
RADICAL
CYBERSECURITY/INFRASTRUCTURE

¿Quiénes somos?

Somos una empresa de Ciberseguridad, dedicada al diseño, implementación y gestión de soluciones tecnológicas. Apoyamos a las empresas a mitigar sus riesgos de negocio, mejorar su postura de seguridad, así como crear sus NOC's, SOC's seguros.

Nos especializamos en servicios de Data Center e Infraestructura, Security Center para redes IT, OT y Ciberseguridad en redes SCADA. Todo esto basado en un equipo de respuesta a incidentes (CERT Radical), un Security Operation Center 24/7 (SOC), Laboratorio de Investigación en Ciberseguridad y Ethical Hacking.

Las 3 S de Radical

- Seguridad informática SOC - CERT
- Servicios de innovación e implementación
- Software defined infraestructure NOC - SDLAN - SDWAN - DC

Misión

Somos una empresa especializada en brindar soluciones de Ciberseguridad e Infraestructura. Nos esforzamos por estar a la vanguardia en tecnología y alcanzar las certicaciones más relevantes de la industria. Proporcionamos soluciones globales y adaptables enfocadas a mejorar la eficiencia, disponibilidad y con habilidad de negocio de nuestros clientes.

Visión

Ser un referente regional en el diseño, implementación y gestión de soluciones de seguridad, servicios y software con innovación, creatividad, capacidad y excelencia para nuestros clientes.

Estrategia

Poseemos un Centro de Operaciones NOC y SOC así como CERT a través de los cuales detectamos, alertamos y mitigamos incidentes de seguridad informática, como también brindamos soluciones proactivas para reducir el número de potenciales incidentes enfocándonos en mitigar las vulnerabilidades humanas (a través de procedimientos preventivos) y vulnerabilidades tecnológicas (a través de programas compensatorios basados en controles tecnológicos).

Los tipos de soluciones que brindamos se basan en la siguiente pirámide de madurez de seguridad.

Características de cada nivel

NIVEL REACTIVO

- TECNOLOGÍA: SIEM, IPS, Threat Intelligence, DDoS, WAF.
- PROCEDIMIENTOS: Inteligencia de vulnerabilidades, parche virtual.
- PERSONAS: Analistas basan investigación en Playbooks.

Características:

- Tecnología basada en filtros para mitigar vulnerabilidades conocidas, firmas, reputación, tipos de ataque.
- Son controles indispensables para mitigar los riesgos del negocio.
- Son utilizados para reducir la cantidad de brechas que llegan al SOC.
- Alineados con normas regulatorias.

NIVEL PROACTIVO

- TECNOLOGÍA: BDS, Monitoreo de usuarios y comportamiento.
- PROCEDIMIENTOS: Simulaciones de brechas, baselines.
- PERSONAS: Organización posee Security Awareness Training.

Características:

- Se reduce el número de incidentes porque las personas se encuentran concientizadas.
- No solo se trata de prevenir sino que se piensa en la potencial brecha.
- La empresa hace ejercicios de simulación de brechas para medir su manejo de incidentes.

- La simulación y el análisis de brechas permite mejorar los controles de los servicios reactivos.

- Análisis de amenazas de día cero, APT, mayor visibilidad de métodos de ataques conocidos.

- Monitoreo para entender anomalías y afinar los casos de curso.

NIVEL AUTOMATIZADO

- TECNOLOGÍA: Machine Learning, Inteligencia Articial.
- PROCEDIMIENTOS: Índices de Comprometimientos.
- PERSONAS: Nivel estratégico de investigación ya que la tecnología se encarga de los procesos rutinarios.

Características:

- Se eliminan procesos rutinarios de investigación y análisis ya que lo hace la teconología, por ejemplo, el análisis de vulnerabilidades y hacking ético se realiza a través de agentes automatizados.

- Se utiliza tecnología que en base a índices de comportamiento, descrube nuevas amenazas en base a Machine Learning e Inteligencia Artificial.

- Creación automática de reglas de seguridad en soluciones perimetrales y en el endpoint para blindar y contener una brecha.

- Información utilizada para descubrir nuevos métodos de ataques y realizar investigación avanzada.

- Permite hacer ingeniería reversa de malware para mejorar los controles proactivos.

Seguridad informática SOC / CERT

Prevención proactiva de incidentes de seguridad, monitoreo, detección y análisis en tiempo real de actividades anómalas, a través de la recolección y retención de archivos de logs provenientes de distintas fuentes de datos.

Respuesta de incidentes por medio de la coordinación efectiva de recursos, mediante el uso apropiado del tiempo, herramientas y la aplicación de un plan de contramedida.

Proporcionar el status del nivel de seguridad de la empresa por medio de reportes basados en alertas, incidentes y tendencias de seguridad.

Proporcionar la infraestructura adecuada y personal calificado para las operaciones designadas.

Concientización de usuarios y entrenamiento (e-learning).

Ayudar en el cumplimiento de normativas de seguridad tales como: PCI DSS, ISO 27001, entre otros.

Base instalada de Radical

Entre los clientes que tenemos:

SECTOR GUBERNAMENTAL

- Instituto Ecuatoriano de Seguridad Social.
- Comando Conjunto de las Fuerzas Armadas.
- Corporación Nacional de Telecomunicaciones.
- Superintendencia de Bancos del Ecuador.
- ASTINAVE
- Servicio de Rentas Internas, entre otros.

SECTOR PRIVADO

- Cooperativa “29 de octubre”.
- Aseguradora del Sur.
- PEPSICO, entre otros.

SECTOR FINANCIERO

- BanEcuador.
- Banco Central del Ecuador.
- Banco Pichincha.
- Banco de Loja.

SECTOR ACADÉMICO

- Yachay.
- Universidad de las Fuerzas Armadas.

Experiencia de Radical

Radical tiene más de 18 años en el mercado ecuatoriano ofreciendo soluciones innovadoras de tecnología. A continuación un breve resumen de las principales implementaciones:

- Del 2001 al 2009 fue la representante de la marca 3Com en el Ecuador.
- En el año 2001 implementamos la primera solución de telefonía IP en Ecuador.
- En el año 2005 implementamos la primera solución de Sistemas de Prevención de Intrusos en el Ecuador en el Comando Conjunto de las Fuerzas Armadas.
- En el año 2009 implementamos la segunda red nacional de MPLS del Ecuador en el Comando Conjunto de las Fuerzas Armadas.
- En el año 2010 presentamos la primera solución de Antimalware más grande a nivel nacional en el IESS para 15.000 usuarios.
- En el año 2013 implementamos la solución de Seguridad en el ISP más grande del país la Corporación Nacional de Telecomunicaciones, CNT, para dar servicio a todo el sector Gobierno. USD 11,2M.
- En el 2014 realizamos la primera implementación en el Ecuador de Data Centers Modulares en Yachay e Hiperconvergencia.
- En el 2015 implementamos el primer SOC en el Ecuador.
- En el 2016 el Banco Pichincha contrata los servicios del SOC de Radical recibiendo el reconocimiento de la ARCOTEL por las labores realizadas en Ciberdefensa y comienza el CERT de Radical.
- En el 2017 Radical comienza la instalación el Data Center Modular de CENTURYLINK en Quito.
- En el 2018 somos reconocidos a nivel mundial por LACNIC y FIRST como CERT especializado en Gobierno, Banca e Infraestructuras Críticas.

Data center e infraestructura

Nuestro principal objetivo es brindar apoyo a nuestros clientes para que tengan una plataforma tecnológica moderna y adecuada para enfrentar los continuos cambios tecnológicos. Y de esta manera puedan potenciar su producción a menor costo y con el mayor alcance hacia sus clientes.

Oferta hiperconvergente

Las soluciones hiperconvergentes permiten que el procesamiento, la memoria y el almacenamiento se encuentren en el mismo hardware. Por lo que consumo de energía y espacio se reduce y es posible eliminar de manera drástica la complejidad del almacenamiento.

Security center

Debido a la contínua evolución de la tecnología las organizaciones enfrentan un constante cambio en el entorno de riesgo.

Esta evolución tecnológica convierte a la detección y respuesta de incidentes de seguridad de la información en un desafío para las empresas.

Por este motivo buscamos ser ese aliado estratégico para que las empresas puedan generar mayores ingresos y evitar perjuicios por atacantes, por robos, por fuga de datos, por fraude.

De la misma manera que ellos puedan optimizar sus potenciales digitales para que sus clientes puedan confiar en ellos.

Esto lo logramos con el Security Center que está desarrollado para prevenir, detectar, analizar, contener, responder, remediar ataques cibernéticos a través de tecnología de punta, personal certicado y procesos alineados a estándares internacionales.

Seguridad en Redes SCADA

Un sistema SCADA puede afrontar varios incidentes como un retraso o bloqueo del flujo de información que podría interrumpir su funcionamiento, cambios no autorizados que puede ocasionar daños, infecciones malware tanto en servidores como en computadoras de operarios e incluso interferencia en el funcionamiento de los sistemas de seguridad lo que podría poner en riesgo los equipos y la vida humana.

Nosotros ayudamos a las empresas que tienen infraestructuras críticas como las de manufactura, eléctricas, gas, petróleo, entre otras, a entender y detectar estas amenazas, anomalías y ataques sobre la Red SCADA y poder contenerlos a tiempo.

CERT RADICAL

C-SIRT / Computer Security Incident Response Team

- Personal técnico especializado a desarrollar medidas preventivas y reactivas para contener/mitigar incidentes de seguridad informáticos.
- Centro de referencia en seguridad de la información y empleo de nuevas tecnologías de vanguardia.
- Equipo en pro de la mejora de la seguridad informática con base a la promoción de una cultura de ciberseguridad y buenas prácticas tecnológicas

SOC / Security Operations Center

- Central de monitoreo de seguridad de sistemas informáticos las 24 horas del día.
- Diseño y entrega de servicios en pro de la detección y gestión de amenazas cibernéticas que puedan afectar al core del negocio de una organización.
- Personal especializado con procesos y tecnologías que brindan visión de la seguridad de su organización a través de la primera fase que es la detección, con recomendaciones que lleven a la contención y remediación de las amenazas de TI.

NOC / Network Operations Centers

- Monitoreo de las redes en función de alarmas que indiquen atención prioritaria para evitar impacto en el rendimiento de las redes informáticas de una organización.
- Supervisar y garantizar la estabilidad, capacidad y el buen funcionamiento de la infraestructura de red.

Radical cuenta, entre otras, con las siguientes certificaciones internacionales: DCOS en Operations & Maintenance, SOC³ Sky Trust for Service Organizations, ISO 27001:2017, ISO 9001:2015, ISO 20000:2011, en integración de múltiples plataformas, recolección, retención de logs, análisis de logs y monitoreo de eventos de seguridad, Identificación de amenazas de seguridad, gestión de incidentes y reportes, reacción y control ante amenazas, y soluciones con medidas preventivas.

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

ICSPA

FIRST
Improving Security Together

WARP

CERTIFIED SCADA SECURITY ARCHITECT
IACRB

///AXUR

TREND MICRO

TippingPoint
IPS Expert

ISO 20000:2011

ISO ISO/IEC 27001:2017

ISO 9001:2015

NUESTROS CLIENTES

Telefónica

Agencia de Regulación y Control Hidrocarburífero

EMPRESA ELÉCTRICA QUITO S.A.

Ministerio de Educación

cnt

INEN Servicio Ecuatoriano de Normalización

Registro Civil
Identificación y Cedulación

PEPSICO

BANCO PICHINCHA

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

iess

RadicalLatam @RadicalLatam GrupoRadical

GRUPORADICAL.COM
info@gruporadical.com

ECUADOR
Telfs.: (+593) 23909088 - (+593) 993700193

Pedro Ponce Carrasco E8-06 y Av. Diego de Almagro,
Edif. Almagro Plaza, Of. 816.
Quito -Ecuador

PERÚ
Telfs.: (+51) 959787551 - (+51) 946 422 167

Av. Salaverry 2415, Torre B, oficina 406. San Isidro.
Lima - Perú

BOLIVIA
Telfs.: (+591) 33218852 - (+591) 78458202

Av. San Martín, calle Begonias #38. Santa Cruz.
Santa Cruz - Bolivia

marketing@gruporadical.com