Investigación de Temario

Asignatura: Seguridad Informática

Docente: Rosales Diaz Miron Daniel

Equipo:

- Noé Abel Vargas López
- Juan Alfredo Gomez González
- Jonathan Iram Talavera Pardo
- Jesus Alberto Ramirez González

Grado: 7

Sección: A

Carrera: Tecnologías de la Información Área Desarrollo de Software Multiplataforma

Universidad Tecnológica de Torreón

Unidad I - Principios de Seguridad Informática

1.1. Aspectos éticos y legales del manejo de la información

El manejo de información en el ámbito del software está regido por un marco de **aspectos éticos y legales** que buscan proteger la privacidad y la seguridad de los datos de los usuarios. Estos marcos se centran en cómo los sistemas de software recolectan, almacenan, procesan y comparten la información.

Desde una perspectiva ética, el manejo de la información en el software se basa en principios como el **consentimiento informado**, la **minimización de datos** y la **transparencia**. Los desarrolladores deben diseñar sistemas que soliciten a los usuarios su permiso explícito para recolectar sus datos, limiten la recolección solo a lo estrictamente necesario para el funcionamiento del servicio y ofrezcan una política de privacidad clara y accesible. La **seguridad** es otro pilar ético, ya que es la responsabilidad del desarrollador proteger los datos de accesos no autorizados.

Legalmente, el manejo de información se rige por diversas leyes que imponen obligaciones y sanciones a quienes manejan datos personales.

Ley General de Protección de Datos Personales de México

¿Qué son los datos personales?

Los datos personales son toda aquella información expresada en forma alfabética, numérica, gráfica, acústica, fotográfica o de cualquier otra índole, concerniente a una persona física, que la identifica o la hace identificable.

Estos datos pertenecen a su titular, es información que lo describe, que le da identidad, lo caracteriza y diferencia de otros individuos.

Se agrupan en diferentes categorías:

- Datos de identificación: Nombre completo; nacionalidad; fotografía; lugar y fecha de nacimiento; edad; estado civil; sexo; rúbrica y/o firma autógrafa; firma electrónica; Registro Federal de Contribuyentes (RFC); Clave Única de Registro de Población (CURP); número de seguridad social; matrícula del servicio militar nacional, domicilio; número telefónico; correo electrónico, entre otros.
- **Datos laborales:** Número de empleado; clave de puesto; tipo de personal; cargo o nombramiento asignado; nivel de puesto en la estructura orgánica; fecha de alta en el cargo; información inscrita en documentos de reclutamiento, selección y contratación; incidencia; capacitación; actividades extracurriculares; referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos.
- **Datos patrimoniales:** Número de cuenta; tipo de cuenta; número de tarjeta bancaria; número de cliente; CLABE bancaria; ingresos y egresos, bienes muebles e inmuebles; historial crediticio;

información bancaria, de seguros, de fianzas, de afores y fiscal, servicios contratados, entre otros.

- **Datos académicos:** Calificaciones, Institución académica de procedencia; matrícula escolar, información contenida en el título profesional, cédula profesional, certificados, reconocimientos, entre otros.

¿Qué son los derechos ARCO?

Usted como titular de sus datos personales tiene derecho a:

▼ **Acceso**: Acceder a sus datos personales que se encuentren en posesión del responsable.

> **Artículo 22.** La persona titular tendrá derecho a acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento, a través del aviso de privacidad.

▼ **Rectificación**: Corregir tus datos personales cuando estos resulten inexactos, incompletos o se encuentren desactualizados.

> **Artículo 23.** La persona titular tendrá derecho a solicitar la rectificación o corrección de sus datos personales, cuando resulten ser inexactos, incompletos o no se encuentren actualizados.

▼ **Cancelación**: Cancelar el tratamiento de tus datos personales cuando la finalidad para la cual fueron recabados ha fenecido.

> **Artículo 24.** La persona titular tendrá en todo momento el derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en posesión del responsable.

▼ **Oposición**: Oponerte al tratamiento de tus datos personales.

> **Artículo 26.** La persona titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos.

Derechos de empresa

▼ **Medidas de seguridad:** Las empresas deberán establecer medidas de seguridad en sus software para salvaguardar la información de sus usuarios.

> **Artículo 18.** Todo responsable deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo

existente, las posibles consecuencias para las personas titulares, la sensibilidad de los datos y el desarrollo tecnológico.

▼ **Notificar en caso de riesgo:** Las empresas o cualquier índole que sea responsable de un sistema que maneje información confidencial deberá notificar inmediatamente en caso de existir alguna vulnerabilidad o incidente que ponga en riesgo la integridad de la información de sus usuarios.

> **Artículo 19.** Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento de datos personales que afecten de forma significativa los derechos patrimoniales o morales de las personas titulares le serán informadas de forma inmediata por el responsable, a fin de que pueda tomar las medidas correspondientes a la defensa de sus derechos.

▼ **Aviso de privacidad:** Toda empresa que recopile datos personales está obligada a proporcionar un aviso de privacidad que informe de manera clara y transparente a los usuarios sobre el tratamiento que se dará a su información personal. Este documento debe estar disponible desde el momento de la recopilación de datos y ser fácilmente accesible.

> **Artículo 15.** El aviso de privacidad deberá contener, al menos, la siguiente información:
> **I.** La identidad y domicilio del responsable;
> **II.** Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
> **III.** Las finalidades del tratamiento de datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular;
> **IV.** Las opciones y medios que el responsable ofrezca a las personas titulares para limitar el uso o divulgación de los datos;
> **V.** Los mecanismos, medios y procedimientos para ejercer los derechos ARCO, de conformidad con lo dispuesto en esta Ley, y
> **VI.** El procedimiento y medio por el cual el responsable comunicará a las personas titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

Ley de propiedad Industrial

¿Qué es la propiedad intelectual y por qué es importante protegerla?

El término propiedad intelectual agrupa a todas las obras, inventos, diseños, marcas, patentes, secretos industriales y símbolos que pueden ser registrados y protegidos legalmente para preservar los derechos de sus creadores y propietarios.

Debido a sus características, **la propiedad intelectual tiene valor monetario y es susceptible de explotación comercial tanto por su desarrollador como por un tercero**, a través de acuerdos de venta, transferencia, colaboración o cesión de derechos.

Por ello existen leyes y contratos específicamente diseñados para salvaguardar las prerrogativas de los creadores. En el caso de México, el registro de obras está amparado por:

- Ley Federal de Protección a la Propiedad Industrial (LFPPI)
- Ley Federal de Derecho de Autor (LFDA)

La LFPPI

▼ **E**stablece que la ley tiene como objetivo proteger la propiedad industrial mediante el otorgamiento de patentes y registros, regular secretos industriales, prevenir la competencia desleal, fomentar la actividad inventiva y promover la difusión de conocimientos tecnológicos en México, creando así un marco integral que equilibra la protección de derechos de innovadores con el desarrollo tecnológico nacional.

> **Artículo 2.-** Esta Ley tiene por objeto:
> I.- Proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, esquemas de trazado de circuitos integrados, marcas y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen e indicaciones geográficas;
> II.- Regular los secretos industriales;
> III.- Prevenir los actos que atenten contra la propiedad industrial o que constituyan competencia desleal relacionada con la misma y establecer las sanciones y penas respecto de ellos; LEY FEDERAL DE PROTECCIÓN A LA PROPIEDAD INDUSTRIAL CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN Secretaría General Secretaría de Servicios Parlamentarios Nueva Ley DOF 01-07-2020 2 de 94
> IV.- Promover y fomentar la actividad inventiva de aplicación industrial, las mejoras técnicas, la
> creatividad para el diseño y la presentación de productos nuevos y útiles, y
> V.- Promover la difusión de los conocimientos tecnológicos en el país.

Ley Federal de Derechos de Autor

La LFDA

Esta legislación contempla la salvaguarda de obras literarias o artísticas de creación original que pueden ser divulgadas, reproducidas, interpretadas o ejecutadas en cualquier formato o medio.

Esto quiere decir que en México, el software no se rige por la Ley de Propiedad Industrial, sino principalmente por la Ley Federal Del Derecho de Autor, que lo protege como una obra literaria o expresión original en un conjunto de instrucciones para computadoras. La Ley de Propiedad Industrial protege invenciones, diseños y modelos de utilidad, las cuales pueden aplicarse indirectamente al software si van asociadas a un hardware o tienen un destino industrial específico, pero no protegen el programa en sí mismo como tal. Para el desarrollo de software, es crucial considerar los acuerdos de confidencialidad y cesión de derechos con programadores externos para asegurar la titularidad del código.

¿Qué es la PI del software?

La propiedad intelectual del software, también conocida como software IP, es un código o programa informático que está protegido por ley contra la copia, robo u otro uso que no esté permitido por el propietario. La propiedad intelectual del software le pertenece a la empresa que creó o compró los derechos de ese código o software. Cualquier uso no autorizado de él por parte de otra persona es ilegal.

¿Es el software una propiedad intelectual?

La propiedad intelectual es un tipo de propiedad intangible creada por la mente, como invenciones, obras de arte y literatura, diseños, nombres o imágenes. El software también encaja en esta categoría.

Tipos de propiedad intelectual

Patentes: Son utilizadas para proteger invenciones y descubrimientos. Se trata de un documento otorgado por el Estado que reconoce la titularidad del inventor y le concede derechos exclusivos sobre la propiedad, uso y explotación de su creación.

De esta forma, el titular de la patente puede impedir o autorizar la utilización de su creación por parte de terceros, controlar el proceso de explotación del invento y obtener regalías a cambio, durante un período limitado.

Sin embargo, con la publicación de la patente, el creador hace de conocimiento público la información sobre la descripción de la invención y los dibujos técnicos del modelo, diseño industrial, esquema o procedimiento desarrollado.

Derechos de autor: Así como las patentes protegen invenciones y descubrimientos, los derechos de autor apuntan al resguardo de la prerrogativa de los creadores sobre la propiedad, reproducción, distribución y adaptación de sus obras.

En general, la protección de propiedad intelectual por derechos de autor abarca escritos literarios, artículos periodísticos, obras de teatro, *software*, bases de datos, pinturas, dibujos, esculturas, fotografías, películas, obras musicales y coreografías.

Igualmente, en esta categoría se incluyen diseños arquitectónicos, dibujos técnicos, anuncios, caricaturas, historietas, programas de radio o televisión, obras de arte de compilación (colecciones) o que incluyan diseño gráfico o textil.

Diferencia

A diferencia de una **patente**, que protege la idea o concepto de una invención, los derechos de autor protegen la expresión específica de esa idea. Le da al propietario el derecho exclusivo de copiar, modificar y distribuir o vender esas copias o modificaciones de la propiedad al público.

Los **derechos de autor** del software pueden cubrir el código específico utilizado en el programa o elementos de la interfaz de usuario. Los derechos de autor se obtienen automáticamente mediante la creación de la obra original; a diferencia de las patentes, no

es necesario pasar por un proceso de solicitud. Los derechos de autor generalmente se aplican durante la vida útil del propietario de los derechos de autor más 50 años, o durante 75 años a partir de la publicación en el caso de que el software haya sido creado por un empleado de una empresa. En términos prácticos, si a alguien de su empresa se le ocurre un código único para el software que funciona de cierta manera, ese código está automáticamente protegido por la ley de derechos de autor.

Requisitos para que un software pueda ser protegido de derecho de autor:

Para que un software pueda ser protegido por el derecho de autor, debe cumplir con ciertos requisitos:

- En el caso de las obras de cómputo, se considera que la obra debe ser original y tener suficiente creatividad y originalidad.
- Además, debe tener un lenguaje de programación y cumplir con los requisitos establecidos por la Ley Federal del Derecho de Autor.

> De acuerdo al artículo 101 de la Ley Federal del Derecho de Autor se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Importancia de registrar obras de cómputo

Protección legal: El registro de una obra de cómputo otorga al autor la protección legal necesaria para defender sus derechos de propiedad intelectual en caso de que alguien intente plagiar, copiar, distribuir o utilizar su software sin su autorización. Al estar registrada, la obra es reconocida legalmente como propiedad del autor y este puede hacer valer sus derechos en caso de cualquier infracción.

Evidencia de autoría: El registro de una obra de cómputo proporciona una prueba concreta de que el autor creó la obra y que es el propietario de los derechos de autor. Esto es importante en caso de disputas legales sobre la autoría o la propiedad de la obra.

Valor comercial: El registro de una obra de cómputo también le otorga valor comercial a la obra, ya que muestra que es original y que cumple con los requisitos legales para ser protegida por el derecho de autor. Esto puede ser especialmente importante para empresas que desarrollan software y que desean venderlo o licenciarlo a otras empresas.

Duración de la protección

El registro de una obra de cómputo otorga al autor una protección de derechos de autor por un período de tiempo determinado (generalmente, durante la vida del autor y 100 años después de la muerte del autor). Durante este período, el autor tiene el derecho exclusivo de reproducir, distribuir, exhibir y explotar comercialmente su obra.

En resumen, registrar una obra de cómputo es importante porque otorga protección legal al autor, proporciona una prueba concreta de la autoría y propiedad de la obra, le otorga valor

comercial y otorga una protección de derechos de autor por un período de tiempo determinado.

ACUERDOS DE DERECHOS DE AUTOR EMPRESA-EMPLEADO

Política Institucional

Cuando se contraten empleados externos e independientes para el desarrollo de software, se debe establecer siempre un acuerdo escrito que garantice que la propiedad intelectual del trabajo pertenezca exclusivamente a la empresa y evite su transferencia a terceros.

Aspectos Clave a Considerar

Acuerdos Escritos

Es fundamental contar con contratos escritos al contratar personal externo, ya que estos documentos aseguran que la propiedad del software desarrollado pertenezca a la empresa contratante y no al programador independiente.

Licencias de Software

Definición y Concepto: Una licencia es lo que autoriza a un cliente a utilizar su producto legalmente.

- Cuando alguien paga por el derecho a usar un apartamento, primero debe firmar un contrato o acuerdo con el propietario. Una vez que se ha firmado, el propietario le entrega al arrendatario o al comprador una llave que puede usar para acceder a la propiedad.
- Una licencia de software es tanto el contrato como la llave. Como contrato, constituye un acuerdo de propiedad intelectual de software entre el proveedor y el usuario sobre cómo se utilizará el software.

Importancia de la Protección

No se puede robar un apartamento con mucha facilidad, pero cuando se trata de software, copiar el código o transferir el programa a dispositivos o usuarios no autorizados puede ser muy fácil si no está bien protegido con un buen sistema de administración de licencias.

Tipos de Licencias

El software puede distribuirse bajo diferentes tipos de licencias:

Licencias Propietarias: Incluyen restricciones específicas de uso y mantienen el control total del código fuente por parte del propietario.

Licencias de Código Abierto (Open Source): Permiten acceso al código fuente con ciertas libertades para modificación y redistribución, pero pueden incluir algunas restricciones específicas.

Software Libre (Free Software)

Garantiza las cuatro libertades fundamentales:

- Libertad de usar el programa para cualquier propósito
- Libertad de estudiar cómo funciona el programa y modificarlo

- Libertad de redistribuir copias
- Libertad de mejorar el programa y publicar las mejoras

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

LFPDPPP

Esta ley establece los principios y deberes que deben seguir los desarrolladores de software que procesan datos personales. Obliga a obtener el **consentimiento expreso** del titular, a notificarle el **Aviso de Privacidad** y a garantizar los **Derechos ARCO** (Acceso, Rectificación, Cancelación y Oposición) a los usuarios. Los desarrolladores son considerados **"responsables"** del tratamiento de los datos.

Código Penal Federal

En el ámbito del software, este código tipifica como delitos ciertas acciones relacionadas con el uso indebido de la tecnología. Algunos de los artículos relevantes son los que sancionan la **intercepción de comunicaciones privadas** y el **acceso no autorizado a sistemas informáticos** (artículos 178 a 180), los cuales son aplicables a la **intrusión en bases de datos** o al **robo de información** mediante software malicioso.

Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)

LGTAIP

Aunque esta ley se enfoca principalmente en entidades públicas, establece principios que son aplicables a la gestión de datos por parte del software. Regula cómo los organismos gubernamentales deben manejar la información y proteger la confidencialidad de los datos personales que poseen en sus sistemas informáticos, estableciendo la obligación de publicar información de interés público, incluso en plataformas digitales.

1.2. Estándares del manejo de la información

ISO 27001

¿Qué es la ISO 27001?

- Es un estándar internacional publicado por ISO (Organización Internacional de Normalización) y IEC (Comisión Electrotécnica Internacional).
- Su objetivo principal es proteger la información de una organización mediante la identificación de riesgos, la implementación de los controles adecuados, la creación de políticas, procedimientos, roles y responsabilidades, y un ciclo de mejora continua.
- Los principios fundamentales que protege son: *confidencialidad*, *integridad* y *disponibilidad* de la información.

¿Cómo se relaciona con la seguridad informática?

La seguridad informática es una parte esencial de lo que protege la ISO 27001, pero la norma va más allá: no sólo abarca los aspectos técnicos (hardware, software, redes, cifrado, etc.), sino también aspectos organizativos, de proceso y humanos. Algunas conexiones clave:

- La ISO 27001 exige **gestión de riesgos**: identificar amenazas, vulnerabilidades, impacto potencial, probabilidad, etc.
- Control de accesos, criptografía, control de cambios, auditorías internas, gestión de incidentes, continuidad del negocio, etc.
- Políticas, procedimientos, roles y responsabilidades claras; capacitación al personal; medidas organizativas y físicas también importantes.

Relación con el desarrollo de software

El desarrollo de software es un área que puede generar riesgos específicos para la seguridad de la información, por lo tanto la ISO 27001 tiene requerimientos expresos relacionados con ese ciclo de vida. Algunas formas de relación:

1. **Anexo "Adquisición, desarrollo y mantenimiento de sistemas de información"** (Anexo A en versiones anteriores, control A.14, ahora también actualizado con los controles correspondientes). Este apartado especifica que la seguridad debe estar integrada en todas las fases del ciclo de vida del software: desde la especificación de requisitos, el diseño, codificación, pruebas, despliegue, mantenimiento.
2. **Política de desarrollo seguro**: establecer reglas de codificación segura, restricciones en cambios de software, tratamiento de entornos de desarrollo, pruebas de seguridad.
3. **Protección de datos de prueba**: asegurarse de que los datos usados en pruebas no expongan información sensible, o que estén anonimizados si es necesario.
4. **Revisión técnica y control de cambios**: cada vez que se hace un cambio en el software o en las plataformas de soporte, hay que revisar que no se introduzca una vulnerabilidad.
5. **Entorno de desarrollo seguro**: separación de los entornos de desarrollo, pruebas y producción, controles sobre quién puede hacer qué en cada entorno, gestión del código fuente, versionado, etc.
6. **Mejora continua**: luego de desplegado el software, monitoreo, auditorías, corrección de problemas y ajustes. ISO 27001 fomenta este ciclo.

ISO 17799

¿Qué es la ISO 17799?

- La ISO/IEC 17799 fue una norma internacional titulada *"Information technology — Security techniques — Code of practice for information security management"*.

- Estaba basada en el estándar británico **BS 7799** (la parte de “Código de buenas prácticas”) y fue adoptada por ISO/IEC como guía de buenas prácticas para la gestión de la seguridad de la información.
- La versión más usada fue la edición de 2005 (ISO/IEC 17799:2005).
- En 2007 se renombró como **ISO/IEC 27002**, pasando a formar parte de la familia ISO 27000, manteniendo su función de guía de controles, recomendaciones y mejores prácticas.
- Fue retirada como norma independiente después de ser sustituida oficialmente por ISO/IEC 27002.

¿Cómo se relaciona con la seguridad informática?

La ISO 17799 aporta un conjunto de recomendaciones y buenas prácticas que sirven como marco para mejorar la seguridad de la información en las organizaciones. Aquí algunos puntos clave:

- Define los principios de confidencialidad, integridad y disponibilidad de la información como base para proteger los activos informáticos.
- Contiene numerosos controles, políticas, procedimientos, estructuras organizativas, medidas físicas y técnicas, gestión de incidentes, continuidad del negocio, cumplimiento legal/regulatorio, etc.
- No es una norma certificable (es decir, no da la estructura obligatoria para una certificación), sino una guía de buenas prácticas.
- Se utiliza para orientar políticas de seguridad, evaluaciones de riesgo, definición de controles aplicables, y para asegurar que se consideran los distintos dominios necesarios en seguridad.

Relación con el desarrollo de software

Aunque ISO 17799 no está enfocada específicamente en el desarrollo de software (en el sentido de codificación o ingeniería de software), sí tiene implicaciones importantes para éste. Algunas relaciones:

1. **Adquisición, desarrollo y mantenimiento de sistemas:** Uno de los dominios de control de la ISO 17799 es “Information systems acquisition, development and maintenance” (“Adquisición, desarrollo y mantenimiento de sistemas de información”). Eso significa que la norma recomienda controles que aseguren que los sistemas que se adquieren o desarrollan lo hagan con criterios de seguridad: diseño seguro, pruebas, mantenimiento, etc.
2. **Integración de controles de seguridad durante el ciclo de vida del software: Aunque no prescribe métodos concretos de desarrollo (por ejemplo, ingeniería ágil, pruebas unitarias, etc.), pide que se definan procedimientos y controles para que los cambios en los sistemas o en el software no introduzcan vulnerabilidades. Ejemplo: control de cambios, gestión de vulnerabilidades técnicas, revisiones de seguridad, etc.**

3. **Protección de activos de software/información sensible: Uso de datos de pruebas seguros, protección de código fuente, asegurar que el software y sus componentes cumplan con políticas de seguridad (por ejemplo control de acceso, cifrado si corresponde)**
4. **Continuidad del negocio y recuperación ante incidentes: Para sistemas de software críticos, la norma aconseja tener planes de continuidad, recuperación ante fallos, planes de respuesta a incidentes — lo cual afecta al diseño del software y a su despliegue.**

Limitaciones

- Al ser guía de buenas prácticas, no obliga formalmente a cumplir un conjunto mínimo, ni garantiza certificaciones.
- No define metodologías precisas para el desarrollo seguro de software; las organizaciones deben adaptar los controles a su contexto.
- Puede quedar desactualizada si no se mantiene revisiones frecuentes (y de hecho fue reemplazada por ISO/IEC 27002).

COBIT

¿Qué es COBIT?

- COBIT significa *Control Objectives for Information and Related Technologies* (Objetivos de Control para la Información y Tecnología Relacionada).
- Es un *framework* (marco de referencia) de buenas prácticas para la gobernanza y gestión de las Tecnologías de la Información (TI). Fue desarrollado por ISACA y el IT Governance Institute.
- Surgió en 1996, y ha evolucionado en varias versiones: COBIT, COBIT 2, COBIT 3, COBIT 4 / 4.1, COBIT 5, y más recientemente COBIT 2019.

Principios y estructura principales de COBIT

Algunas de las ideas, componentes y principios que caracterizan a COBIT:

- Satisfacer las **necesidades de las partes interesadas**.
- Considerar la organización en su totalidad (no solo el área de TI): COBIT cubre toda la empresa, y abarca la gobernanza + gestión de TI.
- En versiones recientes (COBIT 2019), se definen *factores de diseño* que ayudan a adaptar el framework al contexto particular de cada organización.
- COBIT se compone de dominios / procesos, objetivos de control, métricas, modelos de madurez, criterios de información (por ejemplo confidencialidad, integridad, disponibilidad, cumplimiento, eficiencia...)

Relación de COBIT con la seguridad informática

COBIT no está centrado únicamente en seguridad, pero incluye la seguridad de la información como uno de sus componentes fundamentales. Aquí cómo se conecta:

1. **Criterios de información**

   COBIT define criterios de información (información confiable, disponible, confidencial, íntegra, conforme a regulaciones, etc.). Estos criterios guían qué se debe asegurar en términos de protección de los datos/información.

2. **Gestión de riesgos**

   En COBIT (especialmente COBIT 5 y COBIT 2019) se incorporan procesos para evaluar y gestionar riesgos de TI, lo cual incluye riesgos relacionados con la seguridad de la información.

3. **Controles, auditoría, cumplimiento**

   COBIT ofrece objetivos de control, procesos de auditoría, métricas de desempeño, lo que ayuda a establecer qué controles de seguridad deben existir, cómo verificar que funcionen, y cómo demostrar cumplimiento ante regulaciones.

4. **Gobernanza de TI**

   Seguridad informática es parte de la gobernanza de TI. COBIT ayuda a que la seguridad no sea algo aislado o puramente técnico, sino que esté alineada con objetivos estratégicos del negocio, roles y responsabilidades claras, políticas de alto nivel, etc.

Relación de COBIT con el desarrollo de software

Aunque COBIT no define metodologías específicas de codificación o tecnologías concretas (eso lo dejan a otros estándares/prácticas), tiene implicaciones importantes para cómo se organiza, controla y supervisa el desarrollo de software:

- **Alineamiento con objetivos de negocio**: Antes de iniciar un proyecto de desarrollo, COBIT ayuda a asegurar que los requerimientos de software se relacionen con objetivos estratégicos, de cumplimiento, de seguridad y de valor para la organización.
- **Controles en el ciclo de vida del software**: COBIT pide que existan controles, auditorías, revisiones de cumplimiento, gestión de cambios en software, medidas de calidad y seguridad. Esto afecta diseño, desarrollo, pruebas, despliegue, mantenimiento.
- **Gestión de riesgos durante desarrollo**: Evaluación de riesgos antes, durante y después del desarrollo, incluido el uso de datos sensibles, dependencias externas, vulnerabilidades, etc. COBIT apoya identificar y mitigar esos riesgos.
- **Medición, monitoreo y mejora**: Uso de métricas/performance para verificar que el software cumple con criterios de seguridad, calidad, disponibilidad, etc., y que los procesos de desarrollo evolucionen. COBIT tiene modelos de madurez para los procesos de TI.

Ventajas de usar COBIT

- Ayuda a tener una visión estructurada y organizacional de TI, no solo técnica.
- Mejora la alineación entre TI y los objetivos del negocio.

- Facilita cumplimiento normativo y auditoría.
- Permite mapear y relacionar diferentes estándares y marcos (por ejemplo GDPR, ISO 27001, ITIL, etc.).
- Ofrece guías para adaptar los controles y definición de procesos según el nivel de madurez de la organización.

NIST

La complejidad de los entornos tecnológicos modernos exige una aproximación estructurada y metódica a la gestión de la información y la ciberseguridad. En este contexto, marcos de referencia y estándares se han vuelto herramientas indispensables para las organizaciones que buscan alinear sus capacidades de TI con sus objetivos de negocio, mitigar riesgos y cumplir con las regulaciones.

Estándares para el Manejo de la Información: NIST

El Rol de NIST en el Ecosistema de la Ciberseguridad Global

El National Institute of Standards and Technology (NIST) es una agencia no reguladora del Departamento de Comercio de Estados Unidos que se ha consolidado como un referente de confianza en la ciberseguridad global. Su misión es promover la innovación y la competitividad a través de la promoción de estándares de medición y guías que establecen puntos de referencia y mejores prácticas para la protección de datos y sistemas. Sus marcos, en particular la serie de publicaciones 800, son recursos de confianza para identificar, detectar y responder a amenazas cibernéticas.

Aunque las directrices de NIST fueron desarrolladas inicialmente para sistemas de información del gobierno federal de EE. UU., su influencia se ha expandido considerablemente.

El Marco de Ciberseguridad (CSF) de NIST: Un Enfoque Holístico a la Gestión de Riesgos

El Marco de Ciberseguridad (NIST CSF) es un conjunto de directrices voluntarias diseñadas para ayudar a las organizaciones a evaluar y mejorar su capacidad para prevenir, detectar y responder a los riesgos cibernéticos. Considerado un "estándar de oro" para la construcción de programas de ciberseguridad, el marco organiza las actividades en un núcleo de seis funciones continuas e interrelacionadas :

- **Identificar**: La primera función se enfoca en comprender los activos de la organización, el entorno empresarial, la gobernanza y los riesgos. Esto permite a los equipos de seguridad tener una comprensión exhaustiva de los recursos más importantes a proteger.
- **Gobernar**: Una adición principal en la versión, CSF 2.0 que subraya la importancia de asegurar que la gestión de riesgos de ciberseguridad se integre a nivel organizacional.

- **Proteger**: Esta función cubre el desarrollo y la implementación de salvaguardas para garantizar la entrega de servicios de infraestructura crítica. Incluye categorías como gestión de identidad, control de acceso y seguridad de los datos.
- **Detectar**: Se refiere a las actividades y controles para monitorear y detectar eventos de ciberseguridad, incluyendo la supervisión continua y el análisis de anomalías.
- **Responder**: Esta función se enfoca en las técnicas para controlar y mitigar incidentes cibernéticos. Las categorías incluyen la planificación, comunicación, análisis y mitigación de la respuesta.
- **Recuperar**: La función final se centra en los procesos para restaurar las capacidades y servicios afectados después de un incidente, asegurando la continuidad del negocio y comunicando la situación a las partes interesadas.

El CSF permite a las organizaciones medir su progreso a través de "niveles de implementación"(tiers), desde el Nivel 1 (Partial), que indica una implementación reactiva, hasta niveles más altos que reflejan un enfoque proactivo y planificado de la seguridad. Las organizaciones también pueden crear "perfiles" que describen su estado de seguridad actual y su estado objetivo, lo que facilita la priorización de las brechas que necesitan ser abordadas.

La Serie de Publicaciones Especiales 800 de NIST: Profundidad Técnica para el Cumplimiento

La serie NIST SP 800 es una colección exhaustiva de más de 200 documentos que ofrecen directrices detalladas sobre las mejores prácticas en ciberseguridad, desde la protección de correo electrónico hasta la seguridad en la nube. Las publicaciones de esta serie son utilizadas en todo el gobierno federal de EE. UU. y sirven como base para las políticas de seguridad de diversas agencias. Algunas de las más relevantes incluyen:

- **NIST 800-171:** Se enfoca en la protección de la Información Controlada No Clasificada (CUI) en sistemas y organizaciones no federales, como contratistas y universidades. Establece 14 familias de requisitos de seguridad, abarcando desde el control de acceso hasta la respuesta a incidentes.
- **NIST 800-53**: Un extenso catálogo de controles de seguridad y privacidad, ampliamente reconocido por su profundidad. Este marco mejora la postura de seguridad de los sistemas federales mediante la implementación de controles adaptados a diferentes niveles de impacto (bajo, moderado y alto).
- **NIST 800-207**: Define los principios de la arquitectura de Confianza Cero (Zero Trust), un enfoque que enfatiza la verificación continua de usuarios, dispositivos y actividades de red para mitigar riesgos avanzados en entornos que incluyen usuarios remotos y activos en la nube.

La Revisión 5 de NIST 800-53 ha unificado los controles de seguridad y privacidad para reflejar las amenazas modernas, des-enfatizando el aspecto federal para fomentar una adopción más amplia en la industria.

ITIL

Estándares para el Manejo de la Información: ITIL

Un Marco para la Gestión de Servicios de TI y la Creación de Valor

ITIL, una sigla que solía significar "Information Technology Infrastructure Library" (Biblioteca de Infraestructuras de Tecnologías de la Información), es un conjunto de mejores prácticas para la gestión de servicios de TI (ITSM) que ayuda a las empresas a obtener el máximo valor de sus servicios de TI, alineándolos con los objetivos de negocio. Este marco es reconocido internacionalmente por establecer el estándar para la entrega de servicios de TI y por alinearse con estándares de calidad como ISO 20000.

La evolución de ITIL ha sido notable. La transición de ITIL V3 a ITIL 4 marcó un cambio fundamental, alejándose del modelo de "ciclo de vida" lineal y centrado en procesos para adoptar un "Sistema de Valor de Servicio" (SVS) flexible y holístico. Este cambio es una respuesta directa a las tendencias de un mercado que favorece las metodologías de desarrollo y operación más ágiles, como DevOps y Lean. ITIL 4 integra diferentes funciones de la organización, como el desarrollo, las operaciones y las relaciones comerciales, y se enfoca en la "co-creación de valor" con el cliente. Esto demuestra que ITIL ha evolucionado para ser un vehículo de cambio que se adapta a las nuevas formas de trabajo.

ITIL y su Relevancia para la Ciberseguridad

Aunque el enfoque principal de ITIL es la gestión de servicios, sus prácticas son directamente relevantes para la ciberseguridad. Varios de sus procesos clave, como la Gestión de Incidentes, la Gestión de Cambios y la Gestión de la Configuración son esenciales para manejar los aspectos operativos de la seguridad de la información. La gestión de incidentes ayuda a identificar y resolver rápidamente los incidentes de seguridad, mientras que la gestión de cambios minimiza los riesgos asociados con las modificaciones del sistema. La gestión de la configuración asegura que el inventario de activos de TI se mantenga actualizado, lo que es crucial para prevenir vulnerabilidades.

La adopción de ITIL proporciona procesos estructurados, una rendición de cuentas clara y prácticas de mejora continua que fortalecen la gobernanza de TI y la gestión de riesgos. La evidencia muestra que ITIL y marcos de ciberseguridad como NIST no son mutuamente excluyentes, sino complementarios. Mientras que NIST se centra en la gestión proactiva de riesgos y el establecimiento de los controles de seguridad (el "qué" se debe hacer), ITIL proporciona la estructura organizacional y las prácticas operativas (el "cómo" hacerlo de manera eficiente). La integración de los controles de riesgo de NIST en las prácticas de gestión de cambios de ITIL garantiza que cada modificación del sistema se evalúe por su impacto tanto técnico como de seguridad, lo que reduce la exposición a amenazas.

1.3 Conceptos de Seguridad

Accesibilidad

Este término suele usarse con distintos matices dependiendo del contexto, pero en seguridad de la información “accesibilidad” se refiere a la capacidad de que los sistemas, servicios, datos o recursos estén disponibles y puedan ser utilizados cuando el usuario autorizado los necesite, sin barreras físicas, lógicas o de diseño. Implica también que los mecanismos de seguridad no impidan excesivamente el uso legítimo; debe buscarse un balance entre seguridad y facilidad de uso.

Confidencialidad

Según ISO/IEC 27000:2018, la confidencialidad es la propiedad de que la información **no se haga disponible ni se revele** a personas, entidades o procesos no autorizados.

Implica medidas como: clasificación de la información, controles de acceso (quién tiene permiso de ver qué), cifrado, condiciones sobre divulgación, políticas que regulen quién puede compartir información, etc.

Disponibilidad

Definido también en ISO/IEC 27000: la propiedad de que la información esté accesible y utilizable **a demanda** por una entidad autorizada.

Esto incluye asegurarse de que los sistemas estén operativos, que haya redundancia (hardware, rutas de comunicación, respaldo eléctrico, respaldo de datos), continuidad operativa, recuperación ante fallos, protección contra ataques que interrumpan servicios (por ejemplo, DDoS), etc.

Integridad

También según ISO/IEC 27000:2018, la integridad es la propiedad de la exactitud y completitud de la información.

En práctica: significa que la información no haya sido alterada de forma no autorizada, que no existan modificaciones accidentales o maliciosas, que los datos transmitidos o almacenados sean fiables, que existan controles como hashing, firmas digitales, registros (logs), mecanismos de validación de entradas/salidas, versiones de datos, backups que permitan restaurar estados correctos si ocurre corrupción.

Autenticación

Según NIST: “verificar la identidad de un usuario, proceso o dispositivo, a menudo como prerequisito para permitir el acceso a los recursos en un sistema de información.”

Es decir, antes de otorgar permisos o acceso, se confirma que quien solicita acceso es quien dice ser. Puede implicar uno o más factores: algo que sabes (contraseña), algo que tienes (token, tarjeta), algo que eres (biometría), etc.

También incluye asegurar que los datos de origen sean confiables, que no haya suplantación, etc.

Control de acceso

Es el conjunto de políticas, mecanismos y procedimientos para **otorgar o denegar** solicitudes de acceso a recursos de información o servicios relacionados, basándose en reglas previamente definidas sobre quién puede, cómo, cuándo, dónde y bajo qué condiciones acceder.

Incluye modelos como control basado en roles (RBAC), basado en atributos (ABAC), acceso obligatorio (Mandatory Access Control, MAC), acceso discrecional (DAC), reglas, listas de control de acceso, autenticación + autorización como componentes, registro (logs) de accesos, revocación de derechos de acceso, etc.

1.4 Conceptos de criptografía

- **Criptografía simétrica**

  La criptografía simétrica (también llamada criptografía de clave simétrica o cifrado simétrico) es un método de cifrado en el cual se usa la *misma clave secreta* para cifrar y para descifrar mensajes. Ambas partes (emisor y receptor) deben acordar de antemano esa clave. Su ventaja principal es que suele ser más eficiente en términos de velocidad y uso de recursos, pero uno de sus retos más importantes es cómo distribuir y proteger la clave secreta.

- **Criptografía asimétrica**

  La criptografía asimétrica, también llamada criptografía de clave pública, es un sistema criptográfico en el que cada usuario posee un par de claves relacionadas matemáticamente: una *clave pública*, que puede difundirse libremente, y una *clave privada*, que se mantiene secreta. La clave pública sirve para cifrar datos (o verificar firmas), y la clave privada para descifrarlos (o generar firmas). Este método permite la confidencialidad sin necesidad de que las partes compartan previamente una clave secreta.

- **Cifrado por bloques y cifrado por flujo**
  - **“Cifrado por bloques” (Block Cipher):**

    Es un esquema de cifrado simétrico que trabaja dividiendo el mensaje original (texto plano) en bloques de tamaño fijo (por ejemplo 64 o 128 bits), y cada bloque se transforma en bloque cifrado usando la misma clave secreta. Para mensajes cuya longitud supera el tamaño de bloque, se usan modos de operación que definen cómo encadenar o procesar los bloques sucesivamente.

    Características:

    - Trabaja con bloques de bits de tamaño fijo.
    - Usa modos de operación (CBC, ECB, CTR, OFB, etc.) para manejar mensajes largos y para proporcionar diferentes propiedades de seguridad.

  - **“Cifrado por flujo” (Stream Cipher):**

    En un cifrado por flujo también se usa clave simétrica, pero el procesamiento es diferente: el cifrado actúa sobre los bits (o bytes) del mensaje de uno en uno (o en

unidades pequeñas), generando una secuencia de claves pseudoaleatorias (“flujo de claves”) que se combinan con el texto plano para producir el texto cifrado. La transformación cambia conforme avanza el flujo.

Características comparativas con el cifrado por bloques:

- Es más adecuado para datos en tiempo real o transmisiones continuas donde no está claro cuánto datos habrá.
- Suele tener menor latencia, menor complejidad de hardware.
- Pero pueden ser más vulnerables si se reutiliza el mismo flujo de claves o semilla (seed) de generación del keystream, etc.

Unidad II - Criptografía

2.1. Algoritmos de cifrado

Algoritmos simétricos

¿Qué es el cifrado simétrico?

El cifrado simétrico es un método de cifrado que emplea una sola clave para cifrar y descifrar datos. Aunque suele ser menos seguro que el cifrado asimétrico, a menudo se considera más eficaz porque requiere menos potencia de procesamiento.

Cifrado: Es el proceso de transformar texto sin formato legible en texto cifrado ilegible para enmascarar información confidencial de usuarios no autorizados.

Casi todo lo que las personas hacen en sus computadoras, teléfonos y dispositivos IoT se basa en el cifrado para proteger los datos y cerciorar las comunicaciones. Puede proteger datos en reposo, en tránsito y mientras se procesan, lo que lo hace fundamental para la postura de ciberseguridad de casi todas las organizaciones.

¿Cómo funciona el cifrado de clave simétrica?

El cifrado simétrico comienza con la generación de claves, que crea una única clave secreta que todas las partes implicadas deben mantener confidencial.

Durante el proceso de cifrado, el sistema introduce el texto simple (datos originales) y la clave secreta en un algoritmo de cifrado de datos. Este proceso emplea operaciones matemáticas para transformar el texto simple en texto cifrado (datos cifrados). Sin una clave de descifrado, descifrar los mensajes cifrados se vuelve prácticamente imposible.

Luego, el sistema transmite el texto cifrado al destinatario, quien utiliza la misma clave secreta para descifrar el texto cifrado de nuevo en texto sin formato, invirtiendo el proceso de cifrado.

El cifrado simétrico implica dos tipos principales de cifrados simétricos: cifrados de **bloque y cifrados** de **flujo**.

- **Los cifrados de bloques**, como Advanced Encryption Standard (AES), cifran los datos en bloques de tamaño fijo.
- **Los cifradores de flujo**, como el RC4, cifran los datos bit a bit o byte a byte, lo que los hace adecuados para el tratamiento de datos en tiempo real.

Los usuarios eligen con frecuencia cifrados de bloque para garantizar la integridad y seguridad de los datos para grandes cantidades de datos. Eligen cifrados de flujo para cifrar flujos de datos continuos más pequeños de manera eficiente, como las comunicaciones en tiempo real.

Por ejemplo, los navegadores web y los servidores web establecen comunicaciones seguras a través de un enlace SSL/TLS. Este proceso implica generar una clave simétrica compartida, llamada clave de sesión, y usar la clave pública del servidor para cifrar y compartir esa clave de sesión entre ambas partes.

Un tercero de confianza, conocido como autoridad de certificación (CA), confirma la validez de la clave pública del servidor y emite un certificado digital, lo que garantiza la autenticidad del servidor y evita ataques de intermediario.

Una vez compartida, la clave simétrica maneja eficientemente todo el cifrado y descifrado de datos. Por ejemplo, un servicio de transmisión de video en tiempo real podría emplear cifrado asimétrico para proteger el intercambio de claves y cifrados de flujo simétricos para el cifrado de datos en tiempo real. Este uso eficiente de la clave simétrica es un beneficio crucial de este enfoque de cifrado combinado.

Dos métodos comunes empleados en el intercambio seguro de claves son **Diffie-Hellman** y **Rivest-Shamir-Adleman (RSA).** Diffie-Hellman es un algoritmo asimétrico que lleva el nombre de sus inventores. Ambos ayudan a establecer un intercambio de claves seguro y garantizan que la clave simétrica permanezca confidencial.

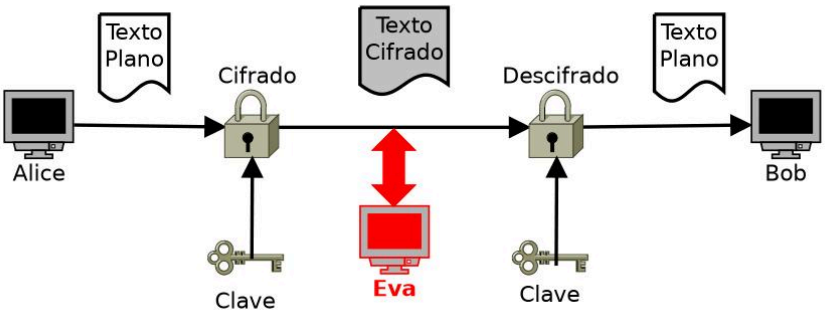
- **Diffie-Hellman** permite que dos partes generen un secreto compartido, como una clave simétrica, a través de un canal inseguro sin tener secretos compartidos previos. Este método garantiza que, incluso si un atacante intercepta el intercambio, no puede descifrar el secreto compartido sin resolver un problema matemático complejo.
- **RSA**, por otro lado, emplea un par de claves públicas y privadas. El remitente cifra la clave simétrica con la clave pública del destinatario, que sólo el destinatario puede descifrar empleando su clave privada. Este método garantiza que solo el destinatario previsto pueda acceder a la clave simétrica.

Ejemplo de cifrado simétrico

Imagine que Alice quiere enviar un documento confidencial a Bob. En este escenario, el cifrado simétrico funcionaría de la siguiente manera:

1. Alice y Bob acuerdan una clave secreta o emplean cifrado asimétrico para el intercambio seguro de claves.
2. Alice encripta el documento usando la clave secreta, convirtiéndolo en texto cifrado ilegible.

3. Alice envía el texto cifrado a Bob.
4. Al recibir el documento cifrado, Bob utiliza la misma clave secreta para descifrarlo de nuevo a su forma original, asegurando su confidencialidad durante toda la transmisión.



Casos de uso del cifrado simétrico

El cifrado simétrico es fundamental para las prácticas modernas de seguridad de datos. Su eficiencia y simplicidad a menudo lo convierten en la opción preferida para diversas aplicaciones. Los usos comunes del cifrado simétrico incluyen:

- Seguridad de los datos (particularmente para grandes cantidades de datos)
- Comunicación y navegación sitio web seguras
- Cloud security
- Cifrado de bases de datos
- Integridad de los datos
- Cifrado de archivos, carpetas y discos
- Cifrado basado en hardware
- Gestión del cumplimiento

Seguridad de los datos

La criptografía simétrica es una de las herramientas de seguridad de datos más críticas y extendidas. De hecho, un reporte reciente de TechTarget encontró que el principal contribuyente a la pérdida de datos fue la falta de cifrado.

El cifrado simétrico es particularmente efectivo para cifrar grandes cantidades de datos porque es computacionalmente eficiente y puede procesar grandes volúmenes de datos rápidamente.

Comunicación y navegación sitio web seguras

Las organizaciones emplean ampliamente el cifrado simétrico para proteger los canales de comunicación. Protocolos como Transport Layer Security (TLS) emplean el cifrado simétrico para proteger eficazmente la integridad y confidencialidad de los datos transmitidos por Internet, incluidos emails, mensajería instantánea y navegación sitio web.

Durante un intercambio SSL/TLS, el cliente obtiene la clave pública del sitio web a partir de su certificado SSL/TSL para establecer una clave de sesión segura, mientras que el sitio web mantiene en secreto su clave privada.

El protocolo de enlace inicial emplea el cifrado asimétrico para intercambiar información y establecer una clave de sesión segura antes de pasar al cifrado simétrico para una transmisión de datos más eficaz. Esta combinación garantiza que los datos sensibles sigan siendo privados y a prueba de manipulaciones durante la transmisión.

Durante un intercambio SSL/TLS, el cliente obtiene la clave pública del sitio web a partir de su certificado SSL/TSL para establecer una clave de sesión segura, mientras que el sitio web mantiene en secreto su clave privada.

El protocolo de enlace inicial emplea el cifrado asimétrico para intercambiar información y establecer una clave de sesión segura antes de pasar al cifrado simétrico para una transmisión de datos más eficaz. Esta combinación garantiza que los datos sensibles sigan siendo privados y a prueba de manipulaciones durante la transmisión.

Cloud security

Mientras que los proveedores de servicios en la nube (CSP) son responsables de la seguridad de la nube, los clientes son responsables de la seguridad en la nube, incluida la seguridad de cualquier dato.

El cifrado de datos a nivel empresarial puede ayudar a las organizaciones a proteger sus datos confidenciales en sus instalaciones y en la nube, garantizando que los datos robados permanezcan inaccesibles sin la clave de cifrado incluso si ocurre una violación de datos.

Cifrado de bases de datos

Las bases de datos suelen almacenar grandes cantidades de información confidencial, desde datos personales hasta registros financieros. El cifrado simétrico puede ayudar a cifrar estas bases de datos o campos específicos dentro de ellas, como los números de tarjetas de crédito y de la seguridad social.

Al cifrar los datos en reposo, las organizaciones pueden garantizar que los datos confidenciales permanezcan protegidos incluso si la base de datos se ve comprometida.

Las funciones hash también desempeñan un papel importante en la verificación de la integridad de los datos. Las funciones hash generan un valor hash de tamaño fijo a partir de los datos de entrada. Estas "huellas digitales" se pueden comparar antes y luego de la transmisión. Si el hash cambió, eso significa que alguien lo manipuló.

Cifrado de archivos, carpetas y discos

Las organizaciones suelen emplear el cifrado simétrico para proteger los archivos almacenados en sistemas locales, unidades compartidas y medios extraíbles.

Cifrado basado en hardware

Para una mayor protección de los datos sensibles, especialmente cuando el cifrado basado en software puede no ser suficiente, las organizaciones suelen emplear componentes de hardware especializados, como chips o módulos de cifrado. Estas soluciones de cifrado basadas en hardware se encuentran habitualmente en teléfonos inteligentes, computadoras portátiles y dispositivos de almacenamiento.

Gestión del cumplimiento

Muchas industrias y jurisdicciones tienen requisitos regulatorios que obligan a las organizaciones a usar ciertos tipos de cifrado para proteger los datos confidenciales. El cumplimiento de estas normativas ayuda a las organizaciones a eludir las sanciones legales y a conservar la confianza del cliente.

Algoritmos comunes de cifrado simétrico

Los algoritmos de clave simétrica más conocidos son:

- Estándar de cifrado de datos (DES) y Triple DES (3DES)
- Estándar de cifrado avanzado (AES)
- Twofish
- Pescado

Estándar de cifrado de datos (DES) y Triple DES (3DES)

IBM® introdujo DES por primera vez en la década de 1970 como el algoritmo de cifrado estándar, una función que desempeñó durante muchos años. Sin embargo, su longitud de clave relativamente corta (56 bits) la hizo vulnerable a ataques de fuerza bruta, donde los actores de amenazas prueban diferentes claves hasta que una funcione.

Triple DES, desarrollado como una mejora, aplica el algoritmo DES tres veces a cada bloque de datos, lo que aumenta significativamente el tamaño de la clave y la seguridad general.

Con el tiempo, algoritmos simétricos más seguros reemplazaron tanto a DES como a Triple DES.

Estándar de cifrado avanzado (AES)

AES generalmente se considera el estándar de oro de los algoritmos de cifrado simétrico. Es ampliamente adoptado por organizaciones y gobiernos de todo el mundo, incluido el gobierno de Estados Unidos. AES ofrece una amplia seguridad con longitudes de clave de 128, 192 o 256 bits. Las longitudes de clave más largas son más resistentes al agrietamiento.

En concreto, AES-256, que emplea una clave de 256 bits, es conocido por su alto nivel de seguridad y suele emplear en situaciones muy delicadas. AES también es muy eficaz tanto en las implementaciones de software como de hardware, por lo que es adecuado para una amplia gama de aplicaciones.

Twofish

Es un cifrado por bloques de clave simétrica conocido por su rapidez y seguridad. Opera en bloques de datos con un tamaño de bloque de 128 bits y admite longitudes de clave de 128, 192 o 256 bits.

Es de código abierto y resistente al criptoanálisis, lo que lo convierte en una opción confiable para aplicaciones seguras. Su flexibilidad y rendimiento se adaptan a implementaciones de software y hardware, particularmente donde la seguridad y el rendimiento son críticos.

Blowfish

Es un cifrado de bloque de clave simétrica diseñado para proporcionar una buena tasa de cifrado en el software y un cifrado de datos seguro. Admite longitudes de clave de 32 bits a 448 bits, lo que lo hace flexible y adecuado para diversas aplicaciones.

Es conocido por su velocidad y eficacia, y es particularmente popular para el cifrado de software. También es muy popular en aplicaciones que necesitan un algoritmo de cifrado simple y rápido, aunque algoritmos más nuevos como Twofish y AES lo reemplazaron en gran medida para la mayoría de los casos de uso.

Algoritmos asimétricos

¿Cómo funciona el cifrado asimétrico?

El cifrado asimétrico mantiene los datos seguros mediante el uso de algoritmos criptográficos para generar un par de claves: una clave pública y una clave privada. Cualquiera puede usar la clave pública para cifrar datos, pero solo aquellos con la clave privada correcta pueden descifrar esos datos para leerlos.

Las llaves funcionan como códigos complejos necesarios para abrir una caja fuerte. Sin la clave criptográfica correcta, los usuarios no pueden descifrar los datos cifrados. En general, cuanto mayor sea el tamaño de la clave, mayor será la seguridad. El cifrado asimétrico es conocido por tener longitudes de clave mucho más largas que el cifrado simétrico, lo que contribuye a su mayor seguridad.

En el cifrado asimétrico, las dos claves sirven para diferentes propósitos:

- La **clave pública** cifra datos o verifica firmas digitales y puede distribuir y compartir libremente.
- La **clave privada** descifra datos y crea firmas digitales, pero debe permanecer secreta para garantizar la seguridad.

La seguridad de la criptografía de clave pública se basa en mantener la confidencialidad de la clave privada mientras se comparte libremente la clave pública. La clave pública sólo puede cifrar datos, por lo que no es de mucho valor para los actores de amenazas. Y debido a que los usuarios nunca necesitan compartir sus claves privadas, reduce en gran medida el riesgo de que los hackers intercepten esas claves mucho más valiosas.

Una vez que las claves privadas y públicas están en su lugar, las personas pueden intercambiar información confidencial. El remitente cifra un mensaje empleando la clave pública del destinatario, y el destinatario emplea su clave privada para descifrar la información.

Piense que el proceso es similar al de un buzón cerrado: cualquiera puede echar una carta en un buzón, pero sólo el propietario puede desbloquearlo y leer el correo.

El cifrado asimétrico también puede ayudar a garantizar la autenticación. Por ejemplo, un remitente puede cifrar un mensaje con su clave privada y enviarlo a un destinatario. El destinatario puede usar la clave pública del remitente para descifrar el mensaje, confirmando así que fue el remitente original quien lo envió.

Los esquemas de cifrado asimétrico se implementan normalmente a través de una **infraestructura de clave pública (PKI).** Una PKI es un marco para crear, distribuir y validar pares de pares de claves públicas y privadas.

Algoritmos de cifrado asimétrico comunes

Los algoritmos de cifrado asimétrico son la columna vertebral de los criptosistemas modernos, proporcionando la base para comunicaciones seguras y protegiendo los datos confidenciales del acceso no autorizado.

Algunos de los algoritmos de cifrado asimétrico más importantes incluyen:

- Rivest-Shamir-Adleman (RSA)
- Criptografía de curva elíptica (ECC)
- Algoritmo de firma digital (DSA)

Rivest-Shamir-Adleman (RSA)

RSA es un algoritmo de cifrado asimétrico que lleva el nombre de sus inventores. Se basa en la complejidad matemática de los números primos para generar pares de claves. Usa un par de claves pública y privada para el cifrado y descifrado, lo que lo hace adecuado para la transmisión segura de datos y firmas digitales.

El algoritmo RSA ayuda con frecuencia a proteger los protocolos de comunicación, como HTTPS, SSH y TLS. A pesar de haber desarrollado en la década de 1970, RSA sigue siendo ampliamente empleado debido a su robustez y seguridad. Varias aplicaciones dependen de RSA, incluido el email seguro, las VPN y las actualizaciones de software.

Criptografía de curva elíptica (ECC)

ECC es un método de cifrado asimétrico basado en las propiedades matemáticas de curvas elípticas sobre campos finitos. Ofrece una seguridad estable con longitudes de clave más cortas que otros algoritmos, lo que da como resultado cálculos más rápidos y un menor consumo de energía.

La eficiencia de ECC lo hace ideal para aplicaciones con potencia de procesamiento y duración de la batería limitadas, como aplicaciones móviles, aplicaciones de mensajería segura y dispositivos IoT.

Algoritmo de firma digital (DSA)

El Algoritmo de Firma Digital (DSA) permite a organizaciones e individuos crear firmas digitales que aseguren la autenticidad e integridad de los mensajes o documentos.

Estandarizada por el NIST, la DSA se basa en el problema matemático del logaritmo discreto y aparece en varios protocolos de seguridad. DSA se emplea a menudo en aplicaciones que requieren la firma y verificación seguras de documentos, como la distribución de software, las transacciones financieras y los sistemas de votación electrónica.

Casos de Uso para el cifrado asimétrico

Cuando la seguridad es primordial, las organizaciones se apoyan en el cifrado asimétrico. Los casos de uso comunes de cifrado asimétrico incluyen:

- Navegación sitio web
- Comunicaciones seguras
- Firmas digitales
- Autenticación
- Intercambio de claves
- Tecnología Blockchain

2.2. Algoritmos Hash

Conceptos Fundamentales del Hashing Criptográfico

Un algoritmo hash es una función matemática unidireccional que toma una entrada de tamaño arbitrario (como un archivo o una cadena de texto) y produce una salida de tamaño

fijo, conocida como resumen (digest), valor hash o "huella digital". La naturaleza unidireccional de la función hace que sea computacionalmente inviable revertir el proceso para recuperar los datos originales a partir del resumen. Los hashes se utilizan para una variedad de propósitos, incluyendo la verificación de la integridad de los datos, el almacenamiento seguro de contraseñas y la creación de firmas digitales. La propiedad de que incluso un cambio mínimo en la entrada produce un resumen drásticamente diferente es fundamental para su utilidad.

SHA

¿Qué son los algoritmos hash – SHA?

- Un **algoritmo hash** es una función matemática que toma una entrada (mensaje, archivo, contraseña, etc.) y produce una salida de longitud fija llamada **hash** o **digest**.
- El objetivo es que sea **único** (o al menos difícilmente repetible), de manera que pequeñas variaciones en la entrada generen cambios drásticos en la salida.
- **SHA** significa Secure Hash Algorithm (Algoritmo de Hash Seguro). Fue desarrollado inicialmente por la **NSA** y publicado como estándar por el **NIST** (National Institute of Standards and Technology).
- Existen varias versiones de SHA:
  - **SHA-1** (160 bits, hoy considerado inseguro).
  - **SHA-2** (SHA-224, SHA-256, SHA-384, SHA-512).
  - **SHA-3** (más reciente, basado en el algoritmo Keccak).

Relación con la seguridad informática

Los algoritmos hash (en especial SHA-2 y SHA-3) son fundamentales en seguridad informática porque permiten:

1. **Integridad de datos**
   - Se usa SHA para generar resúmenes digitales de archivos o mensajes.
   - Si el hash cambia, significa que el contenido fue alterado.
   - Ejemplo: verificar que un software descargado no fue manipulado.
2. **Firmas digitales y certificados**
   - Los hash son parte de los algoritmos de firma digital.
   - Se aplica SHA al documento - se firma el hash en lugar de todo el documento - permite autenticidad y no repudio.
3. **Gestión de contraseñas**
   - En sistemas, las contraseñas no se guardan en texto plano sino como hash.

- Cuando un usuario inicia sesión, el sistema calcula el hash de la contraseña ingresada y lo compara con el hash almacenado.

4. **Criptografía moderna**
    - SHA es parte de protocolos como **TLS/SSL**, **IPSec**, **Bitcoin**, **Blockchain**, **PKI** (infraestructura de clave pública).

Relación con el desarrollo de software

En el desarrollo de software, los algoritmos SHA tienen aplicaciones muy prácticas:

- Almacenamiento seguro de contraseñas
    - Un sistema bien diseñado nunca guarda contraseñas en texto plano.
    - Se usan funciones hash (con salts o combinadas con algoritmos de derivación de claves como PBKDF2, bcrypt, scrypt o Argon2).
- Control de versiones y validación de integridad
    - Git, por ejemplo, usa SHA-1 (aunque está migrando por temas de seguridad) para identificar commits y verificar integridad.
- API y autenticación
    - Tokens, firmas de peticiones y verificaciones usan SHA (ejemplo: HMAC-SHA256).
- Blockchain y criptomonedas
    - SHA-256 se usa en Bitcoin y otras cadenas de bloques para validar transacciones, generar direcciones y minar bloques.
- DevSecOps y distribución de software
    - En pipelines de CI/CD se calculan hash SHA256 de binarios para comprobar que no se corrompan en el despliegue.

Ventajas

- Rápidos de calcular.
- Resúmenes de longitud fija, independientemente del tamaño del archivo.
- SHA-2 y SHA-3 son actualmente seguros.

Desventajas

- SHA-1 está roto: existen colisiones prácticas (dos mensajes diferentes que producen el mismo hash).
- SHA por sí solo **no debe usarse para almacenar contraseñas** sin técnicas adicionales (salt, key stretching), porque los ataques de fuerza bruta y diccionario lo pueden vulnerar.

MD5

MD5: El Origen de un Gigante y su Funcionamiento Técnico

El MD5 (Message-Digest Algorithm 5) fue diseñado en 1991 por Ronald Rivest como sucesor del algoritmo MD4 y se convirtió rápidamente en un estándar de facto. Fue adoptado por gobiernos y empresas para una amplia gama de aplicaciones, desde la verificación de la integridad de archivos hasta la protección de contraseñas. El algoritmo toma un mensaje de entrada de cualquier tamaño y lo procesa en bloques de 512 bits para generar un resumen de 128 bits, que comúnmente se representa como un número hexadecimal de 32 dígitos. El proceso implica una serie de operaciones lógicas sobre variables internas inicializadas con valores fijos, lo que garantiza que la salida sea consistente para una entrada determinada.

El Declive de MD5: Vulnerabilidades Críticas y la Realidad de los Ataques

A pesar de su popularidad histórica, el MD5 está "criptográficamente roto" y ya no se considera seguro para fines criptográficos. Su principal debilidad es su susceptibilidad a los “ataques de colisión”, donde un atacante puede encontrar dos entradas distintas que producen el mismo valor hash. Esta vulnerabilidad se demostró públicamente en 2004, lo que llevó a los expertos en seguridad a recomendar el uso de otros algoritmos.

Otra debilidad crítica es la alta velocidad de computación de MD5, que lo hace vulnerable a los “ataques de fuerza bruta”. Con el aumento exponencial de la potencia computacional, según la Ley de Moore, los atacantes pueden calcular miles de millones de hashes por segundo, lo que hace que los ataques de diccionario y las "tablas arcoíris" sean triviales. Esto expone una verdad fundamental: la seguridad de un algoritmo criptográfico no es una propiedad estática, sino que depende de la evolución del poder de cómputo del adversario. El fallo de MD5 no fue una falla en su diseño para la tecnología de 1991, sino un fracaso de la industria en anticipar cómo la Ley de Moore lo volvería obsoleto.

Consecuencias en el Mundo Real y Alternativas Seguras

Las vulnerabilidades de MD5 no son solo teóricas. Se han explotado en casos de alto perfil con consecuencias significativas. En 2008, investigadores demostraron que era posible falsificar un certificado SSL/TLS con la misma firma digital. Un caso aún más grave fue el del malware "Flame" en 2012, que utilizó un ataque de colisión de prefijo elegido para generar un certificado falso de Microsoft, lo que le permitió eludir los controles de seguridad y propagarse por los sistemas como si fuera un software legítimo.

A pesar de que las fallas de MD5 fueron conocidas desde hace más de una década, el algoritmo sigue siendo utilizado en muchos sistemas, incluso en 2019, debido a la inercia tecnológica y el costo percibido de la migración. Sin embargo, el consenso es claro: MD5 debe ser abandonado por completo para cualquier propósito de seguridad.

Referencias bibliográficas

Cifrado y Criptografía

- IBM. (2023). ¿Qué es el cifrado asimétrico? https://www.ibm.com/mx-es/think/topics/asymmetric-encryption
- Utimaco. (2023). ¿Qué es la criptografía simétrica? https://utimaco.com/es/servicio/base-de-conocimientos/gestion-de-claves-y-secretos/que-es-la-criptografia-simetrica
- Utimaco. (2023). ¿Qué es la criptografía asimétrica? https://utimaco.com/es/servicio/base-de-conocimientos/gestion-de-claves-y-secretos/que-es-la-criptografia-asimetrica
- NordVPN. (2023). Cifrado de bloque vs. cifrado de flujo. https://nordvpn.com/es-mx/blog/block-cipher-vs-stream-cipher/
- GeeksforGeeks. (2023). Diferencia entre cifrado de bloque y cifrado de flujo. https://www.geeksforgeeks.org/computer-networks/difference-between-block-cipher-and-stream-cipher/

Algoritmos de Hash

- KeepCoding. (2023). ¿Qué es SHA-1? https://keepcoding.io/blog/que-es-sha-1
- Simplilearn. (2023). Algoritmo MD5: Cómo funciona, aplicaciones y limitaciones. https://www.simplilearn.com/tutorials/cyber-security-tutorial/md5-algorithm
- Atsec. (2021). El auge y caída de MD5. https://www.atsec.com/rise-fall-of-md5/
- Okta. (2023). MD5: ¿Qué es y por qué ya no debería usarse? https://www.okta.com/identity-101/md5/
- Avast. (2023). Algoritmo de hash MD5. https://www.avast.com/es-es/c-md5-hashing-algorithm
- Pimpale, S. (2021). ¿Por qué MD5 ya no es seguro? https://medium.com/@shital.pimpale5/why-is-md5-no-longer-secure-4c2c89713eb2
- Radware. (2023). Flame: Malware de ciberespionaje. https://www.radware.com/security/ddos-knowledge-center/ddospedia/flame/
- Sophos. (2017). Algoritmo MD5: Las horas contadas. https://news.sophos.com/es-es/2017/01/27/algoritmo-md5-las-horas-contadas/

Normas y Estándares

- NQA. (2023). Guía para la implementación de la norma ISO 27001. https://www.nqa.com/es-es/certification/standards/iso-27001/implementation
- Fortinet. (2023). ISO/IEC 27001. https://www.fortinet.com/lat/resources/cyberglossary/iso-iec-27001

- NormaISO27001. (2023). A14 - Adquisición, desarrollo y mantenimiento de los sistemas de información. https://www.normaiso27001.es/a14-adquisicion-desarrollo-y-mantenimiento-de-los-sistemas-de-informacion
- GlobalSuite Solutions. (2023). ¿Qué es la norma ISO 27001 y para qué sirve? https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve
- PiraniRisk. (2023). ISO 27001: Qué es y cómo implementarla. https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla
- Luis, G. V. (2023). Estándares de seguridad informática. https://luisgv01.github.io/Ovi/estandseguinf.html
- UPV. (2023). Publicación sobre seguridad informática. https://riunet.upv.es/entities/publication/ab5ae4f9-ce99-4720-9aa7-c2c7664a6dd2
- Concytec. (2023). Publicación sobre seguridad informática. https://alicia.concytec.gob.pe/vufind/Record/1728-2969_25c6cffd4c602737462ea01945a1908b

Marcos de Referencia

- InvGate. (2023). COBIT: Qué es y para qué sirve. https://blog.invgate.com/es/cobit
- CIO. (2023). COBIT: Un marco para la alineación y la gobernanza. https://www.cio.com/article/1314368/cobit-un-marco-para-la-alineacion-y-la-gobernanza.html
- Fortinet. (2023). ¿Qué es COBIT? https://www.fortinet.com/lat/resources/cyberglossary/what-is-cobit
- Veza. (2023). Cumplimiento NIST. https://veza.com/blog/nist-compliance/
- CMS. (2023). Instituto Nacional de Estándares y Tecnología (NIST). https://security.cms.gov/learn/national-institute-standards-and-technology-nist
- IBM. (2023). ¿Qué es NIST? https://www.ibm.com/think/topics/nist
- Ivanti. (2023). ¿Qué es ITIL? https://www.ivanti.com/glossary/itil
- ITSM Tools. (2023). ITIL 4 explicado. https://itsm.tools/itil-4-explained/
- IBM. (2023). Biblioteca de Infraestructura de Tecnología de la Información. https://www.ibm.com/es-es/think/topics/it-infrastructure-library
- NIST. (2023). Marcos de referencia. https://www.nist.gov/frameworks
- NIST. (2023). Laboratorio de Tecnología de la Información. https://www.nist.gov/itl

Seguridad y Control de Acceso

- NIST. (2023). Control de acceso. https://csrc.nist.gov/glossary/term/access_control
- SailPoint. (2023). Triada CIA. https://www.sailpoint.com/identity-library/cia-triad

- Fortinet. (2023). Control de acceso. https://www.fortinet.com/resources/cyberglossary/access-control
- NIST. (2023). Autenticación. https://csrc.nist.gov/glossary/term/authentication

Propiedad Intelectual

- DocuSign. (2023). Contratos de protección de propiedad intelectual. https://www.docusign.com/es-mx/blog/desarrolladores/contratos-proteccion-propiedad-intelectual
- Thales. (2023). Protección de la propiedad intelectual del software. https://cpl.thalesgroup.com/es/software-monetization/protecting-software-intellectual-property
- Diputados. (2020). Ley Federal de Protección a la Propiedad Industrial. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPPI.pdf
- Diputados. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
- Diputados. (2023). Protección de derechos de propiedad industrial. https://www.diputados.gob.mx/bibliot/publica/libros/forodsdi/MONTERRE/Proderau.htm
- Open Source Initiative. (2023). Definición de código abierto. https://opensource.org/osd
- Concreta Legal. (2023). Propiedad intelectual de software en México. https://concretalegal.com/blog/propiedad-intelectual-software-mexico/
- GNU Project. (2023). ¿Qué es el software libre? https://www.gnu.org/philosophy/free-sw.html
- IBM. (2023). Cifrado simétrico. https://www.ibm.com/mx-es/think/topics/symmetric-encryption