

Capítulo 5: todo debe protegerse

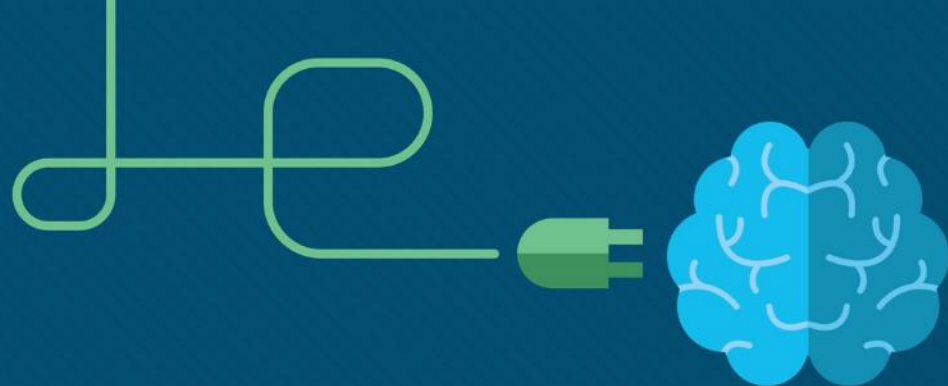
Materiales del Instructor

Introducción a Internet de las cosas v. 2.0



Capítulo 5: todo debe protegerse

**Introducción a Internet de las cosas
v. 2.0: guía de planificación**



Capítulo 5: todo debe protegerse

Introducción a Internet de las cosas v. 2.0



Capítulo 5: Secciones y objetivos

- 5.1 Seguridad en el mundo digitalizado
 - Explique por qué la seguridad es importante en el mundo digitalizado.
 - Explique la necesidad de seguridad en el mundo digitalizado.
 - Explique cómo ayudar a proteger el mundo corporativo.
 - Explique cómo proteger los datos personales y los dispositivos.

5.1 Seguridad en el mundo digitalizado

¿Por qué la seguridad es tan importante?


Tipos de datos

PII	Información
Número de seguridad social	Valor del pluviómetro
Dirección de correo electrónico	Número de automóviles en la intersección
Números de cuentas bancarias	Uso de la emergencia hospitalaria por estado
Factura de matrícula estudiantil	Capacidad aérea promedio
Clasificación crediticia	Lectura del termómetro residencial
Número de tarjeta de débito	Datos demográficos
Huellas digitales	Valores migratorios
Fecha de nacimiento	Cultivos de papas promedio por provincia
Nombre de usuario/contraseña	Próximo horario de trenes por estación
Número de identificación del vehículo (VIN)	Consumo de gas promedio por vuelo
Información hipotecaria	
Dirección particular	
Fotografías de Facebook	

- La cantidad, el volumen, la variedad y la inmediatez de los datos generados han cambiado.
- La información de identificación personal (PII, personally identifiable information) o la información confidencial (SPI, sensitive personal information) son datos sobre una persona viva que se pueden utilizar de forma individual o con otra información para identificar, contactar o localizar a una persona específica.
- Los datos informativos también pueden contener información confidencial con respecto a secretos corporativos, patentes de productos nuevos o seguridad nacional.

¿Por qué la seguridad es tan importante?

Práctica de laboratorio: tipos de datos



Cisco Networking Academy®

Mind Wide Open™

Lab – Types of Data (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. This lab can be done as independent work by a student or as a group discussion.

Objectives

Select 3 or 4 "non-traditional" objects or places that could now contain sensors. List the types of data that could be collected by the sensors. Determine if any of the collected data is sensitive.

Background / Scenario

It is important to recognize where sensors are being used in our world today and what types of data they are collecting. We need to determine if the collected data is sensitive in nature. If it is sensitive, is it PII or who might benefit from stealing it?

Required Resources

- none

Step 1: Select 1 or 2 more objects or places that already (or could) contain sensors.

1> car GPS


2> fitness wristband (eg. FitBit)

3> _____

4> _____

Step 2: List types of data that could be collected from entry 1 or 2, and entry 3 or 4 of the sensors from above

Sensor	Type of Data	Sensitive? PII?	Useful to: Hackers Companies Government Cities



Cisco

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco PUBLIC.

Page 1 of 2

filiales. Todos los derechos reservados. Información confidencial de Cisco.

¿Por qué la seguridad es tan importante?

¿Quiénes desean nuestros datos?



▪ Los buenos

- Empresas legítimas que tienen un acuerdo para usar los datos recopilados sobre usted.
- Nosotros aceptamos esto en "Términos y condiciones" o "Términos de servicio y acuerdos"
- Los hackers de sombrero blanco que prueban la seguridad para ayudar a proteger los datos.

▪ Los malos

- Los hackers de sombrero negro, desean tener acceso a los datos recopilados por varias razones infames:
- Para acceder a las ID y las contraseñas de usuario para robar identidades
- Acceder a los datos para cometer un delito.
- Vender la información a un tercero.
- Modificar los datos o deshabilitar la funcionalidad en un dispositivo.
- Interrumpir o dañar la imagen de una empresa legítima.
- Crear inestabilidad política o para divulgar una posición política.

¿Por qué la seguridad es tan importante?

Datos en las manos equivocadas

- Las credenciales de inicio de sesión y otros datos personales de más de un millón de cuentas de Yahoo y Gmail se ofrecen para venta en la Web oscura.
- Los delincuentes cibernéticos penetraron en Equifax (EFX), una de las oficinas de créditos más grandes en julio de 2017 y robaron los datos personales de 145 millones de personas.
- Una infracción de MyFitnessPal afectó a 150 millones de usuarios.
- Los atacantes de ransomware robaron las cuentas de 57 millones de conductores y pasajeros de Uber.



¿Por qué la seguridad es tan importante?

Práctica de laboratorio: huella digital de Internet



Lab 5.1.1.5 – Internet Fingerprint

Instructor Note: Red font color indicates text that appears in the instructor copy only.

Objectives

The purpose of this lab is to introduce the aspect of “fingerprinting” an individual using the worldwide web. The objective is to introduce various methods to extract as much information as possible using only the Internet browser and various sites effectively.

Part 1: Obtain as much information about yourself using the Internet Edge, Google Chrome and Firefox through the use of the Google search engine.

Part 2: Use various sites to augment the information gathered using the Google search engine.

Part 3: Compare and contrast the information collected using the Google search engine and the various sites stipulated.

Part 4: Create an internet fingerprint of yourself using all the information gathered and evaluate what information you would not want made public.

Background / Scenario

Whenever a person browses the internet, your various details like your background, politics, ethnicity, preferences, etc. are gathered by the various sites one visit. As you visit sites small “cookies” are planted into your PC in relation to the web browser and sites visited. These cookies contain small pieces of data based on your browsing patterns and sites visited. The social media sites gather a vast volume of your personal data prior to allowing you access to use the sites. All this personal information can be mined by anyone who may choose to do so. Thus browsing the internet is like leaving a sprinkling trail of cookie crumbs that will lead to a more detailed picture of yourself available to anyone searching the internet about you.

Note: Please ensure the PC is running windows 8 or 10 with access to the latest version of Microsoft Edge and Google Chrome or Mozilla Firefox. The PC must have access to the internet.

Note: Please ensure windows enhanced security is turned off on the PC prior to commencing. If you are unsure please contact your instructor.

Required Resources

- One PC running windows 8 or 10 with internet access

Note: PC must have the latest version of Microsoft Edge, Google Chrome and Mozilla Firefox pre-installed. Enhanced Internet security must be turned off on the respective PC.














1: Use Mozilla Firefox to gather information about yourself

- Open up Mozilla Firefox and navigate to the <https://google.com> site.
- Enclose the first and last name of the person you’re searching for in quotes when you enter it into the search box (like “John Smith”). In this lab the person you are gathering data on is yourself.
- You can include other relevant words, like your profession, employer, location, or even a screen name that you may have used.
- If the person you’re searching for is likely to appear on a particular web site—like a school—search only that site using the site: URL operator (like [site:centrinnalcollege.com](https://www.centrinnalcollege.com) “John Smith”).
- You can also search for people by face, search for them on Google Images to get a quick visual—especially useful for people with common names, or to determine the gender of a name you never heard before. Search all the social media sites that are exposed linked to your search.
- Document all the information you have gathered from this search.

¿Por qué la seguridad es tan importante?

Buenas prácticas de seguridad

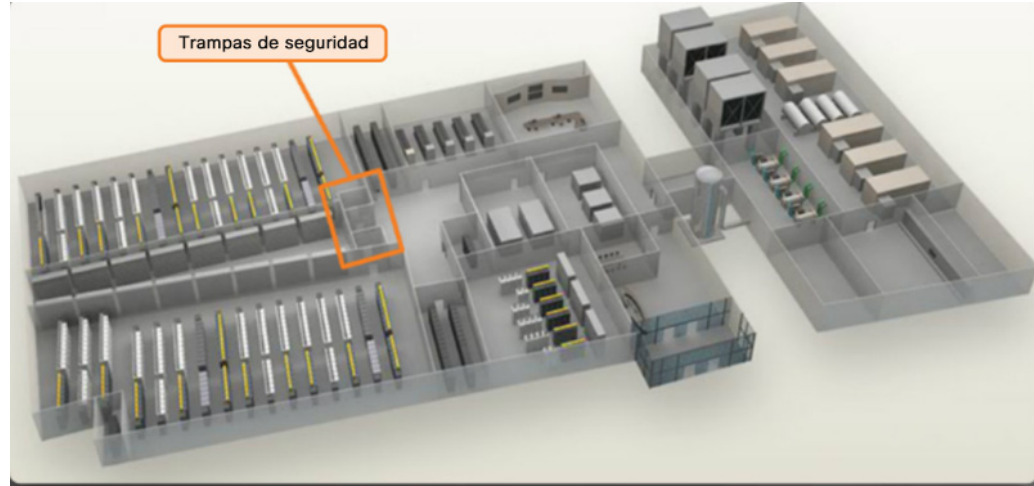
Buenas prácticas de seguridad

Evaluación de riesgos de rendimiento		Pruebe periódicamente las respuestas ante incidentes	
Cree una política de seguridad		Implemente el monitoreo, el análisis y las herramientas de administración de la red	
Medidas de seguridad físicas		Implemente dispositivos de seguridad de la red	
Medidas de seguridad de Recursos Humanos		Implemente una solución de seguridad de terminales integral	
Realice y pruebe las copias de respaldo		Capacite a los usuarios	
Mantenga parches de seguridad y actualizaciones		Cifre datos	
Implemente controles de acceso			

Protección del mundo corporativo

Seguridad física

- **Seguridad fuera del perímetro:** agentes de seguridad, cercas, puertas, videovigilancia continua y alarmas de violación a la seguridad en las instalaciones.
- **Seguridad del perímetro para interiores:** videovigilancia continua, detectores de movimiento electrónicos, trampas de seguridad, y sensores de acceso de biometría y de salida.



Desafíos de seguridad de los dispositivos de IoT



- **Creciente cantidad de dispositivos:** la cantidad de sensores interconectados y dispositivos inteligentes crece exponencialmente, lo cual aumenta la oportunidad para que se produzcan ataques.
- **Ubicación no tradicional de dispositivos:** algunos dispositivos conectados de IoT pueden interactuar con el mundo físico.
- **Falta de posibilidad de actualización:** los dispositivos de IoT con sensor habilitado pueden estar ubicados en lugares remotos o inaccesibles en los que la intervención o configuración humana es prácticamente imposible.

Protección del mundo corporativo

Uso de Wi-Fi seguro

Pasos para proteger su red inalámbrica empresarial

Cambie la contraseña de administrador predeterminada



Configure el router inalámbrico para utilizar el cifrado WPA2-AES



Cambie el identificador de conjunto de servicios (SSID) de la red



Mantenga el firmware del router inalámbrico actualizado



No anuncie el nombre del SSID



Use el filtro de dirección del control de acceso a medios (MAC)



Cree una red inalámbrica para usuarios temporales



Deshabilite la función de administración remota del router inalámbrico



Habilite el firewall integrado



Proteja físicamente el router inalámbrico



Protección del mundo corporativo

Protección de dispositivos


- **Mantenga el firewall activo**
- **Administre su sistema operativo o navegador web**
- **Proteja todos sus dispositivos**
- **Utilice Antivirus y Antispyware**



Protección de dispositivos



Packet Tracer: proteja un router inalámbrico

**Cisco** Networking Academy[®]Mind Wide Open[™]

Packet Tracer – Secure a Wireless Router (Instructor Version)

Objectives

- Create a home network with a secure wireless router

Introduction

In this activity, you will configure a wireless router to:

- Modify the default password.
- Modify the default SSID and do not broadcast.
- Use WPA2 Personal as security method.
- Rely on MAC filtering to increase security.
- Disable remote management.

Step 1: Load the .pkt file

- a. Load the 5.1.2.6 Packet Tracer – Configure Wireless Security.pkt file.
- b. Press the **power** button on Laptop1 to turn it off.
- c. Drag the **Ethernet** port to the **Modules** list to remove it.
- d. Drag the **WPC300N** module to the empty slot on **Laptop1** and press the **power** button to boot **Laptop1**.

Step 2: Modify the default password.

- a. Click on the wireless router and select the **GUI** for configuration.
- b. Click **Administration > Management**
- c. Modify the router password to a stronger one. Change the password to **aC0mpAny3**. Note that the new password has 8 characters with upper and lower case digits and some of the vowels have been changed to numbers. Select **Save Settings** at the bottom of that screen.

Step 3: Modify the default SSID name and disable the broadcast feature.

- a. Click **Wireless** and modify the SSID name to **aCompany**.
- b. Select **SSID Broadcast** and click **Disabled**. Click **Save Settings** at the bottom of that screen.

Check the topology. Has Laptop0 lost connectivity with the wireless router? If so, why?

Yes - Because Laptop0 has not been configured with the new SSID name.

Step 4: Configure WPA2 security on the wireless router.

- a. Return to the wireless router GUI tab. Click **Wireless > Wireless Security**. Change Security Mode to **WPA2 Personal**. AES is currently the strongest encryption protocol available. Leave it selected.
- b. Configure the passphrase as **aCompWiFi**. Scroll to the bottom of the window and click **Save Settings**.

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

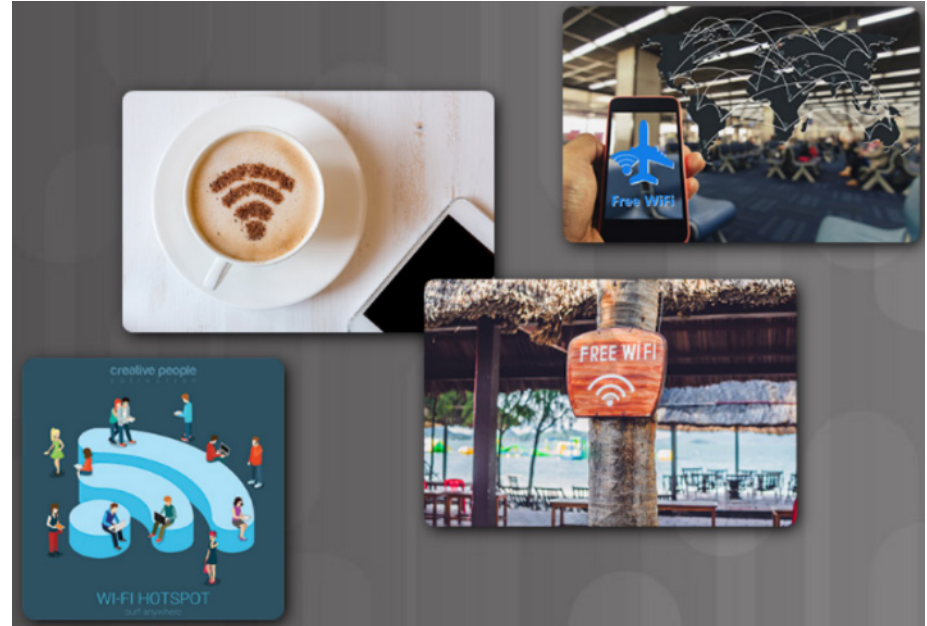
Page 1 of 3



Protección de datos personales y dispositivos

Puntos de acceso públicos

- Reglas de seguridad que se deben seguir al usar una zona de cobertura Wi-Fi pública o no segura:
 - No acceda ni envíe información personal confidencial
 - Verifique que la computadora esté configurada para compartir archivos y datos multimedia, y que requiere la autenticación de usuario con cifrado.
 - Utilice túneles y servicios cifrados de red privada virtual (VPN, virtual private network).
- Bluetooth puede ser atacado por hackers a fin de espiar algunos dispositivos, establecer controles del acceso remoto, distribuir malware y consumir baterías.
 - Apague el cuando no lo utilice.



Configuración de una VPN en smartphones

How to manually set up a VPN from the Android settings

- Step 1 • Unlock your phone.
- Step 2 • Open the **Settings** app.
- Step 3 • Under the **Wireless & networks** section, select **More**.
- Step 4 • Select **VPN**.
- Step 5 • At the top-right corner you will find a plus sign (+), tap it.
- Step 6 • Your network administrator will provide you with all your VPN information. Simply select your
desired protocol and enter all the information.
- Step 7 • Tap **Save**.
- Step 8 • You can connect by going back to the VPN settings and selecting your VPN of choice. You will
be asked to enter a username and password.

How to manually set up a VPN on your iPhone or iPad

- Step 1 • Launch **Settings** from your Home screen.
- Step 2 • Tap **General**.
- Step 3 • Tap **VPN**.
- Step 4 • Tap **Add VPN Configuration**. If you have one already configured, select the **VPN client** you want to use and toggle the **Status** switch on.
- Step 5 • Tap **Type**.
- Step 6 • Select your **VPN type** from IKEv2, IPSec, or L2TP.
- Step 7 • Tap **Add Configuration** in the upper left corner to go back to the previous screen.
- Step 8 • Enter the **VPN settings information** including description, server, and remote ID.
- Step 9 • Enter your **authentication login** including your username (or certificate), and password.
- Step 10 • If you use a proxy, enable it by tapping **Manual** or **Auto**, depending on your preferences.
- Step 11 • Tap **Done**.

Practica de laboratorio: descubra su propio comportamiento riesgoso en línea



Cisco Networking Academy®

Mind Wide Open™

Lab – Discover Your Own Risky Online Behavior (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Explore actions performed online that may compromise your safety or privacy.

Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

- a. What kind of information do you share with social media sites? _____
 - 1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
 - 2) Articles and news I find or read (2 points)
 - 3) It depends; I filter out what I share and with whom I share. (1 point)
 - 4) Nothing; I do not use social media. (0 points)
- b. When you create a new account in an online service, you: _____
 - 1) Re-use the same password used in other services to make it easier to remember. (3 points)
 - 2) Create a password that is as easy as possible so you can remember it. (3 points)
 - 3) Create a very complex password and store it in a password manager service. (1 point)
 - 4) Create a new password that is similar to, but different from, a password used in another service. (1 point)
 - 5) Create an entirely new strong password. (0 points)
- c. When you receive an email with links to other sites: _____
 - 1) You do not click the link because you never follow links sent to you via email. (0 points)
 - 2) You click the links because the email server has already scanned the email. (3 points)
 - 3) You click all links if the email came from a person you know. (2 points)
 - 4) You hover the mouse on links to verify the destination URL before clicking. (1 point)
- d. A pop-up window is displayed as you visit a website. It states your computer is at risk and you should download and install a diagnostics program to make it safe: _____
 - 1) You click, download, and install the program to keep your computer safe. (3 points)
 - 2) You inspect the pop-up windows and hover over the link to verify its validity. (3 points)
 - 3) Ignore the message, making sure you don't click it or download the program and close the website. (0 points)
- e. When you need to log into your financial institution's website to perform a task, you: _____

5.2 Resumen del capítulo

Resumen

- La cantidad, el volumen, la variedad y la inmediatez de los datos generados han cambiado.
- La información de identificación personal (PII, personally identifiable information) o la información confidencial (SPI, sensitive personal information) son datos sobre una persona viva que se pueden utilizar de forma individual o con otra información para identificar, contactar o localizar a una persona específica.
- Los datos informativos también pueden contener información confidencial con respecto a secretos corporativos, patentes de productos nuevos o seguridad nacional.
- Los hackers de sombrero blanco prueban la seguridad para ayudar a proteger los datos.
- Los hackers de sombrero negro desean tener acceso a los datos recopilados por varias razones infames.
- **Seguridad fuera del perímetro:** agentes de seguridad, cercas, puertas, videovigilancia continua y alarmas de violación a la seguridad en las instalaciones.
- **Seguridad del perímetro para interiores:** videovigilancia continua, detectores de movimiento electrónicos, trampas de seguridad, y sensores de acceso de biometría y de salida.

Resumen (continuación)

- Desafíos de seguridad de los dispositivos de IoT:
 - **Creciente cantidad de dispositivos:** la cantidad de sensores interconectados y dispositivos inteligentes crece exponencialmente, lo cual aumenta la oportunidad para que se produzcan ataques.
 - **Ubicación no tradicional de dispositivos:** algunos dispositivos conectados de IoT pueden interactuar con el mundo físico.
 - **Falta de posibilidad de actualización:** los dispositivos de IoT con sensor habilitado pueden estar ubicados en lugares remotos o inaccesibles en los que la intervención o configuración humana es prácticamente imposible.
- Conozca los pasos para proteger la red inalámbrica de su empresa.
- Pasos para la protección de sus propios dispositivos:
 - Mantenga el firewall activo
 - Administre su sistema operativo o navegador web
 - Proteja todos sus dispositivos
 - Utilice Antivirus y Antispyware

Resumen (continuación)

- Los sensores inteligentes en nuestros hogares aumentan la posibilidad de que surjan problemas de seguridad.
- Reglas de seguridad que se deben seguir al usar una zona de cobertura Wi-Fi pública o no segura:
 - No acceda ni envíe información personal confidencial
 - Verifique que la computadora esté configurada para compartir archivos y datos multimedia, y que requiere la autenticación de usuario con cifrado.
 - Utilice túneles y servicios cifrados de red privada virtual (VPN, virtual private network).
- Establezca una VPN en su smartphone.

