



Estándares de protección de datos

Angel Martinez

angel.martinez@wizeline.com

Acerca de mí



Angel Martínez
Staff Software Engineer

- 8 años de experiencia
- 5 años en Wizeline
- Diseño de arquitectura y soluciones

Puntos importantes



Identifícate en Zoom utilizando tu nombre y apellido.



Mantén tu micrófono apagado durante el transcurso de la sesión.



Utiliza el chat para hacer tus preguntas durante la sección de Q&A.



Procura enfocar tus preguntas al tema presentado.



Apaga tu cámara en caso de tener problemas con tu conexión.

■ Código de conducta



Sé respetuoso, no hay malas preguntas o ideas.



Sé cordial y paciente.



Sé cuidadoso con tus palabras.

Objetivo

Al final de esta sesión podrás:

- Reconocer la importancia de la privacidad de datos así como las diferentes maneras de garantizar su cumplimiento.

Tabla de Contenidos

Introducción

Privacidad de los datos



Protección de datos

¿Regulaciones, leyes, o estándares?



Incidentes de seguridad

Manejo de incidentes



Buenas prácticas

¿Cómo nos podemos prevenir?



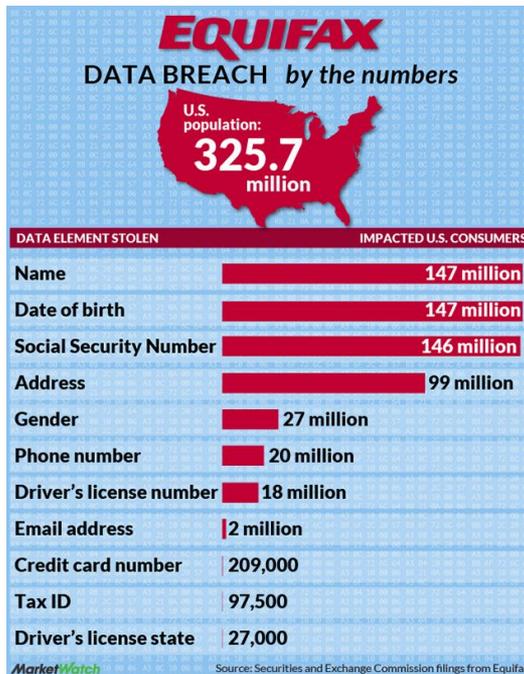
Ejercicio de código

Ejemplo





Introducción



En 2017, Equifax sufrió una brecha de seguridad que expuso información de 147M de usuarios
(de las más grandes, costosas y perjudiciales de la historia)



Datos personales

Datos personales

- Información privada que **nos hace** identificables como individuos

Datos no personales

- Información pública que **no nos hace** identificables como individuos

Privacidad de datos

- Mantener la información resguardada de **forma segura**, garantizando así la no interacción con entidades externas



Datos personales

Datos personales

- Nombre
- NSS
- Domicilio
- Correo electrónico
- Teléfono
- CURP
- Datos biométricos
- Información financiera
- Información médica
- Información de geolocalización

Datos no personales

- Número de empleado en una compañía
- Correo de trabajo
- Foto de perfil
- Nombres de usuario
- Lugar de trabajo
- Educación
- Fecha de cumpleaños
- Gustos e intereses
- Información pública

Privacidad de datos

- Cifrado robusto
- Comunicación segura
- Ciclo de vida de la información
- Implementación de:
 - Roles
 - Grupos
 - Políticas
 - Permisos



Datos personales

Consentimiento de datos

- **Consentimiento tácito (explícito) del usuario** para la gestión de datos

Tratamiento de datos personales

- Implica la obtención, uso, divulgación y almacenamiento de datos personales

Derecho a la protección de datos

- Importancia y derecho constitucional del uso y manejo de información personal



Datos personales

Consentimiento de datos

- ¿Cuándo y por qué?
- Términos y condiciones
- Aviso de privacidad

Tratamiento de datos personales

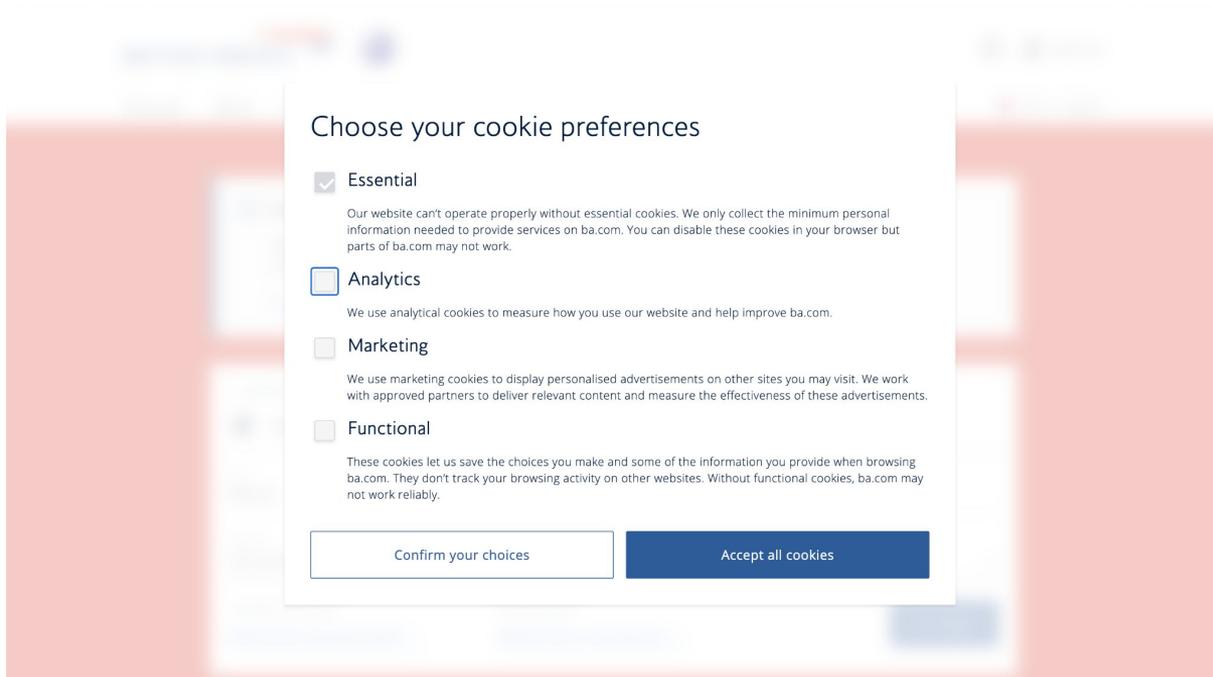
- ¿Quién, qué, dónde?
- Acceso
- Manejo
- Almacenamiento
- Aprovechamiento
- Transferencia
- Comunicación
- Disposición

Derecho a la protección de datos

- Artículo 16, párrafo segundo de la constitución

 Ejemplo

British Airways Site



The screenshot shows a white modal dialog box titled "Choose your cookie preferences" centered on a blurred background of the British Airways website. The dialog box contains four sections, each with a checkbox and a description:

- Essential**
Our website can't operate properly without essential cookies. We only collect the minimum personal information needed to provide services on ba.com. You can disable these cookies in your browser but parts of ba.com may not work.
- Analytics**
We use analytical cookies to measure how you use our website and help improve ba.com.
- Marketing**
We use marketing cookies to display personalised advertisements on other sites you may visit. We work with approved partners to deliver relevant content and measure the effectiveness of these advertisements.
- Functional**
These cookies let us save the choices you make and some of the information you provide when browsing ba.com. They don't track your browsing activity on other websites. Without functional cookies, ba.com may not work reliably.

At the bottom of the dialog box, there are two buttons: "Confirm your choices" (a white button with a thin border) and "Accept all cookies" (a solid blue button).

Importancia

- Preservan la privacidad de las personas
- Ofrecen seguridad en el tratamiento de los datos
- Protegen contra los ciberataques
- Adaptan a las regulaciones que evolucionan constantemente
- Implementan tecnología reciente
- Demuestran los valores y la ética de la compañía
- Protegen a los usuarios, **pero también nos protegen a nosotros mismos**
- **Los usuarios tienen derechos sobre el uso y protección de datos personales**

Consecuencias

- Costos de remediación
 - Notificación a los afectados
 - Implementación de controles físicos y lógicos
 - Instalaciones
 - Infraestructura
 - Código
 - Políticas
 - Procedimientos
 - Controles de seguridad
 - Monitoreo

Consecuencias

- Daño a la privacidad de las personas
 - Robo de identidad
 - Fraude financiero
- Pérdida de confianza
 - Afecta la reputación
 - Decrementa el precio de las acciones
 - Pérdida de contratos
- Sanciones legales
 - Multas y compensaciones
 - Revocación de licencias
 - Demandas y acciones legales

Tabla de Contenidos

Introducción

Privacidad de los datos



Protección de datos

¿Regulaciones, leyes, o estándares?



Incidentes de seguridad

Manejo de incidentes



Buenas prácticas

¿Cómo nos podemos prevenir?



Ejercicio de código

Ejemplo



■ Protección de datos

Protección de datos

Leyes de protección de datos

- Normativas legales emitidas por **gobiernos** y **autoridades regulatorias**
- Establecen **derechos** y **responsabilidades**
- **Regulan** el tratamiento

Regulaciones de datos

- Normativas que **complementan o detallan** las leyes de protección de datos
- Orientación **adicional** sobre el cumplimiento
- Establece **normas, estándares y regulaciones** de protección

Estándares de datos

- Normativas establecidas por **entidades independientes** para promover las mejores prácticas en cuanto a protección y gestión de datos
- **Guías** para el cumplimiento de leyes
- Se pueden considerar **certificaciones** (en algunos casos)

Protección de datos

Consentimiento de datos

- GDPR (UE)
- CCPA (California)
- INAI (México)
- LFPDPPP (México)
- LGPDPSO (México)
- **Ejemplo:**
El **consentimiento** siempre **debe ir ligado a finalidades específicas e informadas** en el aviso de privacidad

Regulaciones de datos

- EIPD (Evaluaciones de Impacto de Protección de Datos)
- HIPAA (USA)
- **Ejemplo:**
La pérdida de un registro médico o un dispositivo que lo contenga, acredita una violación a la regulación

Estándares de datos

- ISO 27001 (Gestión de seguridad de la información)
- PCI DSS
- OWASP (Guía)
- NIST (Framework de ciberseguridad)
- **Ejemplo:**
PCI DSS Req 8.2.3 indica el uso de políticas de contraseñas seguras



- https://micrositios.inai.org.mx/marcocompetencias/?page_id=370#

The screenshot shows a dark-themed header for the INAI website. On the left, there are four icons: a fingerprint, a brain, a padlock, and a gear. The main text in the header reads "APRENDE Y ENSEÑA DATOS PERSONALES" in large white letters, with "Conocimientos y habilidades en Protección de Datos Personales" in smaller pink and green text below it. The INAI logo is on the right. A blue navigation bar contains the following menu items: Inicio, Datos personales, Derecho a la privacidad, Entorno digital, Protege tu información, Sección profesores, and Conoce más. The main content area has a light background with a central white box containing the following text:

Normativa y legislación en PDP

Leyes en México para la protección de datos personales

Fundamento constitucional y nociones generales

La protección de datos personales es un derecho humano, reconocido en el artículo 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición.[1]



- <https://gdpr-info.eu/art-84-gdpr/>

Enter number / search term → without clicking in the field
🔍

GENERAL DATA PROTECTION REGULATION (GDPR)
RECITALS
KEY ISSUES
🇪🇺 DSGVO

GDPR

Chapter 1 (Art. 1 – 4) ▼

General provisions

Chapter 2 (Art. 5 – 11) ▼

Principles

Chapter 3 (Art. 12 – 23) ▼

Rights of the data subject

Chapter 4 (Art. 24 – 43) ▼

Controller and processor

Chapter 5 (Art. 44 – 50) ▼

Transfers of personal data to third countries or international organisations

Chapter 6 (Art. 51 – 59) ▼

Independent supervisory authorities

Chapter 7 (Art. 60 – 76) ▼

Cooperation and consistency

Chapter 8 (Art. 77 – 84) ▲

Remedies, liability and penalties

Art. 77 – Right to lodge a complaint with a supervisory authority

Art. 78 – Right to an effective judicial remedy against a supervisory authority

Art. 79 – Right to an effective judicial remedy against a controller or processor

Art. 80 – Representation of data subjects

Art. 81 – Suspension of proceedings

Art. 84 GDPR

Penalties

1. ¹ Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. ² Such penalties shall be effective, proportionate and dissuasive.
2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Suitable Recitals

(149) Penalties for infringements of National Rules, (150) Administrative Fines, (151) Administrative Fines in Denmark and Estonia, (152) Power of Sanction of the Member States

← Art. 83 GDPR
Art. 85 GDPR →

GDPR

Table of contents

proprietary + confidential

HIPAA

- <https://www.hhs.gov/hipaa/index.html>

The screenshot shows the U.S. Department of Health and Human Services website. At the top, there is a search bar and a navigation menu with links for 'About HHS', 'Programs & Services', 'Grants & Contracts', and 'Laws & Regulations'. Below the navigation is a 'Health Information Privacy' section with buttons for 'HIPAA for Individuals', 'Filing a Complaint', 'HIPAA for Professionals', and 'Newsroom'. The breadcrumb trail reads: 'HHS > HIPAA Home > For Professionals > The Security Rule > Security Rule Guidance Material > Cyber Security Guidance Material'. On the left is a sidebar menu with categories like 'HIPAA for Professionals', 'Regulatory Initiatives', 'Privacy', 'Security', 'Breach Notification', 'Compliance & Enforcement', 'Special Topics', 'Patient Safety', and 'Covered Entities & Business Associates'. The main content area features the title 'Cyber Security Guidance Material' with social media icons and a paragraph: 'In this section, you will find educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to a cyber-related security incidents.' Below this is a sub-section titled 'Cyber Security Checklist and Infographic' with a paragraph: 'This guide and graphic explains, in brief, the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.' Two links are provided: 'Cyber Security Checklist - PDF' and 'Cyber Security Infographic [GIF 802 KB]'.

PCI DSS

- https://listings.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf



PCI DSS Prioritized Approach for PCI DSS 3.2

PCI DSS Requirements v3.2	Milestone					
	1	2	3	4	5	6
<p>8.2.3 Passwords/passphrases must meet the following:</p> <ul style="list-style-type: none"> Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. <p>Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.</p>		2				

Tabla de Contenidos

Introducción

Privacidad de los datos



Protección de datos

¿Regulaciones, leyes, o estándares?



Incidentes de seguridad

Manejo de incidentes



Buenas prácticas

¿Cómo nos podemos prevenir?



Ejercicio de código

Ejemplo



■ Incidentes de seguridad

EIPD (Evaluación de impacto de datos personales) - Art 35 GDPR

- **Análisis de riesgos** para la evaluación de impacto relacionado con la privacidad
- El **objetivo** es la adopción temprana de **medidas** para la mitigación

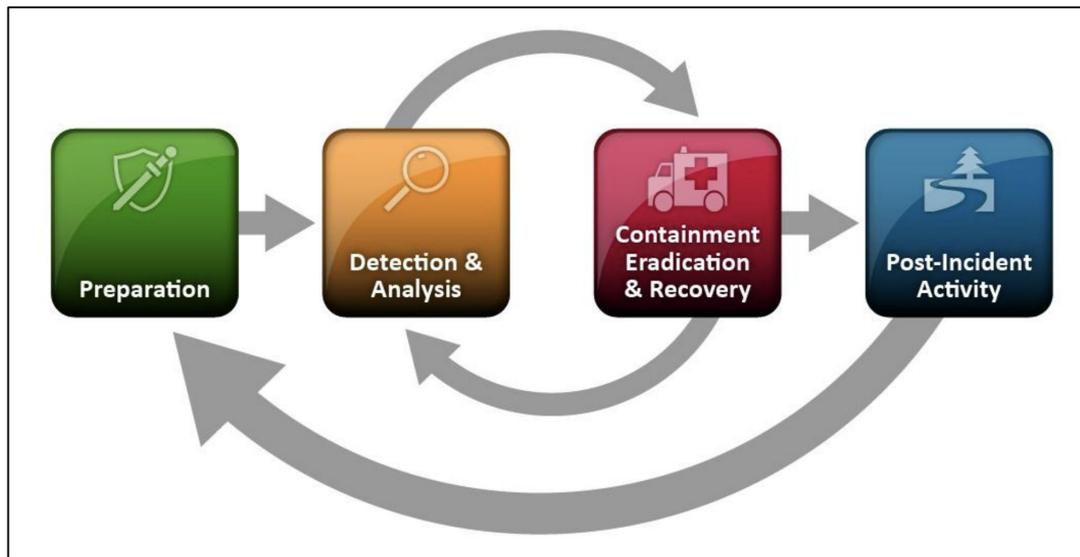


Manejo de incidentes - Plan de respuesta de incidentes (IRP)

- Proceso organizacional para la respuesta efectiva a ciberataques, basandose en:
 - Identificación
 - Investigación
 - Entendimiento
 - Priorización
 - Mitigación
 - Aprendizaje
 - Documentación

Manejo de incidentes - NIST Incident Response Framework (800-61)

- Guía de manejos de incidentes de seguridad (Publicación 800-61)
- Actividad cíclica basada en el aprendizaje y mejora continua de los procedimientos organizacionales de seguridad



Preparación

- Debe de existir un inventario de los recursos de IT
 - Configuraciones, servidores, redes, software, etc
- Identificar cuáles de ellos tienen acceso o almacenan información sensible
- Tener una línea base (tráfico normal) como umbral en las herramientas de monitoreo
- Determinar a qué se le denomina incidente y qué es un falso positivo o comportamiento esperado

Detección y análisis

- Recolección de información a través de las fuentes de datos internas y externas
- Identificación de indicadores (sospechosos) que actúan como precursores o bases de un incidente en progreso o futuro
- Identificación de una línea base de comportamiento para los sistemas afectados
- Correlación de eventos relacionados y desviación de los mismos

Contención, erradicación, y recuperación

- Bloqueo del ataque antes de su expansión
- Implementaciones de soluciones temporales o permanentes
- Identificación de la causa raíz y toma de acciones
- Aislamiento y recuperación de componentes comprometidos
- Implementación de medidas de seguridad para evitar ataques futuros por razones ya conocidas
- Recuperación de componentes a un estado normal

Actividad post-incidente

- Cuestionario de información relevante sobre el incidente para identificar:
 - Qué sucedió?
 - Cuándo sucedió?
 - Cómo se resolvió?
 - Cuánto tiempo se demoró?
 - Qué se hizo bien?
 - Qué se hizo mal?
 - Qué se puede mejorar o hacer diferente?
 - Qué lecciones aprendimos?

Actividad

Repasemos los conceptos



Tabla de Contenidos

Introducción

Privacidad de los datos



Protección de datos

Regulaciones, leyes, o estándares?



Incidentes de seguridad

Manejo de incidentes



Buenas prácticas

Cómo nos podemos prevenir?



Ejercicio de código

Ejemplo



■ Buenas prácticas



Buenas prácticas

Conocimiento y cumplimiento legal

- CISO garantiza el seguimiento al cumplimiento de las leyes y regulaciones

Políticas y procedimientos internos

- Alinear las políticas internas y procedimientos internos para asegurar el cumplimiento

Capacitación

- Capacitación regular y constante al personal

Buenas prácticas

Tratamiento de datos

- Identificar el flujo de la información así como el objetivo de uso

Auditorías

- Evaluar constantemente el cumplimiento de las leyes

Monitoreo

- Monitoreo continuo a nivel aplicación e infraestructura para la detección oportuna de incumplimientos, vulnerabilidades, o ataques



Buenas prácticas

Evaluación de terceros

- Evaluación de entidades que interactúan con los datos en nombre de nuestra organización

Gestión de incidentes

- Procedimientos para identificar, informar y remediar violaciones

Adopción de estándares

- Basarse en un marco de referencia o estándar existente para garantizar la implementación de mejores prácticas

Tabla de Contenidos

Introducción

Privacidad de los datos



Protección de datos

¿Regulaciones, leyes, o estándares?



Incidentes de seguridad

Manejo de incidentes



Buenas prácticas

¿Cómo nos podemos prevenir?



Ejercicio de código

Ejemplo



■ Ejercicio de código

Recapitulación



Hemos hablado acerca de:

- Autorización
- Autenticación
- Consecuencias
- Ataques comunes
- Técnicas de prevención
- Ejemplo

¿Preguntas?



Retroalimentación

Déjanos saber tu retroalimentación





Gracias.