PORTAFOLIO CIBERSEGURIDAD

INFORMÁTICA Y TECNOLOGÍA RED OPERATIVA

- La información es un activo fundamental para cualquier entidad, por lo cual resulta importante velar por su **confidencialidad, integridad y disponibilidad**, estableciéndose como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

- Consciente de las necesidades del entorno actual, las entidades a través del proceso de implementación de un **Sistema de Gestión de Seguridad de la Información** como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, buscan alcanzar las vulnerabilidades de las redes y los accesos, con la cual se ayuda a la reducción de costos operativos y financieros establece una cultura de seguridad y garantiza el cumplimiento de los requisitos legales, contractuales, regulatorios y de negocio vigentes

COMO ACTUAN LOS CIBER DELICUENTES

- Los ciberdelincuentes no son lobos solitarios en el sentido más estricto de la expresión. Incluso los que trabajan sin ayuda comparten, tarde o temprano, información con otros colegas para lograr romper sistemas. Y lo hacen a través de internet, donde también venden el botín obtenido. Operan en la red oscura, o *darknet*, llamada así por su alto nivel de encriptación.


Ingenieros Social
Agentes de Amenaza

Aprovechan contraseñas expuestas

CONTRASEÑAS Y DIRECCIONES IP PEGADAS EN PARED Y EQUIPOS.

ROBAN INFORMACIÓN IMPORTANTE

Información Personal

- Nombre completo
- Fecha de nacimiento
- Datos biométricos
- Número de pasaporte
- Documento de identidad
- Tarjetas de crédito
- Teléfono
- Correo electrónico
- Dirección de su casa

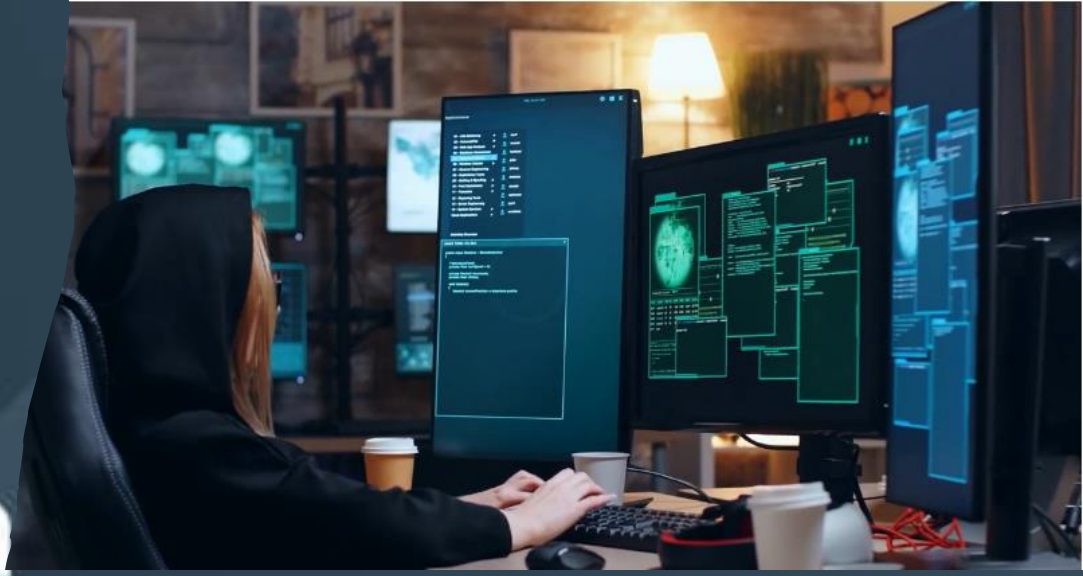
iTERO

Juice Jacking

Ransomware

¡Estar alerta!

- Suplantación de identidad
- Promociones interesantes
- Premios
- Multas de transito
- Entidades oficiales suplantadas
- Correos bancarios de cambio de claves.
- Suplantación web



El correo electrónico es el principal vector de infecciones

Correos Electrónicos

ÍTERO

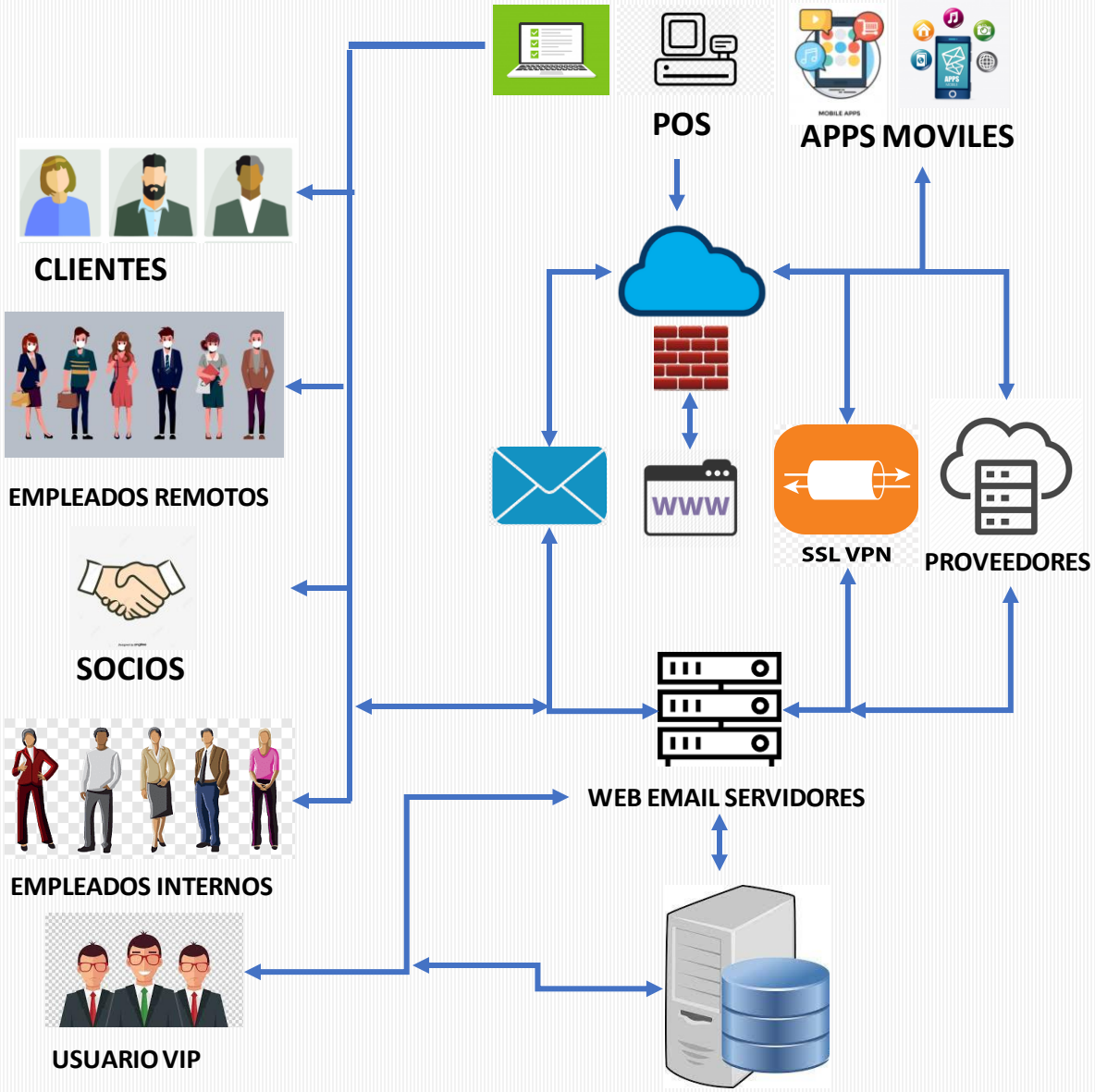
SUPERFICIE DE ATAQUE

PREOCUPACIONES DE NEGOCIO

- USUARIO VIP
- Amenazas internas
- Vulnerabilidad de gestión de Riesgos
- Hallazgo de la consultoría IT
- Monitoreo Continuo
- Requerimientos regulatorios

VECTORES DE ATAQUE

- Vulnerabilidad de app móviles
- Vulnerabilidad de app Web
- Vulnerabilidad de red
- Vulnerabilidad terminales POS
- Vulnerabilidad de Bases de Datos
- Ingeniería Social
- Amenazas web y Malware
- Debilidad en la cadena de suministro



EXFILTRACION DE DATOS

SUPERFICIE DE ATAQUE INTERNA

PREOCUPACIONES DE NEGOCIO

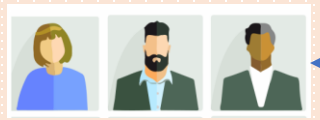
- USUARIO VIP
- Amenazas internas
- Vulnerabilidad de gestión de Riesgos
- Hallazgo de la consultoría IT
- Monitoreo Continuo
- Requerimientos regulatorios

VECTORES DE ATAQUE

- Vulnerabilidad de app móviles
- Vulnerabilidad de app Web
- Vulnerabilidad de red
- Vulnerabilidad terminales POS
- Vulnerabilidad de Bases de Datos
- Ingeniería Social
- Amenazas web y Malware
- Debilidad en la cadena de suministro

Atacante

EXFILTRACION DE DATOS



CLIENTES

EMPLEADOS REMOTOS

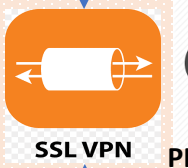
SOCIOS

EMPLEADOS INTERNOS

USUARIO VIP

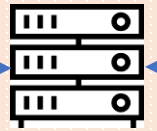
POS

APPS MOVILES



SSL VPN

PROVEEDORES



WEB EMAIL SERVIDORES

Bases de datos y archivos de servidores

SUPERFICIE DE ATAQUE EXTERNA

PREOCUPACIONES DE NEGOCIO

- USUARIO VIP
- Amenazas internas
- Vulnerabilidad de gestión de Riesgos
- Hallazgo de la consultoría IT
- Monitoreo Continuo
- Requerimientos regulatorios

VECTORES DE ATAQUE

- Vulnerabilidad de app móviles
- Vulnerabilidad de app Web
- Vulnerabilidad de red
- Vulnerabilidad terminales POS
- Vulnerabilidad de Bases de Datos
- Ingeniería Social
- Amenazas web y Malware
- Debilidad en la cadena de suministro

Atacante

EXFILTRACION DE DATOS

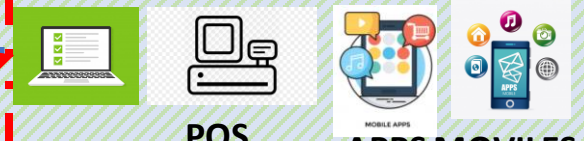
CLIENTES

EMPLEADOS REMOTOS

SOCIOS

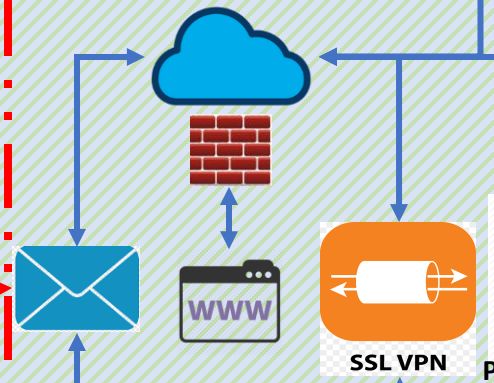
EMPLEADOS INTERNOS

USUARIO VIP



POS

APPS MOVILES



SSL VPN

PROVEEDORES

WEB EMAIL SERVIDORES

Bases de datos y archivos de servidores

COMO SABER SI NECESITO SEGURIDAD

ITERO

- Se han presentado virus y Malware en la red últimamente.
- Su red de internet es lenta en general.
- Tiene servicios de negocios publicados / expuestos a clientes / proveedores.
- Se desconoce el uso de la red, ¿quien entra?, ¿desde donde?¿y que hace?.
- ¿La empresa ha abierto nuevas sedes?.
- Desconoce el uso del canal de internet.
- Los empleados tienen mucho tiempo libre, redes sociales etc.
- ¿Se cuenta con equipos de seguridad básicos?
- La administración de la seguridad esta a cargo solo del área IT.
- No hay una estrategia alineada con el Negocio.
- La estrategia de seguridad no se encuentra alineada con toda la organización

ÍTERO

PARA QUÉ SEGURIDAD?

- Asegurar que el Know How se quede en La empresa
- Asegurar el buen nombre de la empresa
- Asegurar la continuidad del negocio
- Servicios publicados estén disponibles
- Agilizar los procesos con proveedores
- Proveer accesos seguros a servicios corporativos
- Asegurar el uso de los recursos de la compañía
- Asegurar el cumplimiento regulatorio y de negocio
- Facilitar la trazabilidad ante eventos de la red
- Optimizar los recursos y su asignación
- Promover el uso de dispositivos personales en la red
- Dedicar sus recursos humanos al core del negocio

Seguridad Informática

Objetivo

La información es un activo fundamental para cualquier entidad, por lo cual resulta importante velar por su confidencialidad, integridad y disponibilidad, estableciéndose como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. p ciberseguridad testing pentes.

Servicio

Evaluaciones BIA, DRP, Pentesting. Caja Negra, Caja Blanca, Prevención perdida de datos DLP, Encriptación cifrado de Datos, Protección de equipos de usuarios. Site survey de seguridad informática, Security Process Outsourcing (SPO), Auditoria Código Fuente, Computación Forense, Gobierno Riesgo y Cumplimiento (GRC), Monitoreo y Gestión de Eventos (C.S.O.C.)

Entregables

Reportes de vulnerabilidades.
Corrección de vulnerabilidades y políticas de seguridad.
Pruebas continuas ,Automatización, Rendimiento, Hacking Ético

Equipos activos de Seguridad

FORTINET

SOPHOS

cisco

Servicios

- Firewalls de red.
- Protección contra rasomware
- Cloud Security.
- End point protection.
- Seguridad nube Híbrida.

Objetivo

Proporcionar y diseñar los equipos para la seguridad de la red de nuestros clientes.

Entregables

Instalación, configuración, administración establecimiento de políticas.

www.iterosas.com

+57 3172948391

1. ¿Qué es lo que desea proteger?
2. ¿Cuál es su preocupación de seguridad?
3. ¿Esta obligado por normativa a cumplir una norma o circular en Seguridad?
4. ¿Qué plataforma de seguridad tiene?
5. ¿Requiere servicio en premisas o centralizado?.
6. ¿tiene en alta disponibilidad su información?
7. ¿Quién administra la ciberseguridad en su empresa?
8. ¿Cuántas sedes posee?
9. ¿Cantidad de usuarios?
10. ¿Cantidad de dispositivos concurrentes?
11. ¿Qué filtros de seguridad tiene?
12. ¿Qué aplicaciones están ralentizadas?
13. ¿Cuántos usuarios aceden de afuera de la red?
14. ¿Cuántas aplicaciones están en servidores de sitio y cuantas en la nube?