XXIII Congreso Latinoamericano
de Auditoría Interna y Evaluación de Riesgos
Santa Cruz, Bolivia

CLAIN 2019
MAYO
16 Y 17

ASOBAN
ASOCIACIÓN DE BANCOS PRIVADOS DE BOLIVIA

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

"El enfoque de la auditoría interna ante la revolución digital y las innovaciones disruptivas"

Auditoría de Tecnologías con un enfoque de hacker ético

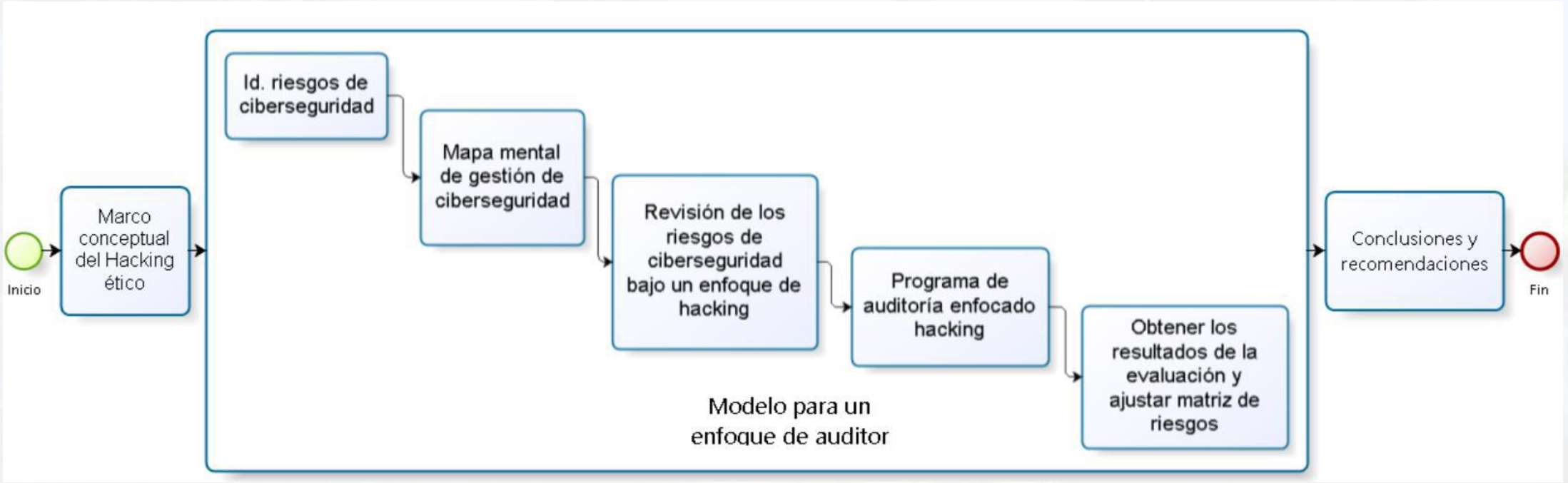
Mayo 2019

Ing. Sergio Azahuanche Gutiérrez,
CISA, CISM, CRISC, CSXF, ISO 31000 Senior Lead Manager, ISO 22301 Lead Auditor, COBIT-F 4.1 / 5 / 2019, ITIL

linkedin.com/in/sergio11584/

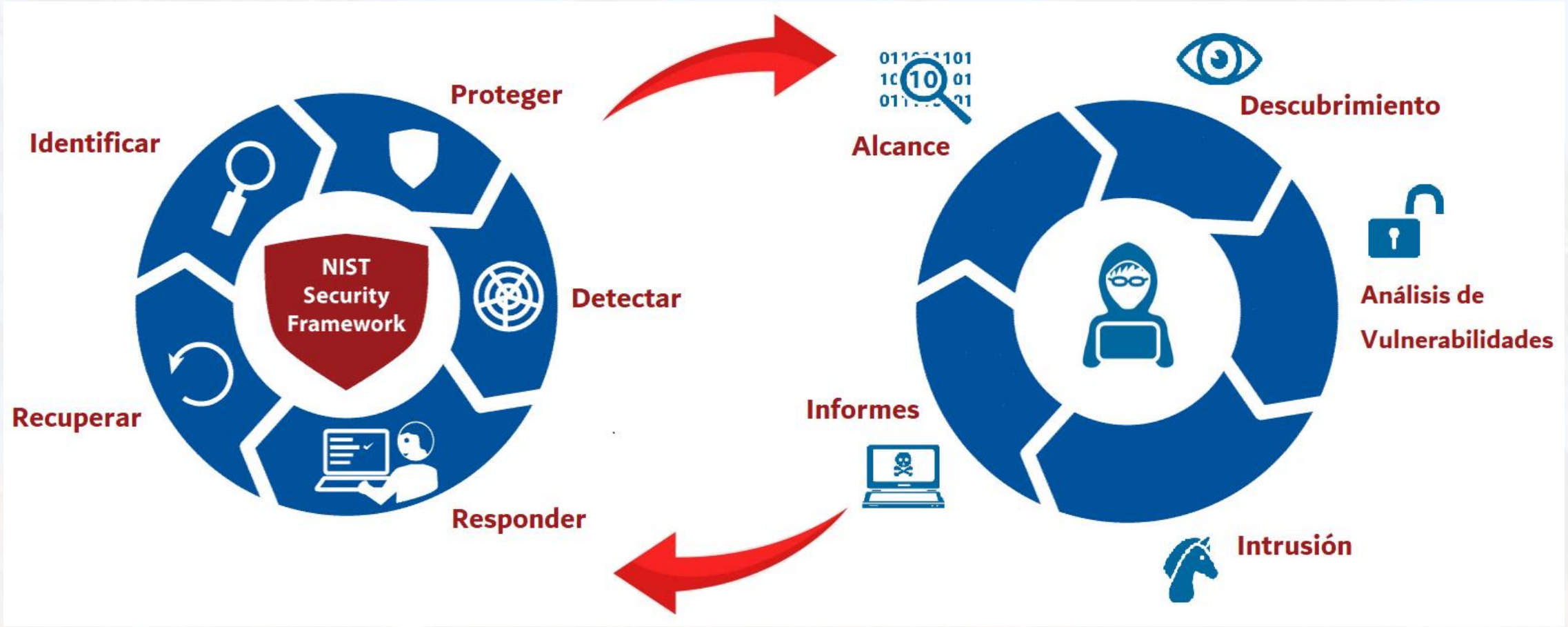
XXIII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos
Santa Cruz, Bolivia
CLAIN 2019
MAYO
16 Y 17
ASOBAN
FELABAN

#modelo_hacking_auditor



#fases_hacking

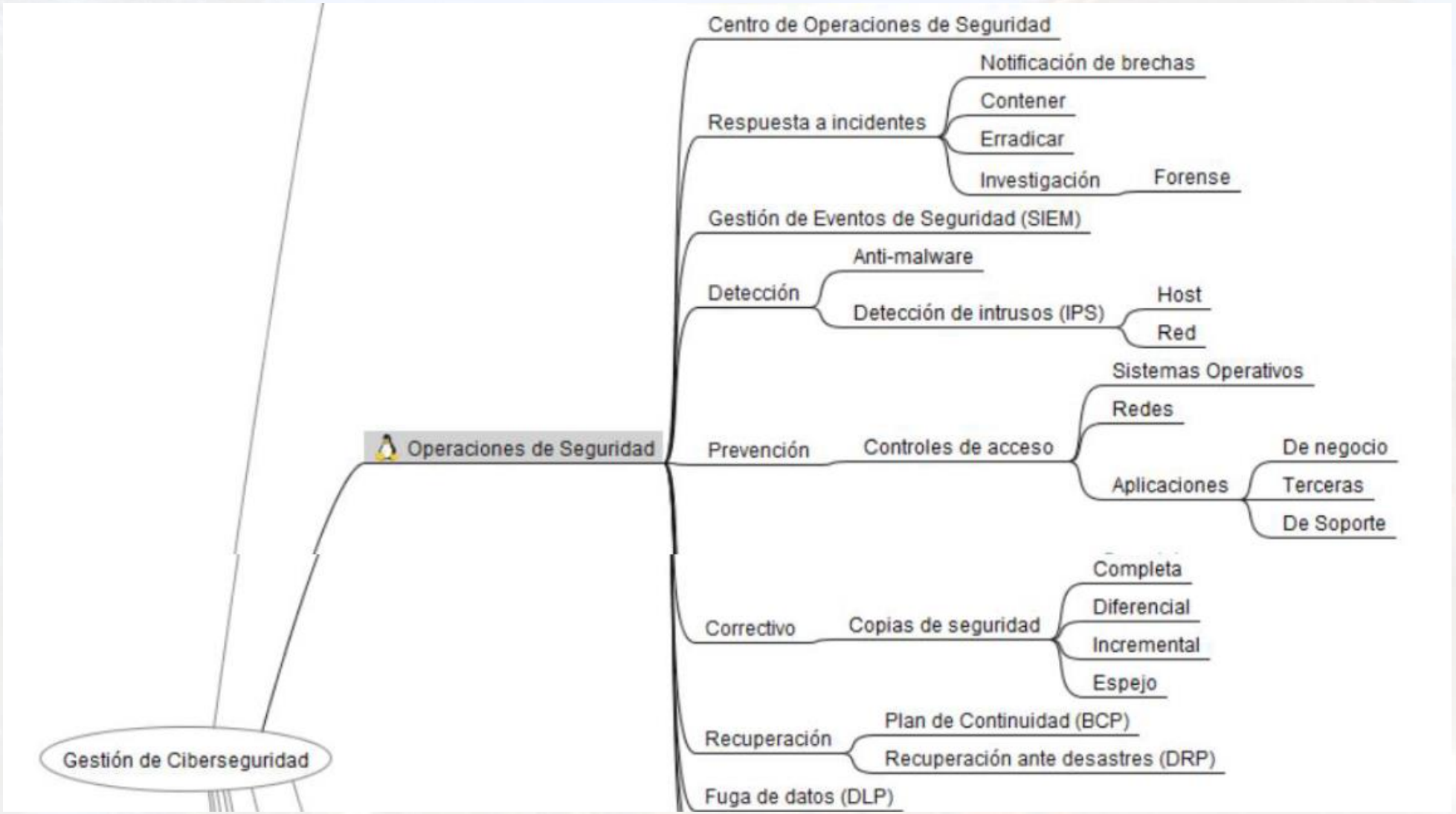
#modelo_enfoque_auditor_hacking_etico



Paso 1: Identificación de riesgos de ciberseguridad

Proceso	Subproceso	Código de Riesgo	Descripción del riesgo inherente	Probabilidad	Impacto	Riesgo inherente calculado	Riesgo inherente normalizado *escala: 1-5*	Nivel del Riesgo Inherente normalizado
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Gestión de la cultura del Banco en materia de seguridad de la información	RI.001	Riesgo que los empleados no reconozcan sus responsabilidades en relación a la seguridad de información que manejan, exponiéndola al riesgo de robo, fraude y mal uso de las instalaciones y medios.	2-Improbable	2-Bajo	4	2	Bajo
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Concientización sobre la seguridad de la información, educación y capacitación	RI.002	Riesgo que los empleados y proveedores no comprendan sus responsabilidades en relación a la seguridad de información que manejan, exponiéndola al riesgo de robo, fraude y mal uso de las instalaciones y medios.	3-Posible	3-Medio	9	3	Medio
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Gestión de Identidades	RI.003	Posibilidad que el controlador de dominio no controle adecuadamente los privilegios de los usuarios; incluyendo permisos de Administrador.	4-Probable	3-Medio	12	4	Alto
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Política de Gestión de acceso	RI.004	Probabilidad de fuga de información y/o brechas de seguridad debido al no retiro oportuno de acceso a instalaciones, aplicaciones y activos de información en general	3-Posible	2-Bajo	6	3	Medio
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Gestión de contraseñas y autenticación secreta	RI.005	Probabilidad de fraudes, interrupciones y fallas de seguridad, debido a que se utilizan políticas débiles de seguridad, estos no han sido implementados o no se cumplen	4-Probable	3-Medio	12	4	Alto
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Administración de usuarios privilegiados	RI.006	Probabilidad que se pueda violar o evadir las políticas de seguridad del Banco mediante el uso de códigos de usuario, claves de acceso y perfiles de acceso predefinidos por el fabricante.	3-Posible	3-Medio	9	3	Medio
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Gestión de las vulnerabilidades técnicas	RI.007	Probabilidad de fallas en la seguridad de la información por ausencia de revisiones independientes	4-Probable	3-Medio	12	4	Alto
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Código malicioso en estaciones y servidores	RI.008	Protección contra software malicioso: No se cuenta con controles efectivos y en funcionamiento para la prevención, detección y desactivación de software malicioso.	3-Posible	3-Medio	9	3	Medio
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Los registros de auditoría / log son determinados, documentados, implementados y revisados de acuerdo con la política.	RI.009	Probabilidad de fraudes y/u operaciones irregulares cuya información de detalle para análisis e investigación no esté disponible debido a que no se cuenta con pistas de auditoría y/o éstas no cuentan con un procedimiento para hacer su revisión efectiva	3-Posible	3-Medio	9	3	Medio
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Gestión de vulnerabilidades técnicas	RI.010	Posibilidad de interrupción del funcionamiento de algún proceso o servicio del Banco por un ataque relacionado a la red interna del Banco.	3-Posible	4-Alto	12	4	Alto

Paso 2: Mapa mental de la gestión de la ciberseguridad

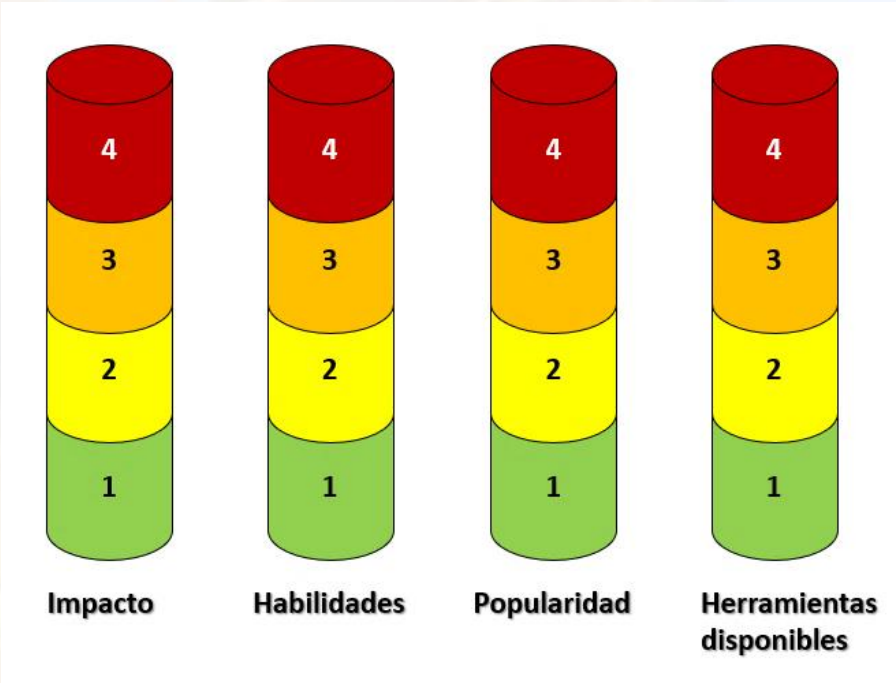

Gestión de Ciberseguridad
Operaciones de Seguridad
Centro de Operaciones de Seguridad
Respuesta a incidentes
Notificación de brechas
Contener
Erradicar
Investigación
Forense
Gestión de Eventos de Seguridad (SIEM)
Detección
Anti-malware
Detección de intrusos (IPS)
Host
Red
Prevención
Controles de acceso
Sistemas Operativos
Redes
Aplicaciones
De negocio
Terceras
De Soporte
Correctivo
Copias de seguridad
Completa
Diferencial
Incremental
Espejo
Recuperación
Plan de Continuidad (BCP)
Recuperación ante desastres (DRP)
Fuga de datos (DLP)

Paso 3: Revisión de los riesgos de ciberseguridad bajo enfoque de hacking

#componentes_del_riesgo

Componente a evaluar	Descripción del componente del riesgo
1. Nivel de Impacto (I)	El daño potencial causado por la ejecución exitosa del ataque.
2. Habilidades (H)	El grado de habilidad necesaria para ejecutar un ataque (p.e: conocimiento de redes, programación, hardware y software utilitario).
3. Popularidad (P)	La frecuencia de utilización del ataque contra un objetivo en particular; depende de que tan conocido es la técnica de ataque en una población.
4. Herramientas disponibles (HD)	Herramientas de software libre y/o propietario, scripts de desarrollo, desarrollo a medida que puedan estar disponibles en el internet.
Fórmula del puntaje de Riesgo (R):	**R= (I) * 1.25(H) * 1.66(P) * 1.8(HD)**

Figura 11. Componentes evaluados de un potencial ciberataque en una entidad financiera



#tablas_de_puntuacion

Aspectos evaluados	Puntuación			
	4	3	2	1
Nivel de Impacto	Pérdidas de reputación y legal	Pérdidas económicas	Pérdidas aisladas de disponibilidad	Poco impacto
Habilidades	No requiere experiencia técnica alguna	Conocimientos básicos de redes	Conocimientos intermedios en programación y redes	Altamente técnico en redes y programación
Popularidad	Altamente difundido	Difundido en foros especializados	Pocas fuentes se requiere investigación	Nula o muy poco difundido
Herramientas disponibles	Muchas y sin costos	Algunas con costo y gratuitas	Elaboración de Scripts	Muy pocas o nulas

#riesgo = #probabilidad X #impacto

Severidad del Riesgo = Probabilidad por Impacto					
Impacto	Muy significativo	Bajo	Moderado	Alto	Extremo
	Significativo	Bajo	Bajo	Moderado	Extremo
	Poco significativo	Bajo	Bajo	Moderado	Alto
	No significativo	Bajo	Bajo	Moderado	Moderado
		Improbable	Posible	Probable	Altamente probable
	Probabilidad				

Nivel probabilidad	Rangos del puntaje	Clasificación del riesgo	Rangos del puntaje
Improbable	0 - 15	Riesgo bajo	0 - 100
Posible	16 – 70	Riesgo moderado	101 - 350
Probable	71 - 140	Riesgo alto	351 - 650
Altamente probable	> 140	Riesgo extremo	> 650

Paso 4: Programa de auditoría con enfoque de hacking

Programa de Auditoría y/o Aseguramiento de Ciberseguridad
Basado en el Marco de trabajo "NIST Cybersecurity Framework"

Subproceso	*Objetivos de Control*	*Controles*	*Procedimientos a seguir*	*Herramientas disponibles*	*Fase de Ethical Hacking*	*NIST Ref. to COBIT 5*	*Ref. Framework/ Estándares*	*Resultado (Falló o éxito)*
Seguridad en los datos	La información y los registros (datos) se administran de manera coherente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	Los datos almacenados son protegidos	1. Determine si se identifican datos confidenciales o confidenciales en la red de la organización (por ejemplo, clasificación de datos, evaluación de riesgos). 2. Determine si los datos confidenciales están protegidos (por ejemplo, encriptación fuerte según lo definido por las mejores prácticas de la industria) en reposo. 3. Determine si los dispositivos móviles (por ejemplo, computadoras portátiles, tabletas, medios extraíbles) que se utilizan para almacenar datos confidenciales están cifrados. 4. Revise los contratos con terceros que almacenan datos confidenciales para garantizar que se implementen los controles de seguridad adecuados para los datos confidenciales en reposo. 5. Realizar pruebas con un software de desencriptado (forense) para identificar debilidades en el cifrado de los datos almacenados	- Passware Kit Forensic	Intrusión	APO01.06; BAI02.01; BAI06.01; DSS06.06	ISO/IEC 27001:2013 A.8.2.3	
		Los datos en tránsito son protegidos	1. Determine si la información confidencial está protegida (por ejemplo, un cifrado sólido según se define en las mejores prácticas de la industria) cuando se transmite a través de redes de acceso público. 2. Determine si existen políticas adecuadas con respecto a la transmisión de información confidencial o confidencial por correo electrónico. 3. Revise los materiales de capacitación y / o la política de uso aceptable para determinar si los empleados tienen instrucciones sobre la política de la organización con respecto a la transmisión de datos. 4. Revisar los contratos con terceros que transmiten datos confidenciales para garantizar que se implementen controles de seguridad apropiados para la transmisión de datos confidenciales. 5. Realizar escuchas pasivas en redes convencionales e inalámbricas (donde sea aplicable); a fin de identificar si el tráfico de información sensible se encuentra protegido (cifrada), a fin de prevenir los ataques de hombre en el medio. 6. En donde sea posible realizar una captura de tráfico como evidencia de las vulnerabilidades encontradas en las comunicaciones.	- WifiSlax - Wireshark - ShareScan - Cain&Abel	Análisis de Vulnerabilidades/ Intrusión	APO01.06; DSS06.06	ISO/IEC 27001:2013 A.8.2.3; A.13.1.1; A.13.2.1; A.13.2.3; A.14.1.2; A.14.1.3	
		Capacidad adecuada para garantizar la disponibilidad.	1. Revise una muestra de los informes de monitoreo de administración de capacidad utilizados para monitorear recursos críticos como el ancho de banda de la red, la CPU, la utilización del disco, etc. 2. Determine si los recursos tienen la capacidad adecuada (por ejemplo, espacio en disco, CPU). 3. Determine si el riesgo de denegación de servicio distribuido (DDoS) se ha abordado y está en línea con el apetito de riesgo de la organización. Verificar por medio de un análisis de vulnerabilidades para identificar debilidades relacionadas a DDoS en servidores y/o equipos de red del Banco.	- Nessus - OpenVAS - Retina	Análisis de vulnerabilidades	APO13.01 BAI02.01; BAI03.05; BAI04.01; BAI04.02; BAI04.03; BAI04.04; BAI04.05	ISO/IEC 27001:2013 A.12.3.1	

Programa de Auditoría y/o Aseguramiento de Ciberseguridad
Basado en el Marco de trabajo "NIST Cybersecurity Framework"

Subproceso	*Objetivos de Control*	*Controles*	*Procedimientos a seguir*	*Herramientas disponibles*	*Fase de Ethical Hacking*	*NIST Ref. to COBIT 5*	*Ref. Framework/ Estándares*	*Resultado (Falló o éxito)*
Control de Acceso	El acceso a los activos y las instalaciones asociadas se limita a los usuarios, procesos o dispositivos autorizados, y a las actividades y transacciones autorizadas.	Las identidades y las credenciales se administran para dispositivos y usuarios autorizados.	1. Determine si el acceso a los dispositivos de red (por ejemplo, servidores, estaciones de trabajo, dispositivos móviles, firewalls) está restringido por: a. ID de inicio de sesión de usuario únicas b. Contraseñas complejas c. Autenticación múltiples factores. d. Tiempo de espera automático (si se deja desatendido). e. Bloqueo automático después de repetidos intentos fallidos de acceso. d. Cambio de nombres de cuenta y contraseñas de cuentas administrador. 2. Realizar la enumeración de los dispositivos de red bajo revisión; obtener las políticas de contraseñas de dichos dispositivos (p.e: controlador de dominio). 3. Determine si los parámetros de la contraseña cumplen con la política de la organización y / o los requisitos aplicables de la industria. Considera lo siguiente: a. Longitud, complejidad, requisitos de cambio e historial b. Revisar si están los archivos de contraseña cifrados y restringidos. Revisarlo por medio de herramientas de hacking (p.e: john the ripper, metasploit, Cain&Abel) 3. Revise los procedimientos de terminación para asegurarse de que las credenciales sean revocadas o cambiadas cuando un empleado se retire. a. Revise las cuentas para asegurarse de que el acceso de los usuarios se revoque después de la terminación y las cuentas se eliminen según la política.	- Metasploit - Brutus - John the Ripper - Ophcrack - WifiSlax - WifiWay - Cain&Abel - DumpSec	Análisis de vulnerabilidades	DSS05.04; DSS06.03	ISO/IEC 27001:2013 A.9.2.1; A.9.2.2; A.9.2.4; A.9.3.1; A.9.4.2; A.9.4.3	
Control de Acceso		El acceso remoto está gestionado	1. Determine si las políticas y los procedimientos relacionados con las capacidades de acceso de los usuarios remotos se formalizan. Considera lo siguiente: a. Los usuarios remotos (por ejemplo, empleados, contratistas, terceros) con acceso a sistemas críticos son aprobados y documentados. b. Las conexiones remotas solo se abren según sea necesario. c. Las conexiones remotas son registradas, monitoreadas y están encriptadas. d. La autenticación fuerte está en su lugar (por ejemplo, multifactor, parámetros de contraseña segura). e. Se habilita la capacidad de borrar datos de forma remota en dispositivos móviles cuando faltan datos o se roban. g. Se requieren controles de seguridad de la institución (por ejemplo, antivirus, administración de parches) en dispositivos remotos que se conectan a la red. 2. Por medio de un escaneo de vulnerabilidades detectar la falta de parches, aseguramiento y puertos de acceso remoto. 3. Realizar la enumeración del software instalado en los dispositivos de red y equipos móviles (p.e: Servidores, estaciones de trabajo); a fin de identificar aquellos que no disponen de software antimalware.	- Nessus - OpenVAS - WireShark - NMap - ZenMap	Análisis de vulnerabilidades	APO13.01; DSS01.04; DSS05.03	ISO/IEC 27001:2013 A.6.2.2; A.13.1.1; A.13.2.1	

Programa de Auditoría y/o Aseguramiento de Ciberseguridad Basado en el Marco de trabajo "NIST Cybersecurity Framework"								
Subproceso	***Objetivos de Control***	***Controles***	***Procedimientos a seguir***	***Herramientas disponibles***	***Fase de Ethical Hacking***	***NIST Ref. to COBIT 5***	***Ref. Framework/ Estándares***	***Resultado (Falló o éxito)***
Procesos y procedimientos de protección de la información	Las políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración y la coordinación entre las entidades de la organización), los procesos y los procedimientos se mantienen y utilizan para administrar la protección de los sistemas y activos de información.	Se crea y mantiene una configuración básica de los sistemas de tecnología de la información / control industrial.	1. Determine si la organización ha creado o adoptado configuraciones de línea de base (por ejemplo, puntos de referencia del Centro de Seguridad de Internet [CIS], Guías de Implementación Técnica de Seguridad [STIG]) para sistemas (por ejemplo, servidores, computadoras de escritorio, enrutadores). 2. Sistemas de muestra contra las configuraciones de línea de base de la organización para garantizar que se cumplan y cumplan los estándares. 3. Realizar un análisis de la implementación del hardening de los dispositivos de red (p.e: estaciones de trabajo, servidores, firewall, switches, routers, entre otros) por medio de herramientas informáticas.	- Retina - OpenVAS - Nipper	Análisis de Vulnerabilidades	BAI10.01; BAI10.02; BAI10.03; BAI10.05	ISO/IEC 27001:2013 A.12.1.2; A.12.5.1; A.12.6.2; A.14.2.2; A.14.2.3; A.14.2.4	
		Se desarrolla e implementa un plan de gestión de vulnerabilidades.	1. Obtenga el plan de gestión de vulnerabilidades de la organización y asegúrese de que incluya lo siguiente: a. Frecuencia de escaneo de vulnerabilidades segundo. Método para medir el impacto de las vulnerabilidades identificadas (por ejemplo, Sistema de puntuación de vulnerabilidad común [CVSS]) b. Incorporación de vulnerabilidades identificadas en otras evaluaciones de control de seguridad (por ejemplo, auditorías externas, pruebas de penetración) c. Procedimientos para el desarrollo de remediación de vulnerabilidades identificadas. 2. Obtenga una copia de la evaluación de riesgos de la organización para garantizar que se incluyan las vulnerabilidades identificadas durante el proceso de administración de vulnerabilidades. 3. Explotar vulnerabilidades de forma controlada con una herramienta informática; ello, a fin de corroborar el nivel de riesgo (probabilidad e impacto).	- Retina - OpenVAS - Nipper - Nessus - Metasploit	Intrusión	APO04.03	ISO/IEC 27001:2013 A.12.6.1; A.18.2.2	

Paso 5: Obtener resultados de la evaluación y ajustar matriz de riesgos

Proceso	Subproceso	Código de Riesgo	Descripción del riesgo inherente	Probabilidad inicial estimada	Impacto	Nivel del Riesgo Inherente preliminar	Riesgo inherente preliminar calculado (tradicional)	Probabilidades post-análisis mediante hacking				Puntaje de Riesgo (metodología propuesta)	Riesgo actual normalizado
								Nivel de impacto organizacional	Habilidades	Popularidad	Herramientas disponibles		
Gestión de la ciberseguridad en las plataformas distribuidas del Banco	Administración de usuarios privilegiados	RI.006	Probabilidad que se pueda violar o evadir las políticas de seguridad del Banco mediante el uso de códigos de usuario, claves de acceso y perfiles de acceso predefinidos por el fabricante.	3 Posible	3 Medio	Medio	9	3	3	4	4	538	Alto
	Gestión de las vulnerabilidades técnicas	RI.007	Probabilidad de fallas en la seguridad perimetral por ausencia de revisiones de análisis de vulnerabilidades regulares	3 Posible	3 Medio	Medio	12	3	3	3	4	403	Alto
	Código malicioso en estaciones y servidores	RI.008	Protección contra software malicioso: No se cuenta con controles efectivos y en funcionamiento para la prevención, detección y desactivación de software malicioso.	3 Posible	3 Medio	Medio	9	4	3	2	2	179	Moderado
	Los registros de auditoría / log son determinados, documentados, implementados y revisados de acuerdo con la política.	RI.009	Probabilidad de fraudes y/u operaciones irregulares cuya información de detalle para análisis e investigación no esté disponible debido a que no se cuenta con pistas de auditoría y/o éstas no cuentan con un procedimiento para hacer su revisión efectiva	3 Posible	3 Medio	Medio	9	4	1	2	2	60	Bajo
	Gestión de vulnerabilidades técnicas	RI.010	Posibilidad de interrupción del funcionamiento de algún proceso o servicio del Banco por un ataque relacionado a la red interna del Banco.	3 Posible	4 Alto	Alto	12	4	2	3	3	269	Moderado

#conclusiones

- Se mejora sustancialmente la estimación de los riesgos tomando en cuenta los componentes que influyen a un potencial incidente de ciberseguridad.
- Auditoría debe conocer las características particulares de la infraestructura tecnológica a evaluar y sus controles de ciberseguridad.
- Disponer de herramientas de hacking para las evaluaciones.
- El equipo de auditoría requiere de una alta capacidad técnica.
- Los aspectos de Gobierno de Seguridad de la Información deben ser conocidos y evaluados por Auditoría previo al inicio de una auditoría de ciberseguridad.

YOU HAVE BEEN
HACKED !

MUCHAS GRACIAS