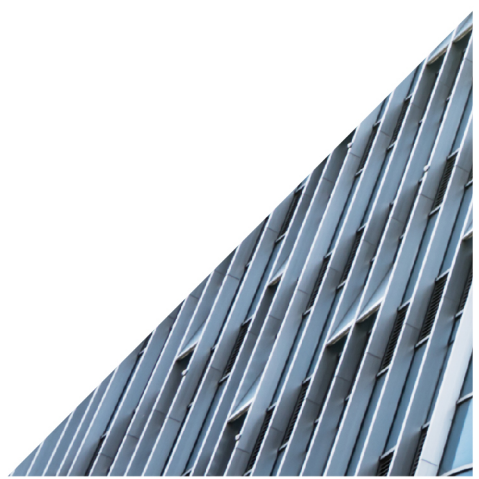
cybertrust

INSPIRANDO CONFIANZA

Auditoría en Ciberseguridad

jose.lagos@cybertrust.cl

Relator: José Lagos



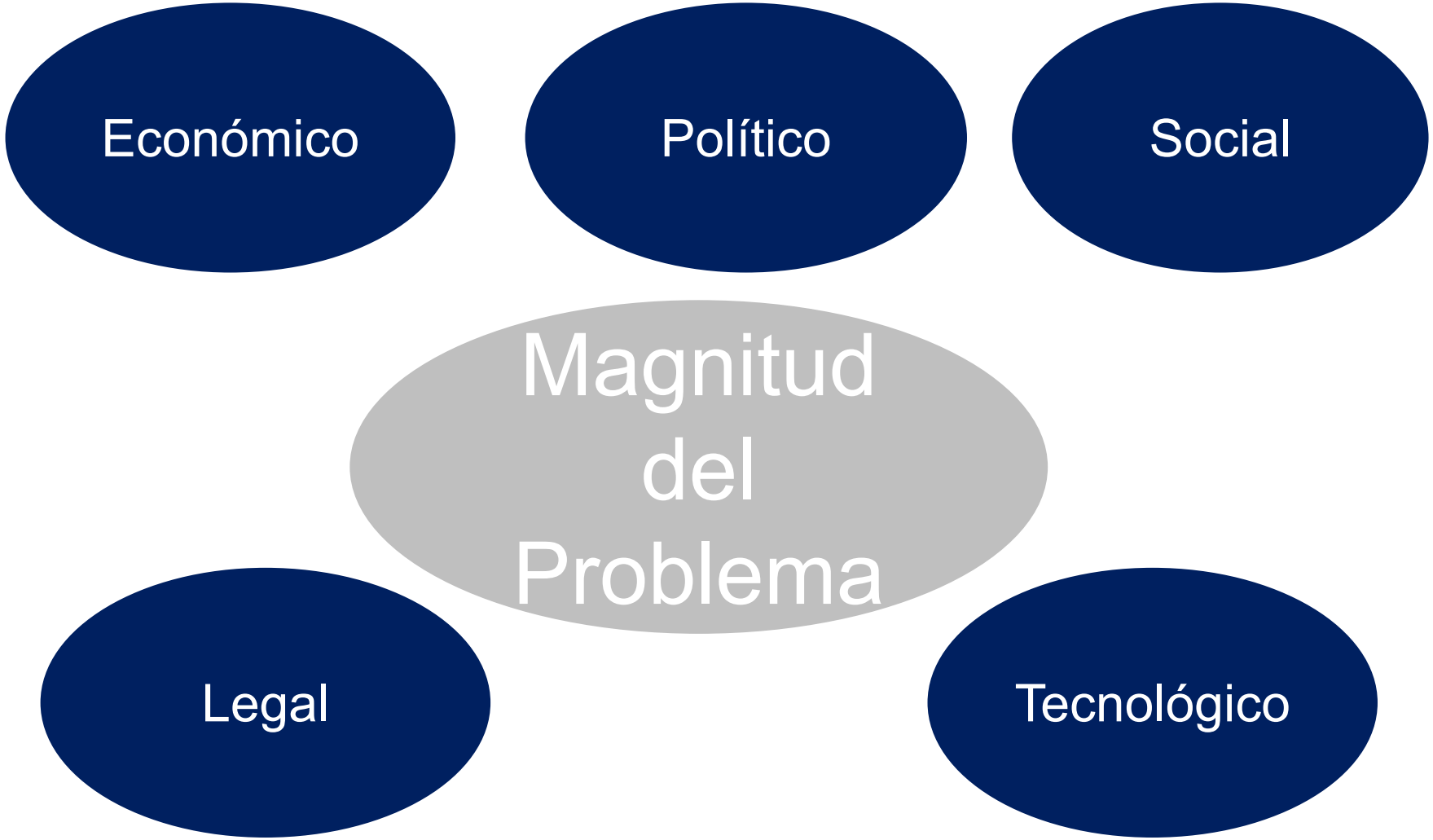
www.cybertrust.cl

Contenidos

- Magnitud del Problema
- Fundamentos de Auditoría en Ciberseguridad
- Las tres líneas de Defensa
- Frameworks de Ciberseguridad
- NIST Cybersecurity Framework
- Programa de Auditoría y Objetivos de Control

Magnitud del Problema

Magnitud del Problema



El Costo del Data Breach

El costo de las brechas de datos excederá los US 3 trillones para el 2019

El gasto en Ciberseguridad excederá los US 1.5 trillones para el 2021

Costo promedio de una brecha de datos es US 22.000 por día

El costo por registro de una brecha de datos es de US 142

El Impacto para las Organizaciones es crítico

Riesgo Operacional - Ciberseguridad

Definición de Ciberseguridad

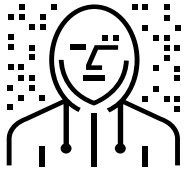
La Ciberseguridad es la sinergia de tecnologías, procesos y prácticas, que permiten proteger la información, las redes, los sistemas, aparatos electrónicos y los programas utilizados para recopilar, procesar, almacenar y proteger la información, de ataques, daños y accesos no autorizado.

La Ciberseguridad se preocupa por proteger todo lo que está dentro de una red, hardware, software e información, que es procesada y almacenada dentro de un sistema aislado o transportado por ambientes interconectados.

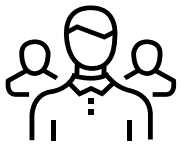
Vectores de Ataque

Ciber Crimen

Insider



Usuario No Intencional

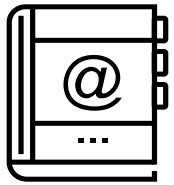


Estado o Nación

Hacktivismo

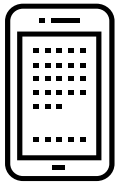
Qué Quiero Proteger

Email Corporativo

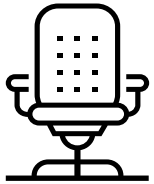


Colaboradores de Servicio al Cliente

Endpoint - Celular

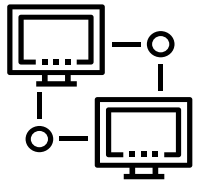


Ejecutivos / Gerentes



Aplicaciones Móviles

Dispositivos de Red

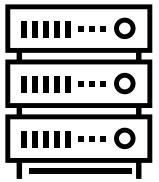


Qué Quiero Proteger – Cont,

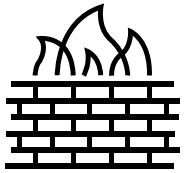
Endpoint Laptop

Endpoint Workstation

Endpoint Server

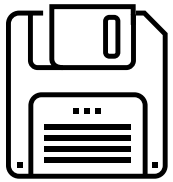


Network Firewall



Registro de Clientes

Respaldos

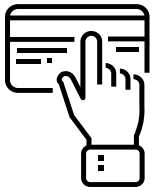


Qué Quiero Proteger – Cont,

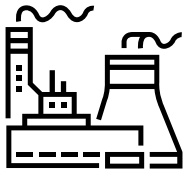
Network de Proveedor Externo

Información Personal o Sensible (PII)

Información de la Tarjeta de Crédito



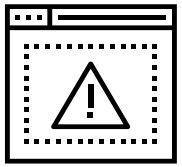
Infraestructura Crítica



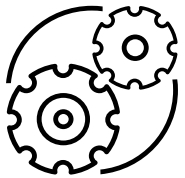
Amenazas / Vulnerabilidades

Tecnología No Autorizada

Usuario Remoto

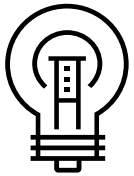


Error de Procesos

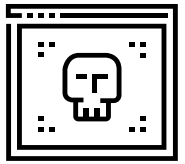


Error Humano

Entrenamiento Inadecuado

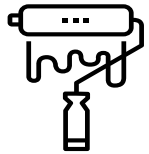


Proveedor

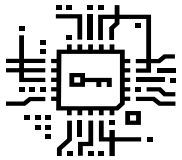


Amenazas / Vulnerabilidades – Cont,

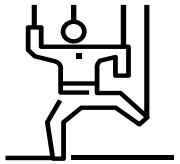
Defacement Sitio Web



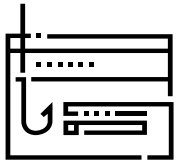
Error de Encriptación



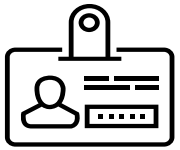
Ingeniería Social



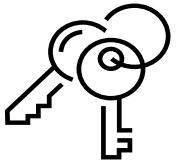
Phishing



Obtención de Privilegios

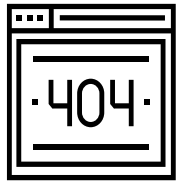


Acceso Físico No Autorizado



Que Objetivos deseo Cumplir

DIsponibilidad

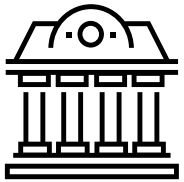


Integridad

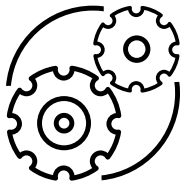
Confidencialidad

Posibles Impactos

Financiero

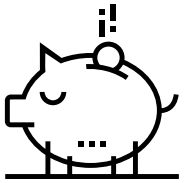


Operational

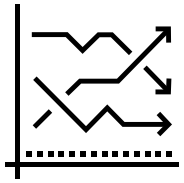


Legal

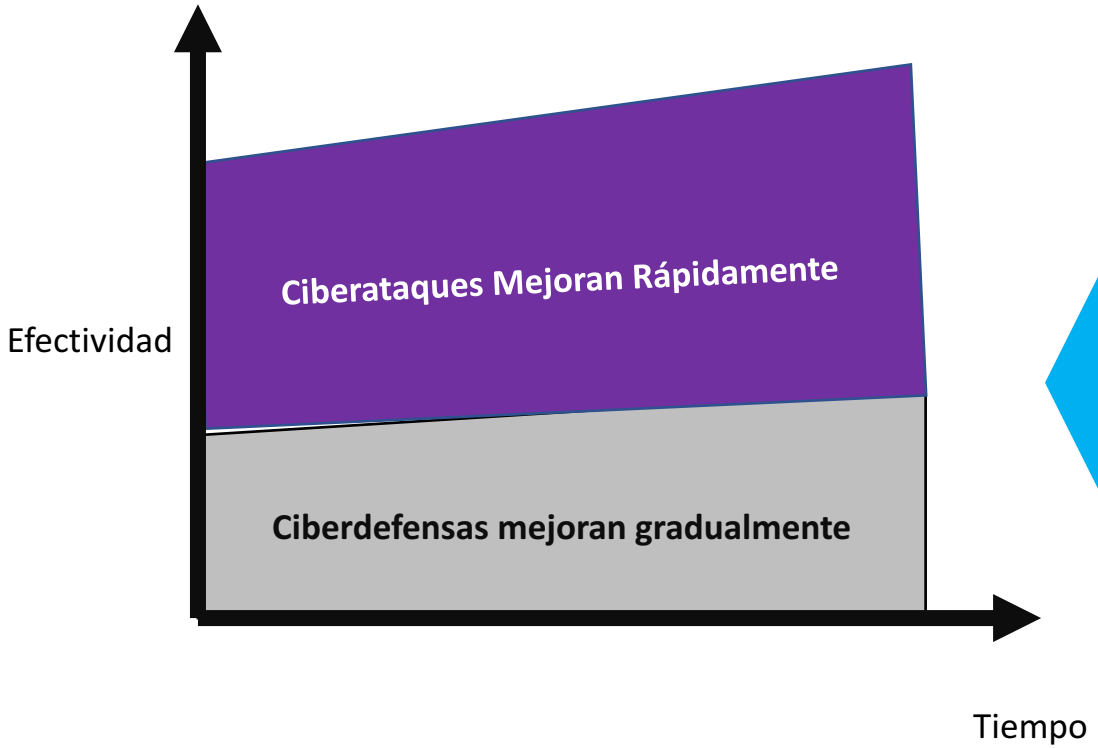
Recursos Humanos



Reputacional



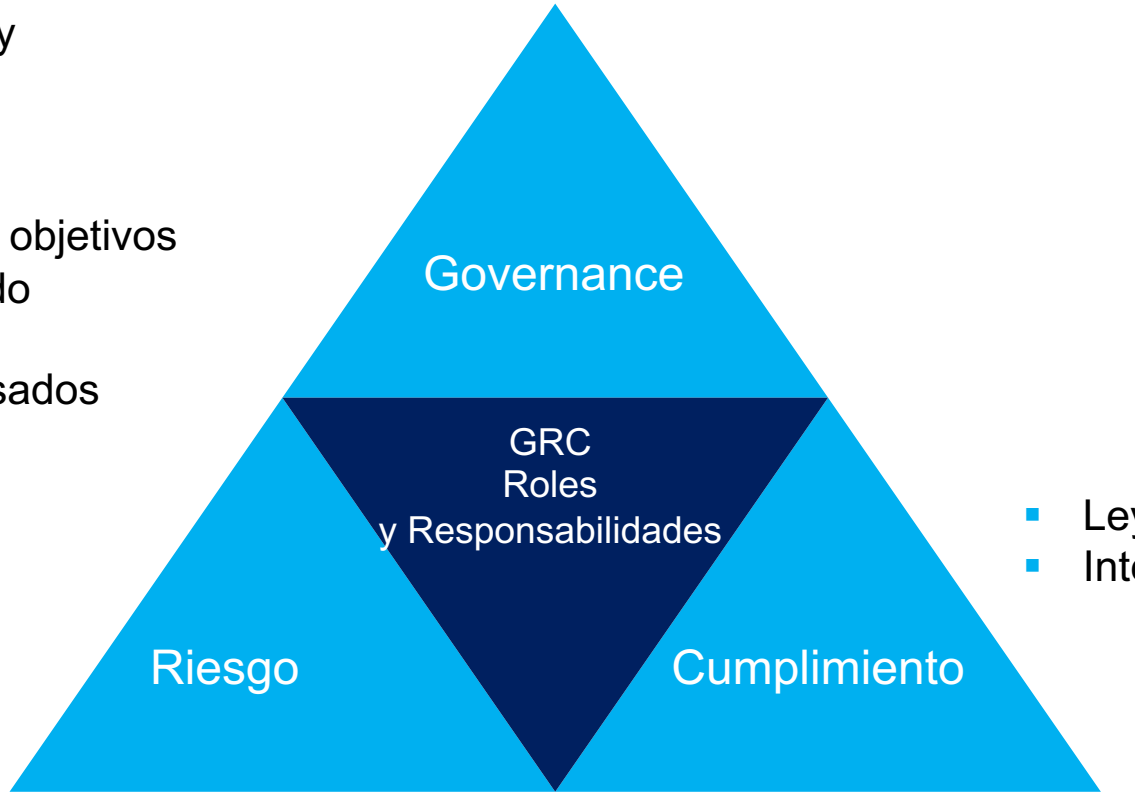
Minimizando El GAP



Fundamentos de Auditoria

Gobernabilidad, Riesgo y Cumplimiento

- Responsabilidad del Directorio y Management
- Provee dirección estratégica en Ciberseguridad
- Asegura el cumplimiento de los objetivos
- Verifica que el riesgo esta siendo administrado adecuadamente
- Verifica que los recursos son usados adecuadamente



- Leyes, standares, regulaciones.
- Internon y externo

- Incluye la identificación, análisis, priorización y administración de los riesgos
- Es necesario definir el apetito al riesgo en ciberseguridad
- Los organizaciones para administrar los riesgos de ciberseguridad deben implementar controles

Gobernabilidad, Riesgo y Cumplimiento – Cont,

1era Línea Defensa

- La gerencia asume la responsabilidad por los temas de Ciberseguridad y delega la responsabilidad en funciones especializadas.
- Los controles, métricas, indicadores y revisiones periódicas sirven como un instrumento para identificar debilidades.
- Identifica las mejoras en Ciberseguridad que son requeridas para proteger el activo digital de la organización.

2da Línea Defensa

- La segunda línea de defensa con la primera línea de defensa, aseguran que los riesgos de Ciberseguridad son identificados, entendidos, documentados y mitigados a través del diseño e implementación de controles.

3ra Línea Defensa

- Evaluación independiente en los aspectos de pruebas y aseguramiento.

Auditoría en Ciberseguridad

La Auditoría de Ciberseguridad, provee a la administración de una evaluación independiente **de la efectividad de los procesos de Ciberseguridad**, las políticas, procedimientos, gobernabilidad y otros controles.

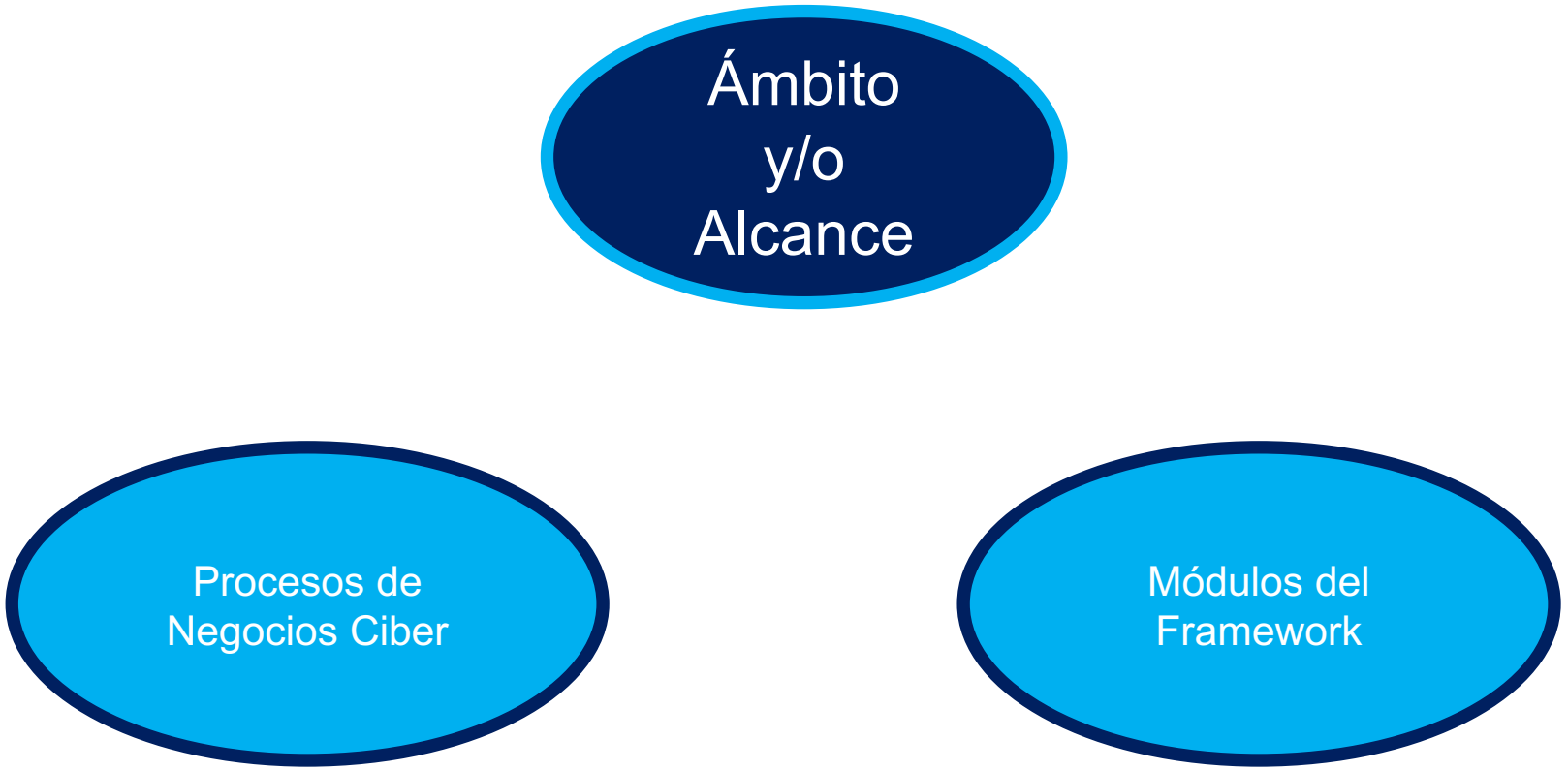
Auditoría en Ciberseguridad

Provee a la administración una visión independiente de la efectividad de los procesos, personas y tecnologías que asociadas a Ciberseguridad

Objetivos

- Proveer a la administración con una evaluación independiente de las políticas, procedimientos y su efectividad operativa (diseño y operación de controles)
- Identificar controles de ciberseguridad que pueden afectar la confidencialidad, integridad y disponibilidad de los activos críticos de la empresa
- Analizar la efectividad del programa de respuesta a incidentes y cibercrisis
- Evaluar el cumplimiento de las leyes y regulaciones asociadas a ciberseguridad

Auditoría en Ciberseguridad – Cont,



Procesos de Negocio de Ciberseguridad

Areas Funcionales de Ciberseguridad

Gobernabilidad

Ejecutar la estrategia de Cibereguridad: asegurar alineamiento con el negovcio y métricas de seguimiento

Gestión de Riesgos

Identificar y priorizar las áreas de mayor impacto potencial para el negocio.

Gestión de Cumplimiento

Asegurar que existan controles de seguridad adecuados para demostrar el cumplimiento de las obligaciones reglamentarias y contractuales; monitorear el acceso y los datos mínimos necesarios (Acceso / Datos)

Gestión de vulnerabilidad

Identifique y elimine las debilidades en los sistemas (por ejemplo, análisis de vulnerabilidades, parches, seguridad de la aplicación)

Protección d Datos

Proteja los datos directamente a lo largo de su ciclo de vida en reposo y en movimiento (por ejemplo, DLP, Encriptación)

Gestión de Identidad y Acceso

Asegúrese de que solo los usuarios autorizados tengan acceso a los recursos

Gestión de amenazas

Supervise a los actores que intentan causar daño y evítelo (por ejemplo, firewall, IDPS, correo electrónico / proxy web, AV, registro)

Arquitectura de seguridad

Determine cómo deben diseñarse e integrarse los controles de seguridad en el entorno general

Respuesta Investigativa y Forense

Responder en caso de incidentes

Cultura y Administración del cambio

Mantenga la conciencia de seguridad y asegúrese de que el cambio se mantenga en la base de usuarios

Procesos de Negocio de Ciberseguridad

1. Gestión de Políticas y Administración de Excepciones

2. Proyectos y Revisión de Cambios de Seguridad

3. Gestión de Riesgos

4. Gestión de Controles

5. Auditoría y Seguimiento de Observaciones

6. Auditoría e Inventario de Activos

7. Administración de Cambios

8. Base de Datos de Administración de Configuración

9. Revisión de Proveedores y Administración de Riesgos

10. Respuestas a Ciberataques

11. Plan de Desastres

12. Administración de Vulnerabilidades y Seguimiento

13. Desarrollo y Administración de Parches

14. Monitoreo de Seguridad

15. Administración de Password y Llaves

16. Recertificación Periódica de Accesos y Cuentas

17. Actividades de Auditoría de Cuentas Privilegiadas

Procesos de Negocio de Ciberseguridad

CONTROLES
Naturaleza

ADMINISTRATIVOS

Incluyen todas las actividades que no necesariamente tienen que llevarse a cabo **por medios técnicos.**

Algunos ejemplos son las Políticas, entrenamientos, los controles manuales y las medidas de planificación.

La **eficacia de estos controles** depende de la concientización y la aceptación de los colaboradores

FISICOS

TECNICOS

se apoyan o habilitan por medios **técnicos**, como el software antivirus y los sistemas de control de acceso.

En muchos casos, el funcionamiento de los **controles técnicos puede automatizarse**, por ejemplo, el software antivirus puede mover un programa malicioso en cuarentena o eliminarlo sin manual acción.

CONTROLES
Tiempo

PREVENTIVAS

Entran en vigor **antes de que ocurra un evento**.

Garantizan de antemano que se previene un evento adverso o se produce un evento no deseado.

Generalmente, son la primera opción en ciberseguridad porque los impactos negativos y los daños resultantes se pueden evitar por completo.

DETECTIVOS

Entran en vigor mientras ocurre un evento. Se centran en la detección de eventos adversos.

A menudo desencadenan controles correctivos.

CORRECTIVOS

Las salvaguardias correctivas entran en vigor después de que ocurre un evento.

Se utilizan para corregir los efectos negativos de los eventos adversos.

ADMINISTRATIVOS

PREVENTIVOS

- Políticas y Procedimientos
- Necesidad de saber
- Separación de Funciones
- Concienciación y formación
- Comprobaciones de antecedentes
- Clasificación de Datos
- Control de Versiones
- OutSourcing

PREVENTIVOS

TECNICOS

- Sistemas de control de acceso
- Control de aplicaciones
- Seguridad de la red
- Hardening
- Desarrollo seguro de software
- Cifrado
- Prevención de fugas de datos (DLP)
- Resiliencia técnica

ADMINISTRATIVOS

DETECTIVO

- Gestión de incidentes
- Pruebas
- Supervisión
- Rotación de trabajos y vacaciones
- Informes Resiliencia técnica

TECNICOS

DETECTIVO

- Protección contra malware
- Sistemas de detección de intrusiones
- Supervisión de la integridad de archivos
- Seguimientos de auditoría

ADMINISTRATIVO

CORRECTIVO

- Gestión de la Continuidad del Negocio
- Respuesta a incidentes
- Seguros

TECNICO

CORRECTIVO

- Gestión de parches
- Recuperación ante desastres
- Backups

Framework de Ciberseguridad

¿Porqué Implementar un Framework de Ciberseguridad ?

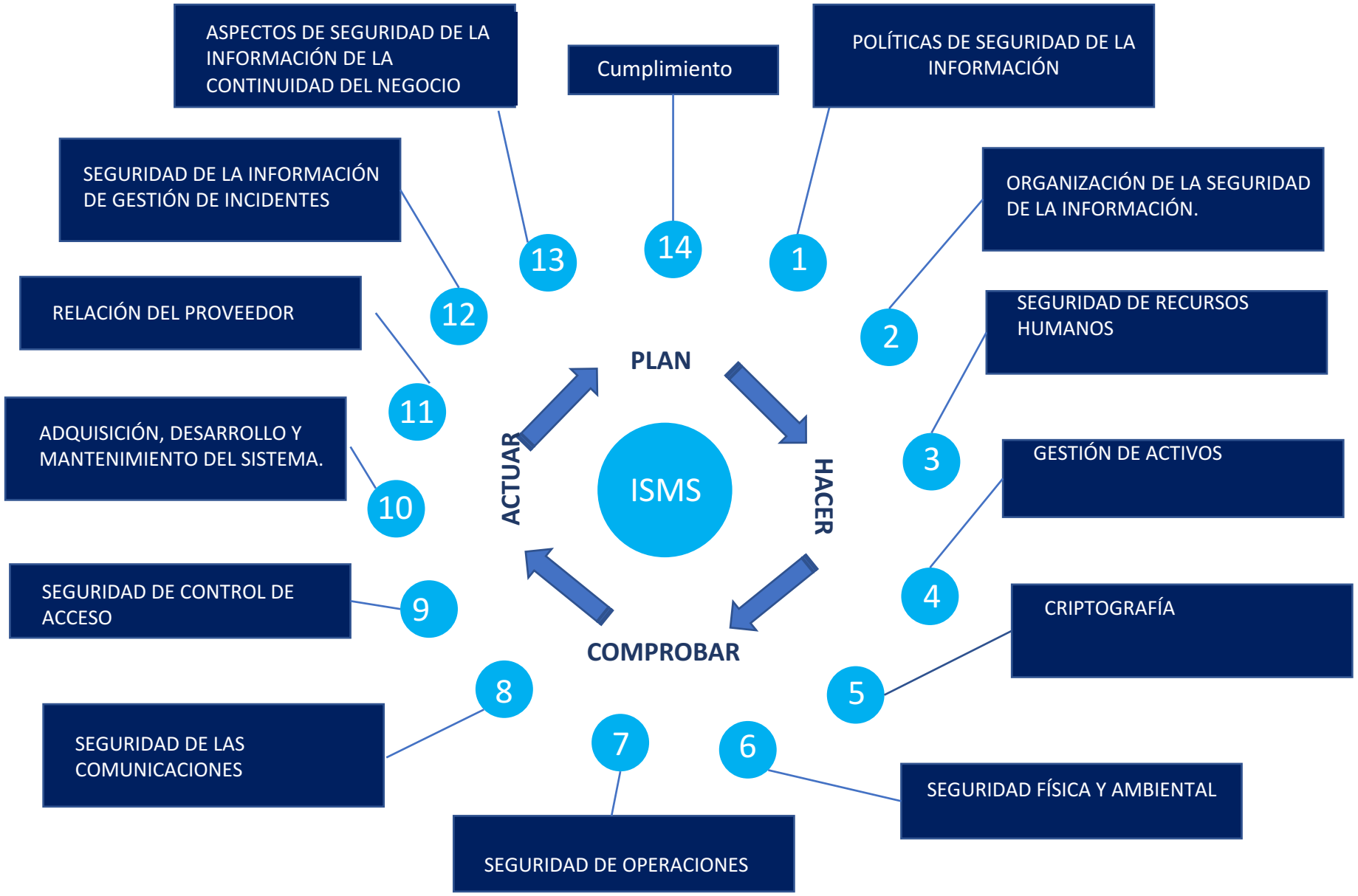
¿Qué Framework Implementar ?

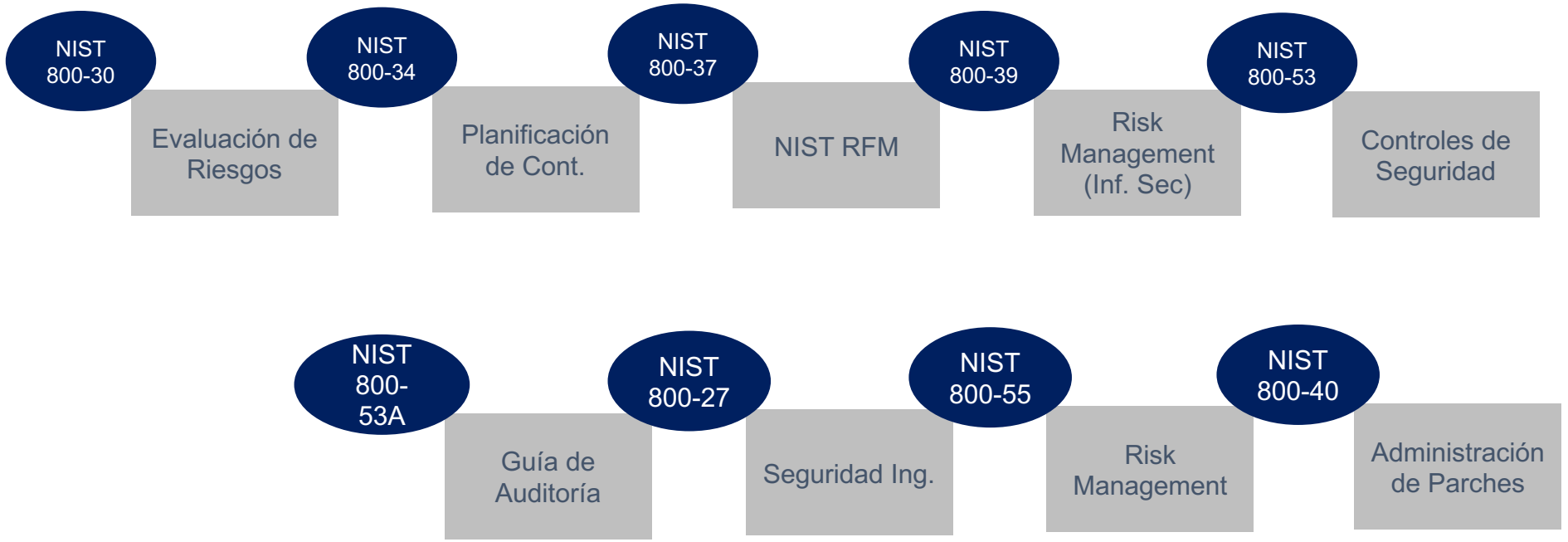
PCI- DSS

PCI – DSS provee una línea base de requerimientos técnicos y operacionales diseñados para proteger los datos del titular de la tarjeta

1. Construir y Mantener redes y sistemas seguros
2. Proteger los Datos del Titular de la Tarjeta
3. Mantener un Programa de Administración de Vulnerabilidades
4. Implementar medidas de control de acceso
5. Monitorear y probar las redes regularmente
6. Mantener una Política de Seguridad de Información

International Organization for Standardization


ISMS
PLAN
HACER
COMPROBAR
ACTUAR
1
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
2
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
3
SEGURIDAD DE RECURSOS HUMANOS
4
GESTIÓN DE ACTIVOS
5
CRIPTOGRAFÍA
6
SEGURIDAD FÍSICA Y AMBIENTAL
7
SEGURIDAD DE OPERACIONES
8
SEGURIDAD DE LAS COMUNICACIONES
9
SEGURIDAD DE CONTROL DE ACCESO
10
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA.
11
RELACIÓN DEL PROVEEDOR
12
SEGURIDAD DE LA INFORMACIÓN DE GESTIÓN DE INCIDENTES
13
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTINUIDAD DEL NEGOCIO
14
Cumplimiento



National Institute of Standards and Technology

Center of Excellence

Identificar	Proteger	Detectar	Responder	Recuperar
Administración de Activos	Control de Acceso	Anomalías y Eventos	Planificación de Respuesta	Planificación de Recuperación
Ambiente de Negocios	Entrenamiento y Awarness	Monitoreo Continuo de Seguridad	Comunicaciones	Mejoramiento
Gobernabilidad	Seguridad de Datos	Proceso de Detección	Análisis	Comunicaciones
Evaluación de Riesgos	Proceso y Procedimientos de Protección de Información		Mitigación	
Estrategia de Administración de Riesgos	Mantenimiento		Mejoramiento	
	Tecnología de Protección			

Mejores Prácticas

OWASP TOP TEN

CIS 20

OWASP TOP TEN

A1 : Inyección de Código	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
A2 : Pérdida de Autenticación	Las funciones de la aplicación relacionados a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
A3 : Exposición a Datos Sensibles	Muchas aplicaciones web y APIs, no protegen adecuadamente datos sensibles, tales como información financiera, de salud o información personalmente identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjeta de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado de almacenamiento y tránsito.

OWASP TOP TEN

A4 : Entidades Externas XML (XXE)	Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URL o archivos internos en servidores no actualizados, escánear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicios (DoS).
A5 : Pérdida de Control de Acceso	Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos.
A6 : Configuración de Seguridad Incorrecta	La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc.

A7 : Secuencia de Comandos en Sitios Cruzados (XSS)	Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada, o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta javascript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar(defacement) los sitios web, o redireccionar al usuario hacia un sitio malicioso.
A8 : Deserialización Insegura	Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.
A9 : Componentes de Vulnerabilidades Conocidas	Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el atacante puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.
A10 : Registro y Monitoreo Insuficiente	El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de procesos internos.

Básico

1. Inventario y Control de Activos de Hardware
2. Inventario y Control de Activos de Software
3. Administración Continua de Vulnerabilidades
4. Uso controlado de Administración de Privilegios
5. Configuración Segura de Hardware y Software sobre dispositivos móviles, laptops, estaciones de trabajo y servidores
6. Mantenimiento, Monitoreo y análisis de Logs de Auditoría

CIS 20

Fundacional

CIS 20

7 Protección Browser Web e Email

8 Defensas de Malware

9 Protección y Limitación de puertos de red, protocolos y servicios

10 Capacidades de Recuperación de Datos

11 **Configuración Segura para dispositivos de red, tales como firewalls, routers y switches**

12 Defensa en Capas

13 Protección de Datos

14 Acceso controlado basado en la necesidad de saber

15 Control de Acceso Wireless

16 Monitoreo y Control


Organizacional
17
Implementar un programa de Awarness y Entrenamiento
18
Aplicación de Software Seguro
19
Administración y Respuesta a Incidentes
20
Test de Penetración y Ejercicios de Red Team
CIS 20

NIST Cybersecurity Framework

Identificar	Proteger	Detectar	Responder	Recuperar
Administración de Activos	Control de Acceso	Anomalías y Eventos	Planificación de Respuesta	Planificación de Recuperación
Ambiente de Negocios	Entrenamiento y Awarness	Monitoreo Continuo de Seguridad	Comunicaciones	Mejoramiento
Gobernabilidad	Seguridad de Datos	Proceso de Detección	Análisis	Comunicaciones
Evaluación de Riesgos	Proceso y Procedimientos de Protección de Información		Mitigación	
Estrategia de Administración de Riesgos	Mantenimiento		Mejoramiento	
	Tecnología de Protección			

Identificar

Administración de Activos

Objetivo de Control	Controles
Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr objetivos comerciales se identifican y administran de manera consistente con su importancia relativa para los objetivos comerciales y la estrategia de riesgo de la organización.	**C1** **Los dispositivos y sistemas físicos dentro de la organización son inventariados.**
	C2 **Control - Las plataformas de software y las aplicaciones dentro de la organización son inventariadas**
	C3 **Control - La comunicación organizacional y los flujos de datos están mapeados**
	C4 **Control - Se catalogan los sistemas de información externos**
	C5 **Los recursos (por ejemplo, hardware, dispositivos, datos y software) se priorizan según su clasificación, criticidad y valor comercial.**
	C6 **Control - Se establecen los roles y responsabilidades de Ciberseguridad para toda la fuerza laboral y terceros interesados (por ejemplo, proveedores, clientes, socios)**

Programa de Auditoría

C1
Los dispositivos y sistemas físicos dentro de la organización son inventariados.

Obtener una copia del inventario de dispositivos físicos y sistemas. Revise el inventario considerando lo siguiente:

- El alcance de los dispositivos y sistemas físicos se basan en el apetito de riesgo de la organización (Por ejemplo, los sistemas que contienen información)
- Integridad del inventario.
- El proceso de recopilación de inventario garantiza que los nuevos dispositivos se recopilen con precisión y de manera oportuna.
- Frecuencia de revisiones de inventario

Programa de Auditoría

C2
Control - Las plataformas de software y las aplicaciones dentro de la organización son inventariadas

Obtener una copia del inventario de software. Revise el inventario considerando lo siguiente:

- El alcance del inventario de software se basan en el riesgo de la organización.
- Integridad del inventario.
- El proceso de recopilación de inventario garantiza que los nuevos software se recopilen con precisión y de manera oportuna.
- Frecuencia de revisiones de inventario

Programa de Auditoría

C3

Control - La comunicación organizacional y los flujos de datos están mapeados

- Asegúrese de que la organización mantenga copias actualizadas y precisas de los diagramas de flujo de datos (DFD), los diagramas de red lógica (LND) y/u otros diagramas para mostrar la comunicación organizacional y el flujo de datos.

Programa de Auditoría

C4
Control - Se catalogan los sistemas de información externos

Si los sistemas de información de la organización están alojados en proveedores externos, obtener una copia del inventario de sistemas externos.

- El alcance del inventario de software se basa en el riesgo de la organización.
- Integridad del inventario.
- El proceso de recopilación de inventario garantiza que los nuevos sistemas se recopilen con precisión y de manera oportuna.
- Frecuencia de revisiones de inventario

Programa de Auditoría

C5
Los recursos (por ejemplo, hardware, dispositivos, datos y software) se priorizan según su clasificación, criticidad y valor comercial.

- Obtenga una copia del programa de clasificación de datos de la organización (la clasificación también se puede identificar en la evaluación de riesgos o en el análisis del impacto en el negocio).
- Revise el programa para detectar si los recursos son clave.

Programa de Auditoría

C6

Control - Se establecen los roles y responsabilidades de Ciberseguridad para toda la fuerza laboral y terceros interesados (por ejemplo, proveedores, clientes, socios)

- Revise las políticas de ciberseguridad, las políticas de seguridad de la información, las descripciones de los puestos de trabajo, los acuerdos, los cuadros RACI, los acuerdos de nivel de servicio (SLA) y/o los contratos para determinar si incluyen funciones y responsabilidades de ciberseguridad.

Puntos de Interes de Auditoría

- Relación Estrategia Ciber vs Estrategia de Negocio
- Roles y Responsabilidades 1era, 2da y 3ra Línea de Defensa
- Políticas y Procedimientos
- Separación de Funciones (Administración vs Monitoreo)
- Metodología de Gestión de Riesgos
- Inventario de Activos, Procesos y Servicios
- Proceso de Gestión de Vulnerabilidades
- Proceso de Gestión de Incidentes
- Casos de Uso y Reglas de SIEM y otros dispositivos
- Controles de Acceso Lógico
- Usuarios Privilegiados (PIM)
- Planes de Continuidad de Negocio (BCP, DRP)
- Planes de Crisis y Pruebas de Simulación
- Proveedores Críticos (SAE16 vs SOC2)

Preguntas & Respuestas