Nombre: Security Trust

Participantes:
Marco Batista, Jorge Garriguez, Alejandro Hernando, Iván Martín, Saul Sáez, Raúl Cadena.
***Creación de una empresa de consultoría de Seguridad Informática, Detalles de la empresa (descripción, experiencia, equipamiento...)**

Descripción

Nuestra misión
↦Brindar un servicio de calidad y valor agregado buscando la satisfacción de nuestros clientes.

Nuestra Visión
↦Ser un referente de tendencia y tecnología en el mercado nacional e internacional.

Nuestros Valores
↦Seriedad
↦Responsabilidad
↦Compromiso

Experiencia:
Hemos trabajado durante más de una década con grandes empresas dedicadas a la informática tales como IBM, Activision, Intel, Microsoft...,
Colaborando activamente con estas empresas hemos logrado mediante proyectos dedicados a la seguridad con los datos de estas entidades evitar diversos tipos de hackings, y ayudarles a resolver distintos problemas técnicos que les surgen.

Ubicación:

Calle de Pablo Luna, cercano a las 4 torres (Paseo de la Castellana)

Equipamiento

El **Sistema Operativo** que utilizamos es **Kali, una distribución de linux.** Uno de los mejores del mercado orientado a la seguridad informática para empresas, ya que están constantemente sorprendiendo con soluciones innovadoras y prácticas para los clientes. luego mis compañeros tratarán este tema más a fondo.

* Presentación de los empleados (formación...)

CADA UNO

El rápido desarrollo de la tecnología trae consigo nuevos y peligrosos riesgos para las empresas, pero nosotros estamos preparados para protegerte. Tenemos técnicos de seguridad altamente cualificados, con las certificaciones de los principales fabricantes y con una enorme experiencia, por lo que estamos muy preparados para asistirte en la seguridad informática de tu empresa, estos son algunos de los cargos más importantes:

Formación: Ciclo Formativo Grado Superior - Informática y Comunicaciones
En el que adquirió los conocimientos necesarios para su empleo, como aplicaciones web, fraude, arquitecturas y paradigmas.

Funciones en la empresa son:

- La gestión del riesgo asociado a las diferentes iniciativas de la empresa en materia de seguridad, regulación, fraude y riesgo tecnológico.
- El análisis de los requisitos funcionales y técnicos de la iniciativa, identificando las principales amenazas y riesgos asociados, para definir contramedidas que los mitiguen.
- La implementación técnica de las medidas de seguridad en base a las arquitecturas de la empresa, siguiendo las directrices de las áreas especialistas de Security Architecture.

  Entre otras.

- **Jorge Garriguez**

Formación: Titulado en Ingeniería Informática.

Funciones:

- Es el encargado de definir la arquitectura de la seguridad de la red y sus políticas de acceso y control. Debe administrar y velar por la aplicación de la política de seguridad de la compañía, con especial atención a los procedimientos que garanticen la seguridad y protección a nivel digital y tecnológico.
- Es el intermediario entre la empresa y la compañía contratada para la realización de auditorías externas si se da el caso. En estos casos, debe trabajar cumpliendo con la política de seguridad de la empresa con responsabilidad pero también facilitando el trabajo de dicha empresa.

- **Alejandro Hernando**

Formación: Ciclo Formativo de Grado Superior internacional de Ciberseguridad

Funciones:

- Colabora con los clientes para buscar soluciones de seguridad adecuadas para cada cliente,es decir, busca soluciones para temas más específicos de cada cliente,teniendo siempre en cuenta que el mundo de la ciberseguridad es un campo disruptivo e innovador que cambia con regularidad
- Gestiona varios equipos de ciberseguridad para poder dar una solución rápida y efectiva, es uno de los pilares de los proyectos de ciberseguridad que tiene la empresa.
- Organiza todo tipo de proyectos para diferentes empresas, y es ella la que los lleva a cabo junto a un equipo de profesionales en el ámbito de la informática.

- **Iván Martin**

Formación: Titulado en Ingeniería de la Ciberseguridad
(Dentro de la ciberseguridad se ha especificado en el campo de la Ingeniería de la Seguridad Cibernética.)

Funciones:

- Tiene la tarea de aplicar un enfoque de ingeniería para diseñar e implementar sistemas de seguridad para detener ciberataques de alto nivel.
- Dentro de su tarea también debe de desarrollar planes y políticas de seguridad, implementar soluciones, mitigar vulnerabilidades, investigar infracciones y responder a incidentes que puedan haber causado a la empresa.
- Además cómo siempre se desarrollan nuevos sistemas de hackeo nuevos y que pueden afectar a la empresa, se tiene que estar muy actualizado y estar siempre atento para después diseñar un sistema que pueda reprimir ese ataque.

- **Saúl Sáez**

Formación: Máster en Ciberseguridad

Funciones:

- Realiza la fundamental labor de prevención de nuevos riesgos mediante la investigación de posibles vulnerabilidades del sistema. Además, debe supervisar todos los cambios que se produzcan en materia de seguridad informática y estar al día de las nuevas amenazas que aparecen en el mundo de la seguridad informática para prepararse ante ellas de manera preventiva.
- Es el encargado de responder y dar solución a posibles problemas e incidencias que se presenten en el día a día en la empresa mediante una planificación de reportes y actuaciones.

- **Marco Batista**

Soy el jefe , también conocido como CEO, me encargo de la gestión y dirección de la empresa, así como de las relaciones internacionales y públicas de esta, dirigidas hacia nuestros diversos clientes, es decir, con otras empresas.

Nuestra filosofía es clara, la seguridad al 100% no existe, por ese motivo es importante dotar la infraestructura de las máximas capas posibles de protección para proteger de los ciberataques y en caso de desastre, recuperar en el mínimo tiempo posible todo el servicio.

Por ello, te enseñamos los distintos tipos de seguridad informática más comunes entre las empresas y usuarios y que combinados nos proveen una seguridad informática adecuada para poder seguir trabajando sin preocupaciones:

* Productos y servicios que se ofrecen

JORGE, SAÚL Y RAÚL

Seguridad informática en red

Se encarga de defender cualquier información que es accesible mediante internet de amenazas como virus, troyanos, phising, software espía, robo de datos o la suplantación de identidades. Para poder defender a nuestro cliente, nos encargamos de que tenga el software actualizado continuamente y le sea imposible recibir un ciberataque, aunque también actualmente estamos realizando nuestro propio SOCs (centro de operaciones de seguridad) en el que tenemos equipos de última generación.

Seguridad informática en software

La seguridad en cuanto al software tiene como función defender las aplicaciones de los equipos de las amenazas que pueda recibir y para ello lo que hacemos es instalar los mejores antivirus para que tengan listas actualizadas de los virus del momento, y además, tenemos personal que también tiene esa función por sí al programa se le escapase algo.

Seguridad informática en hardware

Este tipo de seguridad tiene que ver con los dispositivos que se usan para escanear un sistema o para el control del tráfico de una red.
El hardware pertenece a la parte física de tu dispositivo Algunos de los hardware con los que trabajamos son FIREWALLS PROXY Y otros cortafuegos con el objetivo de examinar la vulnerabilidad de tu dispositivo
De todos los tipos de seguridad informática, los sistemas de seguridad de este tipo son los que proporcionan los niveles de protección más altos y robustos.

Entonces, los **PRODUCTOS Y SERVICIOS** que ofrecemos son los siguientes:

Consultoría de seguridad

Creación y diseño por parte de nuestros técnicos e ingenieros en tus proyectos de seguridad informática.

Auditorias de seguridad

Realizamos informes periódicos sobre el estado de la seguridad informática y accesos en tu empresa.

Hacking ético

Nuestros analistas descubren agujeros de seguridad en sus sistemas informáticos, ayudándole a protegerse.

1. **Software antivirus “high equality”: PROXYTRUST**

   Nos permite contar con medidas de protección efectivas ante la detección de malware u otros elementos maliciosos, por medio de ofrecer la posibilidad de eliminar las posibles amenazas o poner al dispositivo en estado de “cuarentena”.

2. **Firewall perimetral de red: FASTFIREWALL**

   Escanea los paquetes de red, incluso puede clasificar los archivos utilizando varios parámetros. Así, se puede inspeccionar con eficiencia el tráfico web, identificar a usuarios, bloquear el acceso que no está autorizado, entre otras acciones.

3. **Servidor proxy. SSL**

   Por medio de ella, se puede bloquear sitios web que se estimen como peligrosos o prohibidos dentro del ambiente laboral.

   Por otro lado, nos permite establecer un sistema de autentificación, el cual limita el acceso a la red externa, permitiendo contar con registros sobre sitios, visitas, entre otros datos.

4. **Cifrado de punto final o end point disk encryption.**

   Protege a los sistemas operativos instalados en las empresas de la instalación de archivos de arranque corruptos, bloqueando los archivos almacenados en computadores, servidores, entre otros puntos finales.

5. **Escáner de vulnerabilidades. Open Vulnerabilities**

   Consiste en un software mucho más avanzado que la media que se encarga de detectar, analizar y gestionar los puntos débiles del sistema.

   Gracias a esta plataforma, podemos mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias. Además, permite alertar en tiempo real, lo que ayuda a la solución de problemas de forma oportuna y sin comprometer la continuidad del negocio.