José Carlos López Henestrosa

Normativa de ciberseguridad

Tarea 5: Normativa vigente de ciberseguridad de ámbito nacional e internacional

Índice

Caso práctico **2**
Apartado 1: Normas nacionales e internacionales **3**
Propón tres controles de cada proceso de seguridad de la normativa NIST aplicados al contexto de FlutterTech 3
Apartado 2. Sistema de gestión de seguridad de la información basado en ISO 27001 ..... **5**
Desarrolla un contexto descriptivo de la organización alineado con los requisitos de información del estándar ISO 27001 5
Propón al menos tres controles del Anexo A de la norma ISO 27001 para la mitigación de riesgos identificados en el contexto anterior 7
Desarrolla tres métricas de seguridad para FlutterTech. Estas métricas deben permitir evaluar la eficacia del SGSI implantado en la empresa 8
Apartado 3. Sistema de gestión de continuidad de negocio basado en ISO 22301 ..... **9**
Realiza un análisis de impacto en la continuidad de los sistemas centrales de FlutterTech que dan servicio a sus aplicaciones móviles 9
Establece un valor justificado para el MTPD, el RTO y el RPO 11
Apartado 4: Esquema nacional de seguridad **12**
Categoriza los sistemas asociados al desarrollo y mantenimiento de las aplicaciones móviles críticas de FlutterTech, en función del escenario definido en el caso práctico y por la prestación de servicios a las Fuerzas y Cuerpos de Seguridad del Estado 12
Desarrolla una declaración de aplicabilidad (SoA) justificada, indicando qué medidas de seguridad del ENS se aplicarán y por qué 14

Caso práctico

La compañía FlutterTech S.A. se dedica al desarrollo de aplicaciones móviles multiplataforma utilizando el framework Flutter, ofreciendo soluciones tanto a particulares como a empresas.

FlutterTech cuenta con una cartera de 300.000 usuarios activos en España que utilizan sus aplicaciones, muchas de las cuales operan bajo un modelo de suscripción mensual con una tarifa media de 23,50 €.

La empresa tiene presencia en 32 países, lo que le ha permitido trabajar con clientes multinacionales. Durante el año 2022, FlutterTech logró adjudicarse el desarrollo y mantenimiento de las aplicaciones móviles oficiales de todas las embajadas extranjeras en España.

Uno de sus principales clientes es una entidad bancaria internacional con un alto nivel de exigencia en materia de ciberseguridad. Entre sus requisitos destaca que los servicios de desarrollo cumplan con la certificación ISO27001.

La sede central de FlutterTech se encuentra en Málaga, y fue inaugurada en el año 2020. Las instalaciones cuentan con climatización inteligente, jardines en las azoteas para mejorar la eficiencia térmica, recogida de agua de lluvia para el riego de zonas verdes, y un sistema de paneles solares para reducir el consumo energético.

Además, una parte de los terrenos de la empresa ha sido acondicionada como zona verde pública, en colaboración con el ayuntamiento, mejorando el entorno para los residentes. También se ha invertido en la mejora de los accesos por carretera a la zona empresarial donde se encuentra su sede.

En los últimos meses, FlutterTech ha logrado un importante contrato con una institución de las Fuerzas y Cuerpos de Seguridad del Estado, para el desarrollo de aplicaciones móviles seguras y accesibles. Debido a la criticidad del servicio, FlutterTech ha sido designada como proveedor de servicio esencial.

Con este nuevo contrato y los compromisos ya existentes, FlutterTech iniciará el despliegue de un Sistema de Gestión de Seguridad de la Información (SGSI) y un Sistema de Gestión de Continuidad de Negocio (SGCN). Asimismo, deberá cumplir con el Esquema Nacional de Seguridad (ENS) y con la Directiva NIS, dado que sus aplicaciones forman parte de servicios críticos para la seguridad nacional.

En esta tarea se requerirá de los conocimientos adquiridos a lo largo de la unidad para desarrollar los contenidos requeridos en el ejercicio.

Apartado 1: Normas nacionales e internacionales.

Propón tres controles de cada proceso de seguridad de la normativa NIST aplicados al contexto de FlutterTech

NOTA: Ten en cuenta que FlutterTech desarrolla aplicaciones móviles que deben cumplir con altos estándares de seguridad para clientes como bancos o instituciones públicas. Puedes centrarte en los controles más relevantes para este tipo de entorno.

Identificar (ID):

- **Gestión de activos**: Inventario detallado de todos los dispositivos, servidores y repositorios de código que intervienen en el desarrollo y mantenimiento de aplicaciones.
- **Evaluación de riesgos**: Implementación de auditorías periódicas para identificar vulnerabilidades en el desarrollo de software y la infraestructura de TI.
- **Cumplimiento normativo**: Establecimiento de políticas alineadas con la ISO 27001, la ENS y la NIS para garantizar el cumplimiento de los requisitos regulatorios.

Proteger (PR):

- **Control de acceso**: Implementación de autenticación multifactor (MFA) para los desarrolladores y empleados que accedan a los entornos de desarrollo y producción.
- **Protección de datos**: Encriptación de datos en reposo y en tránsito en todas las aplicaciones para garantizar la confidencialidad de la información de los clientes.
- **Capacitación en seguridad**: Programas de formación continua para concienciar a los empleados sobre las mejores prácticas en materia de ciberseguridad.

Detectar (DE):

- **Monitorización continua**: Implementación de un SIEM para detectar accesos sospechosos o incidentes de seguridad.
- **Análisis de anomalías:** Uso de IA para identificar patrones inusuales en el tráfico de datos o accesos no autorizados a las aplicaciones.
- **Pruebas de penetración:** Realización periódica de pruebas de intrusión en las aplicaciones desarrolladas para clientes sensibles, como bancos o cuerpos de seguridad.

Responder (RS)

- **Plan de respuesta a incidentes**: Desarrollo y simulación de procedimientos de respuesta ante ciberataques para garantizar una actuación rápida y eficaz.
- **Comunicación de incidentes**: Establecimiento de canales de notificación para clientes, reguladores y usuarios en caso de brechas de seguridad.
- **Registro y análisis forense**: Almacenamiento seguro de registros para investigar incidentes y mejorar las defensas ante futuras amenazas.

Recuperar (RC):

- **Plan de recuperación ante desastres**: Implementación de medidas para restaurar los servicios en caso de fallos de seguridad o ciberataques.
- **Copias de seguridad**: Mantenimiento de copias de seguridad encriptadas y redundantes geográficamente para garantizar la continuidad operativa.
- **Evaluación post-incidente**: Realización de revisiones tras cada incidente para identificar mejoras y actualizar los protocolos de seguridad.

Fuentes:

- Sección "**Principales estándares internacionales en ciberseguridad**" del apartado "**1. Normas nacionales e internacionales**" del material didáctico de la unidad 5.

Apartado 2. Sistema de gestión de seguridad de la información basado en ISO 27001.

Desarrolla un contexto descriptivo de la organización alineado con los requisitos de información del estándar ISO 27001

NOTA: Deberás considerar aspectos como los activos de información, partes interesadas, servicios ofrecidos, entornos tecnológicos, regulaciones aplicables, etc.

FlutterTech S.A. es una empresa especializada en el desarrollo de aplicaciones móviles multiplataforma con el framework Flutter. Con una base de 300.000 usuarios activos en España y presencia en 32 países, la organización se ha consolidado como un proveedor clave en soluciones digitales para clientes empresariales y particulares.

Dentro del entorno que rodea a la empresa, encontramos tanto el externo como el interno:

- **Entorno externo**

  FlutterTech atiende a una variedad de clientes, entre los que se incluyen instituciones financieras, organismos gubernamentales y empresas privadas con altos requisitos de seguridad. En cuanto a las normativas de regulación y cumplimiento, la organización debe adherirse a normativas como la ISO 27001, el Esquema Nacional de Seguridad (ENS) y la Directiva NIS, debido a su papel en el desarrollo de aplicaciones para instituciones críticas, como embajadas y cuerpos de seguridad del Estado.

  Por otra parte, el sector del desarrollo de software se enfrenta a cambios continuos en las tecnologías y a amenazas de ciberseguridad, por lo que la empresa debe adaptar constantemente sus protocolos de protección de datos. A esto hay que sumarle la creciente digitalización y el uso de modelos de suscripción, que impactan en la estrategia comercial de la empresa, con una tarifa media de 23,5 € por suscripción mensual.

- **Entorno interno**

  La sede central se encuentra en Málaga. Cuenta con instalaciones eficientes desde el punto de vista energético y un compromiso con la sostenibilidad. Su infraestructura tecnológica incluye un entorno de desarrollo en la nube, repositorios de código gestionados con control de acceso y medidas de seguridad avanzadas.

El equipo está compuesto por desarrolladores, expertos en ciberseguridad y profesionales del cumplimiento normativo. FlutterTech está implementando un Sistema de Gestión de Seguridad de la Información (SGSI) para gestionar los riesgos asociados a sus operaciones.

Respecto a las partes interesadas, tenemos una relación con las expectativas que estas tienen respecto a la seguridad de la información:

PARTE INTERESADA	**EXPECTATIVAS**
Clientes empresariales (banca, gobierno, multinacionales)	Seguridad robusta, cumplimiento normativo, garantía de continuidad del servicio.
Usuarios finales	Protección de datos personales, experiencia segura en aplicaciones.
Reguladores y organismos de certificación	Cumplimiento de ISO 27001, ENS y NIS.
Proveedores y socios tecnológicos	Seguridad en la gestión de accesos y transferencia de datos.
Empleados	Capacitación en ciberseguridad y un entorno seguro de desarrollo.

En relación con los principales riesgos en materia de seguridad de la información, se encuentran los ciberataques dirigidos a sus aplicaciones y bases de datos, la filtración de información sensible de clientes críticos y el cumplimiento regulatorio en mercados internacionales con diferentes normativas.

Para mitigar estos riesgos, se está implementando un SGSI basado en ISO 27001, con controles de acceso, encriptación de datos, auditorías periódicas y planes de respuesta ante incidentes.

Propón al menos tres controles del Anexo A de la norma ISO 27001 para la mitigación de riesgos identificados en el contexto anterior

---

1. **A.9.2.1 Registro de usuarios y cancelación del registro**

   Establecer procedimientos formales para la asignación y revocación de derechos de acceso a sistemas y datos con el fin de garantizar que los empleados y terceros solo tengan acceso a la información necesaria para el desempeño de sus funciones y minimizar el riesgo de accesos no autorizados.

2. **A.15.1.1 Seguridad de la información en las relaciones con los proveedores**

   Implementación de acuerdos contractuales con proveedores y socios tecnológicos que incluyan requisitos específicos de seguridad para garantizar que la gestión de accesos y la transferencia de datos cumplan con los estándares exigidos.

3. **A.18.1.4 Protección de los datos y privacidad de la información personal**

   Aplicación de mecanismos de cifrado en reposo y en tránsito para proteger la información sensible de clientes críticos, en consonancia con regulaciones como el RGPD y los requisitos del ENS.

Fuentes:

- A.9.2.1: https://www.normaiso27001.es/a9-control-de-acceso/
- A.15.1: https://www.normaiso27001.es/a15-relacion-con-proveedores/
- A.18.1.4: https://www.normaiso27001.es/a18-cumplimiento/

Desarrolla tres métricas de seguridad para FlutterTech. Estas métricas deben permitir evaluar la eficacia del SGSI implantado en la empresa

---

1. **Tiempo Medio de Respuesta a Incidentes (MTTR)**

   Mide el tiempo promedio que transcurre desde la detección de un incidente de seguridad hasta su resolución completa.

   $$MTTR = \frac{\Sigma\, Tiempo\ de\ resolución\ de\ cada\ incidente}{Número\ total\ de\ incidentes}$$

   Un valor bajo de esta métrica indica una mejora en la capacidad de la organización para manejar y mitigar incidentes de seguridad de manera eficiente.

2. **Porcentaje de cumplimiento de controles de seguridad**

   Evalúa el grado en que los controles de seguridad establecidos en el SGSI se implementan y mantienen según lo planificado.

   $$\%\ cumplimiento\ de\ controles\ de\ seguridad = \frac{Número\ de\ controles\ implementados\ y\ operativos}{Número\ total\ de\ controles\ planificados} \times 100$$

   Un alto porcentaje refleja una fuerte adherencia a las políticas de seguridad y a una gestión efectiva del SGSI.

3. **Número de vulnerabilidades detectadas en auditorías internas**

   Cuenta la cantidad de vulnerabilidades de seguridad identificadas durante las auditorías internas en un período determinado.

   Una tendencia decreciente en este número apunta a una mejora en la gestión de seguridad de la organización y la efectividad de las medidas preventivas implementadas.

Fuentes:

- Luis Rodríguez Conde. *Gestión de Indicadores.* https://openaccess.uoc.edu/bitstream/10609/64545/5/liziyoTFM0617-ANEXO%20C.pdf

Apartado 3. Sistema de gestión de continuidad de negocio basado en ISO 22301.

Realiza un análisis de impacto en la continuidad de los sistemas centrales de FlutterTech que dan servicio a sus aplicaciones móviles

El escenario a utilizar para este análisis de impacto es el siguiente:

FlutterTech gestiona varios sistemas centralizados que permiten el funcionamiento de todas sus aplicaciones móviles activas. En caso de indisponibilidad de estos sistemas (por ciberataque, fallo crítico, etc.), ninguna de las aplicaciones funcionaría, y no podrían recibirse pagos, emitir actualizaciones, ni ofrecer soporte a usuarios o empresas.

Consecuencias económicas estimadas:

- **Lucro cesante**: por incapacidad de facturación y pérdida de ingresos publicitarios. Se estima una pérdida de 60.000 € por hora de caída del servicio.
- **Compensaciones**: por penalizaciones contractuales con empresas. Los contratos establecen una garantía del 97% de disponibilidad mensual. En caso de caída superior a 30 minutos y con reclamación, a partir de la primera hora se aplican compensaciones de 300.000 € por hora.
- **Imagen y reputación**: se estima la pérdida del 1% de la cartera de clientes por cada incidencia grave, y la caída en nuevas contrataciones. Esto se ha valorado en 200.000 € por incidencia.
- **Sanciones**: FlutterTech es proveedor esencial de aplicaciones para organismos públicos. En caso de caída reiterada o prolongada, podrían aplicarse sanciones regulatorias importantes.

La organización no está dispuesta a asumir pérdidas mayores a 1,25 millones de euros por incidente.

Si tenemos en cuenta las consecuencias económicas estimadas y que FlutterTech no está dispuesta asumir pérdidas mayores a 1,25 millones de euros por incidente, podemos presentar los siguientes escenarios para analizar el impacto de la continuidad de los sistemas centrales de FlutterTech:

- Inactividad de los sistemas debido a un fallo prolongado durante **2 horas**:
  - **Lucro cesante**: 120.000 € (2h × 60.000 €).
  - **Compensaciones**: 300.000 € (solo 1h si aplica).
  - **Daño reputacional**: 200.000 € (una vez por incidente).
  - **Total estimado**: 620.000 € (sin incluir sanciones).

- Inactividad de los sistemas debido a un fallo prolongado durante **3 horas**:
  - **Lucro cesante**: 180.000 € (3h × 60.000 €).
  - **Compensaciones**: 600.000 € (2h × 300.000 €).
  - **Daño reputacional**: 200.000 € (una vez por incidente).
  - **Total estimado**: 980.000 € (supera el umbral).

- Inactividad de los sistemas debido a un fallo prolongado durante **4 horas**:
  - **Lucro cesante**: 240.000 € (4h × 60.000 €).
  - **Compensaciones**: 900.000 € (3h × 300.000 €).
  - **Daño reputacional**: 200.000 € (una vez por incidente).
  - **Sanción por caída prolongada durante 4 horas**: 200.000 €.
  - **Total estimado**: 1.540.000 € (supera el umbral).

Como podemos apreciar, el punto crítico se alcanza a partir de las 3 horas de inactividad, cerca del impacto financiero límite aceptable. Por otra parte, los factores que suponen un mayor riesgo son las compensaciones contractuales (300.000 €/h) y el daño reputacional (200.000 €). No obstante, hay que tener en cuenta que las posibles sanciones regulatorias podrían incrementar el costo total significativamente, como vemos en el último escenario.

Para mitigar los riesgos y reducir el impacto de los escenarios anteriormente expuestos, FlutterTech, debería trabajar en mejorar la capacidad de sus sistemas para operar de manera continua (alta disponibilidad) y redundar los sistemas críticos para poder actuar con rapidez en caso de fallo. Estos puntos podrían incluirse en el Plan de Recuperación ante Desastres (DRP), con un Tiempo de Recuperación Objetivo (RTO) inferior a 1 hora.

Por otro lado, sería conveniente revisar las cláusulas contractuales para reducir las compensaciones, las cuales son un tanto excesivas.

Establece un valor justificado para el MTPD, el RTO y el RPO

- **MTPD (Maximum Tolerable Period of Disruption): 3 horas**

  Dado que la empresa no está dispuesta a asumir pérdidas mayores de 1,25 millones de euros por incidente, y que la pérdida económica estimada es de 660.000 €/hora (sumando lucro cesante y compensaciones), en menos de 2 horas de caída ya se superaría el umbral de tolerancia. Para dar margen a la recuperación, se establece un MTPD de 3 horas, ya que una interrupción más prolongada podría generar daños irreparables en la imagen, sanciones regulatorias y pérdida sustancial de clientes, tal y como se expone en el apartado anterior.

- **RTO (Recovery Time Objective): 30 minutos**

  Los contratos establecen compensaciones a partir de 30 minutos de caída, lo que significa que cualquier interrupción que supere este umbral impactará financieramente a FlutterTech. Por lo tanto, el objetivo debe ser recuperar el servicio en menos de 30 minutos para evitar estos costes y mantener el nivel de servicio comprometido.

- **RPO (Recovery Point Objective): 5 minutos**

  FlutterTech gestiona transacciones financieras y datos en tiempo real, por lo que una pérdida de datos superior a 5 minutos podría ocasionar inconsistencias graves en pagos, actualizaciones y asistencia. Además, un RPO bajo minimiza el riesgo de sanciones regulatorias y de pérdida de confianza de los clientes.

Apartado 4: Esquema nacional de seguridad.

Categoriza los sistemas asociados al desarrollo y mantenimiento de las aplicaciones móviles críticas de FlutterTech, en función del escenario definido en el caso práctico y por la prestación de servicios a las Fuerzas y Cuerpos de Seguridad del Estado

---

La siguiente tabla categoriza los sistemas propuestos en el enunciado. Cabe destacar que algunos ejemplos expuestos no aparecen explícitamente en el caso práctico, pero se añaden para ofrecer una visión general de los sistemas de cada categoría que podrían encontrarse en una organización real.

CATEGORÍA DE SISTEMA	DESCRIPCIÓN	EJEMPLOS EN FLUTTERTECH	NIVEL DE CRITICID.	JUSTIFICACIÓN
Desarrollo y pruebas	Plataformas y herramientas utilizadas para la creación y prueba de aplicaciones móviles.	Repositorios de código, entornos de desarrollo integrados, plataformas CI/CD.	Medio	Esenciales, pero no procesan datos en producción.
Producción	Infraestructura donde se ejecutan las aplicaciones en servicio.	Servicios en la nube, contenedores Docker, servicios de backend y APIs expuestas a usuarios finales.	Crítico	Contienen datos en tiempo real y afectan directamente a los usuarios finales.
Seguridad y monitoreo	Herramientas para la detección de amenazas, gestión de accesos y cumplimiento normativo.	SIEM, firewalls, autenticación multifactor, herramientas de auditoría y análisis de vulnerabilidades.	Alto	Claves para proteger las aplicaciones y los datos sensibles.
Gestión y cumplimiento normativo	Plataformas para garantizar el cumplimiento de regulaciones de seguridad.	SGSI basado en ISO 27001, herramientas de cumplimiento ENS/NIS, sistemas de auditoría interna.	Alto	Aseguran que FlutterTech cumpla con las leyes y normativas vigentes.

Continuidad y respaldo	Infraestructura para garantizar la disponibilidad y recuperación ante incidentes.	Copias de seguridad en la nube, planes de recuperación ante desastres (DRP), servidores redundantes.	Crítico	Permiten la recuperación ante fallos o ataques, y aseguran la operatividad de los servicios esenciales.

Desarrolla una declaración de aplicabilidad (SoA) justificada, indicando qué medidas de seguridad del ENS se aplicarán y por qué.

FlutterTech S.A. es un proveedor de desarrollo de aplicaciones móviles críticas para clientes que exigen un alto nivel de seguridad, como entidades bancarias y las Fuerzas y Cuerpos de Seguridad del Estado. Como proveedor de servicios esenciales, la empresa debe cumplir la categoría alta del ENS para asegurar la integridad, disponibilidad y confidencialidad de la información.

Esta Declaración de Aplicabilidad detalla los controles de seguridad del ENS que han sido adoptados y justifica su aplicación en el contexto de la organización.

CÓDIGO ENS	MEDIDA DE SEGURIDAD	JUSTIFICACIÓN DE APLICABILIDAD
MP.01	**Política de seguridad**	Es obligatorio definir y mantener una política de seguridad que regule la protección de datos en las aplicaciones móviles críticas y en los entornos de desarrollo.
OP.05	**Control de accesos**	Dado que FlutterTech maneja información sensible de organismos de seguridad, se aplica autenticación multifactor, gestión de accesos basada en roles (RBAC) y monitorización de accesos privilegiados.
PR.04	**Protección de la información en tránsito y en reposo**	La información de usuarios y clientes críticos debe estar cifrada con algoritmos robustos para evitar intercepciones o filtraciones.
PR.07	**Registro y monitorización de actividad**	Implementación de un SIEM para detectar y responder a incidentes en tiempo real.
PR.12	**Protección contra código malicioso**	Se usan herramientas de análisis de código estático y dinámico para encontrar fallos de seguridad en las aplicaciones antes de ponerlas en funcionamiento.
OP.08	**Gestión de incidentes de seguridad**	Se ha desarrollado un Plan de Respuesta a Incidentes (PRI) que establece los procedimientos a seguir en caso de ciberataques y fugas de datos.
MC.03	**Respaldo y recuperación ante desastres**	FlutterTech mantiene copias de seguridad cifradas y con redundancia geográfica, y realiza pruebas periódicas de recuperación.

MP.04	**Cumplimiento normativo y auditoría**	La empresa está sujeta a auditorías periódicas para verificar el cumplimiento de ENS, ISO 27001 y NIS, lo que reduce los riesgos legales y operativos.

Fuentes:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191
- Inforges. *¿Qué es ENS Esquema Nacional de Seguridad?* https://inforges.es/blog/que-es-ens-esquema-nacional-de-seguridad
- Guía CCN-CERT sobre la categorización de sistemas en el ENS. https://www.ccn-cert.cni.es/es/documentos-publicos/x-jornadas-stic-ccn-cert/1954-como-categorizar-un-sistema-en-el-ens/file?format=html
- DeleteTechnology. *Requisitos y Niveles de Seguridad del ENS.* https://www.deletetechnology.com/blog/requisitos-y-niveles-de-seguridad-del-ens
- Amazon Web Services. *Esquema Nacional de Seguridad (categoría Alta).* https://aws.amazon.com/es/compliance/esquema-nacional-de-seguridad