ALE | Where Everything Connects

# Ciberseguridad en el campus en la era de IoT y del RGPD



Alcatel·Lucent Enterprise

## Tabla de contenido

# Introducción

La ciberseguridad del campus siempre es uno de los temas que más preocupan en la educación superior. Por segunda vez en tres años, la seguridad de la información encabezó la lista de la encuesta anual de Educause realizada a los directores de TI de educación superior sobre los 10 principales problemas de las TI[1]. Esto no debería ser una sorpresa, según el informe más reciente de investigación de infracciones de datos (Data Breach Investigations Report, DBIR) de Verizon[2]. El informe, que muestra una tendencia creciente de la ciberdelincuencia, identifica como los tres sectores más atacados los de finanzas y seguros, salud y educación.

La seguridad de la información en la educación siempre ha sido un tira y afloja entre la facilidad de uso y la seguridad total; a veces la seguridad gana, pero la prioridad suele ser la facilidad de uso. A esto se añade la nueva legislación europea sobre privacidad conocida como Reglamento General de Protección de Datos[3, 4], (RGPD) y la introducción de una amplia variedad de dispositivos IoT, por lo que es natural que la seguridad de la información y la protección de la reputación de la institución sean la principal preocupación de los directores de TI del sector de la educación.

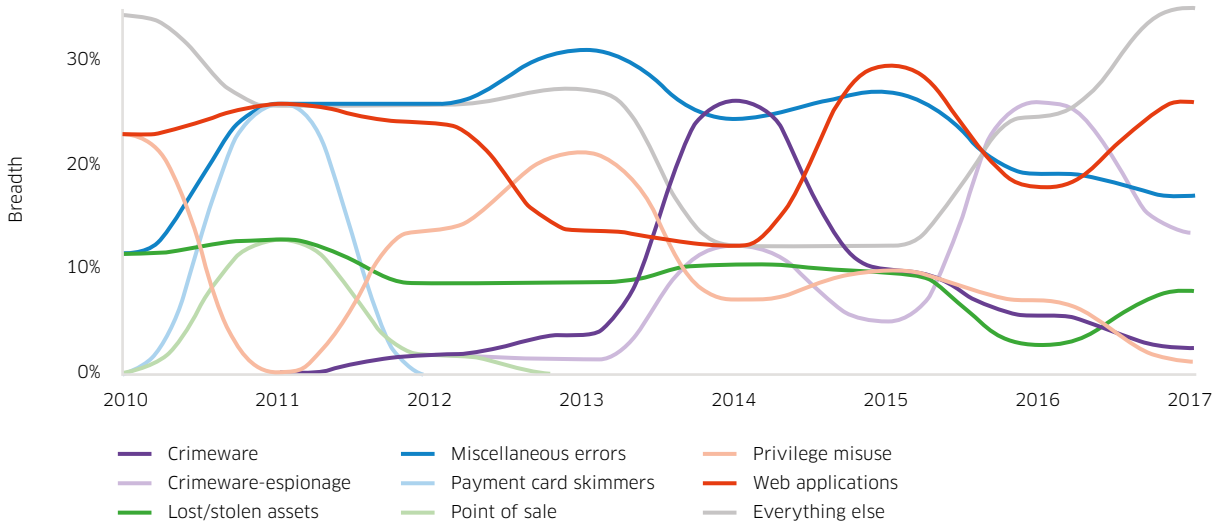
Este enfoque en la seguridad de la información llega en buen momento. Nunca antes la tecnología de la información ha desempeñado un papel tan importante en la educación. Ya sea a la hora de investigar sobre un tema lectivo o al enviar trabajos, la tecnología de la información está en el centro de la pedagogía y de las estrategias implementadas para identificar y ayudar al éxito académico de los estudiantes.

El Informe sobre investigación de infracciones de datos de Verizon de 2018 proporciona una perspectiva muy interesante sobre los vectores de ataque y las motivaciones de la actividad cibernética maliciosa.

**Tabla 1. Resumen de las infracciones de datos en el sector de la educación en 2017**

| | |
|---|---|
| Frecuencia | 292 incidentes, 101 con divulgación de datos confirmada |
| Tres patrones principales | Todo lo demás, los ataques de aplicaciones web y errores varios representan el 76 % de las infracciones |
| Actores de las amenazas | Externos (81 %), internos (19 %), partner (2 %), varios participantes (2%) (infracciones) |
| Motivos de los actores | Financieros (70 %), espionaje (20 %), diversión (11 %) |
| Datos comprometidos | Personales (72 %), secretos (14 %), médicos (11 %) |

**Figura 1. Patrones vistos en las infracciones en el sector de la educación**




1 EDUCAUSE Center for Analysis and Research (ECAR), "Top 10 IT Issues 2018," EDUCAUSE Research Snapshot, *EDUCAUSE Review*, 29 de enero de 2018.

2 Verizon Enterprise, "Verizon Data Breach Investigations Report (DBIR) 2018", abril de 2018, páginas 29-30

3 https://eugdpr.org

4 https://gdpr-info.eu

Esta papel blanco explora la implementación de estrategias de seguridad basadas en el riesgo, como el concepto de "defensa en profundidad". Este concepto promueve la protección de una red de equipos con una serie de mecanismos defensivos individuales, de modo que si se lanza un ataque, el atacante deberá traspasar varias capas independientes para tener éxito.

A lo largo de este documento se hará referencia a la "tríada CIA". Este concepto identifica los objetivos cibernéticos que poseen información "Confidencial", que afectan a la "Integridad" de la información o que impiden su "Accesibilidad". La tríada CIA es útil cuando se asignan valores de riesgo y se formulan políticas de seguridad en todo el campus. Por ejemplo, un ordenador portátil robado o perdido que contenga información de identificación personal (PII) se clasificaría como un ataque a la información confidencial y un hacker que modificase las notas con éxito estaría violando la integridad del sistema de información de los estudiantes. Asimismo, las impresoras BYOD que se encuentran en los dormitorios de los estudiantes podrían elegirse para participar en un ataque de Denegación de servicio (DoS), que se clasificaría como un ataque de disponibilidad, porque el objetivo de un ataque DoS es inundar un servidor web con tantas solicitudes falsas que el servidor dejará de responder a solicitudes legítimas.

A los efectos de este documento, las amenazas de seguridad de la información se denominarán actividades cibernéticas maliciosas, que el gobierno federal de los EE. UU. define como:

> "Actividades, distintas de las autorizadas por o de acuerdo con la ley de los EE. UU., que buscan comprometer o menoscabar la confidencialidad, integridad o disponibilidad de ordenadores, sistemas de información o comunicaciones, redes, infraestructuras físicas o virtuales controladas por ordenadores o sistemas de información, o la información que reside en ellos".

Estos son algunos ejemplos de los efectos de la actividad cibernética maliciosa:

> "La manipulación, interrupción, negación, degradación o destrucción de ordenadores, sistemas de información o comunicaciones, redes, infraestructuras físicas o virtuales controladas por ordenadores o sistemas de información, o la información que reside en ellos".

El año 2018 ha sido decisivo con la llegada masiva de dispositivos de Internet de los objetos a los campus y la introducción de normativas de privacidad en el ciberespacio, específicamente el Reglamento General de Protección de Datos de la Unión Europea. El RGPD tiene implicaciones para universidades de todo el mundo y ambos temas se tratarán en profundidad.

## Reglamento General de Protección de Datos

La Unión Europea promulgó el RGPD el 25 de mayo de 2018 para devolver a los ciudadanos el control de su información cibernética. En esencia, el RGPD otorga a todos los residentes de la UE el derecho a saber y decidir cómo se utilizan, almacenan, protegen, transfieren y eliminan sus datos personales. Las personas también pueden solicitar la eliminación de todos sus datos para ejercer su "derecho al olvido". A diferencia de la definición de información de identificación personal de otros países, el RGPD también cubre los datos de ubicación, incluidas las direcciones IP, lo que podría tener un gran impacto en la implementación de Servicios basados en la ubicación (LBS) en el campus o incluso en los registros de los equipos de la red.

Como la legislación de privacidad más progresista del mundo, además de los derechos detallados anteriormente, el RGPD también tiene el poder de sancionar el incumplimiento. Las infracciones del RGPD podrían resultar en multas por incumplimiento del 4 % de los ingresos mundiales anuales o de 23 millones de dólares, la mayor cantidad de las dos.

La planificación para el RGPD estaría incluida en la sección de confidencialidad de la tríada CIA y se tratará específicamente en la sección de seguridad de las aplicaciones.

## Internet de los objetos

Internet de los objetos es un tema interesante. A diferencia de las redes definidas por software (SDN), que requieren una implementación consistente por parte de la comunidad de redes, los dispositivos IoT ya están en el campus y seguirán creciendo. Un dispositivo IoT es un dispositivo conectado que

tiene la capacidad de enviar o recibir información sin que sea necesaria la intervención humana. En un campus, esto puede incluir una impresora Wi-Fi de consumo, cámaras de seguridad y sensores de IoT, o incluso proyectores para auditorios/aulas.

Con un uso normal, estos dispositivos son esencialmente inofensivos. Sin embargo, dado que son dispositivos de red y tienen un sistema operativo, están expuestos a los ataques de los piratas informáticos y al malware. Esto les pone en peligro de ser reclutados y esclavizados en un ejército de bots. Quizás recuerde el ataque distribuido de denegación de servicio (DDoS) de octubre de 2016[5] contra Dyn, un proveedor de servicios de nombres de dominio con sede en los EE. UU. y clientes en Europa y Norteamérica. Dyn fue atacada tres veces en el mismo día. El análisis resultante confirmó que los dispositivos IoT (cámaras, monitores para bebés, enrutadores Wi-Fi e impresoras) se habían visto comprometidos por una variante de malware basada en el código fuente del virus Mirai.

La planificación de IoT se encuentra principalmente en la sección de "Accesibilidad" de la tríada CIA y se tratará específicamente en la sección de seguridad de acceso a redes.

## Defensa en profundidad

La defensa en profundidad es la práctica de defender un ordenador con capas de dispositivos o estrategias de seguridad independientes. Originalmente fue concebido por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) como un enfoque integral para proteger la información. Este concepto gira en torno a tres ejes:

1. Personas: la seguridad de la información es el objetivo del liderazgo de TI e incluye la aplicación de servicios de seguridad como disponibilidad, integridad, autenticación, confidencialidad y no repudio. La aplicación de estos servicios debe basarse en el paradigma Proteger, Detectar y Reaccionar. También se incluyen aquí las prácticas de contratación/despido y la formación.
2. Tecnología: incluye el hardware y el software que impiden el acceso a los contenidos de un sistema.
3. Operaciones: se centra en todas las actividades necesarias para mantener la postura de seguridad de una organización en el día a día y puede incluir evaluaciones de seguridad del sistema, recuperación y reconstitución, control de cambios y administración de datos.

El resto de esta ficha técnica explorará estas áreas de enfoque a través de la exploración de las siguientes capas: seguridad periférica de la red, seguridad de las aplicaciones, seguridad de la red LAN, segmentación de la red y gestión de la red.

### Servicios de seguridad periférica de la red

El extremo de la red es el punto en el que la red interna de la institución interactúa con otra red, que puede ser de un operador, de una red de investigación o educación, o de Internet pública. Esta es la primera capa en una arquitectura de defensa en profundidad. Esta capa también puede verse como una protección de la garantía de información frente a los "Bárbaros que están a la puerta" y su actividad maliciosa.

El extremo de la red tiene tráfico entrante y saliente, lo que significa que necesitamos abordar cada tipo de tráfico.

#### Tráfico entrante

Tráfico entrante: tanto si es un enlace WAN, la Internet pública o un enlace de una red de investigación, se deben aplicar todas o algunas de las siguientes tecnologías:

1. Cortafuegos: normalmente, en una zona desmilitarizada (DMZ), un cortafuegos puede realizar varias tareas de seguridad, como NAT (traducción de direcciones de red), VPN (red privada virtual) y, por supuesto, aplicar la lógica de la seguridad al tráfico.
2. Sistema de detección de intrusos (IDS)/Sistema de prevención y detección de intrusos (IDP): son importantes para proteger la red contra ataques. Existen dos tipos:
    1) Basado en la firma, que reconoce los patrones de abusos conocidos
    2) Basado en anomalías, que reconoce las desviaciones de la actividad de la red "base"

5 https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

3. Red privada virtual (VPN): proporciona una conexión cifrada a la red local. Este tipo de conexión es mejor para conseguir comunicaciones seguras y generalmente emplea esquemas de autenticación multifactor (MFA).
4. Filtros de SPAM: considerados por muchos como un cortafuegos del servidor de correo electrónico. La sofisticación y las capacidades de los filtros de SPAM han aumentado para identificar archivos adjuntos infectados con malware, direcciones falsificadas (phishing) y otros ataques. Según el informe sobre infracciones de los datos de Verizon, el phishing es una de las principales formas de ataque para la educación superior. Implementar un filtro de SPAM puede ayudar a reducir la cantidad de ataques.
5. Filtro de tráfico web: algunos cortafuegos pueden realizar esta tarea y no todas las instituciones implementan un filtro de tráfico web por seguridad. Sin embargo, esta tecnología ofrece a las universidades la posibilidad de permitir o denegar el acceso a sitios web desde su red. Este dispositivo de seguridad, que se ve con mayor frecuencia en educación primaria y secundaria, ayuda a mantener a los usuarios fuera de los sitios que pueden provocar una infección o pérdida de control.
6. Supervisión de seguridad de la red: aplicaciones como Bro[6] o Splunk[7] pueden proporcionar datos útiles sobre el tráfico de la red y las posibles anomalías de seguridad.

### Tráfico saliente

Además de solicitar tráfico, una red también enviará información fuera de la red. Aunque este tipo de tráfico no suele ser sospechoso, supervisarlo puede informar a la institución si existe infracción de la seguridad (como dispositivos IoT atacados por un malware que participan en un ataque DDoS).

El tráfico saliente debe atravesar las defensas del tráfico entrante, pero hay una tecnología que es útil para proteger el tráfico saliente: el cifrado.

1. El cifrado MACSec también se conoce por la designación IEEE 802.1AE. Esta tecnología admite las transmisiones cifradas a través de un enlace. Por ejemplo, si tiene un sitio de recuperación de desastres (DR) para su data center, puede poblar ese sitio a través de un enlace cifrado MACSec, asegurando la confidencialidad y la integridad de los datos y la autenticación del origen de los mismos.

## Seguridad de las aplicaciones

La siguiente capa que se utiliza actualmente para abordar las amenazas de ciberseguridad es la seguridad de las aplicaciones. Esta capa abarca tanto los dispositivos informáticos del usuario final como las aplicaciones basadas en la red. La seguridad de las aplicaciones es una herramienta importante en el arsenal de seguridad de una universidad. Aborda los dominios de confidencialidad e integridad de la tríada CIA y es importante tenerla en cuenta al implementar las protecciones del RGPD.

Las tecnologías y tácticas de esta capa incluyen:

1. Cifrado de datos: los dos principales sistemas operativos de PC tienen funciones de cifrado de datos de disco. Esto es importante, ya que protege los datos del usuario de los accesos accidentales. El cifrado de almacenamiento de red está ganando popularidad y mejora la integridad y la confidencialidad de la información.
2. Autenticación multifactor (MFA): la autenticación multifactor es un mecanismo que requiere que dos dispositivos trabajen en conjunto para acceder con éxito a una aplicación o recurso. Por lo general, el flujo consiste en un ID de usuario y una contraseña, luego se ingresan una serie de números y se envía un mensaje de texto al smartphone del usuario. Esto proporciona otra capa de confirmación de que la persona es quien dice ser. Otro mecanismo para ofrecer MFA es usar tokens de hardware como los de RSA y Google en lugar un mensaje de texto en el smartphone. Esta estrategia tiene la ventaja de que puede utilizarse en la VPN y con otras estrategias de comunicación seguras.

6 https://www.bro.org
7 https://www.splunk.com

3. Microsegmentación: el data center ha evolucionado de servidores físicos a servidores virtuales, con docenas de servidores virtuales que ocupan el espacio de uno o dos servidores físicos. Sin embargo, los riesgos aumentan con esta densidad. Los cortafuegos de inspección de estado tradicionales no tienen la capacidad de analizar, a la velocidad de cable, los flujos de tráfico de un data center. VMWare[8], un importante proveedor de hipervisores, ha implementado una tecnología denominada "microsegmentación". Esto significa que, ahora, cada aplicación puede tener su propio perímetro de seguridad sin depender exclusivamente de las VLAN.

Las prácticas que se implementan en esta capa deben incluir:

4. Formación de concienciación sobre seguridad para el usuario final: esta actividad generalmente se lleva a cabo durante el mes de concienciación sobre la seguridad (octubre). Sin embargo, a lo largo del año se deben emitir recordatorios periódicos sobre phishing, spear phishing y explotaciones de ingeniería social (divulgación de credenciales) para ayudar a reducir el área de superficie de este vector de ataque.
5. Parches de seguridad: es importante probar las actualizaciones de las aplicaciones y los parches de seguridad antes de aplicarlos. Sin embargo, los lanzamientos del fabricante son importantes y hay que darles prioridad. Según el informe sobre infracciones de datos de Verizon, el 6 % de los ataques exitosos atacaron las brechas de seguridad que un parche hubiera cubierto. De hecho, algunos de los ataques más dañinos ocurrieron debido al retraso en la aplicación de los parches.

## Seguridad de acceso a la red

Las redes de área local (LAN) y las redes de área local inalámbricas (WLAN) son puntos de entrada para los usuarios de ordenadores del campus. Una conexión LAN generalmente supone conectar físicamente un cable de conexión Ethernet desde el dispositivo de red a un puerto de pared RJ-45. Una conexión WLAN no necesita conectividad física, ya que utiliza el chip de Wi-Fi integrado en el dispositivo para detectar la red y conectarse a ella.

Las universidades siempre han tenido que buscar un equilibrio entre la facilidad de uso y la seguridad total. Es importante no hacer que el acceso seguro resulte muy complicado, de lo contrario, los estudiantes y otros usuarios, buscarán una solución alternativa o aumentará la cantidad de dispositivos "Shadow IT" (TI en la sombra). Por ejemplo, en algunos campus, los invitados necesitan un patrocinador para poder autenticarse en la red. En otros, lo normal es enviar a los invitados a un portal de autoservicio donde proporcionarán su información personal, aceptarán las condiciones de uso y se registrarán. Ambos métodos brindan la misma protección a la red, pero uno es uno de ellos resulta algo más caro que el otro.

En una arquitectura de defensa en profundidad, la seguridad de acceso a la red es una de las inversiones más importantes. Esta capa tiene que ver con las 4 "A": autenticar, autorizar, auditar y administrar. La autenticación correcta lleva a la autorización para acceder a los recursos de red permitidos para una función específica. La auditoría está relacionada con la supervisión del comportamiento y del tráfico de la red. Si se detectan anomalías, se deben administrar reglas de cuarentena o de tráfico de la red.

Las tecnologías de seguridad de acceso a la red que admiten las 4 "A" incluyen:

1. 802.1X: un estándar IEEE para el control del acceso a la red basado en puertos que proporciona un mecanismo de autenticación para los dispositivos LAN y WLAN. El 802.1X requiere un solicitante (ordenador o dispositivo que solicita acceso), un autenticador (por lo general el conmutador Ethernet, WLAN AP o controlador) y un servidor de autenticación (por lo general un servidor RADIUS o EAP). El solicitante proporciona las credenciales al servidor de autenticación. Si son correctas, el autenticador concede acceso a la red.
2. Biométrico: un nuevo método de autenticación de seguridad y que potencialmente es más fácil de usar que consiste en el uso de datos biométricos o de algo que sea exclusivo del usuario, como una huella digital, el reconocimiento de iris o la voz. Aunque este método no sirve para los dispositivos IoT, proporciona una manera fácil de conceder a acceso a la red a una persona.

8 https://www.vmware.com

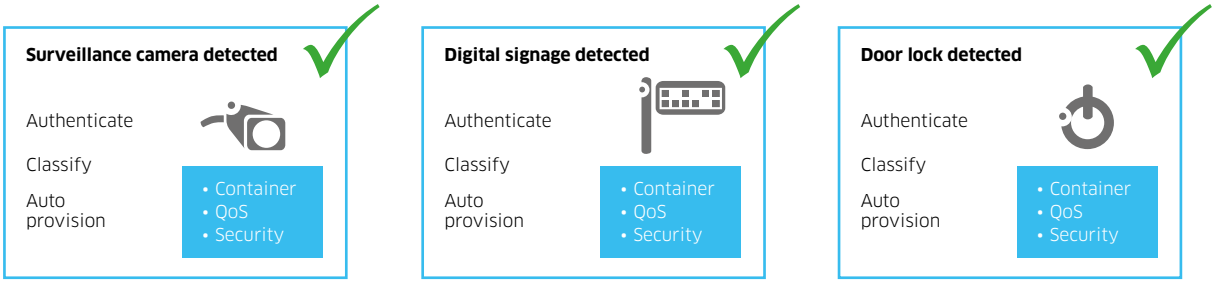
3. Cifrado: aunque se ha mencionado anteriormente como uno de los mecanismos de seguridad para los datos en reposo y en tránsito entre data centers, el cifrado MACSec es cada vez más frecuente en la LAN, desde el núcleo hasta la periferia. Además, los estándares WLAN IEEE han abordado el cifrado con el estándar 802.11i, que protege las transmisiones Wi-Fi, desde el punto de acceso hasta el usuario, contra ataques de punto de acceso falso o Man-in-the-Middle (una de las razones principales para no utilizar el WI-Fi público y sin cifrar). Además, la alianza Wi-Fi anunció recientemente WPA3 (Acceso protegido Wi-Fi 3). WPA3 añade nuevas funciones para simplificar la seguridad Wi-Fi, permitir una autenticación más robusta, ofrecer una mayor capacidad criptográfica para los mercados de datos muy sensibles y, al mismo tiempo, mantener la resiliencia de las redes de misión crítica.
4. Sistema operativo reforzado: muchos dispositivos de red se adquieren con perfiles de autenticación de administrador predeterminados. Lamentablemente, estos valores predeterminados nunca se cambian (algo que sucede aún con más frecuencia con los dispositivos IoT), lo que hace que el dispositivo sea un objetivo fácil para la entrada de malware o incluso para cambios de código. Un SO de dispositivo reforzado es uno que mezcla el código y la ubicación de la memoria para que la infracción con éxito de un dispositivo no se repita de manera automática. Además de proteger la integridad del dispositivo, un sistema operativo reforzado también puede tener las siguientes características:
    1) Reconocimiento y mitigación de ataques DoS: algunos dispositivos de infraestructura de red pueden reconocer que se está produciendo un ataque DoS y frustrarlo inmediatamente eliminando el tráfico ofensivo.
    2) Reconocimiento de ataques basados en IP: algunos dispositivos de infraestructura de red pueden integrarse con SNORT u otros productos IDS/IDP y reaccionar ante una firma positiva de ataque de IP y poner en cuarentena el tráfico ofensivo.
5. Políticas de acceso a la red unificadas: después de una autenticación con éxito, esta estructura autoriza el acceso a la red basándose en parámetros como la dirección MAC, la hora del día, la función del usuario, el departamento (como estudiante, invitado, profesorado, personal, proveedor, administración, admisiones, deportes) o incluso la ubicación desde la que se autentican. Esta estructura admite tanto el acceso LAN como el WLAN. Elimina las falsas coincidencias y la duplicación de los perfiles de seguridad, y proporciona un acceso a la red consistente y seguro.
6. Dispositivos IoT: las políticas unificadas de acceso a la red son una característica fundamental para la habilitación de dispositivos IoT. Además, la huella digital del dispositivo DHCP puede identificar rápidamente los dispositivos IoT de múltiples fabricantes. Esta función aprovecha las opciones DHCP, que proporcionan información específica del proveedor sobre el hardware del dispositivo o del sistema operativo. El intercambio se realiza mediante las opciones DHCP, tal y como se definen en RFC 2132. Las opciones[9] que utilizan DHCP proporcionan datos sobre el proveedor, el dispositivo y el sistema operativo que, combinados, constituyen la "huella digital" del dispositivo. Por ejemplo, una reciente convocatoria de propuestas de CCTV la ganó un solo fabricante. Estos nuevos productos coexistirán con las antiguas cámaras CCTV. Con la implementación de UNAP, el equipo de seguridad tiene dos formas de identificar y aplicar las reglas de seguridad de la red: huellas digitales DHCP o enmascaramiento de la dirección MAC. El enmascaramiento de la dirección MAC utiliza los primeros 24 bits de la dirección MAC, que contienen el identificador único de organización (OUI)[10]. Al utilizar la UNAP con una política de direcciones MAC enmascaradas, la institución podría implementar sus nuevas cámaras de vigilancia de forma rápida y segura. La identificación de huellas digitales DHCP permitiría al campus identificar todas las cámaras de CCTV y aplicar políticas de seguridad coherentes.

La identificación de dispositivos mediante huellas digitales DHCP suele ser compatible con los sistemas WLAN, sin embargo, es más potente cuando se incluyen también los dispositivos LAN, ya que no todos los dispositivos IoT se conectan a la red a través de Wi-Fi.

9 http://www.ietf.org/rfc/ rfc2132.txt

10 http://standards-oui.ieee.org/oui/oui.txt

**Figura 2. Autorreconocimiento y clasificación**

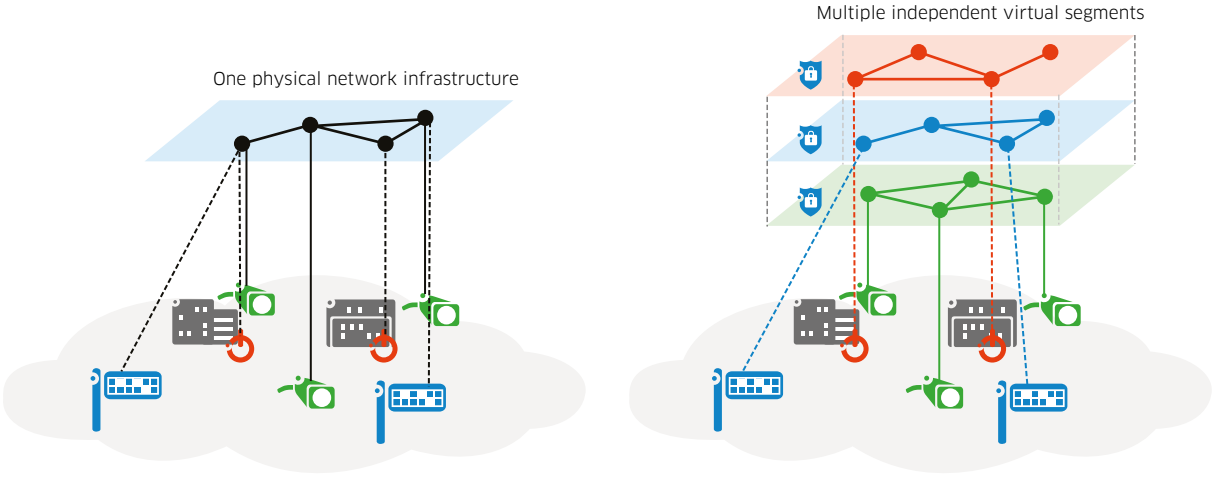



## Segmentación de red

Con la introducción de la conmutación LAN, la segmentación de la red pasó de la segmentación física a incluir LAN virtuales (VLAN). Esto permite limitar los servicios de red a los usuarios que son miembros de la VLAN, esencialmente protegiendo las aplicaciones y los servicios. La mayoría de los equipos de red admiten hasta 4096 VLAN, lo que debería ser más que suficiente, pero en realidad puede convertirse en un desafío y debe diseñarse correctamente.

El tema de la sobrecarga de la VLAN es real y se ha abordado en varias tecnologías utilizadas por los campus. MPLS (conmutación de etiquetas multiprotocolo)[11] y su derivado, Conexión de ruta más corta (SPB – IEEE 802.1aq)[12], Ambos utilizan el concepto de "interfaces de servicio" para seguir segmentando la actividad de la red.

**Figura 3. SPBM - Segmentación de red, sin Spanning Tree**




## Gestión de la red

La gestión de la red es una aplicación que los proveedores de equipos de infraestructura suelen pasar por alto. Hay muchas razones que lo explican. El principal es la prevalencia de aplicaciones de terceros que gestionan entornos de múltiples proveedores. Sin embargo, existen compensaciones cuando se utiliza un sistema de gestión de red (NMS) de terceros. Muchas de las plataformas NMS que ofrecen los proveedores pueden integrarse con derechos de asistencia, e incluso sugerir versiones de mantenimiento que solucionen posibles errores en la implementación. Además, los sistemas de gestión de red OEM pueden proporcionar una gran cantidad de estadísticas, análisis y tendencias que permiten la administración proactiva de la red.

11 https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

12 https://en.wikipedia.org/wiki/IEEE_802.1aq

Los profesionales de las TI en el sector educativo también están empezando a analizar las capacidades de la tecnología Deep Packet Inspection (DPI) para la infraestructura LAN. La capacidad de saber qué aplicaciones consumen la mayor cantidad de ancho de banda puede proporcionar información a todo el departamento de TI sobre dónde deben realizarse las inversiones. Por ejemplo, si el tráfico hacia o desde la aplicación LMS es lo que más ancho de banda consume, probablemente sería bueno revisar los recursos asignados a la VM LMS, o si se basa en el cloud, investigar la experiencia del usuario y determinar si se necesita más inversión para aumentar el ancho de banda, la memoria, el procesamiento o el almacenamiento.

Con respecto a la ciberseguridad en el campus, la plataforma NMS es el punto de partida. NMS ofrece multitud de posibilidades, como habilitar el acceso a CLI cifrado o SSL en los equipos de la infraestructura, implementar políticas de acceso a la red unificadas, supervisar el tráfico en busca de anomalías o poner en cuarentena a dispositivos y usuarios con conductas incorrectas.

Además de una plataforma NMS sólida, deben tenerse en cuenta algunos programas de terceros:

1. perfSONAR[13]: aunque se trata de una herramienta que utilizan muchas instituciones de investigación, tiene capacidades que pueden ayudarle a comprender el rendimiento completo de su red. Este es un resumen de sus funciones:

   "Garantizar que las cosas funcionen bien, de manera integral, es fundamental. La supervisión en un único dominio es una práctica común y aceptada. Es difícil llevar a cabo la supervisión del rendimiento en varios dominios con las herramientas tradicionales. perfSONAR es una infraestructura de prueba y medición ampliamente implementada en redes e instalaciones científicas de todo el mundo para supervisar y garantizar el rendimiento de la red".
2. Herramientas de perfSONAR que ofrecen soluciones para problemas adicionales:
   1) pScheduler: pruebas de rendimiento en ubicaciones remotas
   2) OWAMP: comprobaciones continuas de latencia y pérdida de paquetes

## Resumen

Las instituciones educativas son el tercer sector del mundo al que se dirigen más ataques. La ciberseguridad en la educación es mucho más que algo que "está bien tener". Es una dimensión crítica en la arquitectura de la organización y contribuye a la imagen positiva de la marca de una universidad.

La implementación de un plan de seguridad basado en el riesgo permite a las universidades asignar el presupuesto en función de sus necesidades o riesgos. La arquitectura de defensa en profundidad garantiza que los atacantes deban vencer a diferentes tecnologías durante el ataque para tener éxito.

La utilización de la tríada CIA para la clasificación de confidencialidad, integridad y disponibilidad de los recursos cibernéticos, ayuda a determinar el riesgo para la institución y la importancia del tema.

La implementación de las 4 "A" (autenticación, autorización, auditoría y administración) proporciona una estructura unificada para el acceso y el comportamiento de la red en las redes LAN y WLAN.

La segmentación de la red con MPLS o SPB permite el control granular de los servicios y de los dispositivos/usuarios que acceden a esos servicios.

Por último, la formación: la tecnología de seguridad y la arquitectura desempeñan un papel muy importante a la hora de proteger sus activos. Sin embargo, tal y como se identifica en muchos estudios, el phishing y los errores de los usuarios son los métodos de infracción más frecuentes. Ofrecer formación sobre ciberseguridad a estudiantes, profesores, personal y proveedores ayuda a reducir su principal factor de riesgo.

13 https://www.perfsonar.net/about/what-is-perfsonar/

## Referencias y recursos

Instituto Nacional de Normas y Tecnología: este enlace le lleva a la página de inicio del marco de seguridad cibernética del NIST: https://www.nist.gov/cyberframework

EDUCAUSE: una asociación sin ánimo de lucro que ayuda a la educación superior a incrementar el impacto de las TI. Los resultados de la encuesta anual de 2018 “Top 10 IT Issues” (los 10 principales problemas de las TI) y los enlaces a otros recursos están disponibles aquí: https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education



Alcatel·Lucent Enterprise