2021

Estado de la Seguridad Digital de las empresas en España según las propias compañías

opencloud factory

opennac enterprise

Índice

Introducción

En diciembre tuvieron lugar las XIV Jornadas STIC organizadas por el **CCN-CERT**. En una edición distinta (no presencial) por la situación actual pero tan enriquecedora e interesante como todas las anteriores, decidimos contar con buena parte de los Responsables de Seguridad de la Información asistentes a dichas Jornadas para llevar a cabo nuestra Segunda Edición del Informe de Estado de Seguridad de las empresas en España según las propias compañías. Queríamos contar, un año más, con sus impresiones acerca del escenario de seguridad digital para este 2021 que afrontan tanto empresas privadas como administración pública basada en su experiencia en el día a día.

A lo largo de las próximas páginas el lector podrá ver **cómo los Responsables de Seguridad han percibido el impacto del Covid en la operativa de ciberseguridad de sus empresas y organismos, así como cambios significativos respecto a concienciación y presupuesto derivados de la situación originada por la pandemia.** Así, desde OCF hemos decidido incluir los datos más relevantes del año anterior para que el lector del presente informe pueda tener una perspectiva certera de evolución y cambio respecto a diferentes cuestiones.

La pasada edición de este informe fue un éxito en cuanto a participación y público interesado en conocer la percepción en cuanto a ciberseguridad de sus homólogos. Por ello, desde **Open Cloud Factory** queremos consolidar este informe un nuevo año contando con el doble de participantes en la encuesta que en la anterior edición (representantes de más de 150 empresas y organismos públicos).

Para **Open Cloud Factory** y de acuerdo con el éxito del presente informe en su anterior edición, es un orgullo poder aportar la visión de buena parte de las personas implicadas a diario en la seguridad digital de las principales empresas y organismos del país y extraer conclusiones a partir de sus respuestas.

La consecución de este informe es motivo de orgullo para nosotros, al igual que también lo es la reciente aparición de nuestra tecnología en el Gartner Market Guide for Operational Technology Security (siendo el segundo Market Guide de la prestigiosa consultora Gartner en el que somos incluidos, junto al Market Guide for Network Access Control), así como la inclusión de OCF en todas las categorías del ECSO Cybersecurity Market Radar (principal organismo de ciberseguridad a nivel europeo).

*Como CEO de **Open Cloud Factory**, espero que el presente informe te resulte una guía útil e interesante para ti y tu organización. Disfruta de su lectura.*

Albert Estrada
CEO y Fundador Open Cloud Factory

Key Findings de este informe

Se ha duplicado el número de empresas que perciben que su seguridad digital es baja

En 2020

se incrementó en un 150% el número de empresas que llevó a cabo un proyecto Cloud

70%

de los ataques a empresas estuvieron relacionados con accesos no autorizados y ataques de ingeniería social.

83%

de las empresas está sujeta a un marco de buenas prácticas.

Sectores encuestados

En esta encuesta han participado, principalmente, empresas de seis sectores: Tecnología, Educación, Servicios, Finanzas, manufacturación y otros como medios de comunicación, sanidad y energía. Además, ha participado una amplia representación del sector público español.

40%
Administración Pública

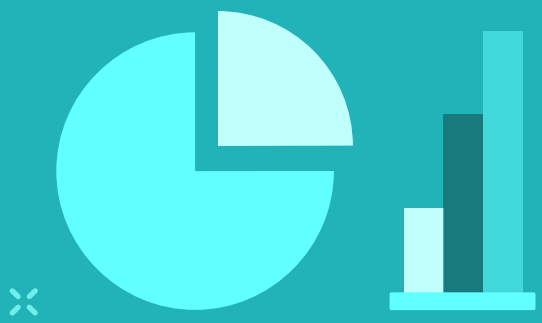
29%
Tecnología

11%
Finanzas, Manufacturación y otros

10%
Educación

10%
Servicios

Principales resultados de la encuesta



Manteniendo el enfoque en una nueva edición de este documento, las propias empresas contestarán a esta pregunta:

¿Cuentan las empresas con un nivel de seguridad digital aceptable?

A través **17 preguntas con una muestra de más de 150 compañías y organismos de la administración pública**, así como el análisis de las respuestas de las empresas por parte de Open Cloud Factory, extraeremos una serie de conclusiones sobre los conceptos más relevantes para conseguir una seguridad digital robusta.

Aumenta la concienciación de las empresas en términos de seguridad y baja la percepción de disponer de un presupuesto adecuado. Son dos hechos relacionados entre sí, ya que una vez se es consciente de la importancia de la ciberseguridad el siguiente paso es tratar de encontrar los recursos para asumir el reto de establecer controles de seguridad y con ello evaluar el presupuesto asignado a dicho objetivo.

1. Aumenta la concienciación de las empresas en términos de seguridad, baja la percepción de disponer de un presupuesto adecuado.

La seguridad digital de las compañías tiene que ser uno de los puntos de mejora constante que las empresas han de establecer. La seguridad digital permite mantener el resto de los procesos de la organización en marcha: una pequeña brecha en la seguridad supone una gran fuente de riesgo por donde pueden colarse las amenazas que tratan de alterar las cadenas de producción, la gestión de datos o comprometer información importante para la empresa.

Por tanto, **un nivel bajo de seguridad digital aumenta la posibilidad de fracaso en la consecución de los objetivos de la empresa.**

El 90% de las empresas conoce los beneficios de desarrollar planes de seguridad digital en su empresa y el riesgo de descuidarla y consideran que la importancia que tiene la seguridad digital en su empresa es, por lo menos, adecuado. Más de la mitad opina que la importancia que tiene es muy alta.

90%

de las empresas conoce los beneficios de desarrollar planes de seguridad digital para su empresa. Esto contrasta con la asignación de presupuesto, que no cuenta con el mismo nivel de importancia.

Estos datos contrastan con la asignación de presupuesto, que no refleja el mismo nivel de importancia. La inversión en ciberseguridad de las compañías es menor que el grado de percepción de importancia de la seguridad digital. El número de aquellas empresas que consideraban que tenían un presupuesto alto el año pasado se ha reducido a la mitad mientras que se ha duplicado el número de empresas que lo consideran bajo.

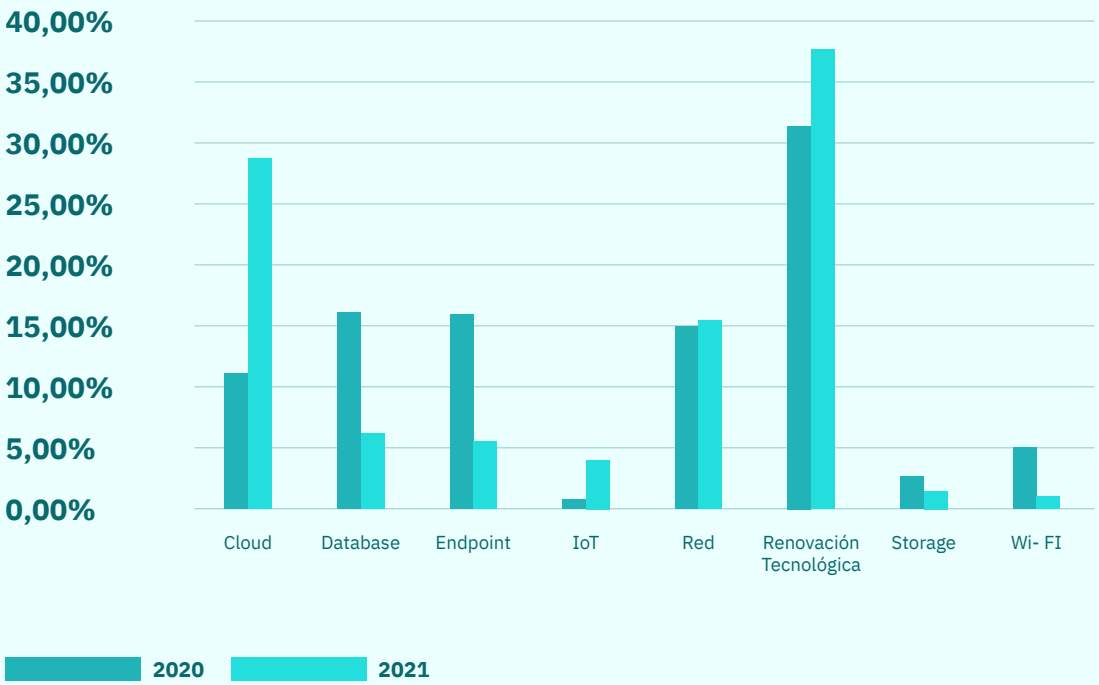
Está claro que el contexto actual de teletrabajo ha dejado en evidencia la falta de herramientas tecnológicas para establecer medidas de contingencia seguras en tiempos de pandemia. En la mayoría de los casos los empleados entendieron lo imperativo que resulta contar con herramientas seguras de trabajo. Para algunos de estos casos los empleados notaron que sus empresas no contaban con la infraestructura requerida y su conclusión fue que las organizaciones no asignan el presupuesto adecuado a las cuestiones de ciberseguridad.

Suponemos que los retos afrontados a consecuencia del teletrabajo generalizado a causa de la pandemia han dejado entrever las debilidades y el mayor esfuerzo necesario para reforzar la seguridad. Un año más sigue siendo mayor el número de empresas que conocen la importancia de seguridad digital frente aquellas que destinan un mayor presupuesto.

El departamento encargado de la seguridad tiene asignado un presupuesto que después se divide en distintas porciones para diversos proyectos o gastos fijos. Durante la encuesta se ha preguntado acerca de los proyectos de nuevas tecnologías que las empresas han llevado a cabo.

La renovación tecnológica sigue siendo el proyecto más comúnmente llevado a cabo entre las empresas debido a la alta obsolescencia que tienen los dispositivos tecnológicos. Este hecho hace que se reduzca la cantidad de presupuesto destinado a otros proyectos que sirven para mejorar los procesos en cuanto a eficiencia o seguridad. Pese a ello, durante el último año se han disparado los proyectos de implementación de Cloud entre las empresas. La necesidad de teletrabajar durante el último año y el cambio de procesos que ello supone hizo obligatorio buscar formas alternativas para dar continuidad al trabajo. **Los proyectos de Cloud permitieron a las empresas continuar con su operación, acceder de manera remota a la información y los servicios corporativos necesarios para poder garantizar la continuidad del negocio, por eso se han incrementado en un 150% con respecto al año anterior.** En cambio, el gasto en mejoras de servicios que suponela presencialidad se ha reducido significativamente.

Proyectos de Tecnología llevados más comúnmente a cabo por las empresas

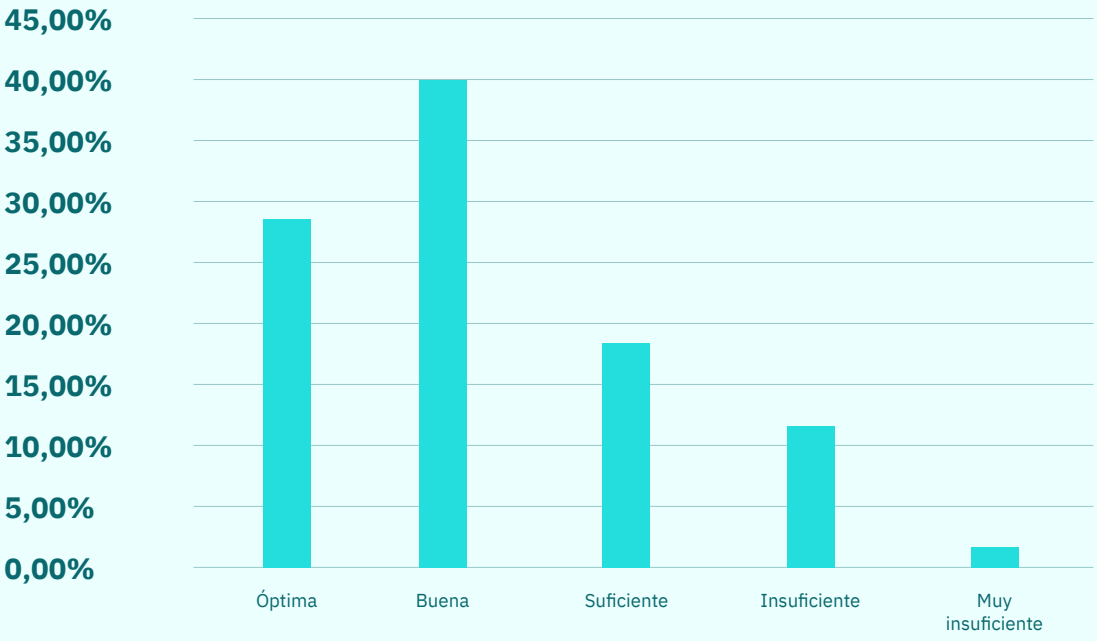


2. ¿Cómo ha sido la respuesta de las empresas en españa al coronavirus y sus desafíos en términos de seguridad?

El Covid-19 ha cambiado muchos escenarios de la cotidianidad, entre ellos ha modificado de manera notable la forma de trabajar en todo el planeta desde principios de marzo. Se declaró la situación de confinamiento para gran parte de la población, lo que suponía que la prohibición de los desplazamientos excepto para aquellos servicios esenciales y que requiriesen una presencialidad. Esto hizo que las empresas llevaran a cabo la implementación de teletrabajo como medida de contingencia para mantener la operación de las empresas; sin embargo, no todas estaban preparadas para este cambio.

Hemos querido conocer cómo fue este proceso para empresas y organizaciones y qué efectos trajo consigo el teletrabajo por lo que desde Open Cloud Factory preguntamos cómo había sido la respuesta de las organizaciones en términos de ciberseguridad.

Valoración de la respuesta de las empresas ante el Covid-19 en términos de ciberseguridad



5. ¿Cómo considerarías que ha sido la respuesta de tu compañía/organismo ante los desafíos del coronavirus en términos de ciberseguridad?	2020	2021
Óptima	N/A	28,50%
Buena	N/A	40,00%
Suficiente	N/A	18,20%
Insuficiente	N/A	11,50%
Muy insuficiente	N/A	1,80%

Casi el 90% considera que la respuesta ha sido por lo menos suficiente, de ellos un 40% considera que la gestión fue buena.

Tan solo poco más de un 10% de los encuestados consideran que la respuesta de sus compañías/ organismos ante los desafíos del coronavirus en términos de ciberseguridad ha sido deficiente.

90%

de las empresas piensa que la gestión de sus empresas frente al Covid-19 en términos de seguridad fue buena.

Al tomarse medidas de contingencia para la operación de las empresas bajo el contexto actual, se hacía evidente que el teletrabajo iba a significar una oportunidad para los cibercriminales para atacar a las empresas debido a que no todas estaban preparadas para trabajar de un modo remoto. Entre los tipos de ataque más comunes destacan la ingeniería social y los accesos no autorizados, juntos suponen casi el 70% de los ataques a empresas.

El teletrabajo puede ser una forma más por parte de las empresas de llevar a cabo las operaciones; sin embargo, no siempre es segura, por lo que hay que tomar los resguardos pertinentes y las medidas necesarias para garantizar la seguridad. El uso de conexiones VPN para los usuarios, la implantación del segundo factor de autenticación, el principio del mínimo privilegio y el zero-trust entre otras medidas, son iniciativas clave para mantener los valores de riesgo en niveles aceptables.

El presente año ha demostrado que varias de las medidas adoptadas por las empresas para hacer frente a los efectos de la pandemia han venido para quedarse. Es importante saber que, si bien la implantación del teletrabajo antes del COVID-19 estaba en auge, no se trataba de una medida generalizada, ya que muchas empresas lo tenían incorporado de manera parcial. Sin duda, estas compañías tuvieron un ventaja sobre las demás ya que su esfuerzo se enfocó en hacer expansiva la medida de teletrabajo y escalar las plataformas tecnológicas a toda la organización.

El teletrabajo trae consigo una concienciación sobre los asuntos de seguridad, incluso para aquellos que no se lo habían cuestionado previamente; el hecho de acceder a servicios e información corporativa de forma remota incrementa y hace evidente las brechas de seguridad de los accesos corporativos. Recordemos que en 2020 se duplicó la cantidad de personas que piensan que la ciberseguridad en sus empresas es baja. Es posible que esto esté vinculado con la mencionada debilidad del acceso remoto a los recursos, que evidencia la necesidad de implementar controles de acceso y de securizar los accesos a servicios y/o información corporativa.

Los resultados muestran que **los proyectos Cloud se han incrementado en un 150% respecto al año anterior.** Llevar los servicios y la información con un proveedor de Cloud libera a las organizaciones de la publicación de servidores corporativos en internet y ejecuta una estrategia de gestión de riesgo conocida como trasferencia de riesgo a su proveedor de Cloud. Los efectos de las medidas de contingencia de la pandemia han afectado al roadmap tecnológico de las organizaciones y han acelerado los procesos de modernización de sus infraestructuras corporativas.

3. El 83% de las empresas está sujeto a un marco de buenas prácticas.

Las compañías tienden a adoptar estándares como ISO 27001, NIST, ENS, entre otros; buscando una guía de buenas practicas para gestionar los diferentes asuntos de seguridad que tienen lugar en el día a día de los departamentos de IT. Gestionar los asuntos de seguridad con un enfoque de riesgo, permite a las organizaciones incrementar sus niveles de concienciación y seguridad.

En España el 83% de las empresas está sujeta a un marco de buenas prácticas que le señala cómo administrar la infraestructura de red para reducir al mínimo los riesgos. Estos estándares aportan otros beneficios como la mejora de la confianza del mercado, la mejora de la imagen, focalizar mejor los esfuerzos de ciberseguridad y evitar las pérdidas de servicios ante una caída de los sistemas.

España tiene su propio estándar de seguridad y que es de obligatorio cumplimiento para las organizaciones públicas y sus proveedores: el **Esquema Nacional de Seguridad**. Este es aplicado por un 38% de las empresas encuestadas. **ISO 27000** es el segundo estándar de buenas prácticas más adoptado con un 27% de las empresas. Por otro lado, el 17% de las compañías no se ajustan a ningún estándar de seguridad todavía, un número significativamente importante. La adopción a un estándar de seguridad se considera un paso necesario en la madurez de los departamentos de IT. Adoptar un framework constituye principalmente un reaprovechamiento de trabajo que ha sido contrastado y estandarizado para no empezar desde cero en el establecimiento de un sistema de gestión de seguridad, conforme a lo anterior es de esperar que según pase el tiempo más empresas empezarán con la adecuación de un estándar de buenas prácticas.

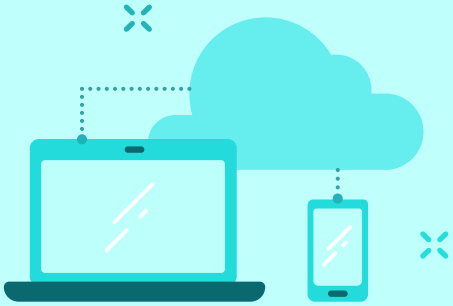
> El ESN es aplicado por un **38%** de las empresas encuestadas. ISO 27000 es el segundo estándar de buenas prácticas más adoptado con un **27%** de las mismas

Una vez las empresas adoptan un marco de buenas prácticas, el proceso es cíclico. La dinámica de **Planear-Hacer-Verificar-Actuar** se convierte en el día a día de las áreas involucrados en las auditorías. Los procesos de auditoría y sus beneficios están bien extendidos entre las empresas: un 60% de ellas tiene entre sus planes de ciberseguridad para el presente año llevar a cabo, al menos una vez, un proceso de auditoría. Este hecho posiciona fundamentalmente a las herramientas que apoyen la auditoría por medio de la automatización de tareas repetitivas como el reporting o el chequeo rutinario.

A menudo la falta de actualización de informes y, en genera,l de la información usada en las auditorías, se encuentra ligada a procesos manuales y, puntualmente, a recursos. La selección de herramientas de automatización de tareas operativas en los departamentos de IT es fundamental para la aceptación, puesta en producción y, en general, el aprovechamiento de una determinada plataforma.

Debido a la naturaleza cíclica de los procesos de auditoría, y la falta de tiempo por parte de la persona a cargo de las actividades reiterativas que demanda cada fase de una auditoría, los departamentos de IT buscan la forma de trasladar estas tareas a recursos más operativos; sin embargo, lo idóneo sería buscar el apoyo de una herramienta tecnológica capaz de llevar a cabo esta labor.

4. Más de un tercio de las empresas no dispone de una herramienta específica para gestionar los accesos a la compañía



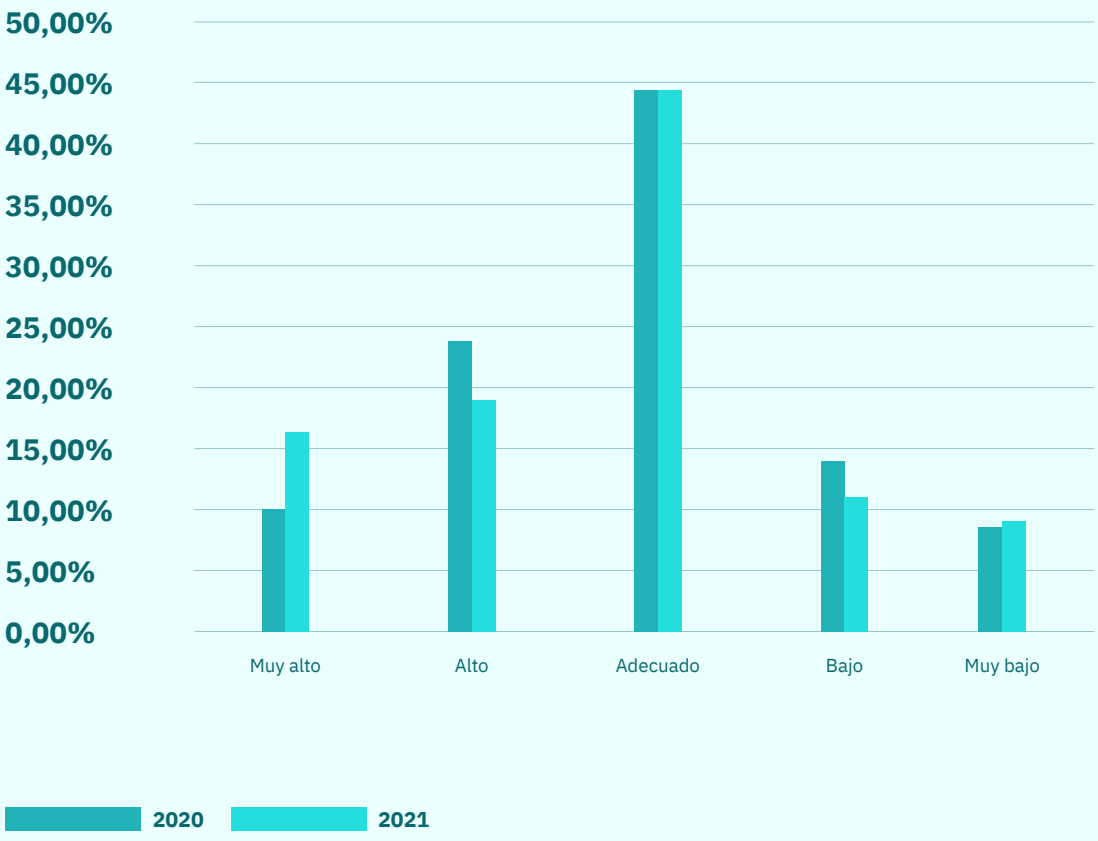
La oferta de herramientas de seguridad en el mercado es muy amplia. Estas soluciones tienen como objetivo proteger al menos una parte de la superficie de ataque de las empresas; sin embargo, existen plataformas fundamentales para el establecimiento de buenas prácticas o directrices básicas de seguridad en las empresas. Este es el caso de los firewalls, las herramientas de control de acceso, o los antivirus, entre otras.

El nivel de concienciación en ciberseguridad año a año se incrementa. Para 2020 hubo una palanca adicional para que los trabajadores entendiéramos de manera reactiva la importancia de la seguridad informática en los ambientes corporativos. La protección en los accesos a los recursos corporativos es fundamental, así como ejercer control de acceso para conexiones en la red cableada, Wi-Fi y VPN es obligatorio cuando se quieren establecer las bases de seguridad en las organizaciones. Por ello el 90% de las organizaciones consideran importante la implementación de un **NAC** en la red corporativa . Una herramienta de **NAC** permite controlar el acceso, establecer políticas de seguridad, aportar visibilidad y gestionar la respuesta ante incidentes, entre otros. El 81% de las compañías consideran que el sistema de control de acceso a los recursos corporativos que tienen activo es al menos adecuado para sus necesidades .

El **90%**
de las organizaciones consideran importante la implementación de un NAC en la red corporativa

Los resultados de la encuesta muestran que un 36% de las empresas no disponen de un canal específico para el acceso de terceros a los recursos de la compañía. Este dato contrasta con el bajo porcentaje, tan solo un 20% de las empresas que creen que su nivel de control de accesos de terceros es bajo o muy bajo. Este número representa más de la mitad de las empresas que no consideró tener un control de acceso a los recursos por parte de terceros, es decir que pese a no gestionar este tipo de accesos de forma especial consideran que su nivel de seguridad es adecuado. Esto evidencia que la **percepción de seguridad es mayor a las medidas eficaces para gestionar los riesgos.** La fuga de información y el acceso no autorizado son riesgos básicos que deben gestionarse en todos los niveles, implementar controles para terceros e invitados es fundamental en ese propósito. En general el control de accesos de terceros es un factor que está bien regulado y así lo creen las empresas que han contestado a la encuesta ya que el 79% consideran apropiado el Control de Acceso de Red de invitados.

Valoración por parte de las compañías del nivel de seguridad en el Control de Acceso de Red y Servicios



Resumen del informe

1 El año 2020 ha sido un año marcado por la pandemia y los cambios que esta ha producido. El mundo de ciberseguridad ha vivido, más que un cambio de tendencia, una aceleración de los procesos hacia los que el mercado iba evolucionando según la dinámica de la sociedad, aumentando considerablemente la concienciación en ciberseguridad.

2 La mayoría de empresas implementó el teletrabajo pese a que este tipo de trabajo no era una realidad para muchas antes de marzo. Según los propios empleados el 90% de las empresas han superado de una forma adecuada los retos que el teletrabajo supuso.

3 La importancia de la seguridad digital en las empresas se ha mostrado evidente a la hora de establecer prioridades, aunque muchas veces esta concienciación no se traduce en una aumento de asignación del presupuesto.

4 El presupuesto está destinado principalemte por la renovación de dispositivos, aunque se ha podido comprobar que este año ha supuesto un punto de inflexión para las tecnologías de Cloud ya que su implementación se ha incrementado un 150% respecto al año anterior.

5 Además, se ha hecho necesario también contar con un sistema que regule el acceso remoto a las redes corporativas. **Las encuestas muestran que el 90% de las empresas considera que una plataforma de control de acceso a la red es una pieza necesaria en su esquema de seguridad corporativo.**

OpenNAC Enterprise es la solución perfecta para la visibilidad, control y compliance de la red corporativa.

Una solución **NAC** (Network Access Control) de visibilidad y control es una pieza fundamental en las infraestructuras IT como indican casi la totalidad de empresas encuestadas (el 90% de las mismas).

Una solución **NAC** gestiona no solo accesos en la red local, sino también accesos en la red de invitados o accesos remotos vía VPN; incluso podría soportar la implementación de más de un factor de autenticación para la validación de identidades.

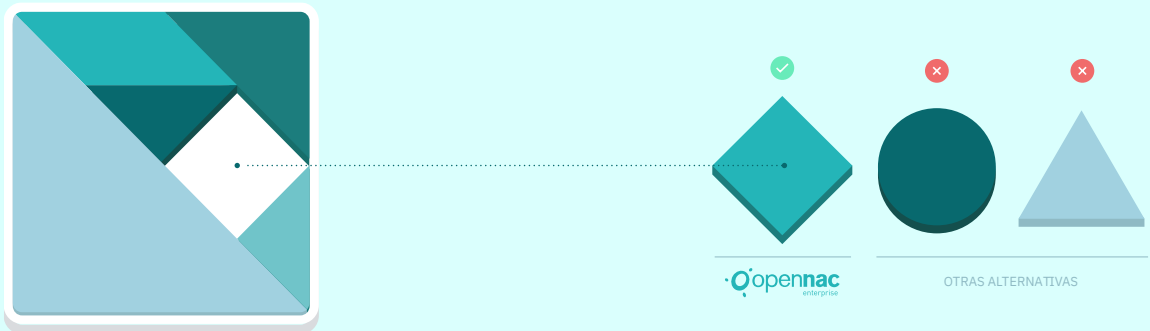
Es imperativo contar con una plataforma **NAC** en las empresas para empezar a establecer los controles básicos de una arquitectura de red segura, que se ajuste con los marcos y estándares de buenas prácticas más conocidos del mercado.

En el escenario actual donde la masificación del teletrabajo es un hecho, como respuesta y medida de prevención de contagio del COVID-19, la implementación de soluciones de acceso remoto seguro es fundamental para la operación en el día a día de las compañías. Así como las personas nos hemos adaptado a las exigencias del contexto de pandemia, las tecnologías también lo deben hacer.
La característica más valorada cuando se habla de plataformas de IT es la adaptabilidad. El grado de adaptabilidad al negocio de las herramientas en IT determinará el valor que aportan, Permitirá el reconocimiento de su importancia como parte de la infraestructura tecnológica y será bien recibida por el equipo técnico. Es necesario que las nuevas tecnologías se acoplen al escenario actual, no agreguen esfuerzos de administración adicionales, sino mas bien automaticen algunas tareas recurrentes, liberando así al equipo técnico de tareas mecánicas.

Adaptabilidad y Personalización de **OpenNAC Enterprise.**

A menudo, las plataformas de seguridad IT presentan demasiadas funcionalidades y demandan despliegues muy robustos. Desde el primer momento parecen muy complejas, nublan el objetivo estratégico de su implantación y terminan por causar mayor resistencia al cambio por parte de los equipos técnicos.

OpenNAC Enterprise se adapta al negocio desde el momento en que se conciben objetivos empresariales por los que se contempla la implementacion de una plataforma de visibilidad y control de acceso. Los clientes pueden personalizar la composicion del producto, el despliegue y la operación, incluso pueden ajustar los dashboards de control, la administración y el reporting de la plataforma, que entre otras cosas agilizara las tareas del equipo técnico.



Modularidad

En primer lugar, la adaptabilidad de **OpenNAC Enterprise** se presenta por medio de su enfoque modular, esta caracteristica de modularidad permite obtener mayor valor de la plataforma en menor tiempo, permite también centralizar esfuerzos y focalizar objetivos durante su implantación. Las empresas puede elegir únicamente el módulo de interés, **OpenNAC Enterprise** se puede adquirir e implementar por módulos funcionales, desplegando sólo las funcionalidades que se adapten a la necesidad de la compañía, de esta manera se reducen riesgos e impactos operacionales durante el proceso de implementación y su despliegue ocurre de manera muy ágill.

Las soluciones tradicionales de visibilidad y control de acceso obligan las empresas a adquirir e implementar una solucion completa que en la mayoria de los casos resulta sobre dimensionada, este hecho genera gran impacto financiero y operacional. **OpenNAC Enteprise** tiene un diseño compuesto por 7 módulos: Visibility, UNAC, Segmentación, Compliance, BYOD, Guest y 2SRA. Cada módulo está orientado a una función determinada que se adaptará a las necesidades especificas del cliente. Las organizaciones unicamente pagaran por el modulo que solucione su problemática.

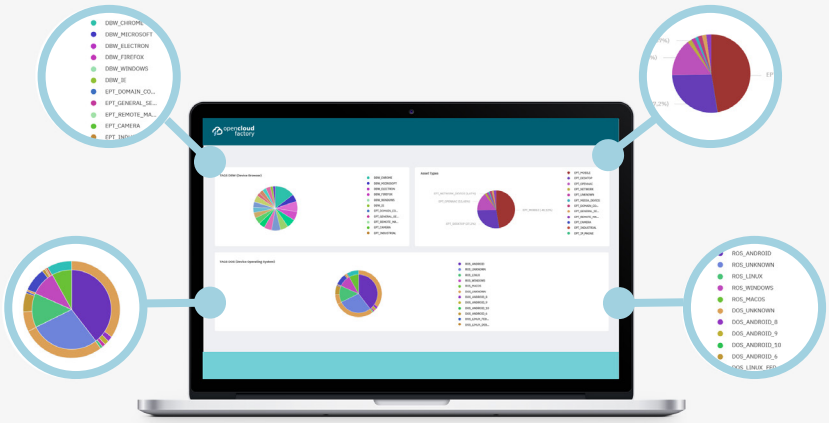
Personalización de Dashboards en OpenNAC Enterprise

Una de las características **más destacadas de OpenNAC Enterprise es la personalizacion de Dashboards de control.** Todos los dispositivos, sus características asociadas y datos recopilados por OpenNAC Enterprise son almacenados en su CMDB y pueden ser explotados de diferentes formas de acuerdo con el requerimiento o el objetivo de cada compañía; de esta manera, satisface la necesidad especifica demandada por el cliente.

Por ejemplo, las empresas que aborden procesos de auditorias de IT que contemplen "Hardening" de dispositivos de red, validación de software instalado en los dispositivos de usuario o el establecimiento de líneas base de configuración; necesitan conocer el avance de implementación de las líneas base, o la mitigación de algún hallazgo específico de la auditoría. Para estos casos, **OpenNAC Enterprise** cuenta con la capacidad de generar dashboards de control que muestran en tiempo real el estado del establecimiento de líneas base de configuración de dispositivos de red o líneas base de software corporativo en dispositivos de usuario, entre otros.

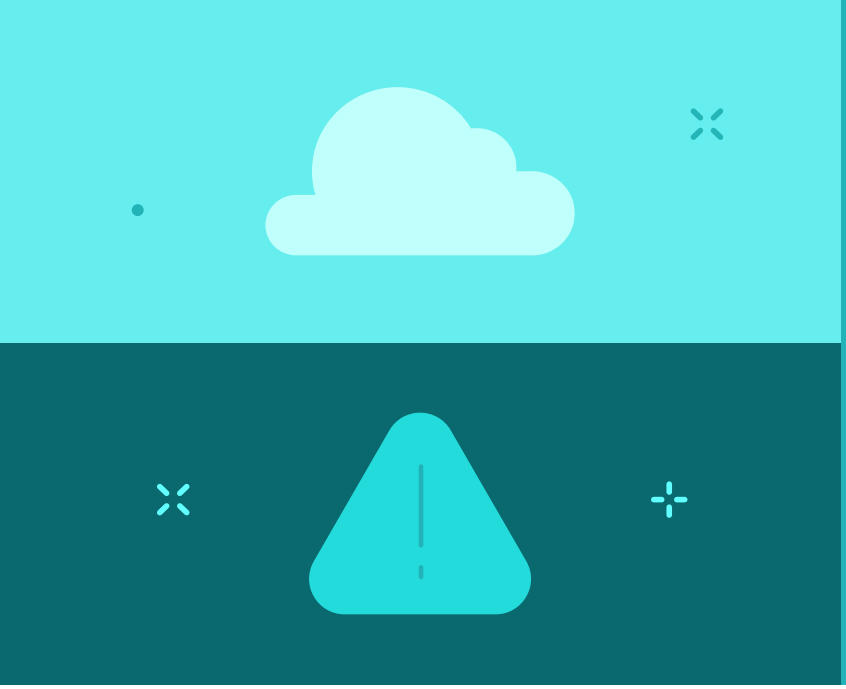
Esta característica resulta muy potente para determinar brechas de seguridad, adicionalmente ahorra tiempos empleados en la generación de reportes.

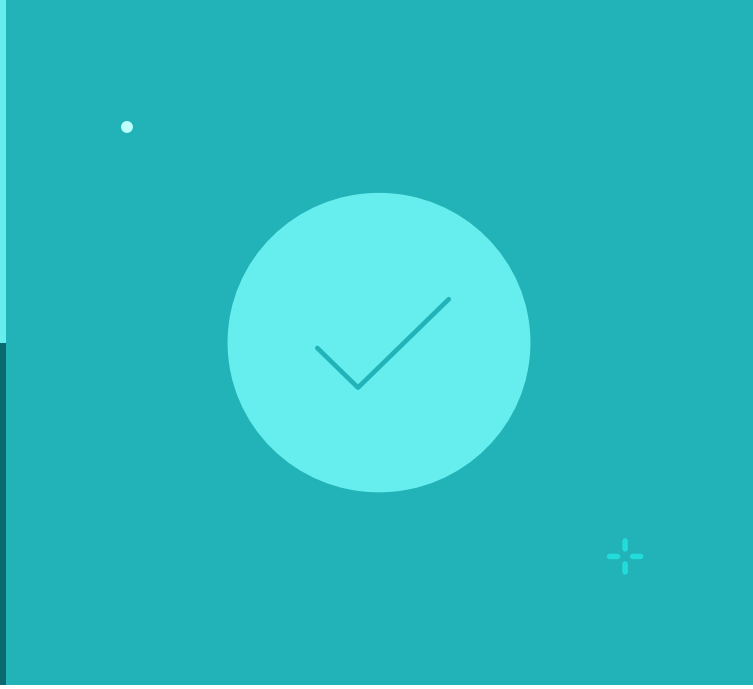
La capacidad de poder personalizar 100% los dashboard de control orientados específicamente a los requerimientos corporativos, dota a **OpenNAC Enterprise** de una capacidad única de adaptabilidad al negocio.



Características principales

- Visibilidad, cuantificación y perfilamiento de activos IT, OT, iOT.
- Monitorización en tiempo real del trafico y todas las conexiones realizadas en red.
- Validación de identidades con uno o dos factores de autenticación en redes cableadas, Wi-Fi y conexiones VP.
- Centralización de políticas de acceso y gestión de identidades.
- Segmentación y micro-segmentación de red, aislamiento de dispositivos, protección de activos críticos, reducción de superficie de ataque.
- Definición de líneas base de seguridad para postura de dispositivos de usuario, servidores y para configuración de los dispositivos de red.
- Automatización de los reportes de auditoria para conocer en tiempo real la brecha de cumplimiento y estimar el tiempo de remediación.
- Establecimiento de túneles VPN de usuarios remotos con 2FA, validación de postura de usuario y monitorización en tiempo real de trafico VPN
- OpenNAC Enterprise se despliega sobre máquinas virtuales, optimice el espacio de rack y escale fácilmente la solución.
- Use su actual infraestructura para enriquecer la información de red y sacar mayor provecho de su inversión a través de la integración con (SIEMs, NGFW, AVs, EDRs, MDMs..)
- Compre únicamente la característica que va a usar, ahorre dinero y optimice su presupuesto tecnológico.
- Se adapta a entornos de electrónica multivendor.
- OpenNAC Enterprise permite la implementación de los estándares de buenas practicas mas utilizados en el mercado: (NIST, ISO 27001, IEC 62443).





Reconocimientos

Gartner

Único fabricante europeo de tecnología NAC incluido en Gartner Market Guide.

Common Criteria

Plataforma certificada en Common Criteria 3.1 release 5 por parte del Organismo de Certificación del Centro Criptológico Nacional OC-CCN de España.

CCN-CERT centro criptológico nacional

Incluido en el catálogo de productos de Seguridad de las Tecnologías de la información y la comunicación del Centro Criptológico Nacional, Ministerio de Defensa - Gobierno de España.

Contacta con nosotros

opencloudfactory.com

+34 91 614 53 22

Twitter

Linkedin

YouTube

SPAIN

SEDE PRINCIPAL
Calle Segundo Mata, 6
Planta 1 Oficina 4B Pozuelo de Alarcón, 28224 Madrid

SPAIN

OCF Industrial Cybersecurity
C/ Gran Vía Don Diego López De Haro, 19-21 planta 2ª
48001 Bilbao

SPAIN

Centro de Desarrollo Barcelona. Carrer Sant Leopold 101, oficina 109, Terrassa, 08221

BRAZIL

Market Place Tower
Av. Dr. Chucri Zaidan, 920
9º andar Cordeiro, São Paulo, CEP: 04583-904

USA

Independence Wharf 470 Atlantic Avenue
Boston, Massachusetts 02210

MEXICO

Presidente Masaryk 111
Piso 1, Miguel Hidalgo
Polanco V Sección
11560 Ciudad de México

opencloud factory

opennac enterprise