# Sistema de Gestión de la Seguridad de la Información y Esquema Nacional de Seguridad

# POLÍTICA INTEGRADA DE SEGURIDAD DE LA INFORMACIÓN

# ÍNDICE

# 1. INTRODUCCIÓN

La **Política Integrada de Seguridad de la información** se elabora en cumplimiento de los requisitos de la Norma ISO 27001:2013 y de las exigencias del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y modificaciones posteriores, que en su artículo 11 establece la obligación de disponer de una Política.

*El Consorci de la Zona Franca de Barcelona* depende de los sistemas TIC (Tecnología de Información y Comunicación) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que deben aplicarse las medidas de seguridad exigidas por la norma ISO 27001:2013 en base al riesgo, y también por el **Esquema Nacional de Seguridad** en base a la categorización de los diferentes sistemas. Debe realizarse un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

*El Consorci de la Zona Franca de Barcelona* debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida de los sistemas, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación asociadas deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.
La Organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

## 1.1 PREVENCIÓN

La Organización debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos según se dispone en la norma ISO 27001:2013 y en el marco operacional del propio ENS. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Organización debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

## 1.2 DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

## 1.3 RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los equipos de Respuesta a Emergencias (CERT).

## 1.4 RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

# 2. ALCANCE

*El Consorci de la Zona Franca de Barcelona* tiene la voluntad de conseguir que los principios de la Política de Seguridad formen parte de la cultura de la Organización para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) en base a un estándar reconocido internacionalmente.

El alcance de la Política de Seguridad de la Información coincide con el alcance del SGSI.

Todo el personal de la Organización, incluyendo colaboradores, usuario y la dirección, debe conocer y cumplir esta política, que se desarrollará mediante normativa, procedimientos, instrucciones operativas, guías, manuales y todos aquellos instrumentos organizativos considerados útiles para alcanzar sus objetivos. Especial consideración merece el **Manual de Seguridad del usuario**, que contiene normas de uso de los sistemas de información de la Organización, cuyas disposiciones son de obligado cumplimiento.

Esta Política Integrada de Seguridad de la Información, además, estará a disposición de todas las otras partes interesadas que lo requieran, focalizando en usuarios, proveedores y clientes.

# 3. ORGANIZACIÓN DE LA SEGURIDAD

## 3.1 LIDERAZGO DE LA DIRECCIÓN

La Dirección de *El Consorci de la Zona Franca de Barcelona* (CZFB) se compromete a liderar el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI), así como las disposiciones indicadas en el RD 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica y modificaciones posteriores.

## 3.2 ROLES, RESPONSABILIDADES Y FUNCIONES

La organización de la seguridad de la información se organiza en torno a un Sistema de Gestión de Seguridad de la Información y a una serie de comités y roles, relevantes para el SGSI y el cumplimiento de las disposiciones del ENS.

## 4. OBJETO DE LA POLÍTICA DE SEGURIDAD

Los motivos para la creación de esta Política de Seguridad por parte del Responsable de Seguridad del SGSI y la Dirección, son varios:

- El principal es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiere para el desempeño profesional, así como evitar serias pérdidas de información y accesos no autorizados a la misma. Los principios que deben respetarse son los siguientes:

    - **Confidencialidad**: la información perteneciente a *El Consorci de la Zona Franca de Barcelona* debe ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

    - **Integridad**: la información de *El Consorci de la Zona Franca de Barcelona* debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.

    - **Disponibilidad:** la información de *El Consorci de la Zona Franca de Barcelona* está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

    - **Autenticidad:** El origen de la información de los ciudadanos tratada por *El Consorci de la Zona Franca de Barcelona* debe ser confiable, es decir, garantizando que quien la proporcione sea realmente quien dice ser.

    - **Trazabilidad:** Garantizar que pueda determinarse en todo momento la trazabilidad respecto a los tratamientos efectuados por *El Consorci de la Zona Franca de Barcelona, respecto a la información* de los ciudadanos para la que sea relevante su conocimiento.

Adicionalmente, dado que cualquier Sistema de Gestión de la Seguridad de la Información debe cumplir con la legislación vigente, se atenderá al siguiente principio:

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta *El Consorci de la Zona Franca de Barcelona*, especialmente lo dispuesto por el ENS y en materia de protección de datos personales.

- Establecer anualmente objetivos de seguridad de la información para la organización y protección de los activos de información de *El Consorci de la Zona Franca de Barcelona*. Dichos objetivos se alcanzarán a través de una serie de medidas organizativas y técnicas, junto a normas concretas y claramente definidas.

- Esta Política de Seguridad será mantenida, actualizada y adecuada a los fines y obligaciones de la organización.

- El resultado de esta Política se plasma en un Sistema de Gestión de Seguridad de la Información.

## 5. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrollará por medio de normativa de seguridad y procedimientos que afronten aspectos específicos.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

## 6. MANTENIMIENTO DEL SGSI

El mantenimiento actualizado del Sistema de Gestión de Seguridad de la información se fundamenta en:

- Estudio y conclusiones de los indicadores definidos.
- Resultado de las auditorías técnicas y de cumplimiento.
- Inputs de terceras partes.

## 7. GESTIÓN DEL RIESGO

La gestión de la Seguridad de la Información en la Organización está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2013 y el ENS.

Se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente pueden afectar a la seguridad de la información de los servicios prestados, consistente en:

- **Identificar los riesgos**, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad de la información.
- **Analizar los riesgos**, en base a la consecuencia de materializarse y de la probabilidad de ocurrencia.
- **Evaluar los riesgos,** según un nivel previamente establecido y aprobado de riesgo ampliamente aceptable, tolerable e inaceptable.
- **Tratar los riesgos** inaceptables, mediante los controles o salvaguardas adecuadas.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año, y basada en una metodología concreta que produzca resultados comparables. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

## 8. MARCO NORMATIVO

Son de aplicación las leyes y normativas del ordenamiento jurídico español, especialmente con relación al **Esquema Nacional de Seguridad**, protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, *El Consorci de la Zona Franca de Barcelona* podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

## 9. DATOS DE CARÀCTER PERSONAL

*El Consorci de la Zona Franca Barcelona* realiza tratamientos en los que hace uso de datos de carácter personal. El Documento de Seguridad de Protección de Datos de la Organización se puede encontrar en las dependencias del *Delegado de Protección de Datos*. Dicho documento recoge los ficheros afectados y tratamientos correspondientes.

Todos los sistemas de información de *El Consorci de la Zona Franca de Barcelona* se ajustarán a los niveles de seguridad requeridos por la normativa, en función de la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

## 10. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Organización tienen la obligación de conocer y cumplir esta Política Integrada de Seguridad de la Información y el Manual de Seguridad del Usuario desarrollado a partir de ella, siendo responsabilidad de la Dirección disponer de los medios necesarios para que la información llegue a los afectados, teniendo en cuenta siempre las disponibilidades presupuestarias de *El Consorci de la Zona Franca de Barcelona*. Todos los trabajadores de la Organización atenderán a una acción de concienciación en materia de seguridad TIC al menos una vez al año.

Se establecerá un programa de acciones en concienciación continua para atender a todos los miembros de *El Consorci de la Zona Franca de Barcelona*, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de la Organización. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir cualquier responsabilidad en la Organización, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

## 11. TERCERAS PARTES

Cuando *El Consorci de la Zona Franca de Barcelona* preste servicios o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Para ello, se establecerán canales para informe y coordinación de los respectivos Roles o Comités de Coordinación del ENS y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. Cuando ***El Consorci de la Zona Franca de Barcelona*** utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política Integrada de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de informe y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. El informe debe ser aprobado por los responsables de la información y los servicios afectados antes de seguir adelante.

## 12. SUPERVISIÓN Y EVALUACIÓN

Con una periodicidad mínima anual se revisará esta Política de Seguridad para adecuarla a los posibles cambios en ***El Consorci de la Zona Franca de Barcelona***, y se analizarán las incidencias y no conformidades encontradas en el sistema elaborando, si procede, una lista de acciones a emprender y ejecutar durante el año siguiente, como objetivos para garantizar la Seguridad de la Información y la protección y buen uso de los recursos de la Organización que la soportan.

Esta Política de Seguridad, la normativa y procedimientos que la desarrollan, y los manuales de seguridad de usuario deberán además seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: variaciones significativas en la plantilla de personal, cambios en la infraestructura, desarrollo de nuevos servicios, entre otros.

Esta Política de Seguridad debe ser difundida a todo el personal, colaboradores externos y usuarios de la red en general, involucrados en la relación con *El Consorci de la Zona Franca de Barcelona* que manejen, o puedan llegar a manejar, información y recursos pertenecientes a la misma.