Seguridad en Internet ¿Cómo proteger los datos personales?

Gerardo Contreras Vega

gcontreras@uv.mx

Universidad Veracruzana
Cuerpo Académico
Aplicación y Enseñanza de la Ingeniería de Software

Universidad Veracruzana

Mayo 2022

Acerca de mi

- Gerardo Contreras Vega
- @puntogmx
- gcontreras@uv.mx
- puntog@gmail.com

¿Por qué?

1

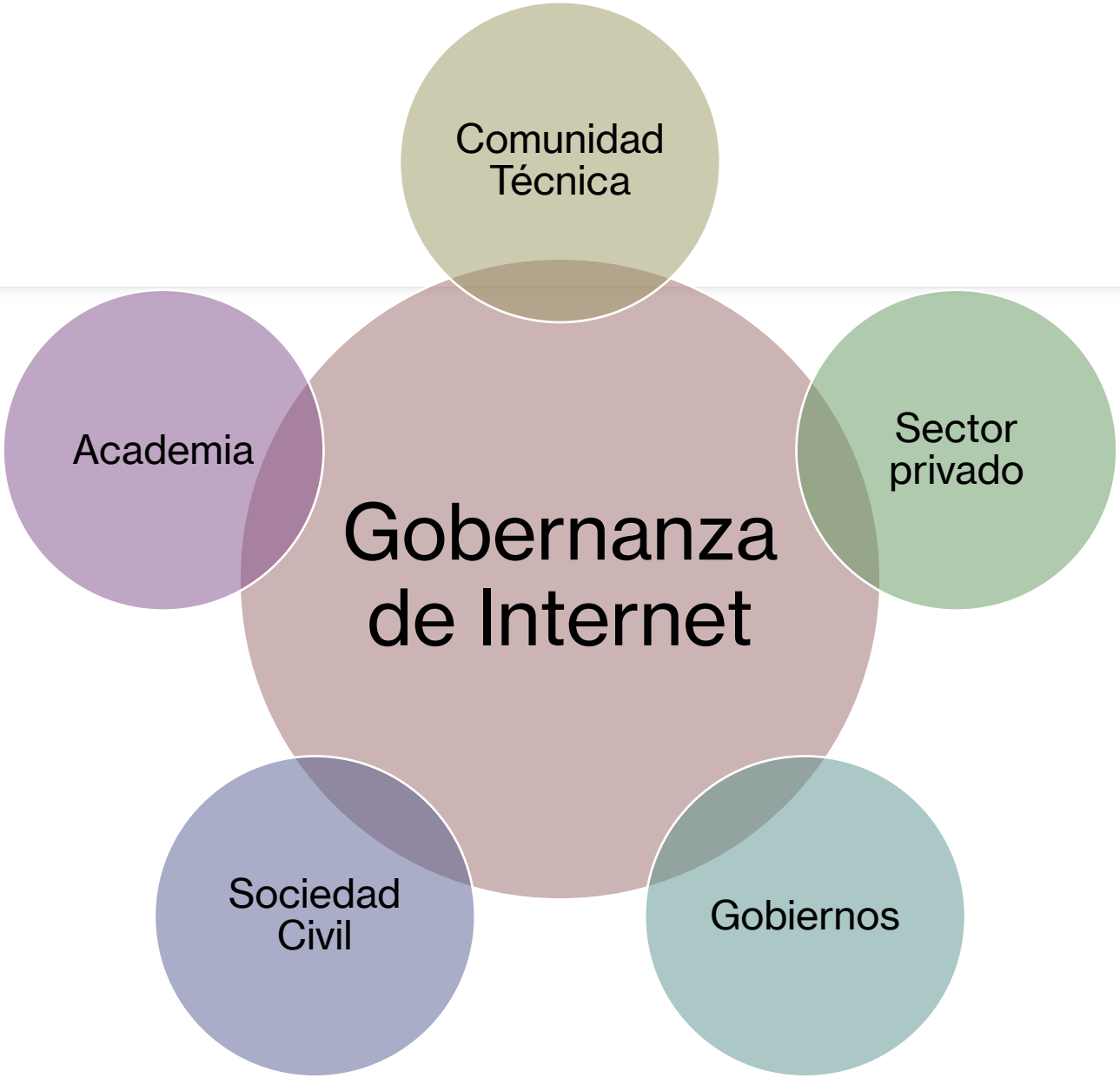
Internet es una poderosa herramienta de transformación.

2

Recurso crítico permite a las personas construir y expresar su individualidad.

Identidad digital

- Se crea a partir de la información y datos personales que publicamos en línea y que nos identifican de manera única como personas.
- Nombre, nick, edad, domicilio, publicaciones.
- Rastros digitales invisibles e involuntarios que vamos dejando cuando usamos nuestros dispositivos electrónicos.
- Revelan detalles sobre la vida privada.


Comunidad Técnica
Academia
Sector privado
Gobernanza de Internet
Sociedad Civil
Gobiernos

Derechos Humanos en Internet

Privacidad en línea y a la libertad de expresión.

Al acceso a la información.

Protegen la diversidad cultural, lingüistica y minoritaria.

Acceso a Internet.

Neutralidad de Internet, al olvido en búsquedas de Internet, seguridad digital, portabilidad.

Derechos de colectivos.

Peligros en Internet

- Ingeniería Social.
- Fraudes.
- Malware.
- Sextorsión.
- Ataques a través de las herramientas de trabajo remoto.
- Grooming.
- Bullying.
- Doxing.

Ingeniería Social

Manipulación de una persona a través de técnicas psicológicas y habilidades sociales con un objetivo específico.

Phishing.

SMShing.

Vishing.

Pretexting.

Spam.

Malware

- Malicious software o software malicioso.
- Virus.
- Gusanos.
- Troyanos.
- Ransomware.
- Adware.
- Spyware.

Sextorsión

Amenaza de revelar información íntima sobre una víctima.

Extorsión, chantaje, amenzas.

Vídeos, fotografías o textos con contenidos sexual.

Ataques a través de herramientas de trabajo remoto

Un ciberdelincuente identifica vulnerabilidades o configuraciones erróneas en el software, redes y las herramientas de trabajo remoto.

Dirigen ataques para infiltrarse en los sistemas de las empresas a través de los dispositivos de los empleados.

Bring Your Own Devices (BYOD).

Grooming

- Acción deliberada de una adulto, hombre o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital que permite la interacción entre dos o mas personas.
- Redes sociales, mensajes de texto, videojuegos, chats, correo electrónico.
- Abuso y agresión sexual, ansiedad y depresión, problemas derivados en el rendimiento académico, sociabilidad y afectividad.

Cyberbullying

- Ciberacoso.
- Es el uso de medio digitales para molestar o acosar a una persona o grupo de personas mediante ataques personales, divulgación de información personal o falsa entre otros medios.

Fraudes

- Ataque que se lleva a cabo de forma masiva a través de publicaciones o mensajes en redes sociales, en la que información no verificada sobre temas que están de moda se utilizan como señuelo para acceder a sitios web falsos, facilitar datos personales y/o bancarios o infectar sistemas de cómputo.
- Phishing.
- SMShing.
- Vishing.

Doxing

- Dropping dox, doxxing.
- Un ciberdelincuente realizan una investigación para recopilar información sobre una persona y publicarla, sin autorización, en la Red con el fin de incitar el acoso.
- “Autodoxxearte”
  - Averiguar que información en línea hay sobre ti.
  - Googléate.
  - Búsqueda inversa de imágenes.

Reflexiones (1/4)

¿Cuánto tiempo estás conectada/o a Internet?

¿Ha aumentado tu teletrabajo/teleestudio o has comenzado a utilizar nuevas herramientas digitales durante la pandemia del COVID-19?

¿Cuáles son los dispositivos electrónicos que utilizas a lo largo del día?

¿Qué medidas utilizar para cuidarlos?

¿Cómo te comunicas con tus amistades y familia?

¿Has tomado alguna medida para tener comunicación segura?

Reflexiones (2/4)

¿HAS COMPARTIDO CON ALGUIEN TUS CONTRASEÑAS?

¿CUÁNDO FUE LA ÚLTIMA VEZ QUE CAMBIASTE TU CONTRASEÑA?

¿TE CONETAS FRECUENTEMENTE A REDES WI-FI PÚBLICAS?

¿CUÁLES SON LOS SITIOS DE INTERNET O APLICACIONES QUE MÁS UTILIZAS?

¿SABES CUÁLES SON SUS POLÍTICAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS?

Reflexiones (3/4)

¿ALGUNAS VEZ HAS COMPARTIDO CON ALGUIEN ALGUNA IMAGEN O VÍDEO ÍNTIMO?

¿HAS RECIBIDO UN CORREO QUE TE PIDIÓ INGRESAR TU INFORMACIÓN PERSONAL O DESCRGAR UN ARCHIVO?

¿TÚ COMPUTADORA O CELULAR SE COMPORTAN EXTRAÑOS DESDE ENTONCES?

¿INSTALAS PROGRAMAS QUE DESCARGAAS DESDE SITIOS NO AUTORIZADOS O CON CRACKS?

¿SABES CÓMO HACER COMPRAS SEGURAS?

Reflexiones (4/4)

¿Qué pasaría si la información o fotografías que tienes en tu computadora o celular desaparecieran, o si una persona accediera a ellas sin autorización?

¿Cuándo fue la vez más reciente que respaldaste tú información?

¿Qué pasaría si tus cuentas de correo electrónico o de redes sociales fuera hackeadas?

¿Tienes la impresión de que tú teléfono te está espiando?

Prácticas básicas de seguridad y autocuidado digital.

Tener distintas identidades en línea

- Contar con diferente correo electrónico para cada una de tus cuentas en línea:
  - Comunicación personal
  - Perfil público
  - Redes sociales
  - Juegos en línea
  - Recibir promociones
- Perfiles profesional y personal separado.

Dispositivos

- Almacenan datos.
- Generan información sobre ti a través de su uso.
- Actualizar el software.
- Utilizar software antivirus.
- Descargar software de sitios de confianza.
- Cifrar información.
- Copias de seguridad.
- Revisar comentarios.
- Bloqueo de dispositivos.

Teléfono celular

- No cargar el celular vía USB en una computadora pública.
- Colocar una contraseña de bloqueo.
- No guardar información sensible.
- Desactivar sincronización automática.
- Respaldar información constantemente.
- Evaluar las apps que se instalan y los permisos que necesitan.
- Leer las cláusulas del contrato de uso de una app y/o servicio.

Contraseñas

No compartir contraseñas.

No almacenarlas en lugares fáciles de descubrir.

Cambiarlas periódicamente.

Utilizar una contraseña diferente en cada servicio.

No utilizar información personal como contraseña.

No utilizar palabras.

La contraseña debe ser fácil de recordar pero difícil de adivinar.

Utilizar mas de 12 caracteres, mayúsculas, minúsculas, números y caracteres especiales.

Contraseñas (2)

- Generadores automáticos de contraseñas.
- Verificación de 2 pasos.
- medffeeAMEhg13*yvxl14:)
- Revisar si tu cuenta ha sido comprometida en https://haveibeenpwned.com/

Navega con menos riesgos

- Utilizar sitios que cifren la información, **https** en lugar de **http**.
- Verificar que es el sitio al que queremos conectarnos.
- Revisar el certificado de seguridad.
- No usar redes públicas para operaciones con datos sensibles.
- Cambiar las contraseñas en el modem.
- Utilizar una Red Privada Virtual (VPN).
- Utilizar navegadores seguros.
- Revisar las extensiones que se instalen al navegador.
- Utilizar navegación privada.
- Revisar uso de cookies.
- Habilitar el modo “no rastrear” del navegador.

Redes sociales

- Valorar que datos personales quieres proporcionar.
- No compartir información para acceder a las cuentas.
- Cerrar sesión.
- No ingresar a la red desde un link desconocido.
- Ver opciones de privacidad en las redes sociales.
- Utilizar la opción “Ver como”.
- Revisar comentarios y fotos en las que te etiquetan.
- No aceptar a todas las solicitudes de amigos.
- Verificar los dispositivos conectados con tu cuenta a la red.
- Revisar los permisos de acceso a tú información por parte de las aplicaciones.
- Desactivar geolocalización.
- No publicar algo que no harías en la vida no en línea.

Seguridad fotos

- Cubrir la cámara de tu dispositivo.
- Considerar los metadatos de una fotografía o vídeo.
- https://similargo.com/es/site/metapicz.com

Cifrar información

- Cifrado simétrico.
- Cifrado asimétrico.
- BitLocker.
- Filevault.
- Veracrypt.
- GNUPG

Respaldos

Realizar respaldo de tú información cada semana o mes.

Respaldar en dos o más soportes: disco duro externo, memoria USB, en la nube.

Los archivos borrados se pueden recuperar.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

Hay mucho por hacer

- Inicia por ti mismo.
- Comparte con los demás.
- La seguridad está en ti.

Referencias y material adicional

- Portal educativo OEA, curso “Seguridad digital con perspectiva de género: Nuestras redes, nuestra seguridad”. https://moocs.educoas.org/course/index.php?categoryid=8. Visitada mayo 2022.
- Violencia contra las mujeres y tecnología: Estrategias de respuesta. https://socialtic.org/wp-content/uploads/2017/12/GuiaEstrategias_Ciberseguras.pdf. Visitada mayo 2022.
- Without My Consent, sample completed evidence chart. https://withoutmyconsent.org/perch/resources/wmc-evidencechartv3.pdf. Visitada mayo 2022.

Referencias y material adicional (2)

- Aplicaciones similares a metapicz. https://similargo.com/es/site/metapicz.com. Visitada mayo 2022.
- Have i been pwned. https://haveibeenpwned.com/. Visitada mayo 2022.
- Oficina de seguridad del internauta, Herramientas gratuitas. https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=115. Visitada mayo 2022.
- ¿Cómo proteger y encriptar tu teléfono celular? https://www.youtube.com/watch?v=uB-ULggNqoA. Visitado mayo 2022.

Referencias y material adicional (3)

- En Internet cuida tu privacidad. https://www.osi.es/es/tu-informacion-personal. Visitada mayo 2022.
- Guía de ciberataques. https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf. Visitada mayo 2022.
- Dominemos la tecnología. https://takebackthetech.net/es. Visitada mayo 2022.
- La violencia de género en línea contra la mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf. Visitada mayo 2022.
- Test para darte cuenta de la violencia digital. https://datacuenta.tedic.org/. Visitada mayo 2022.

Referencias y material adicional (4)

- ¿Qué es ser susceptible de ser intervenido y qué debemos proteger? https://conexo.org/que-es-susceptible-de-ser-intervenido-y-que-debemos-proteger/. Visitada mayo 2022.
- Human Rights and the Internet. https://www.apc.org/sites/default/files/research_poster_structure.pdf. Visitada mayo 2022.
- Estándares para una Internet libre, abierta e incluyente. http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf. Visitada mayo 2022.
- Carta de derechos humanos y principios para Internet. https://drive.google.com/file/d/1REWtM5NmfCIVDWcHBvEcHTyBGm7fgHd9/view. Visitada mayo 2022.

Referencias y material adicional (5)

- Guía de los derechos humanos para los usuarios de Internet. Recomendación CM/Rec(2014)6 y exposición de motivos. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804c177e. Visitada mayo 2022.
- Veracrypt. https://www.veracrypt.fr/code/VeraCrypt/. Visitada marzo 2022.
- Tipos de cifrado para proteger la privacidad. https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad. Visitada mayo 2022.

Universidad Veracruzana

AEIS
Universidad Veracruzana
Cuerpo Académico
Aplicación y Enseñanza de la
Ingeniería de Software

Gracias

Gerardo Contreras Vega

@puntogmx

gcontreras@uv.mx

puntog@gmail.com