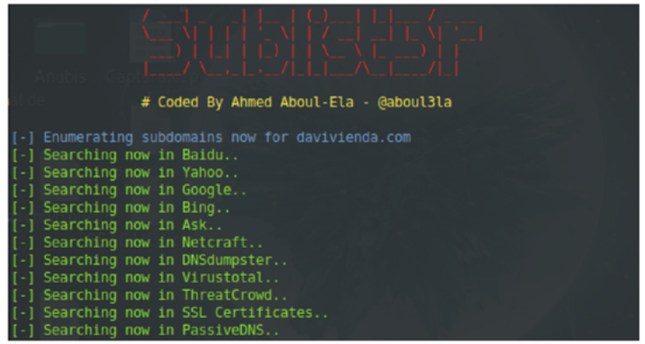
[26] Página oficial: https://www.advanced-ip-scanner.com/es/

9.7.5 Servicios y puertos expuestos

Uno de los procedimientos utilizados en la búsqueda de posibles vulnerabilidades que puedan ser aprovechadas por los ciberdelincuentes, es la enumeración de subdominios.

La herramienta utilizada para esta actividad es Sublist3r, es una herramienta en desarrollo en código Python para encontrar subdominios de un sitio web utilizando OSINT.

Gráfico 23 **Escaneo subdominios**



Fuente: *Elaboración propia.*

Esta herramienta utiliza motores de búsqueda como Google, Bing, Yahoo, Baidu y Ask. También utiliza Netcraft, Virustotal, ThreatCrowd, DNSdumpster y ReverseDNS

Algunos ejemplos son:

-D –Dominio: Para enumerar los subdominios del nombre de dominio.

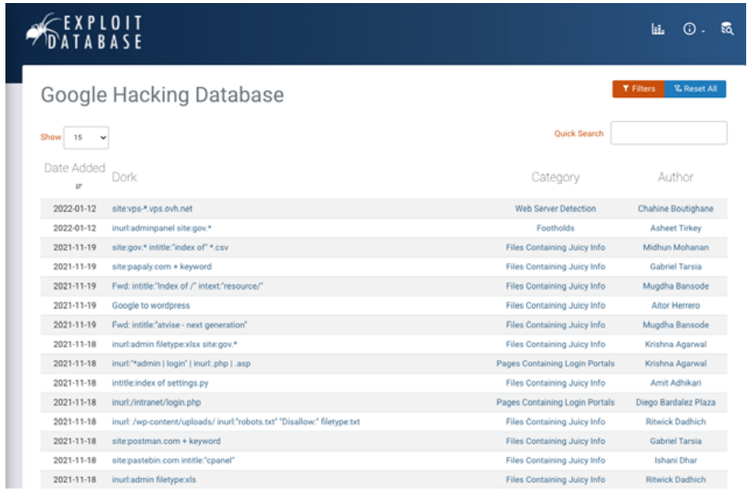
-p –Puertos: Escanea los subdominios y los puertos.

9.7.6 Explotación Vulnerabilidades

Después de realizar la identificación de las posibles brechas conocidas, continuamos con la fase de explotación o reconocimiento de exploits (*software* para la explotación de una vulnerabilidad) para aprovecharse de esta vulnerabilidad. Para ello, utiliza una serie de scripts Lua que están ubicados en una ruta de nuestra máquina y que se pueden invocar con –script o su equivalente – donde se determina si existen vulnerabilidades sobre los puertos abiertos e identificados en la fase de reconocimiento.

Por otra parte, se realiza la identificación de vulnerabilidades con aplicaciones de uso libre como:

Gráfico 24 **Repositorio explotación de vulnerabilidades**



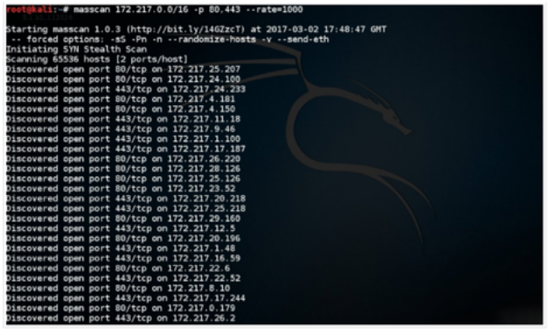
Fuente: *https://www.exploit-db.com/google-hacking-database*

Google Hacking se define como las técnicas o parámetros con comandos de Google para conseguir búsquedas avanzadas o precisas. En el mundo de la seguridad informática es utilizada para temas de OSINT (búsqueda de información en fuentes públicas) o *ethical hacking*, así como para conseguir información de un objetivo (empresas, personas, datos personales, cuentas de correo, etc.).

Análisis Direcciones IP Públicas

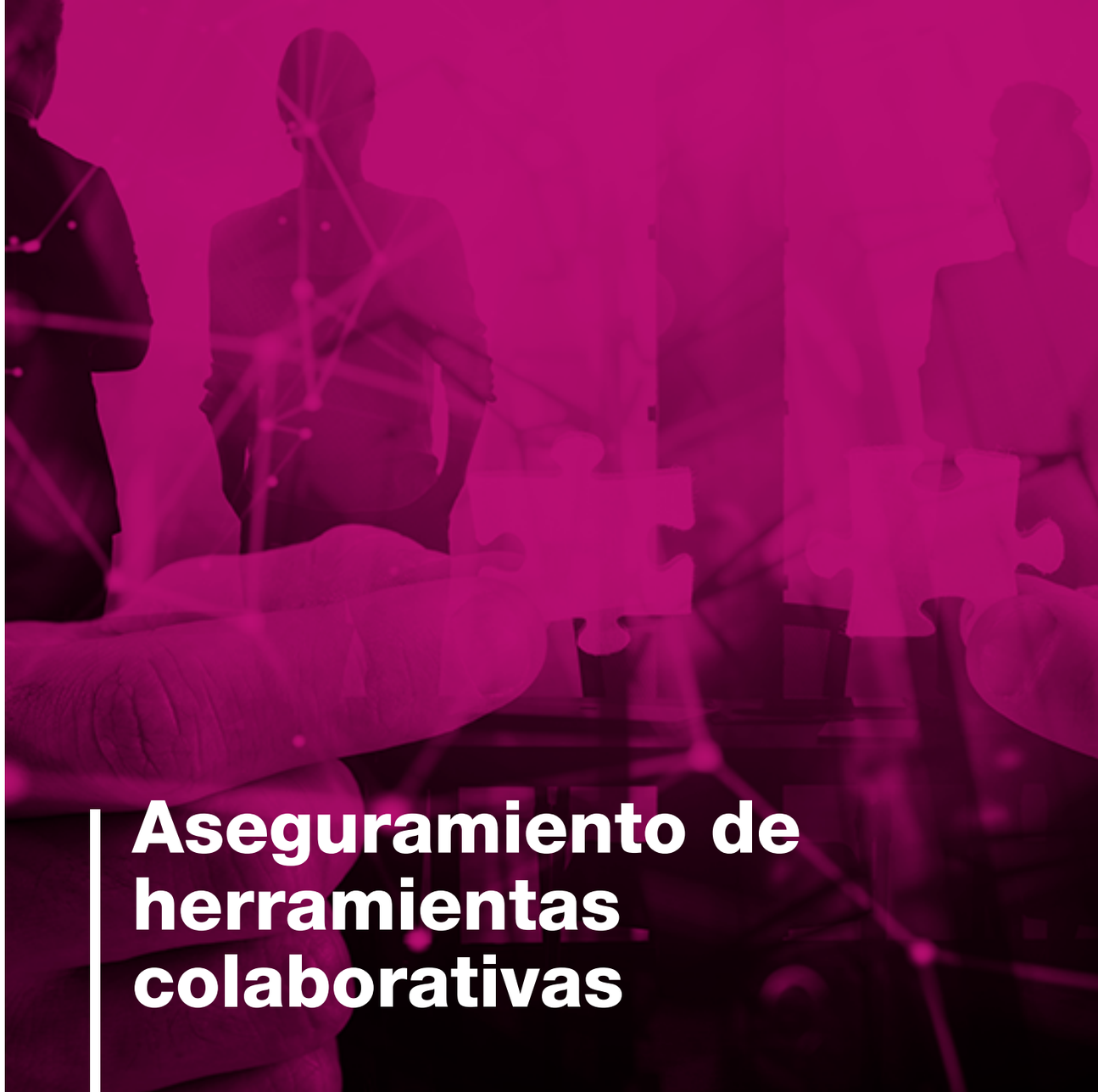
Otra prueba que se realiza es el escaneo de direcciones IP públicas del banco es con la herramienta Masscan, utiliza escaneo asíncrono similar a NMAP. Esta herramienta utiliza puertos personalizados o IP para escanear el objetivo. Masscan es la herramienta más rápida para buscar puertos abiertos. Para demostrar, hemos probado en Kali Linux 2018.4 en VMware.

Gráfico 25 **Demostración MASSCAN**



Fuente: *Elaboración propia.*

Donde visualizamos ingresos, firewall detección de IDS e IPS para comprobar niveles de controles de ciberseguridad. Esta detección de Intrusos (IDS) como los Sistemas de Prevención de Intrusos (IPS) nos asegura que tenemos estos dispositivos para detectar patrones inusuales en la red.



Aseguramiento de herramientas colaborativas

Introducción

A raíz de la pandemia, las empresas adoptaron la modalidad de trabajo en casa o remoto con el fin de salvaguardar la salud de sus empleados; sin embargo, esto ha traído grandes retos en temas de seguridad de la información y ciberseguridad, ya que los niveles de aseguramiento y el ambiente de control para proteger la información que estaban implementados en las organizaciones, no necesariamente son establecidos y/o replicados en ambientes remotos desde donde accede actualmente el empleado.

El teletrabajo ha requerido de una mayor interconectividad y comunicación de los empleados que se encuentran ubicados en diferentes lugares y/o ciudades, por lo que las herramientas o tecnologías colaborativas como las plataformas de comunicación, herramientas de almacenamiento y gestión de correo, cumplen un papel primordial para habilitar el trabajo remoto pero así mismo, representan amenazas y riesgos sobre el aseguramiento adecuado de la información que es almacenada y/o procesada en este tipo de aplicaciones. El uso de estas herramientas no sólo permite el acceso a la información y recursos provistos por las entidades, también permite que se pueda acceder desde cualquier dispositivo corporativo o personal, éstos sin mayores requerimientos de aseguramiento previo.

Las tecnologías colaborativas mantienen en contacto al equipo de trabajo cuando desempeña tareas fuera de la organización: paquetes ofimáticos, videoconferencias, pizarras virtuales, intercambio de documentos y ficheros, chats, etc. Al utilizar estas herramientas se debe proporcionar la seguridad necesaria a la información que se intercambia y por ello establecer una serie de pautas básicas de seguridad.

Por lo anterior, generamos esta guía de trabajo para que las entidades financieras conozcan los riesgos y amenazas del uso de este tipo de herramientas colaborativas y puedan implementar las medidas necesarias para garantizar la protección de la información que se está almacenando y/o procesando a través de estas.

Algunas de las medidas más importantes que se abordarán en esta guía están relacionadas con responder los interrogantes ¿cómo podemos proteger la información fuera de nuestro perímetro? ¿cómo tenemos visibilidad de lo que ocurre en la nube de las herramientas? y ¿cómo aplicamos los mismos controles de seguridad que podemos generar en nuestro entorno e infraestructura en un ambiente empresarial en la nube?

Como parte de esta guía se abordarán los riesgos y controles más relevantes relacionados con el uso de herramientas colaborativas, incluyendo entre otros: (i) controles para prevenir la fuga de información, prevención de *malware* y difusión de *phishing*, (ii) controles para proteger la privacidad de la información, cifrado de la información, copias de seguridad y redundancia, (iii) administración de instalación en dispositivos móviles personales y corporativos, (iv) controles de aseguramiento de las contraseñas, controles de actualización de versiones, (v) controles de restricción de acceso desde cuentas de correo personales y (vi) controles de verificación de vulnerabilidades.

Ecosistema de herramientas colaborativas en el alcance de esta guía:

A continuación, se describen algunas de las herramientas colaborativas que se encuentran en el mercado:

- Microsoft Office 365: es una suite basada en la nube que incluye varios productos de Microsoft (Word, Excel, PowerPoint, Publisher, Access, OneNote, Outlook, Project, Visio, Microsoft Teams) y que está dirigida tanto para consumidores como para el entorno empresarial.

- Microsoft Azure: Azure es una nube pública de pago por uso que permite compilar, implementar y administrar rápidamente aplicaciones en una red global de datacenters de Microsoft.

- Google suite y Google Cloud Platform: Es una plataforma que ofrece más de 90 servicios de tecnología de la información (también llamados productos), que las empresas, los profesionales de TI y los desarrolladores pueden aprovechar para trabajar de forma más eficiente, ganar más flexibilidad y/o permitirles una ventaja estratégica. La suite cuenta con herramientas como correo electrónico (Gmail), herramienta de mensajería (Google Meet), herramienta de almacenamientos (Google Drive) entre otras.

- Zoom: Es una plataforma libre de vídeo, voz, uso compartido de contenidos y chat se puede ejecutar en todos los dispositivos móviles y de escritorio. Zoom es escalable, basada en la nube, y permite el intercambio de archivos, mensajería instantánea y mensajes grupales. Los archivos e información que se comparte son recuperables ya que se almacena en la biblioteca consultable de contenido sincronizado de Zoom.

- Blue Jeans: Herramienta libre que proporciona servicios de videoconferencia interoperables basados en la nube pública. Blue Jeans ofrece una solución de videoconferencia para reuniones de negocios con soporte para compartir contenido, grabar reuniones, chat por texto y múltiples participantes. Puede conectarse desde cualquier dispositivo, tanto iOS como Android, así como desde múltiples plataformas (Google Hangouts, Avaya, Microsoft Lync).

- Slack: Es una plataforma de mensajería basada en canales, es utilizada por un gran volumen de compañías para conectarse. Los equipos de Slack trabajan juntos en canales que se pueden organizar por proyecto, departamento o ubicación de la oficina, facilitando a los usuarios seguir los temas que son asignados, slack se conecta a las herramientas y servicios que las empresas ya usan y centraliza las notificaciones, archivos y datos de cientos de aplicaciones diferentes incluyendo el servicio de correo electrónico. Todo lo que se comparte en Slack se indexa y archiva automáticamente para que las empresas puedan crear una base de conocimiento completa sin esfuerzo.

a. Riesgos emergentes de las herramientas colaborativas y la seguridad de la información

Herramientas colaborativas de comunicación y su uso aumentado durante la Pandemia

Dado que los equipos siguen teletrabajando durante la pandemia COVID-19 utilizando herramientas de comunicación y mensajería instantánea, las entidades ahora enfrentan un riesgo emergente relacionado con la seguridad de la información que se da en comunicaciones internas de los empleados que realizan sesiones de trabajo o reuniones desde sus entornos remotos de trabajo. La empresa y sus departamentos de seguridad deben cuestionar los riesgos de seguridad y responder ¿Cuál es la manera más segura para celebrar reuniones internas e intercambiar información sensible? ¿Cuál de estas maneras presenta las características adecuadas para la preservación de la privacidad de la información de los empleados y la seguridad del contenido publicado/compartido en estas herramientas?

De igual manera, se debe cuestionar si estas herramientas guardan historiales de las conversaciones y/o archivos que han sido compartidos, así como los procesos de borrado seguro de dicha información.

Métodos de cifrados de las herramientas de comunicación, ¿Quién accede a las comunicaciones?

Debido a la sensibilidad y confidencialidad de la información que se comparte en las herramientas colaborativas, un aspecto muy relevante a considerar es el tipo de cifrado que está siendo empleado por la plataforma tecnológica, por ejemplo, si se usa un cifrado *end to end* en donde el mensaje se cifra desde el dispositivo saliente y se descifra en el dispositivo receptor o si por el contrario se emplea un cifrado *To server*, en dónde el mensaje no se cifra durante todo el recorrido, se cifra antes de salir de un dispositivo, pasa por el servidor de la herramienta que se está utilizando (por ejemplo: Google Meet o Microsoft Teams) lo descifra para procesarlo y lo vuelve a cifrar antes de enviarlo a los destinatario(s). Esto significa que alguien que tenga acceso a los servidores podría interceptar las comunicaciones y la información sensible de los mensajes.

Aseguramiento de la información almacenada en Cloud y el modelo de responsabilidad compartida

Los proveedores de servicios en la nube en donde se procesa información sensible (por ejemplo: almacenamiento y correo) están a cargo de la seguridad de la capa física, infraestructura, red, operación y a nivel del sistema y aplicación real en el centro de datos. El cliente, sin embargo, es responsable de las actividades que sus usuarios realizan, los datos almacenados y procesados en la aplicación, y cualquier amenaza que tenga como objetivo los usuarios y la organización a través de la plataforma.

10.1 Aspectos generales

10.1.1 Clases de Herramientas

- **De comunicación:** Se usan en gran mayoría para poder hacer reuniones junto a un cliente o un compañero de la empresa, que están en espacios físicos distintos. Además, se tiene la disponibilidad de hablar con varias personas a la vez, y enviar archivos.

- **De gestión de proyectos:** Son aplicaciones que llevan el seguimiento online de los proyectos en marcha, por ello puedes coordinarte con las empresas que están implicadas en él y saber en qué punto está. Además, permite gestionar la carga de trabajo de cada miembro del equipo.

- **De creación:** Cuando la elaboración de una tarea es cosa de varias personas. Por ello, existen las herramientas colaborativas de creación, y que posibilitan el trabajo online simultáneo desde distintos espacios físicos. Teniendo coordinación y gran eficacia.

10.1.2 Seguridad

Las herramientas colaborativas son una plataforma fundamental en el trabajo de las empresas dado que la globalización obliga a trabajar a distancia, así como la actual situación sociosanitaria. Entre estas herramientas las más empleadas son las aplicaciones para hacer videollamadas, reuniones virtuales. Y es aquí donde cobra toda la relevancia garantizar la seguridad en la configuración de estas herramientas de forma que no se conviertan en un vector de ataque de ciberdelincuentes.

- Descargar únicamente aplicaciones de los markets oficiales o de la web del proveedor.

- Mantener actualizadas las aplicaciones de videollamadas.

- Programar las videollamadas con el número exacto de participantes. Cuando todos los usuarios entren a la sesión, cerrar el acceso a nuevos participantes.

- Todos los usuarios que accedan a la reunión deberán hacerlo con contraseña. En aplicaciones públicas, registrarse con contraseñas que no se utilicen en otros servicios y no compartir públicamente el ID de la reunión.

- El moderador de la videollamada gestiona si esta puede ser grabada. Si está siendo grabada, debe mostrarse a todos los usuarios un indicador visual y sonoro. Además de contar con la autorización de quienes participan para ser grabados.

- Todos los usuarios deben de entrar con un nombre/nick reconocible para el administrador/moderador de la llamada en las conferencias privadas.

- Considerar las videollamadas un canal de comunicación inseguro, no dar datos sensibles como contraseñas

- El moderador de la reunión debe poder gestionar la conexión de los participantes, cerrar micrófonos, deshabilitar contenidos o señal de vídeo. Los participantes no deberían acceder hasta que no se conecte el moderador.

- *Software* de Acceso Remoto: También se utiliza aplicaciones comerciales para el acceso remoto como Team Viewer, LogMein, VNC, entre otros.

10.1.3 Uso

Las herramientas de colaboración se configuran como servicios informáticos que permiten a los usuarios comunicarse y trabajar conjuntamente sin importar que estén reunidos o no en un mismo lugar físico. Se puede compartir información, construir de manera colaborativa y producir conjuntamente nuevos materiales resultado de una edición de archivos en equipo.

El concepto de herramientas de colaboración involucra gran cantidad de aplicaciones y servicios que se ajustan a las necesidades específicas de trabajo:

i. Gestión de Comunidades: permiten crear esquemas para visualizar ideas y flujos en un proceso de cocreación (Mindmeister, Symbaloo).

ii. Entornos de trabajo: aplicaciones para crear equipos sincronizar archivos en la nube, generar documentos y editarlos en cualquier lugar y en tiempo real (Office 365, Gobby).

iii. Comunicaciones: permiten emplear foros, mensajería instantánea, redes sociales privadas (Slack, Yammer).

iv. Telepresencia: permiten montar presentaciones online y organizar reuniones virtuales (Teamviewer, Mikogo).

v. Gestión de Tareas: permiten la coordinación de un equipo que trabaja en un proyecto, facilitando la coordinación de fechas de entrega, personal y construcción del producto final (Base Camp, Dotproyect).

10.2 Auditorías específicas

10.2.1 G-Suite

Actualmente las empresas están migrando a los servicios en nube incluidos las herramientas ofimáticas. Teniendo este nuevo escenario los auditores deben garantizar que el proceso de cambio organizacional al igual que el ambiente de control satisfagan las nuevas necesidades.

Desde el frente de auditoría se realiza el monitoreo a nivel de datos en la G-Suite, con el fin de verificar las medidas de prevención de fuga de información sensible de la entidad contenida en mensajes de Gmail; archivos de Drive; grabaciones de Google Meet, entre otros.

La auditoría debe desarrollar evaluaciones de manera independiente acerca de los riesgos, revisando los controles de TI implementados para la Suite de Google, haciendo énfasis en aspectos como:

- Definición e implementación del Gobierno, políticas, normas, procedimientos y estándares de seguridad.
- Gestión de la configuración y operación de los componentes.
- Gestión y operación de otras herramientas de seguridad implementadas para mantener la seguridad de la información en el uso de la Suite de Google.
- Controles de acceso (autenticación y autorización).
- Controles de TI y de seguridad implementados para la conexión y uso de dispositivos móviles a la Suite de Google.
- Proceso de monitoreo para que sea validada la información, reportes o procesos que se realizan producto del manejo de la herramienta vault.

Actualmente a través de la herramienta “Vault” de Google y por la consola de administración, se efectúan validaciones de información para cada una de las investigaciones y casos a la medida resultantes de diferentes incidentes o fraudes internos/externos. Esta herramienta de control de información y descubrimiento electrónico se utiliza para conservar, retener, buscar y exportar los datos de los usuarios de Google Workspace.

El alcance de revisión de la Suite de Google se encuentra compuesta, principalmente, por las siguientes aplicaciones:

- Consola de Administración
- Gmail: Plataforma de correo
- Docs: Procesador de texto
- Sheets: Hojas de cálculo
- Slides: Presentaciones
- Forms: Permite crear nuevos formularios para capturar información
- Chat: Chat corporativo
- Meet: Herramienta de videoconferencias
- Drive: Espacio de almacenamiento de información en la nube de Google
- Calendar: Agendamiento de reuniones
- Keep: Esquema de Notas
- Sites: Permite crear sitios web internos y externos
- Jamboard: Tablero interactivo y colaborativo
- DataStudio: Para realizar Tableros de Control

10.2.1.1 Gobierno

La herramienta de Google Workspace (G-Suite) se crea con la intención de migrar las aplicaciones instaladas ofimáticas a aplicaciones de la nube por lo cual se debe establecer el marco del proyecto para lograr una migración exitosa. Dentro de los aspectos a tener en cuenta en la revisión están los relacionados con el cambio de cultura, ya que la implementación lleva a cabo el romper paradigmas que se tenían con las herramientas instaladas y que es fundamental en la adopción de la nueva tecnología.

En el marco del proyecto también se debe establecer cómo será la migración y desmonte de las aplicaciones instaladas a las de nube. Fechas finales y migración de la data.

Como estos proyectos son estructurales deben venir de una aprobación de Junta o Comité Ejecutivo donde se pueden extraer los lineamientos de la alta dirección para ser validados durante o posterior al proyecto.

10.2.1.2 Normas, Políticas y Procedimient

Google Workspace (G-Suite) cuenta con estándares y mejores prácticas para la configuración de herramientas de seguridad complementarias que permiten salvaguardar la información y los accesos.

Todas las excepciones a los estándares de aseguramiento deben ser remitidas al Departamento de Seguridad de la Información de la entidad con el fin de evaluar los riesgos y controles compensatorios.

El acceso a las herramientas colaborativas de la entidad se encuentra sujeto a las directrices definidas en la Política de Seguridad de la Información de la organización, así como el uso del correo electrónico, las comunicaciones y los dispositivos móviles deben encontrarse contemplados en dicha Política.

Las herramientas de la entidad deben ser de uso laboral y apoyan los procesos para comunicarse, aprender y trabajar colaborativamente. La información de la entidad es de carácter confidencial por lo tanto no debe ser compartida con personas o grupos no autorizados.

Cuando se requiera compartir un documento por medio de un enlace y dependiendo de la confidencialidad del documento debe marcarse la opción que se ajuste a la necesidad teniendo en cuenta los siguientes criterios:

- Cualquier usuario de la Entidad con el enlace puede ver.
- Cualquier usuario de la Entidad con el enlace puede publicar comentarios.
- Cualquier usuario de la Entidad con el enlace puede editar.

° Si el documento es de alta confidencialidad, se recomienda compartirlo directamente con las personas requeridas y no haciendo uso de los links.

° Se recomienda que el cargue de archivos en los formularios se restringe para cuentas de Google no asociadas a los dominios autorizados por la organización (White List).

° Solamente las personas autorizadas de unidades organizativas específicas podrán hacer el uso de la consola de administración de la G-Suite así como de Vault, de acuerdo a la política.

° Debe establecerse un proceso de monitoreo para que sea validada la información, reportes o procesos que se realizan producto del manejo de la herramienta Vault.

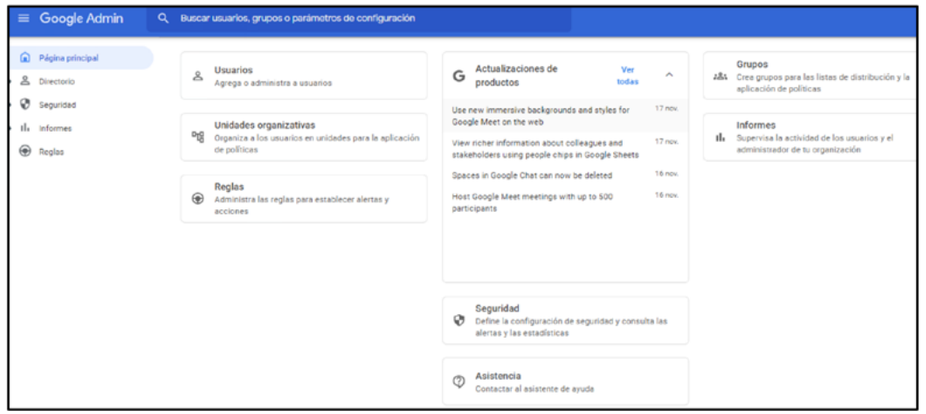
10.2.1.3 Administración y Configuración

- **Consola de administración de Google (Google Admin):**

Google Admin es la consola de administración de G-Suite con la cual se puede añadir usuarios, administrar dispositivos, configurar la seguridad, entre otros ajustes para que los datos siempre estén seguros.

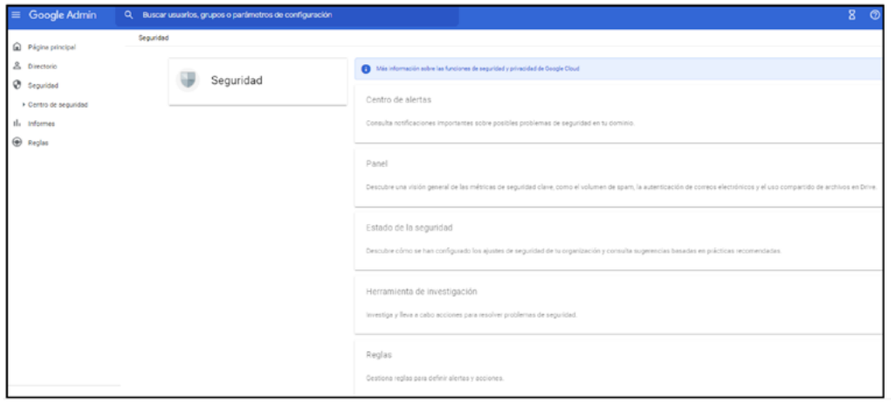
A través de la administración centralizada se realizará la configuración y gestión de los usuarios de forma rápida y sencilla, configurar grupos, obtener analíticas de seguridad, sugerencias de prácticas recomendadas por centro de seguridad y añadir opciones de seguridad como por ejemplo, la verificación en dos pasos (2FA) o el inicio de sesión único.

Gráfico 26 **Google Admin**



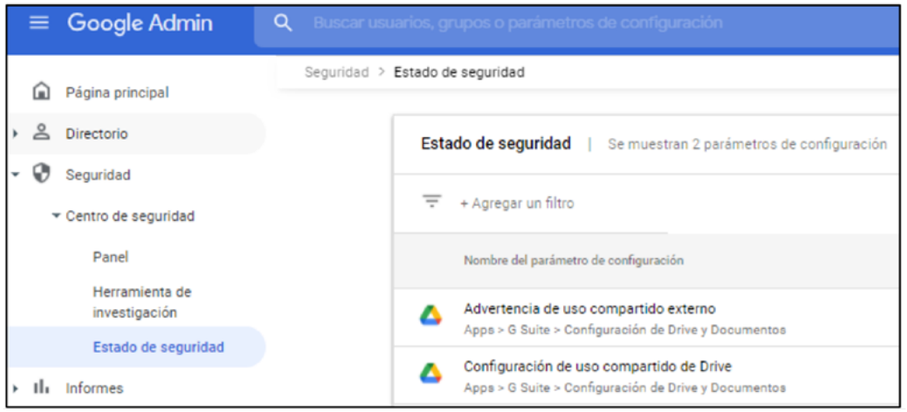
Dentro de la consola existe un módulo de seguridad en el cual se deben definir las alertas y reglas con las cuales se realizará el monitoreo de las acciones que se ejecuten sobre las distintas aplicaciones de la G-Suite (Correo, Drive, chat, entre otros). Adicionalmente, se tendrá una visión de las métricas de seguridad clave, el volumen de *spam*, la autenticación de correos electrónicos y el uso compartido de archivos en drive, así mismo el estado de seguridad de la organización a nivel del Workspace.

Gráfico 27 **Módulo de seguridad**



En el apartado de **Estado de Seguridad**, se debe validar que parámetros de configuración se tienen definidos para la toma de decisiones.

Gráfico 28 **Estado de seguridad**



10.2.1.4 Seguridad de la plataforma

10.2.1.4.1 Roles y Permisos

La plataforma posee un nivel de seguridad alto respaldado por Google, esta plataforma verifica las credenciales del usuario logueado y si pertenece a una organización en específico también se posee una implementación de roles y permisos que permite crear, visualizar y eliminar recursos dependiendo del rol del usuario, estos roles son:

- **Propietario:** Es el rol más importante de toda la jerarquía de usuarios que pueden hacer uso de las herramientas de la G-Suite de Google, es aquél que crea un documento o un proyecto nuevo en alguna de las aplicaciones de la plataforma.

  Este rol además es capaz de otorgar permisos a los usuarios de editor, lector, usuario con permiso para comentar y/o transferir la propiedad del documento a otra persona llegado el caso.

- **Editor:** Este rol permite hacer uso de todas las herramientas disponibles en la aplicación de la GSuite a la cual fue compartido el documento o aplicativo excepto eliminar o transferir propiedad del archivo ya que no pertenece a su cuenta asociada. Adicionalmente, es capaz de compartir el documento a otros usuarios.

- **Lector:** Permite visualizar los diferentes recursos compartidos a los cuales se tiene acceso.

- **Comentador:** Posee los mismos permisos que el lector, a excepción de que este puede realizar comentarios en los diferentes recursos a los cuales tiene acceso.

10.2.1.4.2 Controles para Google Meet

Google Meet es la plataforma con la que millones de usuarios pueden interactuar a través de internet y cada vez son más las personas que utilizan este servicio, por ello google constantemente trabaja para hacer que las videollamadas colaborativas sean cada vez más seguras, una de estas medidas de seguridad se trata de otorgarle al anfitrión de la videollamada el control sobre quienes pueden solicitar acceso a la misma. Las últimas actualizaciones de seguridad implementadas para aquellas personas que no se encuentran invitados de manera directa a una videollamada mediante la invitación de calendario son:

- Cuando un participante es expulsado de una videollamada no podrá volver a ingresar a menos de que sea invitado de nuevo por el anfitrión.

- Cuando se le niega el acceso a un usuario que repetidamente solicita acceso a una videollamada, este será bloqueado automáticamente de la reunión y no podrá volver a solicitar acceso a la misma.

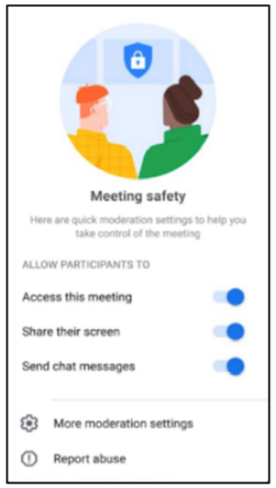
- El anfitrión de la reunión podrá configurar la seguridad de acceso de las videollamadas, por ejemplo, podrá restringir si un usuario solo tiene acceso mediante calendario o solo desde un dispositivo móvil.

- Se pueden bloquear usuarios anónimos (aquellos que no se encuentran con una cuenta de Google iniciada).

- Se puede controlar que participantes pueden hacer uso del chat o presentar en una reunión.

Estas opciones de protección se complementan con las funciones agregadas para prevenir ataques de fuerza bruta, si un atacante posee el link de ingreso e intenta acceder a una reunión, no podrá ingresar a la misma, si por algún error son aceptados se podrán expulsar o bloquear.

Gráfico 29 **Actualizaciones de seguridad para Google Meet**



10.2.1.4.3 Control de seguridad para Google Chat

La reciente actualización de Google Chat introduce nuevas configuraciones de control que mantienen las conversaciones más seguras para todos los usuarios, A continuación se detallan las actualizaciones de seguridad brindadas por google para su herramienta de mensaje directo, Google Chat.

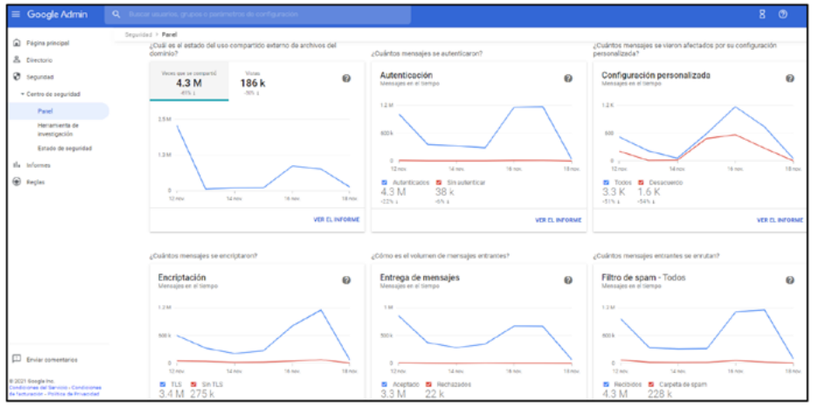
- La primera actualización de seguridad viene de la mano de Gmail al introducir un sistema de protección *anti-phishing* verificando en tiempo real la información suministrada de datos externos y de paso se marca como maliciosas las conversaciones que arrojen indicios de *spam*.
- Ahora es posible marcar y reportar las salas de conversación que se sospechen *spam* o peligrosas.
- De igual manera las invitaciones a salas de chat o conversaciones personales de origen desconocido se pueden bloquear y marcar como *spam* para que no genere molestia en los usuarios de Google Chat.

10.2.1.5 Monitoreo y Registro

- **Consola de administración de Google (Google Admin):**

Dentro de la opción de **Panel** del módulo de Seguridad se debe monitorear el comportamiento de las actividades sobre las distintas aplicaciones de la G-Suite. A través de las siguientes métricas las cuales son exportables se obtendrá un informe el cual debe ser analizado para tomar las decisiones y acciones correspondientes frente a situaciones inusuales identificadas.

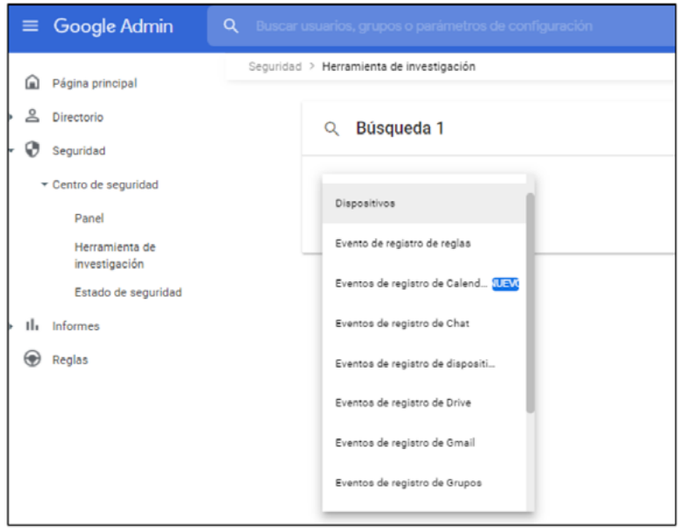
Gráfico 30 **Opción "Panel" del módulo de Seguridad**



En la opción de **Herramientas de investigación**, se debe identificar y clasificar problemas de seguridad y privacidad del dominio, así como tomar medidas al respecto. Dentro de esta herramienta se pueden llevar tareas a cabo como:

- Acceder a datos sobre dispositivos.
- Consultar datos de registro de dispositivos para ver de manera clara los dispositivos y las aplicaciones con los que se ha accedido a los datos.
- Ver datos sobre mensajes de Gmail, incluido el contenido de correos electrónicos.
- Consultar datos del registro de Gmail para detectar y borrar correos electrónicos maliciosos o marcar mensajes como *spam* o *phishing*, así como enviar correos a las bandejas de entrada de los usuarios.
- Ver qué usuarios están suspendidos consultando los resultados de búsqueda.
- Ver datos del registro de Google Drive para investigar el uso compartido, la creación y la eliminación de archivos en la organización y saber qué usuarios han accedido a documentos, entre otros datos.

Gráfico 31 Opción “Herramientas de Investigación” del módulo de Seguridad

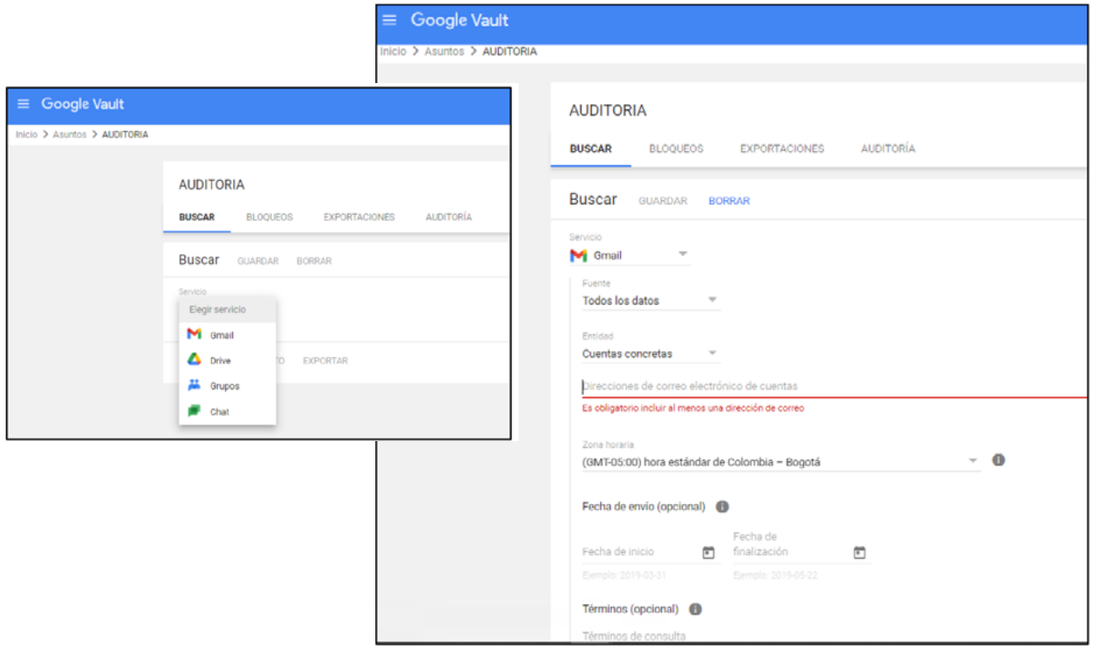


- **Google Vault:**

Vault es una herramienta de control de información y descubrimiento electrónico incluida en Google Workspace, con la cual se debe hacer el monitoreo a la gestión de datos como los siguientes:

- Mensajes de Gmail
- Archivos de Drive
- Mensajes de Google Chat (si el historial está activado)
- Grabaciones de Google Meet, así como registros de chat, preguntas y respuestas, y encuestas que tengan asociados
- Mensajes de Grupos de Google
- Mensajes de texto, mensajes de voz y sus transcripciones, y registros de llamadas de Google Voice para Google Workspace
- Nueva versión de Google Sites
- Mensajes de la versión clásica de Hangouts (si el historial está activado)

Gráfico 32 Google Vault



A nivel de control de acceso y auditoría, se debe controlar quién puede acceder a Vault y qué acciones tiene disponibles. De esta forma, se asegura que sólo los usuarios autorizados tengan acceso a los datos de la organización. Es necesario solo activar Vault para determinadas unidades organizativas y asignarles una función de administrador con privilegios de Vault.

Adicionalmente, monitorizar los logs de auditoría donde vault proporciona un registro completo de las actividades de usuario cuando se crea o edita una regla de conservación, se realiza una búsqueda o se exportan datos. Cabe resaltar que no se puede editar el registro de auditoría.

10.2.2 Office 365

10.2.2.1 Control de acceso

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

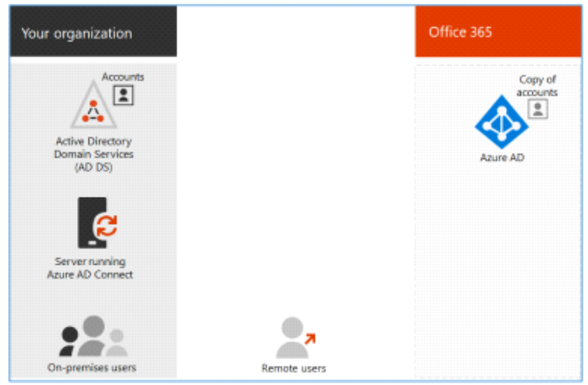
	Identidad solo de nube	Identidad híbrida
Definición	La cuenta de usuario solo existe en el tenant de Azure Active Directory (Azure AD) para su suscripción a Microsoft 365.	La cuenta de usuario existe en AD DS y una copia también se encuentra en el tenant de Azure AD para su suscripción a Microsoft 365. La cuenta de usuario en Azure AD también puede incluir una versión *hash* de la contraseña de la cuenta de usuario.
Cómo autentica Microsoft 365 las credenciales de usuario	El tenant de Azure AD para su suscripción a Microsoft 365 realiza la autenticación con la cuenta de identidad de nube.	El tenant de Azure AD para su suscripción de Microsoft 365 administra el proceso de autenticación o redirige al usuario a otro proveedor de identidades.
Ideal para	Organizaciones que no tienen ni necesitan un AD DS local.	Organizaciones que usan AD DS u otro proveedor de identidades.
Mayor Beneficio	Fácil de usar. No se necesitan servidores o herramientas de directorio adicionales.	Los usuarios pueden usar las mismas credenciales al obtener acceso a los recursos locales o basados en la nube.

(Centro Criptológico Nacional de España, 2019)

Modelo identidad híbrido

- La identidad híbrida usa cuentas que se originan en un AD DS local y tienen una copia en el tenant de Azure AD de una suscripción a Microsoft 365. Sin embargo, la mayoría de los cambios solo fluyen en un sentido.
- Los cambios que realice en las cuentas de usuario de AD DS se sincronizan con su copia en Azure AD. Pero los cambios realizados en cuentas basadas en la nube en Azure AD, como nuevas cuentas de usuario, no se sincronizan con AD DS. Azure AD Connect proporciona la sincronización de cuentas en curso.
- Se ejecuta en un servidor local, comprueba los cambios en AD DS y reenvía dichos cambios a Azure AD. Azure AD Connect permite filtrar las cuentas que se van a sincronizar y si se debe sincronizar una versión hash de las contraseñas de usuario, conocidas como sincronización de hash de contraseña (PHS).
- Al implementar la identidad híbrida, su AD DS local es el origen de autoridad para la información de la cuenta. Esto significa que las tareas de administración se realizan principalmente en el entorno local, que luego se sincronizan con Azure AD.

Gráfico 33 Azure AD



Auditoría avanzada en Microsoft 365

La funcionalidad de auditoría unificada en Microsoft 365 proporciona a las organizaciones la visibilidad de muchos tipos de actividades auditadas a través de los distintos servicios de Microsoft 365.

La auditoría avanzada ayuda a las organizaciones a llevar a cabo investigaciones forenses y de cumplimiento mediante el aumento de la retención de registros de auditoría necesarios para llevar a cabo una investigación.

Esto se logra proporcionando acceso a eventos esenciales (mediante la búsqueda de registros de auditoría en el Centro de cumplimiento de Microsoft 365 y la API de actividad de administración de Office 365) que ayudan a determinar el área que ha sido comprometida y un acceso más rápido a la API de actividad de administración de Office 365.

Buscar el registro de auditoría en el centro de cumplimiento

¿Necesita averiguar si un usuario ha visto un documento determinado o si ha purgado un elemento de su buzón?

Si es así, puede usar el centro de cumplimiento de Microsoft 365 para buscar en el registro de auditoría unificado para ver la actividad de usuarios y administradores en su organización.

Categorías de alertas

Para ayudar con el seguimiento y la administración de las alertas generadas por una directiva, puede asignar una de las siguientes categorías a una directiva.

- Prevención de pérdida de datos
- Información de gobierno
- Flujo del correo
- Permisos
- Administración de amenazas
- Otros

Directivas de alerta en Microsoft 365

- Puede usar las herramientas de directiva de alertas y panel de alertas del portal de Centro de cumplimiento de Microsoft 365 o Microsoft 365 Defender para crear directivas de alerta y, a continuación, ver las alertas generadas cuando los usuarios realizan actividades que coinciden con las condiciones de una directiva de alerta.

- Hay varias directivas de alerta predeterminadas que le ayudan a supervisar actividades como asignar privilegios de administrador en Exchange Online, ataques de *malware*, campañas de suplantación de identidad (*phishing*) y niveles inusuales de eliminaciones de archivos y uso compartido externo.

- Las directivas de alerta le permiten clasificar las alertas que desencadena una directiva, aplicar la directiva a todos los usuarios de la organización, establecer un nivel de umbral para cuando se desencadena una alerta y decidir si se van a recibir notificaciones por correo electrónico cuando se desencadenan alertas.

- También hay una página De alertas en la que puede ver y filtrar alertas, establecer un estado de alerta para ayudarle a administrar alertas y, a continuación, descartar alertas después de haber resuelto o resuelto el incidente subyacente.

Esquema SharePoint uso compartido

Los eventos de uso compartido (sin incluir eventos relacionados con la directiva de uso compartido y los vínculos de uso compartido) son diferentes de los eventos relacionados con archivos y carpetas de una forma principal: un usuario realiza una acción que tiene un efecto en otro usuario. Por ejemplo, cuando un usuario A de un recurso proporciona al usuario B acceso a un archivo. En este ejemplo, el usuario A es el usuario que actúa y el usuario B es el usuario de destino. En el esquema SharePoint archivo, la acción del usuario que actúa solo afecta al propio archivo. Cuando el usuario A abre un archivo, la única información necesaria en el evento FileAccessed es el usuario que actúa. Para solucionar esta diferencia, hay un esquema independiente, denominado esquema de uso compartido SharePoint, que captura más información acerca de los eventos de uso compartido. Esto garantiza que los administradores tengan visibilidad sobre quién compartió un recurso y el usuario con el que se compartió el recurso.

El esquema de uso compartido proporciona dos campos adicionales en un registro de auditoría relacionado con eventos de uso compartido:

- **TargetUserOrGroupType:** Identifica si el usuario o grupo de destino es miembro, invitado, SharePointGroup, SecurityGroup o partner.

- **TargetUserOrGroupName:** Almacena el UPN o el nombre del usuario o grupo de destino con el que se compartió un recurso (usuario B en el ejemplo anterior).

Administración de privacidad de Microsoft

¿Qué es la administración de privacidad?

- Comprender los datos privados que controla su organización y mantenerlos de una manera que reduzca los riesgos para usted, sus clientes y sus socios son el centro de la disciplina de administración de privacidad. Los gobiernos, las industrias y otros organismos normativos han establecido leyes y estándares de administración de privacidad que deben seguirse, incluidas las prácticas sobre cómo se almacenan y comparten los datos y los derechos de las personas a controlar su propia información personal. Los procedimientos recomendados que las organizaciones usan para mantener la información segura y cumplir con estas leyes y estándares están evolucionando continuamente.

- Para ayudar a su organización a satisfacer estas necesidades, la administración de privacidad de Microsoft 365 proporciona soluciones para administrar datos personales en su entorno de Microsoft 365 y proporciona a los trabajadores herramientas para la revisión eficiente de datos, la corrección de problemas y la colaboración.

10.2.2.2 Segregación de funciones y tareas

Roles de administración

Recomendación	¿Por qué es importante?
Tener de 2 a 4 administradores globales	Como solo otro administrador global puede restablecer la contraseña de un administrador global, se recomienda tener al menos dos administradores globales en la organización en caso de bloqueo de cuenta. Pero el administrador global tiene casi un acceso ilimitado a la configuración de la organización y a la mayoría de los datos, por lo que también se recomienda no tener más de 4 administradores globales porque es una amenaza de seguridad.
Asignar el rol menos permisivo	La asignación del rol menos permisivo implica conceder a los administradores los permisos mínimos necesarios para realizar el trabajo. Por ejemplo, si se desea que alguien restablezca las contraseñas de los empleados, no se debería asignar el rol de administrador global ilimitado, sino el de administrador de contraseñas.
Requerir MFA para administradores	Es buena práctica requerir MFA en el inicio de sesión para todos los usuarios, pero es necesario al menos para los administradores. El MFA hace que los usuarios escriban un segundo método de identificación para comprobar que son quienes dicen que son.

- La suscripción de O365 incluye un conjunto de roles de administrador que se pueden asignar a los usuarios de la organización.

- Cada rol de administrador se asigna a funciones empresariales comunes y proporciona a los usuarios permisos para realizar tareas específicas en los centros de administración.

i. Recomendaciones para el rol de administradores

Roles disponibles en el centro de administración de Microsoft 365

El centro de administración Microsoft 365 permite administrar más de 30 roles de Azure AD. Sin embargo, estos roles son un subconjunto de las funciones disponibles en Azure portal.

Rol de administrador	¿A quién se le debe asignar este rol?
Administrador global	Asignar el rol de administrador global a los usuarios que necesitan acceso global a la mayoría de las características y datos de administración en Microsoft Online Services. Proporcionar demasiados usuarios el acceso global es un riesgo para la seguridad y se recomienda tener entre 2 y 4 administradores globales. Solo los administradores globales pueden: -Restablecer contraseñas para todos los usuarios -Agregar y administrar dominios. Nota: La persona que se registró en Microsoft Online Services se convierte automáticamente en un administrador global.
Administrador de facturación	Asignar el rol de administrador de facturación a los usuarios que necesiten hacer lo siguiente: -Suscripciones y licencias de compra -Suscripciones de actualización -Pagar por servicios -Recibir notificaciones por correo electrónico para facturas -Administrar solicitudes de servicio -Supervisar el estado del servicio
Administrador del Departamento de soporte técnico	Asignar el rol de administrador del Departamento de soporte técnico a los usuarios que necesiten hacer lo siguiente: -Contraseñas de REST -Obligar a los usuarios a cerrar sesión -Administrar solicitudes de servicio -Supervisar el estado del servicio Nota: el administrador del Departamento de soporte solo puede ayudar a los usuarios que no son administradores y a los usuarios que tienen asignados estos roles: lector de directorios, invitado, administrador de soporte, lector del centro de mensajes y lector de informes.
Administrador de licencias	Asignar el rol de administrador de licencias a los usuarios que necesiten hacer lo siguiente: -Administrar las licencias asignadas a los usuarios -Administrar las licencias asignadas a grupos mediante licencias basadas en grupos. -Editar la ubicación de uso para los usuarios Nota: este rol no da permiso para comprar o administrar suscripciones, agregar o administrar grupos o editar propiedades de usuario, excepto para la ubicación de uso. Lector de informes Asignar el rol de lector.

Rol de administrador	¿A quién se le debe asignar este rol?
Lector de informes	Asignar el rol de lector de informes a los usuarios que necesiten hacer lo siguiente: - Ver los datos de uso y los informes de actividad - Obtener acceso al paquete de contenido de adopción de Power BI. -Ver los informes y la actividad de inicio de sesión -Ver datos devueltos por la API de informes de Microsoft Graph.
Administrador del usuario	Asignar el rol de administrador de usuarios a los usuarios que necesiten hacer lo siguiente para todos los usuarios: -Agregar usuarios y grupos -Asignar licencias -Administrar la mayoría de las propiedades de los usuarios -Crear y administrar vistas de usuario -Actualizar directivas de expiración de contraseñas -Administrar solicitudes de servicio -Supervisar el estado del servicio El administrador del usuario también puede realizar las siguientes acciones para los usuarios que no son administradores y para los usuarios que tienen asignados los siguientes roles: lector de directorios, invitado, administrador de soporte, lector del centro de mensajes, lector de informes: -Administrar nombres de usuario -Eliminar y restaurar usuarios -Restablecer contraseñas -Obligar a los usuarios a cerrar sesión -Actualizar las claves de dispositivo (FIDO)t.

ii. Registro de actividad

- En lo relativo al registro de la actividad de usuarios y administradores se requiere la activación de la Auditoría de Office 365.

- Cuando se activa la búsqueda de registros de auditoría en el Centro de Seguridad y cumplimiento de Office 365, la actividad de usuario y administrador de la organización se registra en el registro de auditoría y se conserva durante 90 días.

Activar/Desactivar registro de auditoría

- Se debe tener asignado el rol registros de auditoría en Exchange Online para activar o desactivar la búsqueda de registros de auditoría en su organización de Office 365.

- De forma predeterminada, este rol se asigna a los grupos de roles administración de cumplimiento y administración de la organización en la página permisos del centro de administración de Exchange.

- Los administradores globales de Office 365 son miembros del grupo de funciones de administración de la organización en Exchange Online.

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.

Referencias adicionales

- INCIBE. “Políticas de seguridad para la pyme – Almacenamiento en los equipos de trabajo”. Recuperado de: *https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-en-los-equipos-trabajo.pdf*
- INCIBE. “Políticas de seguridad para la pyme – Almacenamiento en la red corporativa”. Recuperado de: *https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-red-corporativa.pdf*
- Proyecto NIST Telework: Working Anytime, Anywhere. *https://csrc.nist.gov/Projects/telework-working-anytime-anywhere/publications.*
- Nist Special Publication 800-114 Revision 1, User’s Guide to Telework and Bring your Own Device (BYOD) Security, disponible en: *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf*
- Centro Criptológico Nacional (2019). “Guía de configuración segura para Office 365”. Recuperado de: *https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4256-ccn-stic-885a-guia-de-configuracion-segura-para-office-365/file.html*
- Centro Criptológico Nacional (2020). “Recomendaciones de ciberseguridad para videollamadas y reuniones virtuales”. Recuperado de: *https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/206-ciberconsejos-videollamada/file*
- Microsoft (2021). “Documentación de cumplimiento de Microsoft 365”. Recuperado de: *https://docs.microsoft.com/es-es/microsoft-365/compliance/?view=o365-worldwide*

ASOBANCARIA