INNOVA COLOMBIA

Juan Sebastián Martínez, Paola Andrea Sánchez rodríguez, Tercer Autor

Politécnico Internacional-Bogotá D.C

juan.martinez.cabezas@pi.edu.co

paola.sanchez.rodriguez@pi.edu.co

Juan.martinez.cabezas@pi.edu.co

I. INTRODUCCION

Innova Colombia, Ubicada en la ciudad de Bogotá D.C nace como una empresa de servicios en el año 2019.Realizando soluciones de tecnología de TI en cuanto a Machin 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. Esto nos convierte en especialistas y líderes en el mercado, al día de hoy INNOVA COLOMBIA se convirtió en una empresa de Innovación nacional y regional. Generando soluciones de alta tecnología para satisfacer tanto el mercado local como internacional, atendiendo la demanda de la falta de soluciones de este tipo. Somos los primeros en Latinoamérica en fabricar un sistema de análisis de datos de alto nivel, para la mejora de soluciones en TI. Somos los primeros en Colombia en realizar una implementación de infraestructura con soluciones 100 % Libres y con soporte especializado.

A. INFRAESTRUCTURA

Fig. 1 Grafico de infraestructura de INNOVA Colombia

B. DISEÑO AQUITECTONICO

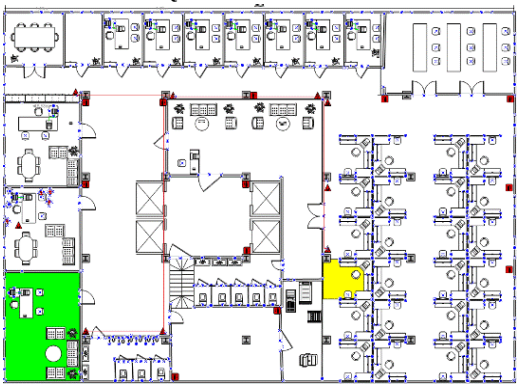
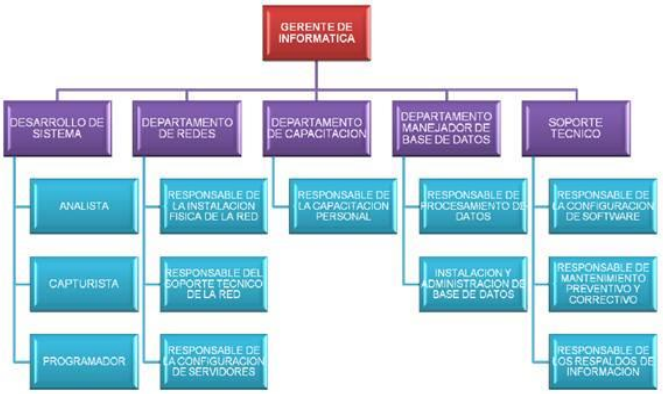


Fig. 2 Plano arquitectónico INNOVA Colombia

C. CARGOS LABORALES



D. TOPOLOGIA EN PACKET TRACER INNOVA COLOMBIA

E. FUNCIONAMIENTO PIN PACKET TRACER (DHCP)

II. DESARROLLO DE CONTENIDOS

A. Políticas de seguridad informática

Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad.
La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

Teniendo en cuenta las políticas de seguridad informática, en INNOVA Colombia contamos con un reglamento estricto que cumple con las políticas de seguridad, dando cumplimiento a:

- Cifrar archivos sensibles.
- Implementar copias de respaldo.
- Usar contraseñas y renovarlas de forma periódica.
- Usar VPN.
- Instalar software antivirus y antimalware.

B. políticas en seguridad de la información.

El objetivo de la seguridad de la información es triple , involucrando los componentes críticos de confidencialidad, integridad y disponibilidad.
Confidencialidad significa protección contra personas no autorizadas acceso.
Integridad significa protección contra modificaciones no autorizadas.
Disponibilidad significa protección contra interrupciones en el acceso.

Aplicando a la empresa INNOVA Colombia, utilizamos la norma internacional de seguridad de la información ISO-27001, dando un total cumpliendo a la norma para lograr una óptima seguridad corporativa.

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

Remediación de Vulnerabilidades consiste en identificar, remediar y verificar que las diferentes vulnerabilidades de los sistemas de información se hayan mitigado.
Análisis consiste en relevar la información actual y proponer los rasgos generales de la solución futura.
Escaneo óptico combina equipo y programas de cómputo especializados. Los equipos capturan una imagen y los programas convierten esa imagen en información que puede ser leída por la computadora.

-Dentro INNOVA Colombia se cuenta con un equipo especializado para lograr un optimo sistema de la información, aplicando diferentes softwares y hardware para mantener una seguridad solida.

D. Gobierno en seguridad informática.

Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio

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

Los *riesgos informáticos* son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las consecuencias pueden ser muy graves en relación a la información que se está manejando.
Una *amenaza* es una posible acción o evento negativo facilitado por una vulnerabilidad que tiene como resultado un impacto no deseado en un sistema o aplicación informática.
Un *evento* es una acción que es detectada por un programa; éste, a su vez, puede hacer uso del mismo o ignorarlo. Por lo general, una aplicación cuenta con uno o más hilos de ejecución dedicados a atender los distintos eventos que se le presenten.
Un *escenario* de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas a un activo.

F. Procesos Core de la organización

El significado de Core Business, que también es conocido como competencia distintiva, se refiere a aquella actividad productiva que desarrolla una empresa y le permite generar valor para poder mantenerse en el mercado. Asimismo, la actividad principal de una empresa debe ser aquella que le aporte mayores ingresos.

G. Procesos Seguridad

La Seguridad de los Procesos es un marco disciplinado para la gestión de la integridad de los sistemas operativos y procesos de manejo de sustancias peligrosas mediante la aplicación de buenas prácticas de diseño, ingeniería, operación y mantenimiento.

H. Clasificación de la información.

La clasificación de la información según ISO 27001 es un proceso en el que la organización evalúa los datos que posee y el nivel de protección que cada uno requiere.

Un sistema típico, debería incluir cuatro niveles de confidencialidad:
Confidencial*:* acceso restringido a la alta dirección.
Restringido*:* directores de área y empleados clave tienen acceso.
Interno: relativo a la información accesible solo los miembros de la organización, pero en cualquier nivel.
Público: todas las personas, dentro y fuera de la organización,

tienen acceso.

I. Evaluación del desempeño

Evaluar el rendimiento o efectividad de nuestro SGSI o de la Seguridad de la información es otro de los requisitos de la norma ISO 27001.

La principal herramienta para medir la efectividad del SGSI es la realización de auditorías internas con intervalos planificados. Una auditoria interna nos revelara como estamos cumpliendo tanto con los requisitos de la norma como con los requisitos específicos de la seguridad de la información que hayamos desarrollado para nuestra organización.

J. Roles y responsabilidades

Junta Directiva: La gobernanza de la ciberseguridad requiere insumos y dirección estratégica.

-Depende del compromiso, los recursos y responsabilidad de la gestión de la seguridad cibernética, y requiere un medio para que la junta determine si su intención ha se ha cumplido.

Miembros de la junta: Deben conocer los activos de información de la organización y su importancia para las operaciones de negocios.

Dirección ejecutiva: Es responsable de garantizar que las funciones organizativas necesarias, los recursos y la infraestructura de apoyo están disponibles y se utilizan adecuadamente para cumplir con las directivas de la junta, cumplimiento normativo y otras demandas.

Director de seguridad(CISO): Es responsable por todos los asuntos de seguridad, tanto físicos como digitales. Asimismo, las responsabilidades y autoridad de los gerentes de seguridad de la información varían dramáticamente entre organizaciones.

Profesionales de la ciberseguridad: Equipo de expertos en la materia y profesionales de la ciberseguridad, incluyendo arquitectos de seguridad, administradores, forense digital, manejadores de incidentes, investigadores de vulnerabilidades y especialistas en seguridad de redes. Juntos diseñan, implementan y gestionan procesos y controles técnicos y responder a eventos e incidentes.