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.

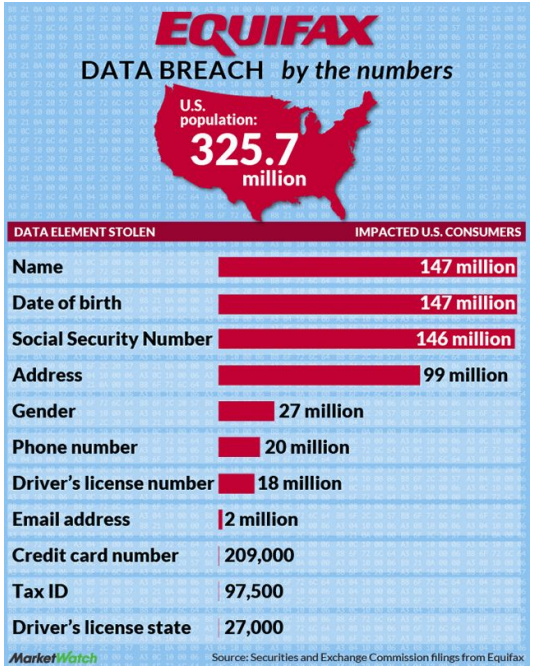
Objetivo

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



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

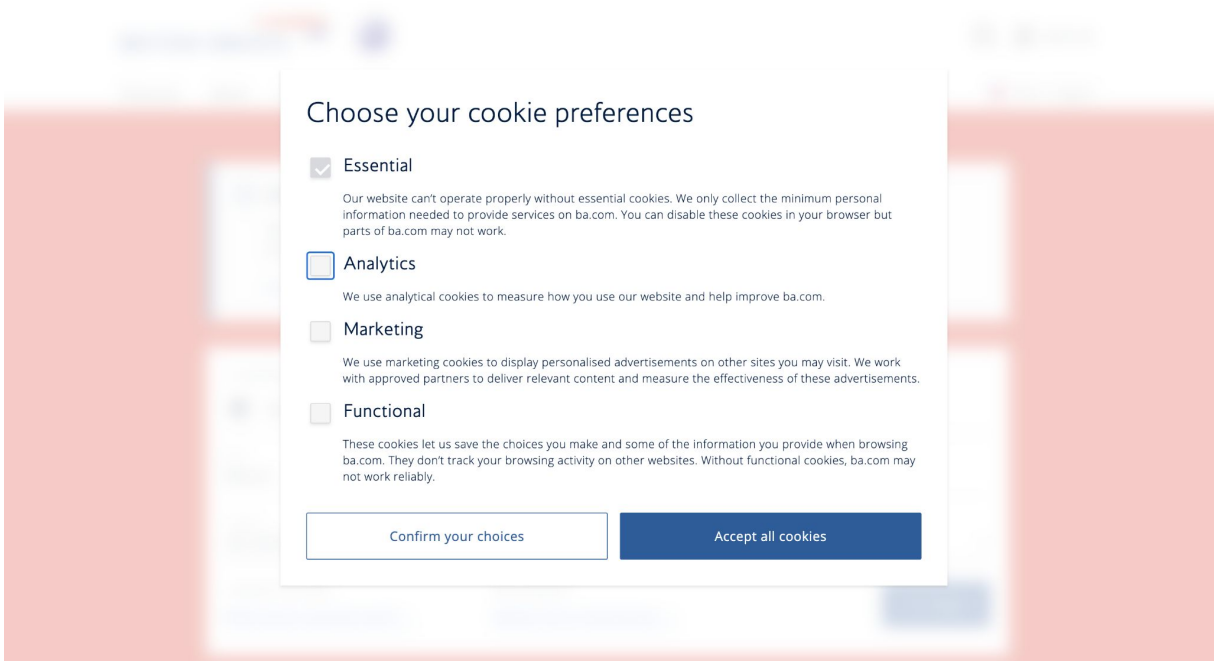
- ¿Quién, qué, dónde?
- Acceso
- Manejo
- Almacenamiento
- Aprovechamiento
- Transferencia
- Comunicación
- Disposición

Derecho a la protección de datos

- Artículo 16, párrafo segundo de la constitución

Ejemplo

British Airways Site



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

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)
- LGPDPPSO (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

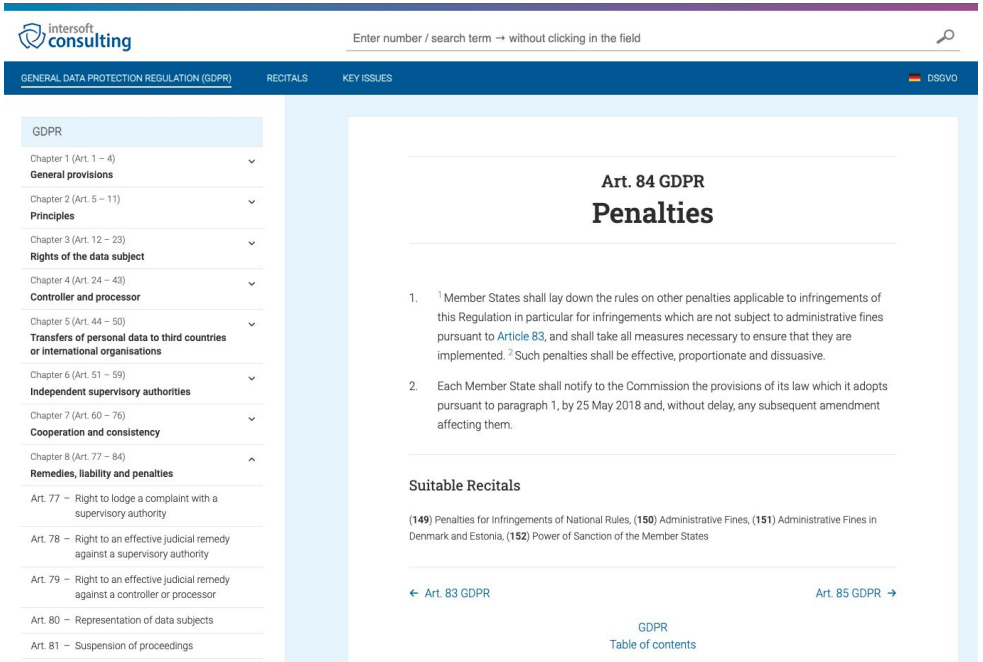
- ISO 27001 (Gestión de seguridad de la información)
- PCI DSS
- OWASP (Guía)
- NIST (Framework de ciberseguridad)
- **Ejemplo:**
  PCI DSS Req 8.2.3 indica el uso de políticas de contraseñas seguras

INAI

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

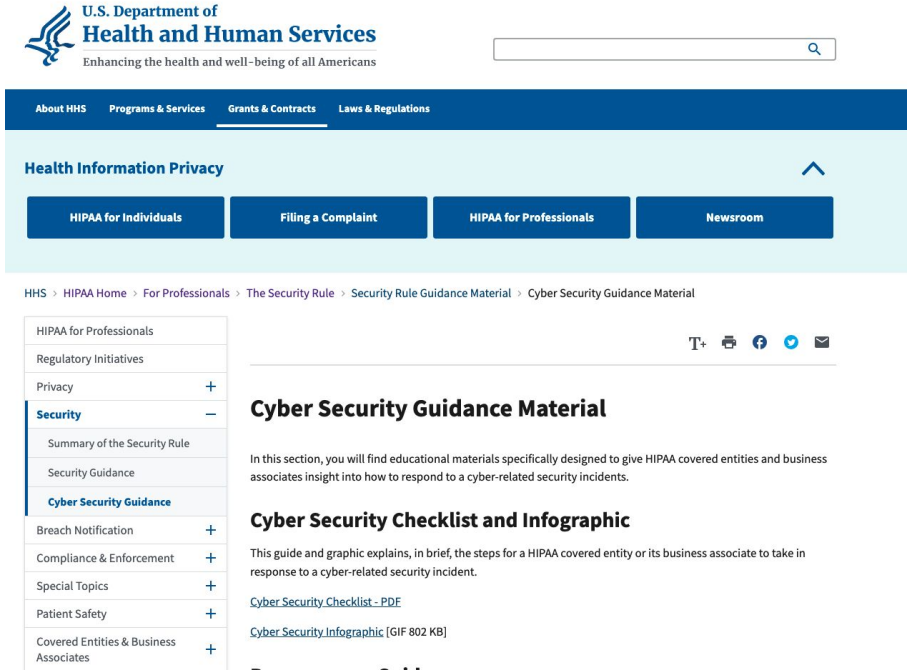
GDPR

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



HIPAA

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



PCI DSS

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

PCI Security Standards Council

PCI DSS Prioritized Approach for PCI DSS 3.2

PCI DSS Requirements v3.2	Milestone					
	1	2	3	4	5	6
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.		2				

Tabla de Contenidos

Incidentes de seguridad

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

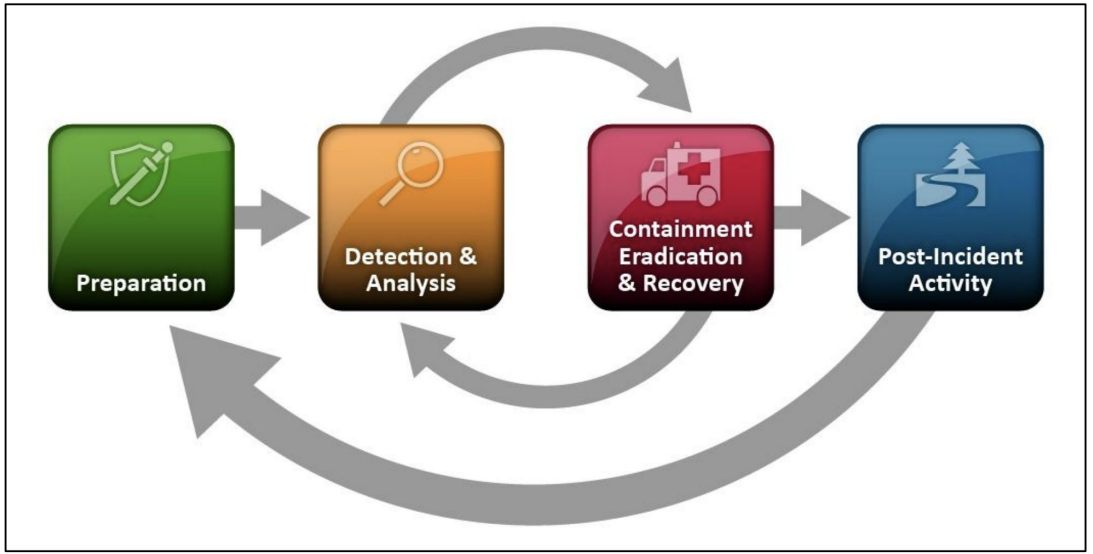
- **Análisis de riesgos** para la evaluación de impacto relacionado con la privacidad
- El **objetivo** es la adopción temprana de **medidas** para la mitigación

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

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

Ejercicio de código

Recapitulación

Hemos hablado acerca de:

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

¿Preguntas?

Retroalimentación

Déjanos saber tu retroalimentación

Gracias.