Ecuador, 03 de Octubre de 2019

Señores
SOCIEDAD EMPRESARIAL DE GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL INTERCULTURAL DEL CANTÓN SAQUISILÍ
Atentamente: Chariguamán Gilson

Referencia:
Propuesta prestación de servicios profesionales para un estudio de seguridad y Auditoria de seguridad informática integral-Técnica del tipo Hacking Ético Modalidad White Box (Caja Blanca)

Cordial Saludo,

Respecto a las necesidades de la empresa **Sociedad de Cliente ficticio** de realizar un estudio de seguridad informática preventivo con el objetivo de poder auditar la eficacia y eficiencia de los actuales controles de seguridad de la infraestructura tecnológica que opera en la empresa en mención, se presenta la siguiente propuesta.

La presente propuesta se estructura de la siguiente manera:

1. Objetivo General del servicio
2. Objetivos Específicos del servicio
3. Alcances
4. Acuerdos de confidencialidad y legalidad
5. Metodología de auditoria utilizada
6. Tipos de análisis técnicos de seguridad que se pueden hacer
7. Fases de las auditorías técnicas de seguridad del tipo Hacking ético y/o Pentesting
8. Tipos de pruebas a realizar
9. Talento humano que realiza el estudio y auditorias de seguridad
10. Herramientas (Software) que apoyan y automatizan el estudio y auditorias de seguridad
11. Buenas prácticas y estándares de seguridad que se usan como guías y criterios en el estudio y auditorias de seguridad
12. Registros de vulnerabilidades
13. Entregables
14. Generalidades
15. Propuesta económica
16. Valores agregados
17. Generalidades

1. Objetivo general del servicio.

El objetivo es determinar por medio de un estudio y auditoria de seguridad informática la situación actual del cliente ficticio, en lo que respecta a la administración de seguridad informática implementada y en operación en la infraestructura tecnológica de la entidad y/o empresa.

1.2 Objetivos Específicos del servicio

- ✓ Evaluar la efectividad de los controles definidos y proponer nuevos controles, de ser necesarios, con el fin de minimizar la exposición de los riegos

- ✓ Realizar un análisis de amenazas basado en fortalezas y debilidades de la infraestructura de Seguridad Informática actual de la entidad

- ✓ Definición de criticidad de los activos de información dentro de la infraestructura tecnológica que se define como alcance en la presente propuesta.

- ✓ Definir matriz de riesgos para minimizar la probabilidad de su materialización, incluir:

    - Análisis de impacto por cada riesgo (el análisis de impacto debe facilitar la clasificación de los activos de TI de acuerdo a su criticidad)
    - Determinación del impacto cualitativo y cuantitativo por pérdida de integridad
    - Disponibilidad y confidencialidad de los activos de TI

- ✓ Determinar los problemas y debilidades de seguridad en los elementos de la red descritos en la infraestructura tecnológica que se define como alcance en la presente propuesta, incluyendo una clasificación de riesgo sobre cada elemento por cada vulnerabilidad encontrada. Para tal efecto se deberá hacer uso, entre otras, tanto de herramientas especializadas automáticas como de la aplicación de técnicas especializadas de hacking ético

- ✓ Efectuar el test de intrusión del tipo Hacking Ético caja blanca, interno y externo, a la plataforma tecnológica que se define como alcance en la presente propuesta, y realizando las pruebas de seguridad que se definen en el ítem "Tipos de pruebas a realizar "del presente documento.

- ✓ Realizar los respectivos informes técnicos, ejecutivos, y planes de acción para cada uno de los hallazgos identificados.

3. Alcance

El alcance la presente propuesta, son los XYZ servidores correspondientes a la Infraestructura tecnológica de la empresa Cliente ficticio, con sus respectivas aplicaciones, servicios de red, dispositivos de red, seguridad, y bases de datos.
Realizar los diferentes test de intrusión del tipo Hacking Ético caja blanca, interno y externo, a la plataforma tecnológica que se define como alcance en la presente propuesta.

Lista de chequeo auditoria de seguridad del tipo Penetration Testing

Criterio de Evaluación	*Pregunta (Cumplimiento)*	*Nivel (Infraestructura/Aplicación)*	*Comentarios (Hallazgos)*	*Cumple*	*No cumple*	*No Aplica*	*Observaciones y Comentarios*	*Impacto Tecnico*	*Impacto*
Control OWASP A2 –Secuencia de Comandos en Sitios Cruzados (XSS)	La aplicación es vulnerable a ataques del tipo Secuencia de Comandos en Sitios Cruzados (XSS- Cross site	Aplicación							
Control OWASP A1 –Inyección	La aplicación es vulnerable a inyecciones del tipo SQL Injection o LDAP Injection	Aplicación							
Control OWASP A3 – Pérdida de Autenticación y Gestión de Sesiones	La aplicación presente vulnerabilidades que permitan a un usuario malicioso obtener información relevante, tales como, cuentas expuestas, contraseñas, identificadores de sesión entre otros.	Aplicación							
Control OWASP A3 – Pérdida de Autenticación y Gestión de Sesiones	Los inicios del sesión en el portal tienen un tiempo de caducidad	Aplicación							
	Se cierra el navegador web que conecta a la aplicación estando en una sesión iniciada, si este se vuelve								

4. Acuerdos de confidencialidad y legalidad:

CODSP garantiza al cliente absoluta reserva y confidencialidad en el manejo de la información y de las vulnerabilidades identificadas en los servidores evaluados. Lo anterior mediante la firma compulsada en Notaria de un acuerdo de confidencialidad entre ambas partes (CODSP y El cliente)

Antes de la ejecución de cualquier prueba de seguridad en el sistema objetivo de evaluación, se deben de realizar los respectivos acuerdos de confidencialidad y tratamiento que se le dará a la información que se logre recolectar e identificar durante las pruebas de seguridad. Para darle complimiento a lo anterior, se realiza de forma ordenada lo siguiente:

- ✓ Firmas de acuerdos de confidencialidad autenticados (Compulsados) entre ambas partes (Consultor CODSP y Empresa Cliente).
- ✓ Presentación del personal y hojas de vida de las personas que van a ejecutar el estudio y las pruebas de seguridad informática a nivel interno y externo
- ✓ Acuerdo de tratamiento de la información **(Protección, Cifrado y codificación de información del cliente)**

5. Metodología de auditoria utilizada

Al ser un estudio estructurado y auditoría de seguridad informática, se sigue de forma secuencial la siguiente metodología de auditoria:

- ✓ Reunión de apertura
- ✓ Entrevistas de auditoria
- ✓ Ejecución de entrevistas y pruebas técnicas
- ✓ Presentación de informes
- ✓ Presentación de hallazgos (no conformidades, acciones de mejora, entre otros)
- ✓ Reunión de cierre de auditoria
- ✓ Seguimientos a planes de acción
- ✓ Cierre de auditoria

6. Tipos de análisis técnicos de seguridad que se pueden hacer

Es importante que como futuros clientes de la empresa CODSP, tengan presente los tipos de Auditoria técnica que se llevan a la práctica en CODSP, las cuales son de 3 tipos de forma general.

6.1. Análisis de Vulnerabilidades (Vulnerability Assessment): Este tipo de pruebas es medianamente intrusiva, y lo que se busca es identificar una serie de vulnerabilidades en los sistemas evaluados, con el fin de clasificarlas, y presentarlas de forma estructurada en un informe.

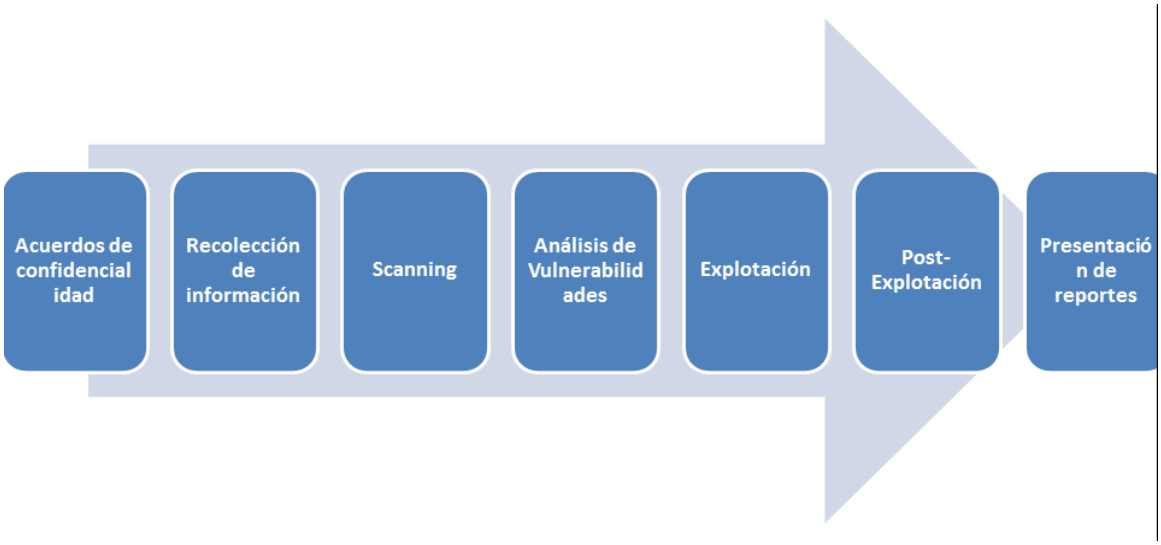
6.2. Test de Intrusión (Penetration Testing) En este tipo de pruebas, se hace también un análisis de vulnerabilidades frente al objetivo, pero además se buscan explotar y aprovechar las vulnerabilidades, para poder comprometer el sistema. Posteriormente se entregan informes técnicos y ejecutivos. Es un tipo de auditoria de seguridad más invasiva que el análisis de vulnerabilidades.

6.3.Hacking Ético: En este tipo de prueba se hacen las dos pruebas anteriormente mencionadas, pero la diferencia con el Test de Intrusión, es que en el Hacking Ético es más completo, todo dispositivo(Firewall, IDS, Router) que se encuentre el analista de

seguridad /Hacker ético) en el camino de la evaluación de los objetivos, se convierte en un blanco de evaluación, con lo que las pruebas se realizan más completas y rigurosas, además de que si se pacta de forma anticipada con el cliente, se pueden realizar pruebas del tipo "Denegación de Servicio e Ingeniería Social", incluso Auditorias del tipo Pentesting físico.

7. Fases de las auditorías técnicas de seguridad del tipo Hacking ético y/o Pentesting)

El proceso metodológico de auditoría informática intrusiva que se llevará a la práctica, según las necesidades y alcance del cliente , es del tipo **Hacking Ético a la infraestructura tecnológica definida como alcance en la presente propuesta**, y se realiza siguiendo de forma estricta y secuencial los siguientes pasos:



Nota: Durante el desarrollo de todas las fases de evaluación, se tiene presente que al ser una prueba del tipo **Caja Blanca (White Box),** el cliente y el evaluador del sistema, conocen los alcances de evaluación, en lo que respecta a las direcciones IP de los objetivos a evaluar, horas de ejecución de los test de intrusión, Equipos y dirección IP de donde se ejecuta el análisis. Además de las herramientas que van a utilizar los evaluadores de seguridad (Profesionales Hackers Éticos) a nivel de aplicación, de sistemas operativos y de Appliance.

A continuación se explica al cliente de forma breve y resumida lo que se llevara a la práctica en cada una de las fases:

7.1 Fase de acuerdos de confidencialidad y pactos sobre trato de la información: Antes de la ejecución de cualquier prueba de seguridad en el sistema objetivo (Cliente) de evaluación, se deben de realizar los respectivos acuerdos de confidencialidad y tratamiento que se le dará a la información que se logre recolectar e identificar durante las pruebas de seguridad. Para darle complimiento a lo anterior, se realiza lo siguiente:

- ✓ Firmas de acuerdos de confidencialidad autenticados entre ambas partes (CODSP y el cliente).
- ✓ Presentación del personal y hojas de vida de las personas que van a ejecutar las pruebas de seguridad a nivel interno y externo
- ✓ Acuerdo de tratamiento de la información **(Cifrado de Información)**

Luego de que se acuerden de forma estructurada los tratamientos y aplicación de confidencialidad a la información, se procede a la ejecución de las pruebas y técnicas, las cuales se describen a continuación:

7.2 Fase Recolección de información: Al ser una prueba de **Hacking Ético**, del tipo **Caja Blanca (White Box),** el evaluador ya conoce los sistemas que se van a evaluar, sin embargo se arma un completo perfil mediante el apoyo de reconocimiento pasivo y activo, para cada objetivo (servidor y servidores asociados, segmentos de red, Routers Públicos/Privados,) haciendo uso de técnicas tradicionales de recolección de información y/o "Footprinting, tales como: **DNS Trasfer Zone, Google Hacking, Extracción de metadatos, OSINT, entre otros**, sobre los host que se tienen definidos de forma previa como alcance de evaluación a nivel del estado de seguridad en el que se encuentran. Esta fase en especial aplica para procesos de auditoria del tipo Hacking ético externo.

7.3 Fase de Scanning : Se llevan a la práctica procesos de escaneo de puertos avanzados, mapeo de la arquitectura de la red, Ping-(Sweeping), Banner Grabbing, e identificación de servicios con sus respectivas versiones, además de identificación de trazar de rutas de red, host asociados, y que se puedan ver desde el exterior.

7.4 Fase de Análisis de Vulnerabilidades: Se realiza proceso de identificación y clasificación de vulnerabilidades, haciendo énfasis en las capa 3 (red), 4 (Trasporte) y 7 (Aplicación) del modelo de referencia OSI. Además de tener presentes vulnerabilidades humanas y funcionales en los sistemas de información definidos dentro del alcance de la prueba de seguridad.

7.5 Fase de Explotación: Con respecto a las vulnerabilidades encontradas, se hace pruebas de negación de servicios (DoS), y explotación de vulnerabilidades críticas, que puedan comprometer la seguridad del sistema. "Las pruebas de negación de servicio y explotación solo se hacen con la previa autorización del cliente". **Es importante tener presente que los procesos de explotación se hacen de forma regulada y controlada, según las leyes informáticas que apliquen a la localización geográfica del servidor, dispositivo de red, dispositivo de seguridad y/o hosts a evaluar.**

En caso de encontrarse vulnerabilidades Criticas, se explota la vulnerabilidad, se intenta escalar privilegios, y se toman algunas muestras de información, además de que se dejan pruebas de intrusión. Las vulnerabilidades que se tratan de explotar son del lado servidor y del lado cliente. **Es importante tener presente que los procesos de explotación se hacen de forma regulada y controlada, según las leyes informáticas que apliquen a la localización geográfica del sitio web a evaluar.**

7.6 Fase complementaria de explotación (POST-Explotación): De forma complementaria se realizan procesos de post-explotación, en los cuales se busca lograr lo siguiente:

- ✓ Cracking (Fuerza Bruta) de Passwords
- ✓ Pivoting hacia otros sistemas
- ✓ Infección de malware (Puertas Traseras, Rootkits, entre otros)

7. Fase de entrega Informes: Por último se analiza toda la información recolectada, para presentarla de forma final por medio un informe estructurado donde se registra el estado de la seguridad de los servidores evaluados, los hallazgos identificados, la clasificación de las vulnerabilidades, el impacto para el negocio y la forma de solucionar los problemas de seguridad encontrados.

Los informes se entregan en formato **Reporte Ejecutivo** (Para personal Directivo, Administrativo y Gerentes) en un lenguaje no técnico, y un **Reporte Técnico** para los Ingenieros, Desarrolladores y Administradores de Tecnologías de Informática y Conectividad (TICs).
Además se orienta en el diseño de un plan de acción para realizar el tratamiento de cualquier vulnerabilidad.

8. Tipos específicos de pruebas a realizar.

Según las necesidades del cliente las pruebas a realizar son las siguientes:

8.1 Pruebas a nivel de Cliente: (Importante tener presente que esta prueba es a nivel de una muestra de equipos de la red a nivel cliente, y de todos los equipos definidos como alcance en la presente propuesta)

- ✓ Debilidades de autenticación
- ✓ Cross Site Script (XSS)
- ✓ Cross Site Request Forgery (CSRF)
- ✓ Ataques Java
- ✓ Ataques de Browser
- ✓ Keylogger
- ✓ PDF maliciosos
- ✓ Ejecutables maliciosos
- ✓ Evasión de sistemas de control y antivirus a nivel cliente

8.2 Pruebas a nivel de Red:

- ✓ Comprobación de password débiles y protocolos de cifrado de password débiles
- ✓ Reconocimiento de Red
- ✓ Sniffing
- ✓ Ataques man-in-the-middle
- ✓ Spoof de DNS
- ✓ ARP-Spoofing
- ✓ Enumeración y Explotación de redes inalámbricas Wi-Fi
- ✓ Scanning
- ✓ Análisis de Vulnerabilidades

8.3 Pruebas alternativas a nivel de Red (Enrutadores):

- ✓ IP-email-Spoof
- ✓ Explotación de Vulnerabilidades
- ✓ Filtering bypass
- ✓ Sniffing
- ✓ Contraseñas débiles en protocolos de administración de Routers y firewalls

8.4 Pruebas a nivel de Sistemas Operativos

- ✓ Identificación de los Sistemas operativos de los equipos objetos de análisis
- ✓ Identificación de los puertos abierto en los objetivos (TCP, UDP)
- ✓ Identificación de los servicios que se están ejecutando en los objetivos.
- ✓ Identificación de vulnerabilidades del S.O.
- ✓ Denegación de Servicios
- ✓ Búsqueda de información sensible accesible por la red, como la existente en las carpetas compartidas

- ✓ Sniffing

8.5 Pruebas a nivel de Servidores Web

- ✓ Identificación del Sistema Operativo de los servidores Objetos de análisis, vulnerabilidades asociadas a no adecuadas prácticas de programación de los mismos
- ✓ Identificación de los Servicios que se están ejecutando en los objetivos
- ✓ Explotación de vulnerabilidades
- ✓ Buffer Overflow (Desbordamientos de memoria)
- ✓ Configuraciones por defecto
- ✓ Negación de Servicios

8.6 Pruebas a nivel de Aplicaciones web

- ✓ Formas
- ✓ Directory Traversal
- ✓ Meta-Caracteres
- ✓ Session Hijacking
- ✓ Códigos de error
- ✓ Buffer Overflow (Desbordamientos de memoria)
- ✓ Rompimiento de Claves
- ✓ XSS
- ✓ SQLi

8.7 Pruebas a nivel de Bases de Datos

- ✓ SQL Injection
- ✓ Consultas Estructurados
- ✓ Claves por Defecto
- ✓ Autenticación de base de datos
- ✓ Extracción de Información Confidencial
- ✓ Análisis de vulnerabilidades de BD

9. Talento, Recurso Humano y Herramientas que apoyan la ejecución del estudio de seguridad y de los procesos de Auditorías técnicas del tipo Hacking Ético (White-Box)

Nuestro talento humano con los siguientes perfiles, le garantiza una alta calidad en los procesos de las pruebas de seguridad informática a sus servidores públicos, tanto a nivel técnico como procedimental.

- ✓ Ingenieros de sistemas con Maestría en Seguridad Informática Internacional.
- ✓ Ingenieros especialistas en Seguridad de Sistemas Operativos
- ✓ Ingenieros certificados como ***Certified Offensive and Defensive Security Professional – CODPS.***
- ✓ Ingenieros capacitados y certificados por el SANS INSTITUTE -**GIAC Certified Incident Handler- SEC560: Network Penetration Testing and Ethical Hacking**
- ✓ Ingenieros certificados en OSCP y CPT con la empresa Offenstive Security, los creadores de Kali Linux

10. Herramientas (Software) que apoyan y automatizan el estudio y auditorias de seguridad

A nivel de herramientas informáticas para Auditorias de seguridad del tipo **Hacking Ético (White-Box)** nuestro equipo de ingenieros se apoya en aplicativos y Appliance tales como:

Durante todo el proceso de ejecución del análisis de seguridad, se ejecutan test automatizados, usando algunas, o todas de las herramientas anteriormente mencionadas, que están a nivel de software libre, como herramientas de pago y

Appliance, sin embargo se hacen pruebas importantes y adicionales llamadas **"Pruebas Artesanales",** donde trasparente a la herramienta usada, se aplica la experiencia y malicia del profesional de seguridad y/o evaluador, al respecto de las pruebas que conforman la auditoría tipo **Ethical Hacking**, identificando situaciones y agujeros de seguridad que no detectan las herramientas automatizadas.

11. Buenas prácticas y estándares de seguridad que se usan como guías y criterios en el estudio y auditorias de seguridad

Para los análisis de seguridad se tiene presente el cumplimiento de las buenas prácticas internacionales a nivel de seguridad de la información, tales como:

- ✓ **Controles Norma ISO 27002**
- ✓ **OSSTMM**
- ✓ **OWASP**
- ✓ **NIST (Technical Guide to Information Security Testing and Assessment)**

12. Registro de Vulnerabilidades:

Todas las vulnerabilidades identificadas, serán registradas aplicando estándares internacionales de registro de vulnerabilidades, tales como:

National Vulnerability Database

OSVDB: The Open Source Vulnerability Database

13. Entregables:

Los entregables esperados en el presente estudio de seguridad son los siguientes:

- ✓ **Informes técnicos.** Se entregan informes y se presentan en una reunión presencial de forma conjunta con las directivas o los Directores de Tecnologías, para conocer los resultados y los hallazgos identificados en la prueba de intrusión (Auditoria de Seguridad) del tipo Hacking Ético (White-Box). En este informe se colocan todas las recomendaciones

- ✓ **El informe ejecutivo (No Técnico**), contiene toda la información necesaria en un lenguaje no técnico, para ser analizado a niveles de exposición y riesgos informáticas para el negocio, por parte de ejecutivos, directores y gerentes.

- ✓ **Plan de acción:** es el documento resultante de las acciones que hay que llevar a la práctica para poder mitigar las vulnerabilidades y debilidades de seguridad identificadas durante las pruebas.

Adicionales: Además se hacen entrega de informes puntuales solicitados por el cliente, según la siguiente necesidad:

Producto 1. Informe detallado y técnico de seguridad con los resultados obtenidos durante todo el proceso de ejecución de las pruebas de intrusión. El informe deberá contener:

- ✓ Descripción de pruebas realizadas
- ✓ Hallazgos encontrados
- ✓ Metodología utilizada
- ✓ Elementos evaluados
- ✓ Puertos y servicios habilitados
- ✓ Listado de vulnerabilidades encontradas en la plataforma tecnológica
- ✓ Descripción de la vulnerabilidad
- ✓ Nivel de criticidad (alto. Medio, bajo)
- ✓ Riesgo asociado o impacto
- ✓ Recomendaciones de mitigación de riesgos e implementación
- ✓ Procedimientos de corrección y conclusiones.

Producto 2. Un documento que contenga:

- ✓ Matriz de riesgos (enfocada a la Dirección de Sistemas)
- ✓ Informe de identificación de controles necesarios para mitigar o transferir el riesgo
- ✓ Informe completo de análisis de amenazas y de vulnerabilidades
- ✓ Informe de los resultados del análisis de impacto
- ✓ Reporte completo y detallada en el que se incluya (la descripción de las actividades llevadas a cabo en cada una de las fases, la información levantada en el proceso, las conclusiones del estudio y todas las recomendaciones asociadas.

Fecha de Entrega: La fecha de Entrega de Informes y reunión Final de presentación de resultados identificados en el estudio de seguridad y la auditoria de sistemas del tipo Hacking Ético, está proyectado establecerse por medio de un común acuerdo entre la CODSP y la empresa cliente

14. Generalidades:

- ✓ El análisis es trasparente a los sistemas operativos, servicios de red, sistemas motores de bases de datos y aplicaciones instalados en los servidores a evaluar.

- ✓ Se indica la dirección IP(s), desde donde el evaluador de seguridad llevara a la práctica el proceso de Auditoria del tipo Hacking Ético externo, a los sitios web y perímetro de la red, con el fin de aplicar el método de auditoría de seguridad del tipo **Caja Blanca (White Box).**

- ✓ Es importante tener presente que algunas pruebas realizadas en algunas de las fases mencionadas, pueden causar **Denegación de Servicios**, por lo que algunas actividades deben de hacerse de forma nocturna, o previamente programadas.

Nota: No se hacen pruebas de Ingeniería Social, excepto que el cliente indique lo contrario. Esto no tendrá cobros adicionales.

15. Propuesta Económica:

DESCRIPCION	VALOR (Dólares Americanos)
Servicios profesionales de estudio y pruebas de seguridad informática a la plataforma tecnológica de la empresa Cliente ficticio	**$**

Forma de Pago: Factura de venta y/o Cuenta de Cobro persona natural

La propuesta incluye:

- ✓ Realización del proceso de auditoría del tipo **Hacking Ético (White-Box).**
- ✓ Asesoría para el tratamiento de acciones de los planes de mejora reportados luego de la auditoria del tipo Hacking Ético
- ✓ Informes ejecutivos y técnicos
- ✓ Asesoría en la construcción del Plan de acción
- ✓ Uso de Appliance de seguridad específicos pertenecientes a la empresa que realiza las pruebas de seguridad.

La propuesta no incluye:

- ✓ La propuesta no incluye instalaciones, ni configuraciones en los sistemas evaluados, solo se menciona la forma de mitigar y controlar de forma adecuada las vulnerabilidad de seguridad previamente identificadas.
- ✓ Implementación de dispositivos de seguridad tales como Firewalls, IDS, Routers.
- ✓ Instalación de ningún tipo de Software de Protección, solo se instalan los software para la capacitación de Hacking ético los cuales podrán usar posteriormente para procesos de evaluación de seguridad a nivel interno a sus sistemas informáticos.

17. Requerimientos específicos por parte del Cliente.

- ✓ Direccionamiento IP de cada uno de los servidores, Host a evaluar, horario de ejecución de las pruebas, con cronograma de trabajo previamente establecido entre ambas partes (CODSP).

- ✓ Permisos para el ingreso del personal que hará las pruebas de seguridad, y para el ingreso de los equipos “Appliance”. Esto aplica, para las pruebas se ejecutan a nivel interno, para la evaluación del aplicativo web, a un nivel que no dependa de la seguridad de la infraestructura tecnológica del Hosting, tal como Firewalls, IDS, Web Aplication Firewall,IDS, entre otros

Atentamente,

Ing. Javier Velásquez
Alcalde del GADMIC SAQUISILI
info@saquisili.gob.ec
https://saquisili.gob.ec