BUSINESS ALLIANCE FOR SECURE COMMERCE

FORO EMPRESARIAL PARA LA FACILITACIÓN Y SEGURIDAD EN LA CADENA DE SUMINISTRO

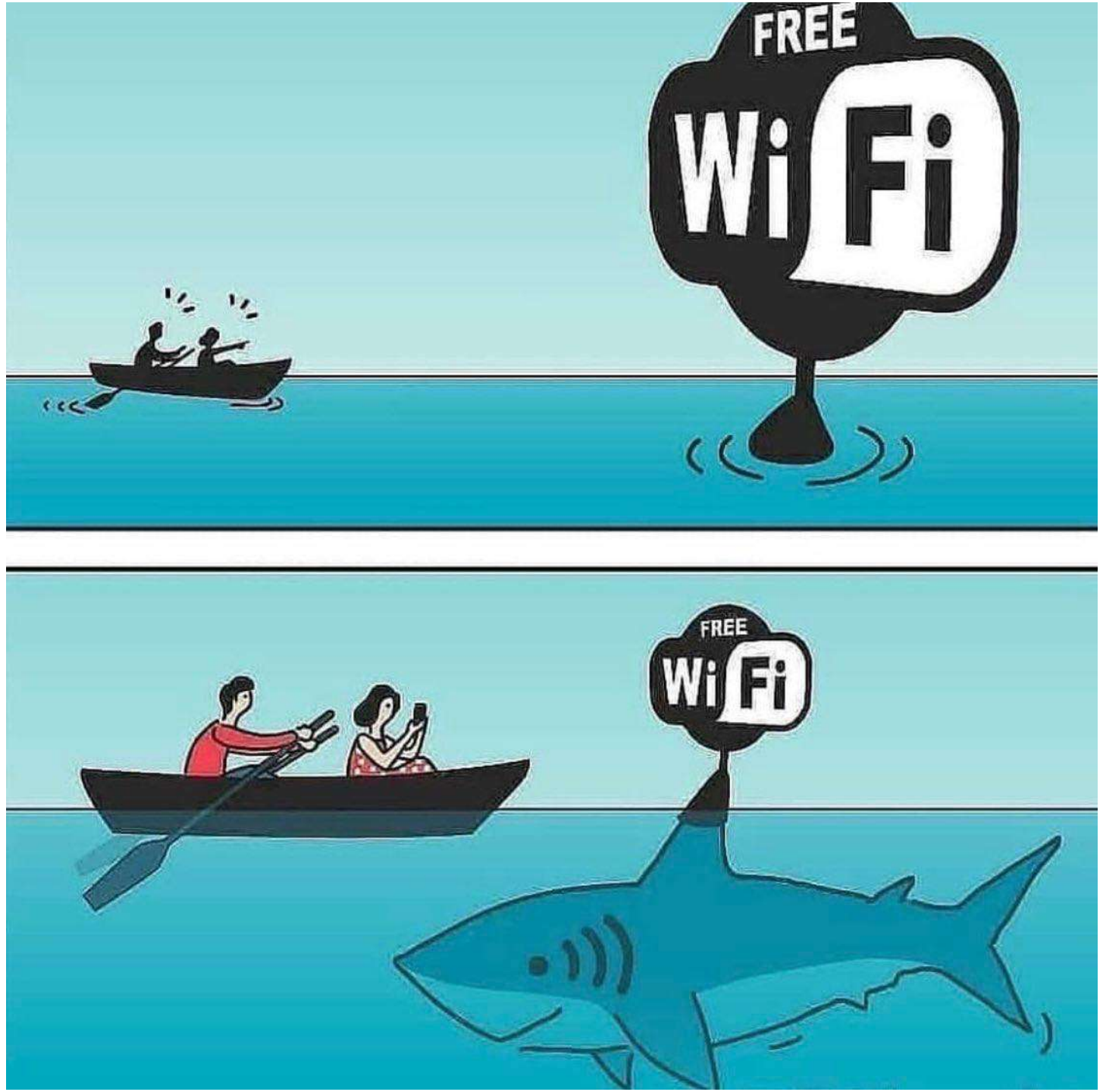
PERSPECTIVAS SOBRE GOBERNANZA DE LA CIBERSEGURIDAD SEGÚN BASC.

Conozca las medidas de ciberseguridad, y últimas tendencias para combatir las amenazas contra sistemas en red y aplicaciones, destinados a hacer parte de una Estrategia de Ciberdefensa. Elementos mínimos de cumplimiento según la norma y estándar internacional BASC

Oscar Andrade

Lo único constante es el cambio.
Lo que no cambia es la astucia
de las personas.. evoluciona.


FREE
WiFi
AVAILABLE
Solve this for
WiFi Password
$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L}\right)$


FREE
WiFi
FREE
WiFi

Norma 6.0

- Seguridad de la Información
- 6.1 Generalidades
- 6.2. Ciberseguridad y las tecnologías de la información

Gobernanza

- Para abordar en forma eficiente la gestión de riesgos de ciberseguridad se requiere gobernanza y una combinación de múltiples estrategias.
- Antes de asumir los proyectos que permitirían mitigar los riesgos de ciberataques es clave desarrollar un plan estratégico que sea aprobado y luego liderado por la alta dirección de la organización.
- La ciberseguridad es parte de la Gestión de Seguridad de la información que, a su vez, es un pilar estratégico de la Gestión de Riesgo Operacional.

DEFINICIONES BÁSICAS

01 Gestión

conjunto de acciones, o diligencias que permiten la realización de cualquier actividad o deseo. Gestión se refiere a todos aquellos trámites que se realizan con la finalidad de resolver una situación o materializar un proyecto.

02 Seguridad de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos o físicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

03 Ciberdelincuencia

Acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.

04 Ciberseguridad

Proceso de identificar, analizar, evaluar y comunicar un riesgo cibernético y aceptarlo, evitarlo, traspasarlo o mitigarlo a un nivel aceptable, tomando en consideración los costos y beneficios para la empresa. Se enfoca en proteger las computadoras, las redes, los programas y los datos del acceso, el cambio y la destrucción no deseados o no autorizados.

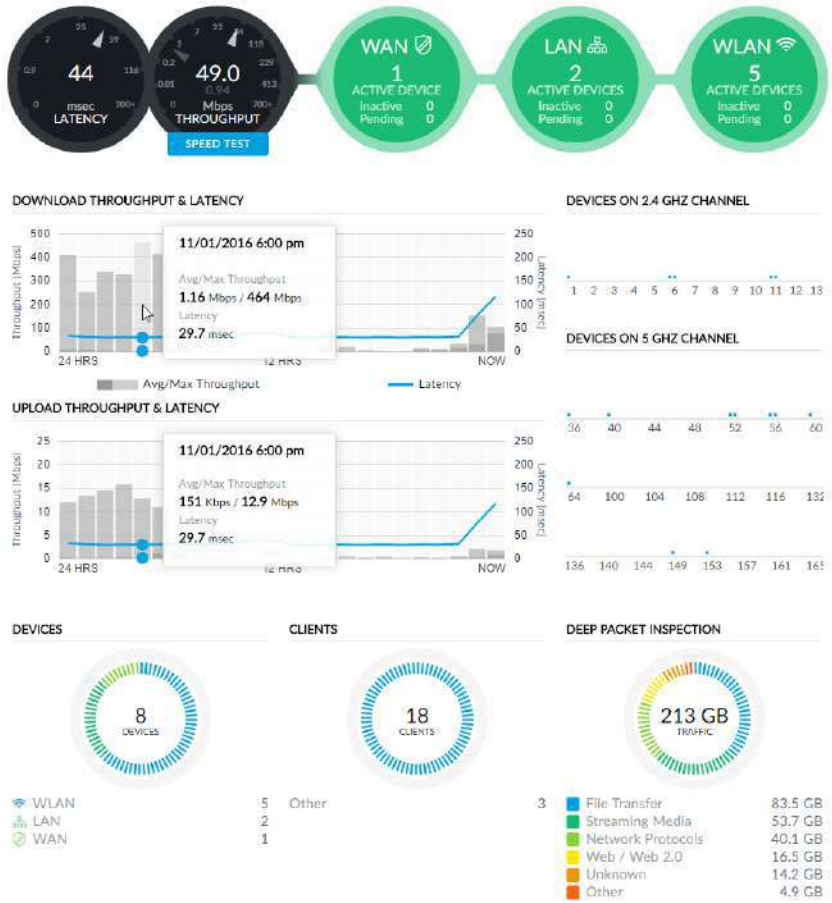
Estándares = Gobernanza

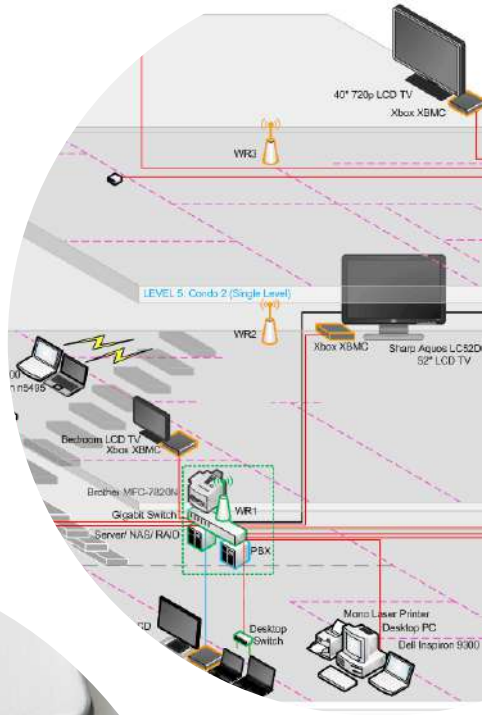
Estándar 6.0.1

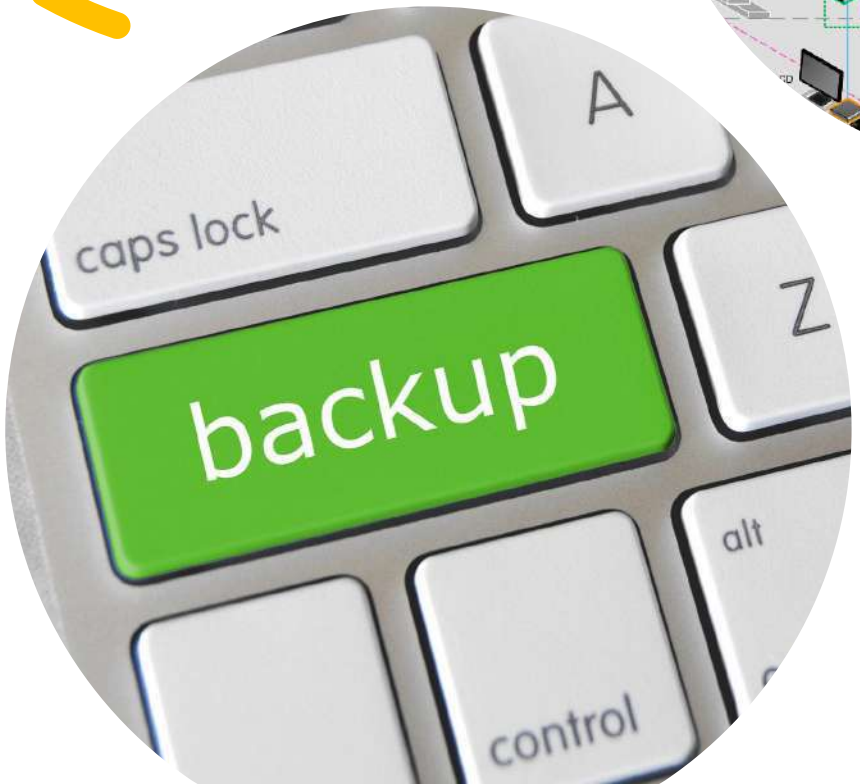
6.1 Generalidades

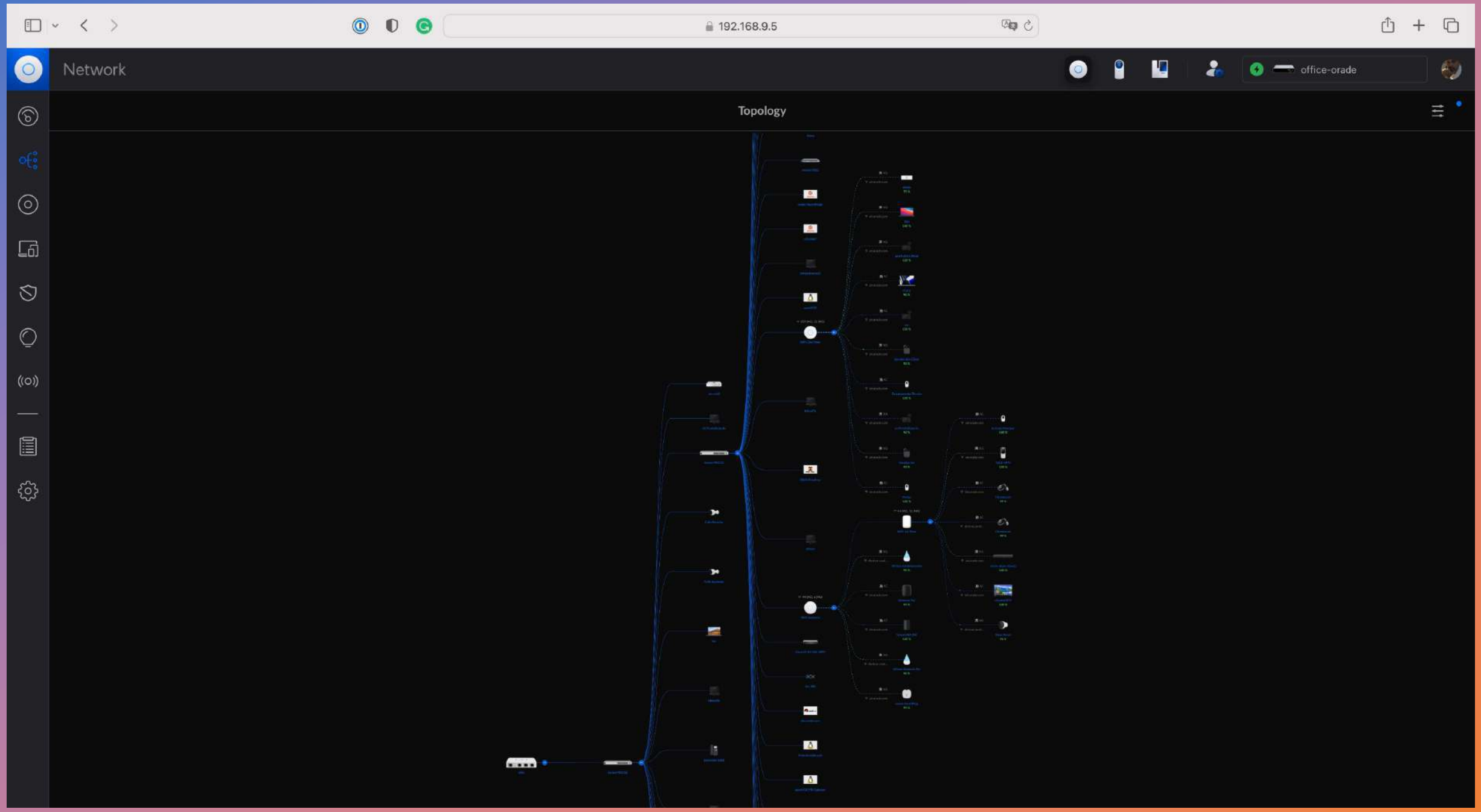
- a) Gestionar y proteger el manejo de la información y los recursos informáticos de la empresa, incluyendo las medidas a aplicar en caso de incumplimiento.
- b) Salvaguardar la información y su confidencialidad, integridad y disponibilidad, en sus diferentes formas y estados.
- c) Proteger la infraestructura de las tecnologías de la información.

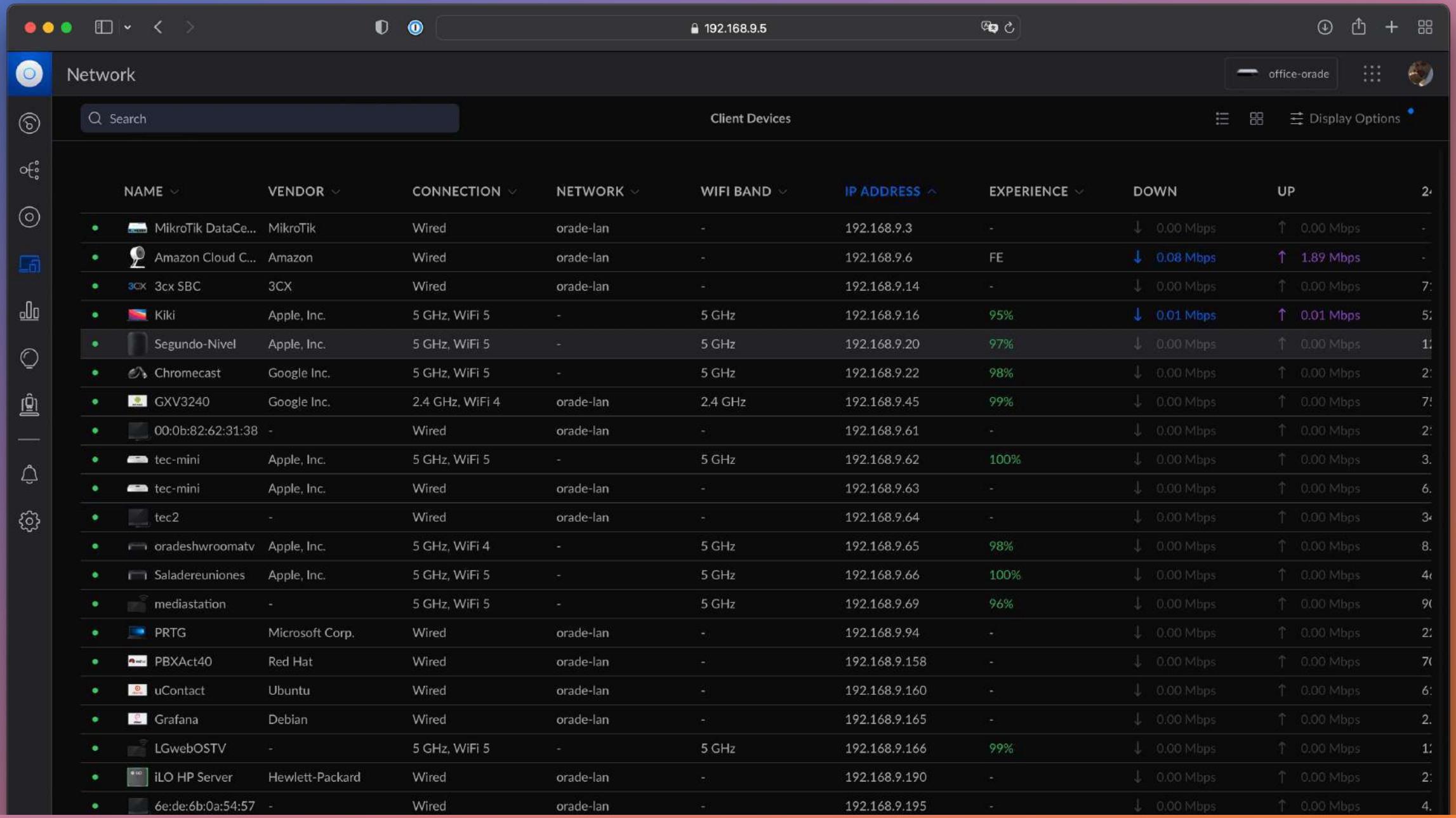
Gestionar y proteger el manejo de la información y los recursos informáticos

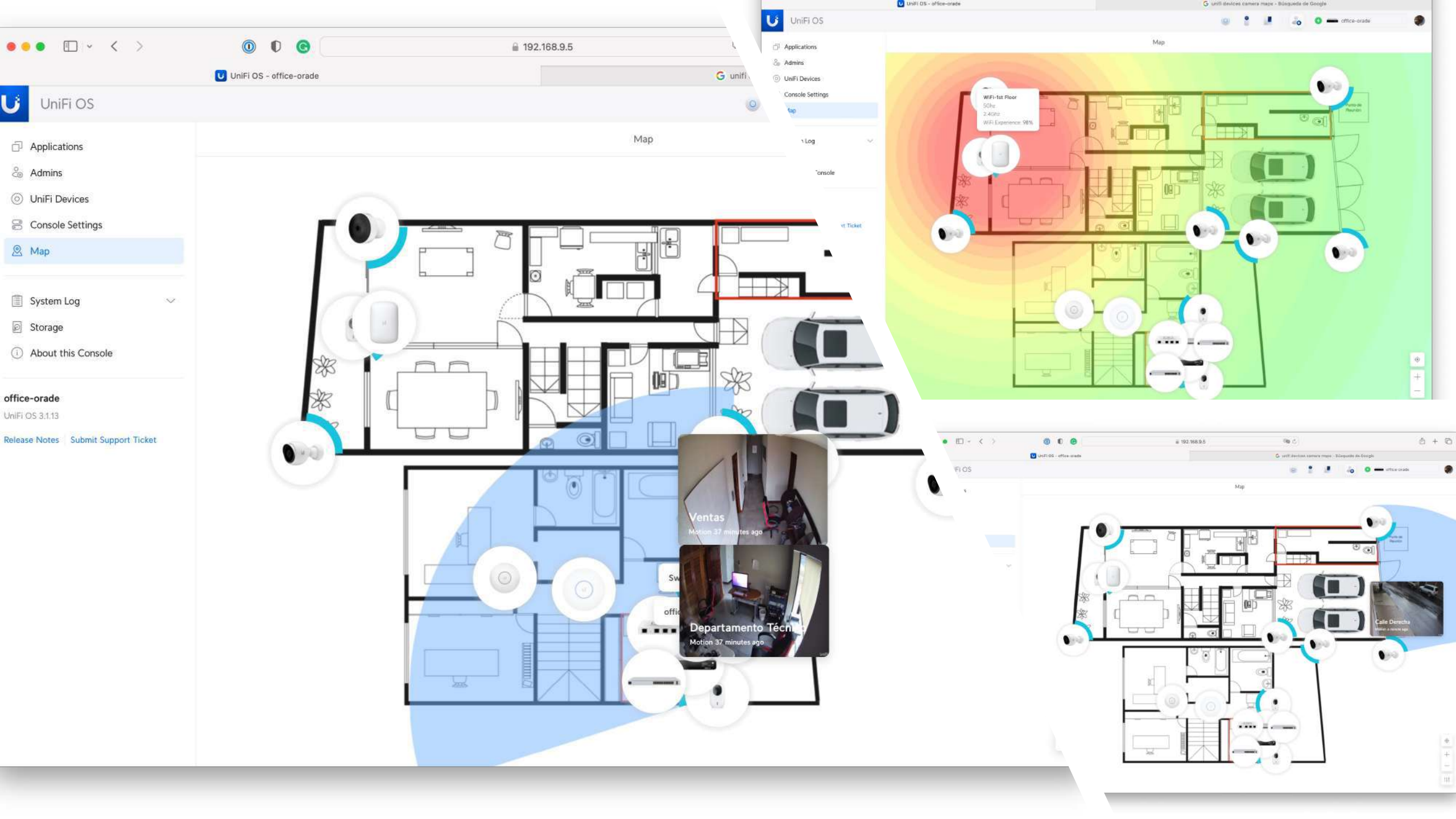







192.168.9.5
Network
office-orade
Topology


192.168.9.5
Network
office-orade
Search
Client Devices
Display Options
NAME
VENDOR
CONNECTION
NETWORK
WIFI BAND
IP ADDRESS
EXPERIENCE
DOWN
UP
MikroTik DataCe... MikroTik Wired orade-lan - 192.168.9.3 - 0.00 Mbps 0.00 Mbps
Amazon Cloud C... Amazon Wired orade-lan - 192.168.9.6 FE 0.08 Mbps 1.89 Mbps
3cx SBC 3CX Wired orade-lan - 192.168.9.14 - 0.00 Mbps 0.00 Mbps
Kiki Apple, Inc. 5 GHz, WiFi 5 - 5 GHz 192.168.9.16 95% 0.01 Mbps 0.01 Mbps
Segundo-Nivel Apple, Inc. 5 GHz, WiFi 5 - 5 GHz 192.168.9.20 97% 0.00 Mbps 0.00 Mbps
Chromecast Google Inc. 5 GHz, WiFi 5 - 5 GHz 192.168.9.22 98% 0.00 Mbps 0.00 Mbps
GXV3240 Google Inc. 2.4 GHz, WiFi 4 orade-lan 2.4 GHz 192.168.9.45 99% 0.00 Mbps 0.00 Mbps
00:0b:82:62:31:38 - Wired orade-lan - 192.168.9.61 - 0.00 Mbps 0.00 Mbps
tec-mini Apple, Inc. 5 GHz, WiFi 5 - 5 GHz 192.168.9.62 100% 0.00 Mbps 0.00 Mbps
tec-mini Apple, Inc. Wired orade-lan - 192.168.9.63 - 0.00 Mbps 0.00 Mbps
tec2 - Wired orade-lan - 192.168.9.64 - 0.00 Mbps 0.00 Mbps
oradeshwroomatv Apple, Inc. 5 GHz, WiFi 4 - 5 GHz 192.168.9.65 98% 0.00 Mbps 0.00 Mbps
Saladereuniones Apple, Inc. 5 GHz, WiFi 5 - 5 GHz 192.168.9.66 100% 0.00 Mbps 0.00 Mbps
mediastation - 5 GHz, WiFi 5 - 5 GHz 192.168.9.69 96% 0.00 Mbps 0.00 Mbps
PRTG Microsoft Corp. Wired orade-lan - 192.168.9.94 - 0.00 Mbps 0.00 Mbps
PBXAct40 Red Hat Wired orade-lan - 192.168.9.158 - 0.00 Mbps 0.00 Mbps
uContact Ubuntu Wired orade-lan - 192.168.9.160 - 0.00 Mbps 0.00 Mbps
Grafana Debian Wired orade-lan - 192.168.9.165 - 0.00 Mbps 0.00 Mbps
LGwebOSTV - 5 GHz, WiFi 5 - 5 GHz 192.168.9.166 99% 0.00 Mbps 0.00 Mbps
iLO HP Server Hewlett-Packard Wired orade-lan - 192.168.9.190 - 0.00 Mbps 0.00 Mbps
6e:de:6b:0a:54:57 - Wired orade-lan - 192.168.9.195 - 0.00 Mbps 0.00 Mbps


192.168.9.5
UniFi OS - office-orade
UniFi OS
Applications
Admins
UniFi Devices
Console Settings
Map
System Log
Storage
About this Console
office-orade
UniFi OS 3.1.13
Release Notes
Submit Support Ticket
Map
Ventas
Motion 37 minutes ago
Departamento Técnico
Motion 37 minutes ago
WiFi-1st Floor
Calle Derecha

Clasificación de la Información

Usuario	Proveedor	Empleado	Cargo	Confidencialidad	Integridad	Disponibilidad	Clasificación
jperez	NA	Juan Pérez	Encargado de Bodega	CLASIFICADA: USO INTERNO	CRUCIAL	ESTANDAR	CRITICIDAD ALTA
hlopez	NA	Hugo López	Contador 1	CLASIFICADA: CONFIDENCIAL	ALTA	DELICADA	CRITICIDAD MEDIA
fperez	NA	Fernando Pérez	Encargado de Tienda	CLASIFICADA: SECRETA	CRUCIAL	DELICADA	CRITICIDAD ALTA
fhernandez	NA	Francisco Hernández		CLASIFICADA: USO INTERNO	BAJA	RELEVANTE	NO CLASIFICADO
ajuarez	NA	Antonio Juárez		CLASIFICADA: USO INTERNO	ALTA	RELEVANTE	CRITICIDAD MEDIA
clopez	NA	Carla López	Asistente de Gerencia	CLASIFICADA: CONFIDENCIAL	ALTA	DELICADA	CRITICIDAD MEDIA
fperez	NA	Fernando Pérez	Encargado de Tienda	CLASIFICADA: USO INTERNO	BAJA	RELEVANTE	NO CLASIFICADO
gherrera	NA	Gustavo Herrera	Gerente Financiero	CLASIFICADA: CONFIDENCIAL	BAJA	RELEVANTE	CRITICIDAD MEDIA
jperez	MacroTEC	Juan Pérez	Encargado de Bodega	CLASIFICADA: USO INTERNO	REEMPLAZABLE	VITAL	CRITICIDAD ALTA
agalvez	NA	Alberto Galvez	IT	CLASIFICADA: USO INTERNO	BAJA	DELICADA	CRITICIDAD MEDIA
clopez	NA	Carla López	Asistente de Gerencia	CLASIFICADA: USO INTERNO	BAJA	DELICADA	CRITICIDAD MEDIA
rlopez	NA	Rolando López	Mercadeo	PUBLICO	REEMPLAZABLE	ESTANDAR	NO CLASIFICADO

6. 2 Ciberseguridad y las tecnologías de la información

- a) Establecer, documentar y mantener criterios de seguridad que permitan identificar y proteger los sistemas de las tecnologías de la información y recuperarla oportunamente en caso de ser necesario
- b) Identificar partes interesadas y su nivel de criticidad en la infraestructura informática (hardware y software) de la empresa.
- c) Comunicar oportunamente información sobre amenazas de ciberseguridad identificadas a las partes interesadas correspondientes.

6. 2 Ciberseguridad y las tecnologías de la información

- d). Clasificar la información de acuerdo con la legislación vigente, sistemas y accesos según el nivel de criticidad y establecer políticas de acceso a la misma.
- e). Utilizar cuentas asignadas para cada usuario que acceda al sistema, con sus propias credenciales de acceso mediante contraseñas u otras formas de autenticación que generen accesos seguros. Estas deben actualizarse periódicamente, cuando existan indicios o sospechas razonables de que están comprometidas.
- f). Limitar los accesos y permisos de los usuarios de acuerdo con las funciones y tareas asignadas, revisándolos periódicamente.

6. 2 Ciberseguridad y las tecnologías de la información

- g). Eliminar el acceso a la información a todos los colaboradores, terceros y usuarios externos al terminar su contrato o acuerdo.
- h). Impedir la instalación de software no autorizado.
- i). Utilizar y mantener hardware y software licenciados y actualizados para proteger la infraestructura de TI contra amenazas informáticas tales como virus, programas espías, gusanos, troyanos, malware, ransomware, entre otros.
- j). Realizar copias de seguridad de la información sensible, manteniendo un respaldo fuera de las instalaciones (física o virtual) con las medidas de seguridad necesarias para impedir que terceros accedan a la información.

6. 2 Ciberseguridad y las tecnologías de la información

- k). Mantener un registro actualizado de los usuarios, su nivel de criticidad y accesos asignados.
- l). Cerrar/bloquear la sesión en equipos desatendidos.
- m). Evaluar mínimo una vez al año la seguridad de la infraestructura de TI (hardware y software), implementando acciones pertinentes cuando se hayan detectado vulnerabilidades.
- n). Establecer procedimientos y controles para identificar y revisar el acceso no autorizado a los sistemas de información, sitios webs o el incumplimiento de las políticas y procedimientos (incluyendo la manipulación o alteración de los datos comerciales por parte de los colaboradores o contratistas).

6. 2 Ciberseguridad y las tecnologías de la información

- o). Revisar las políticas y los procedimientos de ciberseguridad al menos una vez al año y actualizarlas cuando se presenten cambios en el contexto interno o externo, o cuando se materialice algún riesgo.
- p). Emplear tecnologías seguras, como redes privadas virtuales (VPN) o autenticación multifactor para el acceso seguro de los colaboradores y usuarios externos a los sistemas informáticos de la empresa, incluyendo accesos para trabajo remoto o teletrabajo.
- q). Establecer procedimientos para evitar el acceso remoto de usuarios no autorizados, desde dispositivos personales u otros.
- r). Controlar mediante la realización de inventarios periódicos, los medios u otros equipos que hagan parte de la infraestructura informática de la empresa. La eliminación o desecho de los mismos se hará de acuerdo con la legislación vigente.

6. 2 Ciberseguridad y las tecnologías de la información

- s). Restringir la conexión de dispositivos personales y elementos periféricos no autorizados para cualquier dispositivo que forme parte de la infraestructura informática de la empresa.
- t). Vigilar el cumplimiento de las políticas de ciberseguridad y seguridad de la información establecidas en el uso de plataformas y contenido digital, herramientas de videoconferencia, comercio electrónico, entre otras.
- u). Realizar ejercicios prácticos y/o simulacros relacionados con la seguridad de las tecnologías de la información, que permitan determinar la eficacia de las acciones establecidas (ver Norma 6.1 e).
- v). Establecer controles para super usuarios que permitan la continuidad de credenciales de los equipos activos, en caso que aplique.

MUCHAS GRACIAS...

La ciberseguridad no es un destino, es un viaje."
- Richard Clarke.

BASC

BUSINESS ALLIANCE FOR SECURE COMMERCE