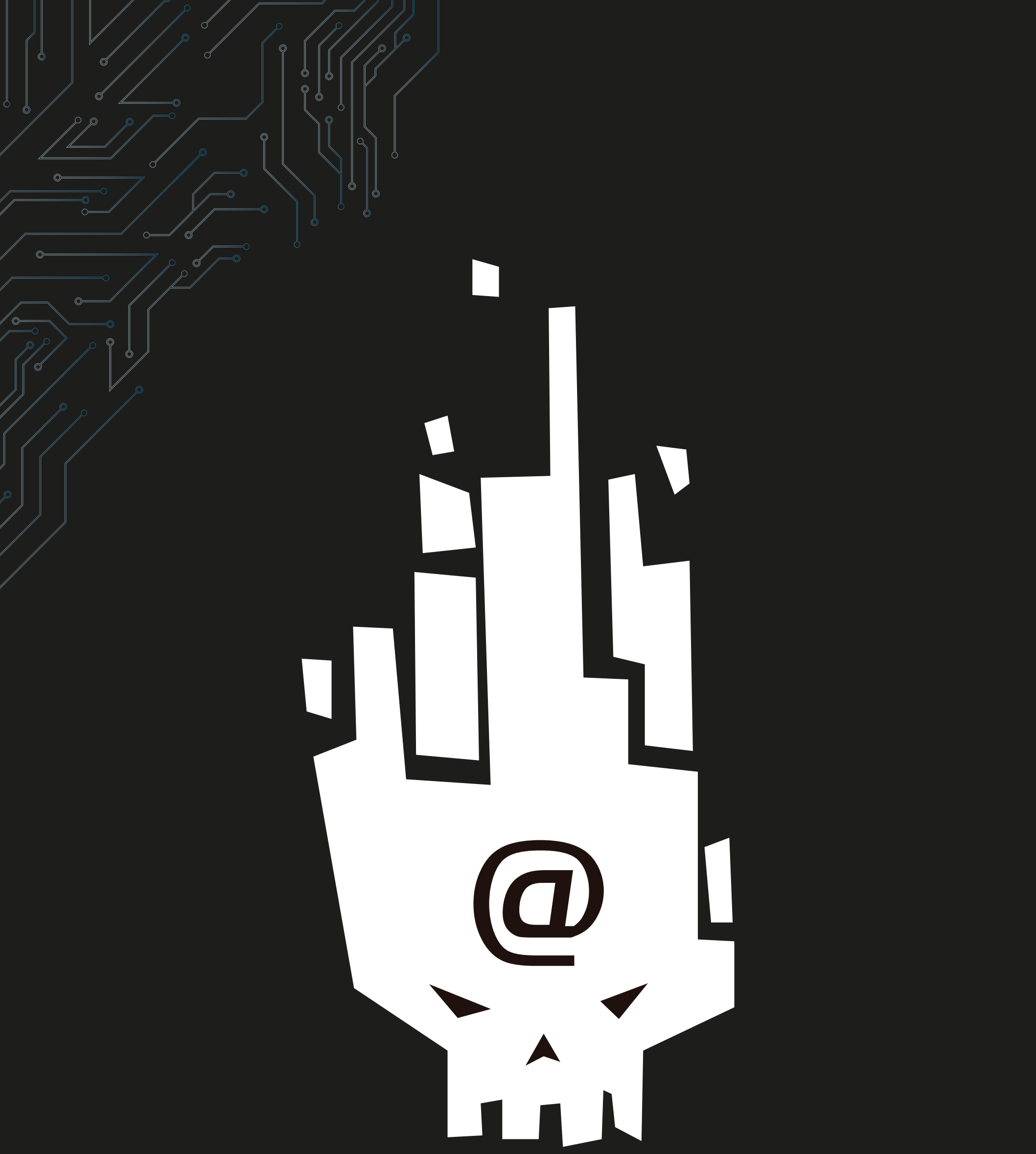


BLACK HAT ARCHETYPE

Desmantelando al Hacker

AÑO Y FECHA:

ORGANIZACIÓN:

NOMBRE:

CORREO ELECTRÓNICO:

Bienvenido a una nueva experiencia, en Black Hat Archetype tenemos un único propósito y es brindarte las herramientas necesarias para que tu organización esté preparada frente a los retos del mundo moderno, gracias a nuestro equipo de trabajo y experiencia logramos estructurar una guía en los campos de Seguridad Informática, Seguridad de la Información, Ciberseguridad y Seguridad Digital. Te invitamos a que vivas esta experiencia de la mano de nuestros asesores especializados, esperamos sorprenderte.

CONTRO DE SEGURIDAD INFORMATICA

CONTRO DE SEGURIDAD DE LA INFORMACIÓN

CONTROLES CRITICOS DE CIBERSEGURIDAD

CONTRO DE SEGURIDAD DIGITAL

NOSOTROS

Somos una compañía con más de 17 años de experiencia en la implementación y el soporte de proyectos de seguridad informática, seguridad de la información, ciberseguridad y ciberdefensa, contamos con un laboratorio de investigación y desarrollo el cual ayuda a soportar los procesos de innovación de la compañía; esto nos ha permitido superar los diferentes retos propuestos por nuestros clientes; gracias al trabajo y el compromiso de los funcionarios de la empresa contamos con las certificaciones ISO 9001 , ISO 14001, ISO 45001, 27001, lo que nos permite ofrecer un servicio de calidad con seguridad, diferencial y personalizado.

ISO 9001:2015 BUREAU VERITAS Certification

ISO 14001:2015 BUREAU VERITAS Certification

ISO 45001:2018 BUREAU VERITAS Certification

ISO 27001:2013 BUREAU VERITAS Certification

MISIÓN

Retornar el valor de la seguridad de la información bien implementada a nuestros clientes.

VISIÓN

Ser la empresa y escuela de los nuevos modelos de seguridad de la información.

BLACK FORTRESS

BHA NEWS

NUESTROS CONTACTOS

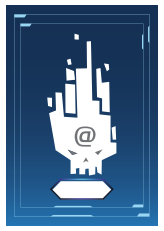
www.desmantelandoalhacker.net

bha news ***bha_cybersecurity*** ***black-hat-archetype*** ***bha - black hat archetype***

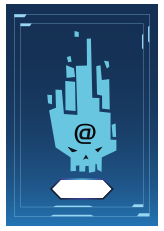
+57 1 8053207 Bogotà D.C. ***+57 4 2315524 Medellìn*** ***+57 317 853 42 00 / +57 316 555 68 39***

PUNTOS DE SEGURIDAD

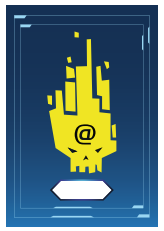
COMODINES



Análisis por vulnerabilidad por terceros.

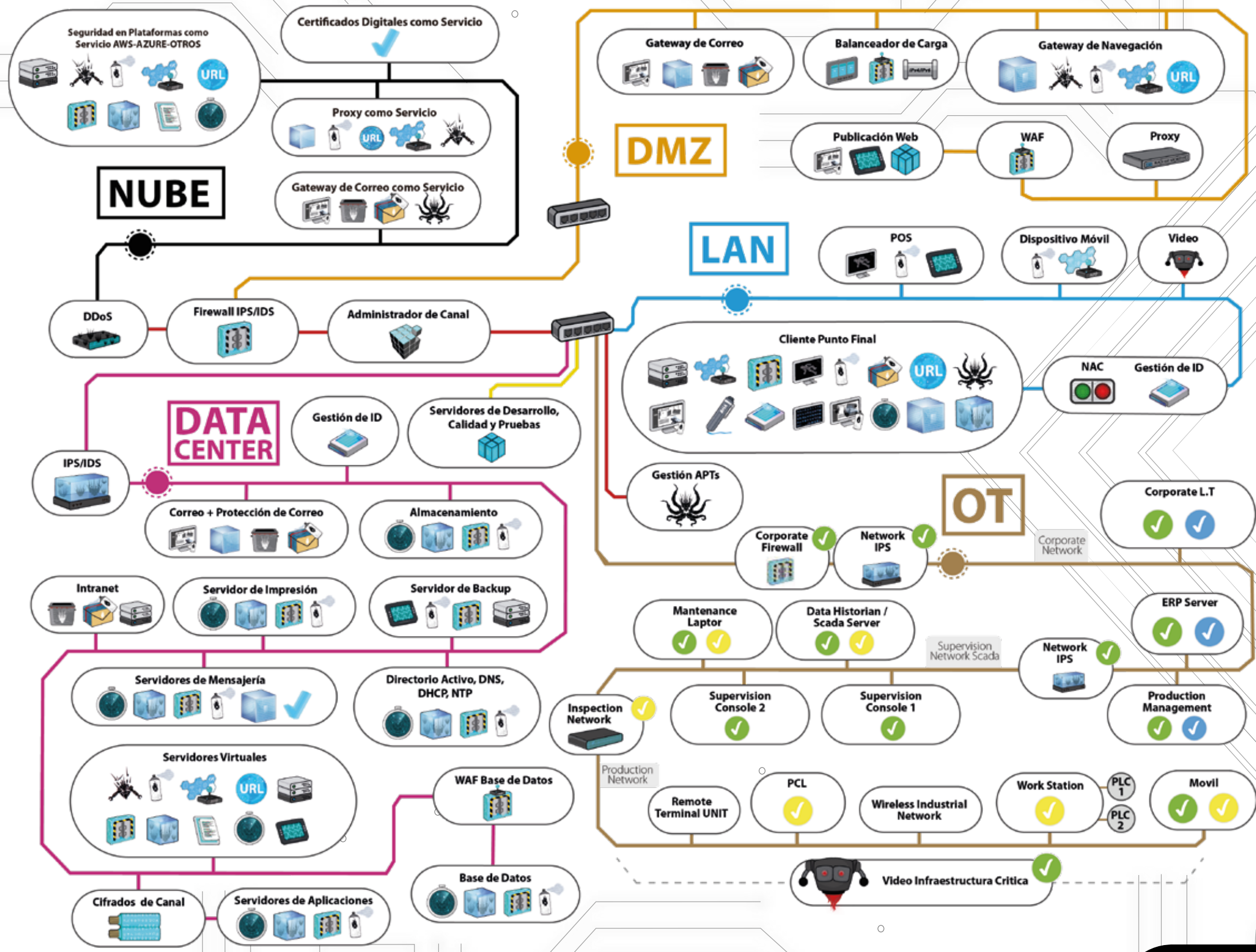


Educación continua.



Ejercicios de continuidad del modelo de negocio.

Ejercicios de Red Team y Blue Team.



BLACK HAT ARCHETYPE
DESMANTELANDO AL HACKER

SOLUCIONES TECNOLÓGICAS

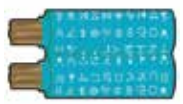
Educación continua.

Análisis por vulnerabilidad por terceros.

Ejercicios de continuidad del modelo de negocio.

Ejercicios de red team y blue team.


Switch


Cifrado de canal


Proxy


Anti Phishing


IPS


Anti Spam


Balanceador de Corga

Controlador de URL


Controlador de URL


Controlador de URL

IPv4/ IPv6


Antivirus de Correo


Administrador de Canal


Gestor de identidad


NAC Network Acess Control


Control de Aplicaciones


Cifrado


Monitoreo de Integridad


Fuga de Información


EDR Analisis Forense


AntiBot

Firmas Digitales


DDoS


Antivirus de Navegación


Backup


Correlación de logs


Certificado Digital


Control de Vulnerabilidad


Control de Amenazas Avanzadas


Ciber camara


Análisis de vulnerabilidad


Servidor virtual


Antimalware


Seguimiento Forense

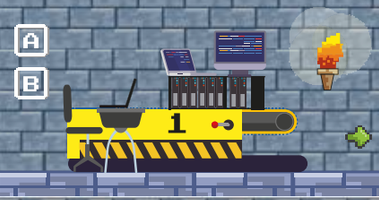
Seguridad Pasiva


Seguridad Activa

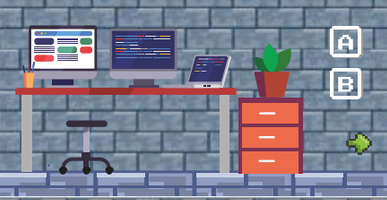
CONTROLES DE SEGURIDAD
INFORMÁTICA

Defiende el castillo.

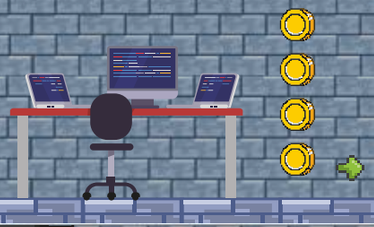
1. Inventarios de Equipos Autorizados y no Autorizados.



2. Inventarios de Software Autorizado y no Autorizado.



3. Reglas de Configuración Basicas de Hardware y Software en Equipos y Servidores.



4. Diagramas de SegmentaciOn de Red.

5. Clasificacion y Redundancia de Soluciones de Seguridad por las Capas de Red.

6. Analisis de Vulnerabilidades .

7. Software Antimalware.

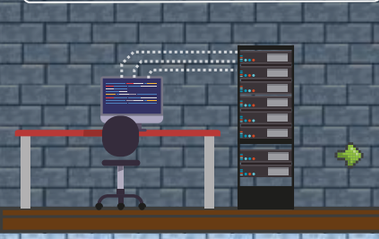
8. Software de Control de Aplicaciones.

¡¡BIEN HECHO!!

13. Instalar y Configurar Soluciones de Defensa Perimetral.

12. Controlar y limitar el uso de puertos, protocolos y servicios en los equipos de red.

11. Configuraciones Seguras para Firewall´s, Switches y Routers.

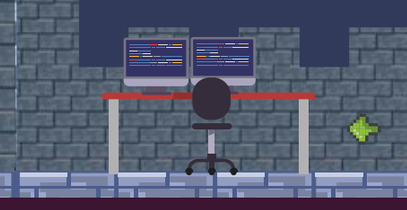


10. Capacidad de Generación de Copias de Respaldo.

9. Control de Redes Inamlambricas.

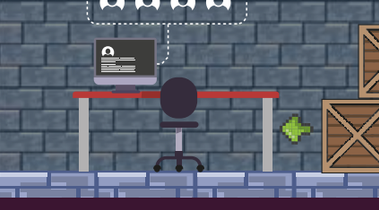
Cuidado! siguiente nivel.

El oro es tuyo!

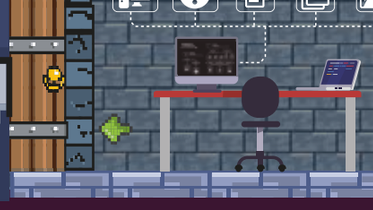


14. Monitoreo y Analisis de Logsa.

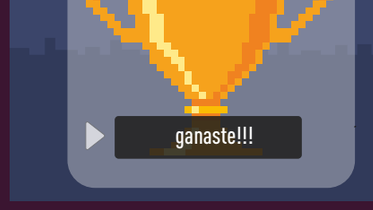
15. Monitoreo y Control de las Cuentas de Usuario.

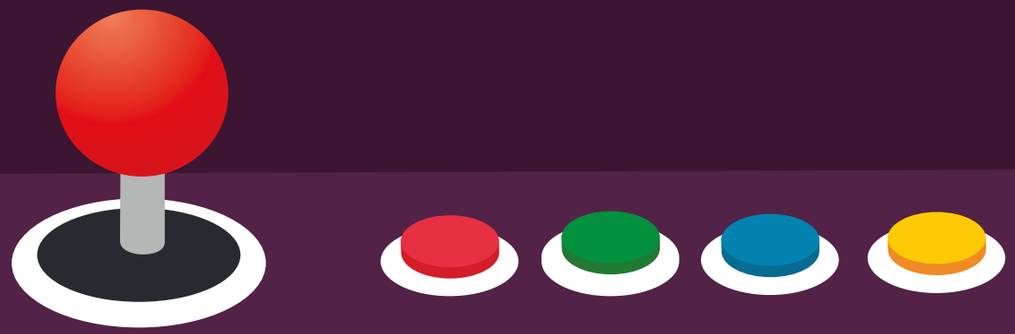


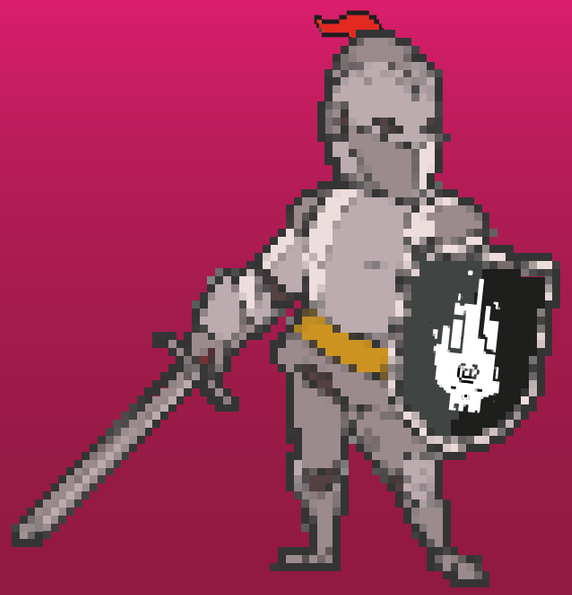
16. Control de Fuga de Información.



ganaste!!!







SEGURIDAD INFORMÁTICA = SEGURIDAD POR CAPAS

Es la practica de prevenir y detectar el acceso no autorizado a un sistema informático mediante el uso de solución tecnológicas y el análisis de logs de las mismas.

Educación continua.

Análisis por vulnerabilidad por terceros.

Ejercicios de continuidad del modelo de negocio.

Ejercicios de Red Team y Blue Team.

Durante el desarrollo del juego ve marcando con una X las casillas de los controles de seguridad informática que actualmente tiene tu organización.

01 02 03 04 05 06 07 08 09 10 11

12 13 14 15 16

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

23 Pruebas de Penetración y Ejercicios de "Red Team".

22 Procesos Basados en Ingeniería Segura.

21 Capacidad de Respuesta a Incidentes.

20 Control de Fuga de Información con Políticas Documentadas y con Análisis de Eventos.

19 Monitoreo y Control de las Cuentas de Usuario.

18 Controles de Acceso a la Red Basados en "Lo que Necesita Saber".

17 Almacenamiento, Mantenimiento, Monitoreo y Análisis de Logs.

16 Instalar y Configurar Soluciones de Defensa Perimetral.

15 Controlar y Limitar el Uso de Permisos de Administrador.

14 Controlar y limitar el Uso de Puertos, Protocolos y Servicios en los Equipos de Red.

13 Configuraciones Seguras para Firewall´s, Switches y Routers.

12 Entrenamiento y Verificación de los Perfiles de Personal del Área de Seguridad.

11 Entrenamiento y Verificación de los Perfiles del Personal del Área de Seguridad.

10 Monitoreo, Gestión y Control de Redes Inalámbricas.

9 Software de Control de Aplicaciones.

8 Software de Seguridad de Punto Final en Equipos y Servidores.

7 Análisis de vulnerabilidades y de Remediación Continuos.

6 Diagramas de Disponibilidad de Red de Activos Físicos Críticos.

5 Etiquetar la Información de uso, como mínimo como: Confidencial de Uso Reservado y Limitado y de Uso Privado y Público.

4 Diagramas de Arquitectura donde se Identifiquen los Puntos por donde pase la Información Relevante en Tránsito, y, la Información Relevante en Reposo.

3 Diagramas de Arquitecturas Identificando la Disponibilidad, la Integridad y la Confidencialidad.

2 Inventario de Software Autorizado que Consuma Información Relevante.

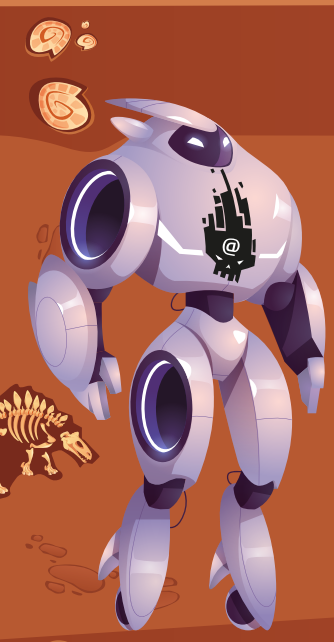
1 Inventario de Equipos Autorizados que consuman Información Relevante.

CONTROLES DE SEGURIDAD

DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN = SEGURIDAD ACTIVOS LÓGICOS

Es la practica de generar seguridad, confidencialidad, integridad y disponibilidad sobre los datos mediante el uso de recursos tecnológicos y convencionales.



Durante el desarrollo del juego ve marcando con una X las casillas de los controles de seguridad de la información que actualmente tiene tu organización.

01 ☐	02 ☐	03 ☐	04 ☐	05 ☐	06 ☐
07 ☐	08 ☐	09 ☐	10 ☐	11 ☐	12 ☐
13 ☐	14 ☐	15 ☐	16 ☐	17 ☐	18 ☐
19 ☐	20 ☐	21 ☐	22 ☐	23 ☐	

Educación continua.

Análisis por vulnerabilidad por terceros.

Ejercicios de continuidad del modelo de negocio.

Ejercicios de Red Team y Blue Team.

CONTROLES CRÍTICOS DE CIBERSEGURIDAD

INICIO

1. Inventario De Equipos Autorizados y No Autorizados.

2. Inventarios de Software Autorizado y no Autorizado.

3. Reglas de Configuración Básicas de Hardware y Software en Equipos y Servidores.

4. Análisis de Vulnerabilidades y de Remediación Continuos.

5. Software de Seguridad de Punto Final en Equipos y Servidores.

6. Diagramas de Disponibilidad de Red de Activos Lógicos Críticos.

7. Diagramas de Disponibilidad de Red de Activos Físicos Críticos.

8. Software de Control de Aplicaciones.

9. Monitoreo, Gestión y Control de Redes Inalámbrica.

10. Generación de Copias de Respaldo Periódicas.

11. Entrenamiento y Verificación de los Perfiles del Personal del Área de Seguridad.

12. Configuraciones Seguras para Firewall´s, Switches y Routers.

13. Controlar y Limitar el uso de Puertos, Protocolos y Servicios en los Equipos de Red.

14. Controlar y Limitar el uso de Permisos de Administrador en los Equipos.

15. Instalar y Configurar Soluciones de Defensa Perimetral.

16. Recopilación, Almacenamiento, Mantenimiento, Monitoreo y Análisis de Logs

17. Controles de Acceso a la Red Basados en "Lo Que Necesita Saber"

18. Monitoreo y Control de las Cuentas de Usuario.

19. Control de Fuga de Información con Políticas Documentadas.

20. Capacidad de Respuesta a Incidentes.

21. Procesos Basados en Ingeniería Segura.

22. Pruebas de Penetración y Ejercicios de "Red Team"

BLACK HAT ARCHETYPE

FINAL

BLACK HAT ARCHETYPE

CONTROLES CRÍTICOS DE CIBERSEGURIDAD

CIBERSEGURIDAD =SEGURIDAD DE PROCESOS CRÍTICOS , ACTIVOS CRÍTICOS FÍSICOS Y ACTIVOS LÓGICOS CRÍTICOS

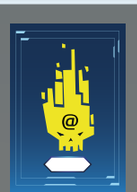
Es la practica de generar seguridad, confidencialidad, integridad, disponibilidad, resiliencia en los activos lógicos y físicos mediante el uso de recursos tecnológicos y convencionales.

Durante el desarrollo del juego ve marcando con una X las casillas de los controles de ciberseguridad que actualmente tiene tu organización.

01	02	03	04	05	06	07	08	09	10	11
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Educación continua.

Análisis por vulnerabilidad por terceros.



Ejercicios de continuidad del modelo de negocio.

Ejercicios de Red Team y Blue Team.

CONTROLES DE SEGURIDAD DIGITAL

24. Control de Fuga de Información con Políticas Documentadas y con Análisis de Eventos.

23. Procesos Basados en Ingeniería Segura.

22. Capacidad de Respuesta a Incidentes .

21. Control de Fuga de Información con Políticas Documentadas y con Análisis de Eventos.

20. Monitoreo y Control de las Cuentas de Usuario.

19.Controles de acceso a la Red basados en "Lo que Necesita Saber".

18. Almacenamiento, Mantenimiento, Monitoreo y Análisis de Logs.

17. Instalar y Configurar Soluciones de Defensa Perimetral.

16. Controlar y Limitar el Uso de Permisos de Administrador.

15. Controlar y Limitar el Uso de Puertos, Protocolos y Servicios en los Equipos de Red.

14. Configuraciones Seguras para Firewall´s, Switches y Routers.

13.Entrenamiento y Verificación de los Perfiles del Personal del Área de Seguridad.

12. Generación de Copias de Respaldo Periódicas.

11. Monitoreo, Gestión y Control de Redes Inalámbricas .

10. Software de Control de Aplicaciones.

9. Software de Seguridad de Punto Final en Equipos y Servidores.

8. Análisis de vulnerabilidades y de Remediación Continuos.

7. Reglas de Configuración Básicas de Hardware y Software en Equipos y Servidores.

6. Etiquetar la Información de Uso, Mínimo: Confidencial de Uso Reservado, Limitado y de Uso Privado y Público.

5. Diagramas de Arquitectura donde se Identifiquen los Puntos por donde pasa la Información Relevante en TI.

4. Diagramas de Arquitecturas Segmentados y Basadas en el Consumo por parte de las Identidades Virtuales.

3. Diagramas de Arquitecturas Identificando la Disponibilidad, la Integridad y la Confidencialidad.

2. Inventario de Software Autorizado que Consuma Información Relevante.

1. Inventario de Equipos Autorizados que Consuman Información Relevante.

SALTAR

DESLIZAR

CONTROLES DE

SEGURIDAD DIGITAL

SEGURIDAD DIGITAL = IDENTIDAD VIRTUAL

Es la practica de generar seguridad, confidencialidad, integridad y disponibilidad sobre los datos mediante el uso de recursos tecnológicos y convencionales.

Durante el desarrollo del juego ve marcando con una X las casillas de los controles de seguridad digital que actualmente tiene tu organización.

01 ☐	02 ☐	03 ☐	04 ☐	05 ☐	06 ☐
07 ☐	08 ☐	09 ☐	10 ☐	11 ☐	12 ☐
13 ☐	14 ☐	15 ☐	16 ☐	17 ☐	18 ☐
19 ☐	20 ☐	21 ☐	22 ☐	23 ☐	

Educación continua.

Análisis por vulnerabilidad por terceros.

Ejercicios de continuidad del modelo de negocio.

Ejercicios de red team y blue team.

SOLUCIONES TECNOLOGICAS

Gracias a nuestra campaña ambiental ***Ciberseguridad Por Un Planeta Vivo*** cada compra realizada a Black Hat Archetype es igual a árboles sembrados.

Haz parte del cambio

Con una visión clara de nuestra responsabilidad y el apoyo de diferentes fundaciones desarrollamos diversas campañas a favor del ambiente. Cada negocio realizado por parte de Black Hat Archetype y tu compañía se vera reflejado en la siembra de arboles nativos en diferentes zonas de Colombia, ¿que esperas para hacer parte del cambio?

CIBERSEGURIDAD POR UN PLANETA VIVO

Nuestros sistemas de servidores funcionan con energía solar.

¿TU ORGANIZACIÓN ESTÁ EN PELIGRO?

PRUEBAS DE CIBERSEGURIDAD

1. Diagnóstico de Seguridad
2. Prueba de Penetración de Seguridad
3. Ponderación de Seguridad

SOLICITA TU PRUEBA DE CONCEPTO GRATIS

C.M.U

Detecta las anomalías dentro de tu infraestructura de una manera eficaz y eficiente, para tomar decisiones rápidas sin discusiones, permitiendo una operatividad óptima.

Acelera y centraliza la detección de amenazas, la respuesta a incidentes y la gestión del cumplimiento normativo para sus entornos en la nube, locales e híbridos.

SOC NOC

CENTRO DE MONITOREO UNIFICADO

GESTION DE MONITOREO A TU MEDIDA IT/OT

OBTÉN TU CERTIFICACIÓN | ISO | PCI

CONSULTORÍAS PROFESIONALES

El servicio de consultoría Black Hat Archetype está desarrollado con los más altos estándares de calidad, gracias a nuestros profesionales experimentados hemos logrado satisfacer las necesidades de nuestros clientes, afrontando juntos momentos cruciales para las organizaciones como: la ampliación de usuarios, apertura de mercados y operaciones en el extranjero, nuevas regulaciones e incidentes de seguridad crítico.

SEGURIDAD DIGITAL

CONSULTORÍA EN

- Ciberseguridad
- Seguridad de la Información
- Seguridad Informatica

¿TU MODELO DE NEGOCIO SE BASA EN PROGRAMACIÓN COBOL ?’

- ACTUALIZA TU COMPAÑÍA
- AHORRA DINERO
- AUMENTA TU COMPETITIVIDAD

COBOL

C SHARP | JAVA | VISUAL ESTUDIO | OTROS

1959 ——— *Ahora*

VIAJE EN EL TIEMPO