INNOVA COLOMBIA

Jorge Daniel León Prieto, Daniel Mauricio Sánchez, Jorman Mosquera

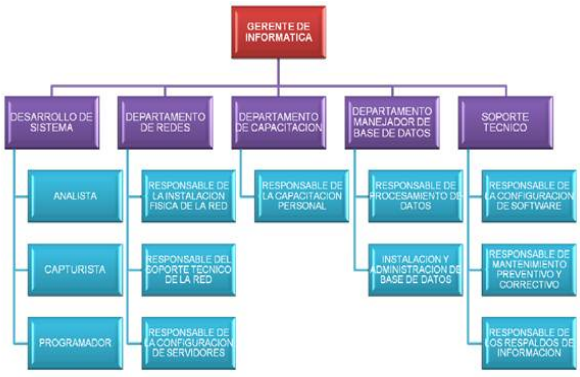
Politécnico Internacional
Bogotá, Colombia
jorge.leon.prieto@pi.edu.co
daniel.sanchez@pi.edu.co
jorman.mosquera@pi.edu.co

***Abstract*— Innova Colombia is a company that makes IT technology solutions in terms of Machine Learning - Big Data - IA. With certified Engineers at all levels and with a free software platform as a serious, safe bet with high levels of processing capacity. In this document we will detail the computer security implementation process, explaining topics such as security policies, architecture, network diagrams, among others. This in order to achieve a secure company in the field of infrastructure and networks. Specific topics such as security, information, networks, protection and infrastructure.**

I. Introducción

Innova Colombia es una empresa que hace soluciones de tecnología de TI en cuanto a Machine Learning – Big Data - IA. Con Ingenieros certificados en todo nivel y con plataforma de software libre como una apuesta seria, segura y de altos niveles de capacidad de procesamiento. En este documento detallaremos el proceso de implementación de seguridad informática, explicando temas como políticas de seguridad, arquitectura, diagramas de redes, entre otros. Esto con el fin de lograr una empresa segura en el ámbito de infraestructura y redes.

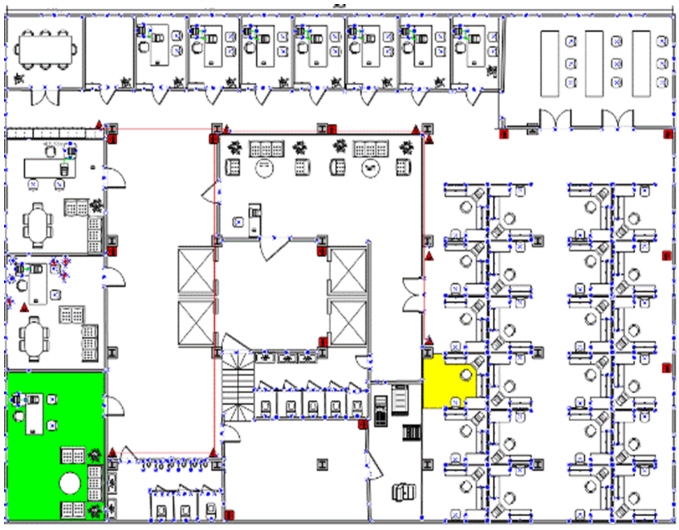
A. Organigrama empresarial



B. Infraestructura

La empresa innova se encuentra ubicada en Bogotá, Colombia, en la siguiente dirección CRA 7 # 23 -65, con el siguiente diagrama de infraestructura.

Adicional cuenta con el siguiente diagrama estructural



II. Desarrollo de Contenidos

Durante la visita a la empresa Innova nos encontramos con bastantes riesgos, y amenazas de seguridad a nivel tecnológico, por lo cual empezamos a realizar el diagnóstico y definir todas las estrategias teóricas y prácticas que nos permitan tener una empresa segura.

A. Políticas de seguridad informática:

1. La seguridad informática abarca un campo muy amplio, puesto que va desde la protección de los dispositivos de la empresa, teniendo siempre en cuenta la información disponible en el cual se basa en**:**

- La confidencialidad, la cual su principal objetivo es impedir que usuarios no deseados accedan al sistema, ni a la información que está disponible.

- La integridad de la información a la que se puede llegar a tener acceso, impidiendo que la información pueda ser manipulada por personal no autorizado o deseado.

- La disponibilidad de la información en cualquier momento a cualquier usuario. Puede ser accesible en cualquier instante y el sistema debe ser capaz de lograr recuperarse.

La empresa implementa métodos para brindar a los usuarios un sistema de seguridad informática de calidad tales como:

- Actualizaciones de los sistemas operativos cada 3 meses.
- Capacitaciones de seguridad informática cada 2 semanas.
- Uso de antivirus en las computadoras.
- Redes y Wifi protegidos.
- Actualización constante de contraseñas seguras.
- Bloquear puertos USB.
- Copias de seguridad que se actualizan cada semana.
- Control y limitación de la utilización de los equipos.

B. Políticas de seguridad de la información:

La política de seguridad de la información persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información.

- **Preservar la integridad, confidencialidad y disponibilidad** de los activos de la información.

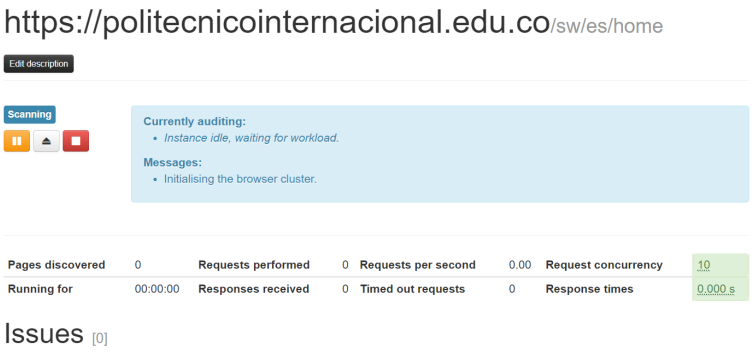
Fomentar la seguridad de la información. Con esto no solo lograremos el cumplimiento de los requisitos de la ley, sino que también la optimización de los recursos humanos, tecnológicos y administrativos.

Los procesos que usará la empresa para proteger la seguridad de la información serán:

- Aseguramiento de las redes Wifi con claves de alta seguridad encriptadas en WPA2.
- Plan de respuesta en caso de haber incidentes.
- Verificación de cumplimiento de las normas internas sobre el manejo de datos e información.
- Comprobación de la seguridad de terceros.
- Formación y capacitación de los empleados.

C. Análisis, Escaneo y Remedición de un sistema de información.

En innova pudimos evidenciar las estrategias que se toman para la evaluación y análisis de vulnerabilidades y amenazas que puedan afectar la infraestructura tecnológica. Utilizando herramientas de escaneo y análisis. Una de ellas es Arachni, ejecutando un ejercicio mostrado en la siguiente imagen.



D. Definición de gobierno en seguridad informática:

Consiste en el liderazgo, estructura organizacional y proceso para proteger la información. El gobierno de seguridad de la información es un subconjunto del gobierno corporativo de la organización; provee información estratégica, garantiza los objetivos establecidos, gestiona los riesgos de forma apropiada, usa los recursos organizacionales de manera responsable y monitorea el éxito o falla del programa de seguridad de la información.

E. Evaluación: Riesgos + Amenazas + Eventos + Incidentes.

En la empresa se realiza la implementación de metodologías de evaluación apropiada para los sistemas informáticos, garantizando su seguridad en:

- Análisis y escaneo de amenazas en la red
- la actualización de los sistemas operativos
- Inclusión de parches de seguridad

F. Definición de procesos Core de la organización

El core de INNOVA es el desarrollo de software enfocado en el maching-learning, big data e IA, utilizando como principal herramienta el uso de software libre.

G. Definición de Procesos Seguridad

En la empresa los procesos de seguridad, consisten en asegurar que los recursos de los Sistema de Información, se utilicen de la forma que ha sido decidido y el acceso de información se encuentre contenida, así como la gestión y el control sea posible por parte del personal autorizado.

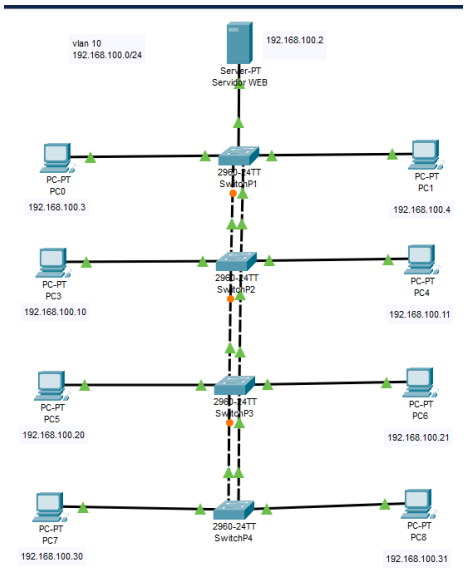
H. Clasificación de la información.

Dentro de la organización clasificamos la información de acuerdo a su contenido de la siguiente manera

- **Confidencial**: Información muy sensible de uso exclusivo de la compañía, su divulgación sin autorización afectaría gravemente a la compañía, inversionistas y clientes.
- **Privada**: Información menos sensible de uso interno de áreas dentro de la compañía como gerencias y directores.
- **Uso interno**: Esta información es de uso de la organización en el día a día, el compartirla sin autorización puede afectar la operación de la empresa.
- **Publica**: Información que puede ser transmitida a toda persona dentro y fuera de la organización sin ningún problema.

I. Diagrama de Arquitectura

Dentro de la información brindada por la empresa se ha realizado un diagrama preliminar sobre como se debería armar el sistema de red de la empresa, el cual se detalla en la siguiente imagen:



En este diagrama presentamos un servidor central donde se encuentran los servicios de email, intranet, página corporativa, entre otros; adicional se realiza la configuración y asignación de rango de IP acorde a cada área (Piso) , todas enrutadas por medio de switch.

J. Calculadora de IP

A continuación se muestra la tabla con el rango de IP asignado a la red de la empresa:

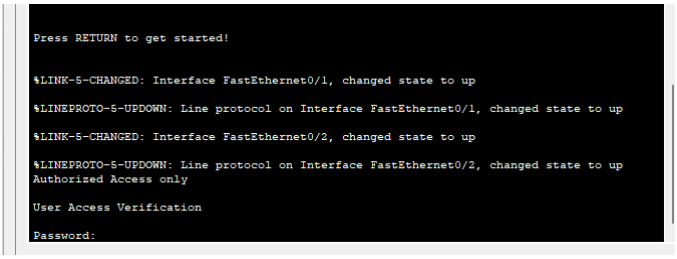
Bloque de direcciones de red	192.168.100.0/24	Intervalo de direcciones de host	192.168.100.1 - 192.168.100.62
Mascara de subred	255.255.255.192/26	Dirección de difusión	192.168.100.63
Número de hosts/subredes	64	Máscara de comodines	0.0.0.63
Número de subredes	4	Notación CIDR	192.168.100.0/26

Detalles de subred

Subnet ID	Subnet Address	Host Address Range	Broadcast Address
1	192.168.100.0	192.168.100.1 - 192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65 - 192.168.100.126	192.168.100.127
3	192.168.100.128	192.168.100.129 - 192.168.100.190	192.168.100.191
4	192.168.100.192	192.168.100.193 - 192.168.100.254	192.168.100.255

K. Configuración de seguridad de SWITCH

Se realiza configuración inicial en al cual establecemos 2 autenticaciones para poder llegar al apartado de configuración de redes internas de la compañía, esto con el fin de evitar accesos no deseados, al ingresar a la configuración del switch nos mostrará la primera pantalla de autenticación:



luego de ingresar en esta pantalla, si deseamos configurar el switch, debemos ingresar la palabra enable, el cual nos mostrara el segundo paso de autenticación

Si logramos acceder a estos dos pasos con los datos de login correcto, podremos acceder y realizar las configuraciones que se requieran.

L. Navegación por la intranet de la empresa

Como parte de la implementacion de seguridad de la informacion dentro de la compañia, se diseña una pagina web en la cual los distintos emleados de la empresa pueden acceder desde sus equipos y consultar informacion corporativa de la empresa. A continuacion unas capturas de este proceso