GRUPO ITE

Unidad de Negocio de Ciberseguridad de ITE

C/ Pitágoras nº 7. Polígono Industrial S. Marcos. 28906 Getafe – Madrid

POLÍTICA DE SEGURIDAD

REVISADO:	APROBADO:
Dirección del SIG:	Director Gerente:
I. Domínguez	Oven Martín

ÍNDICE:

REVISIONES					
Fecha	Rev.	Cambios realizados	Elabora	Revisa	Aprueba
17.02.2017	0.0	Versión inicial	RGM	ID	OM
03.04.2017	01	Cambios en las definiciones de dimensiones de seguridad	RGM	ID	OM
18.04.2017	02	Adecuación del alcance a lo indicado en la oferta	RGM	ID	OM
18.04.2017	04	Cambios para destacar el compromiso de la dirección como comentario del Auditor el día 17-4-17	RGM	ID	OM
30.04.2017	05	Cambio del término Responsable de Seguridad por RSI-SGSI	RGM	ID	OM
28.02.2018	05	Apartado 2, Alcance. Apartado 4, Supervisión y evaluación. Apartado 5, Objetivos de seguridad	ID	OM	OM
01.11.2019	06	Revisión general de adaptación al ENS, ISO/IEC 27001:2017, ISO/IEC 20000-1:2018 e ISO/IEC 22301:2015	JYR	ID	OM
01.07.2020	07	Inclusión de uso de aplicaciones, las exenciones y de las excepciones de la política de seguridad de la información	JYR	ID	OM
02.11.2020	08	Principios de Seguridad de la Información. Definición de Apetito del Riesgo, y aprobación por la Dirección. Segregación de funciones según lo recomendado por el ENS	JYR	ID	OM
21.12.2020	09	Observación 01 del ENS: Marco legal aplicable y referencia a roles y perfiles	JYR	ID	OM
08.04.2021	10	Cambio Nombramientos	JYR	ID	OM
14.10.2022	11	Cambio Nombramientos	JYR	ID	OM
17.02.2023	12	Inclusión de la figura del Punto único de Contacto (POC) de Seguridad	JYR	ID	OM
16.05.2023	13	Revisión general e inclusión de nuevo Responsable Técnico y nueva oficina de Rivas	DCC	JYR	OM

1. OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La unidad de negocio de Ciberseguridad de ITE se crea con el objetivo de prestar servicios en dicha materia a los clientes de ITE. Para la prestación del servicio se maneja habitualmente información que puede ser crítica para el cliente.

Por este motivo, la Dirección General de ITE hace suyo el compromiso de dotar a la unidad de negocio de Ciberseguridad de ITE de las medidas técnicas, organizativas y los recursos humanos necesarios para garantizar:

- La **autenticidad** de las conexiones desde y hacia clientes para evitar suplantaciones de identidad.
- La **confidencialidad** de la información del cliente tanto en nuestras instalaciones como en tránsito, así como de la información propia de la organización para la prestación de servicios de consultoría en materia de ciberseguridad.
- La **integridad** de la información para garantizar la veracidad de los datos obtenidos, procesados y entregados a clientes.
- La **disponibilidad** de la información y los sistemas con los que se presta servicio a clientes, así como la disponibilidad de la documentación técnica y normativa que los soporta.
- La **trazabilidad** y **auditoría** de las acciones, especialmente de las efectuadas por usuarios con privilegios especiales.
- El **cumplimiento** de la legislación vigente y de las normas específicas que afecten a los clientes de la división de Ciberseguridad de ITE dada la naturaleza de los mismos.

Estos objetivos se alcanzarán a través de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el análisis y tratamiento del riesgo, en un modelo de mejora continua, en un sistema de medición de su efectividad y en el establecimiento de unos objetivos de seguridad acordes con la evolución de los servicios y las necesidades del departamento.

2. ALCANCE

El alcance del SGSI es el siguiente:

"El Sistema de Gestión de Seguridad de la Información que soporta las actividades de diseño, desarrollo, implantación y mantenimiento de soluciones de seguridad y disponibilidad de la información de clientes en proyectos de ciberseguridad de acuerdo con la declaración de aplicabilidad".

Los departamentos internos de ITE que de alguna manera se relacionan con la unidad de negocio de Ciberseguridad de ITE serán tratados en este SGSI como suministradores.

Quedan excluidos los servicios que ITE presta a sus clientes y que no tengan que ver directamente con ciberseguridad.

La ubicación física de este alcance es el espacio que ocupa la división de Ciberseguridad de ITE en las oficinas de ITE en calle Marie Curie, 9, 28521 Rivas-Vaciamadrid, Madrid.

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellos usuarios, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

Principio de disponibilidad y continuidad: se garantizará un nivel de disponibilidad en los SSII y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los SSII.

Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los SSII deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

Principio de concienciación y formación: se articularán iniciativas que permitan a los usuarios conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad.

Principio de detección y respuesta: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.

Principio de mejora continua: se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública.

Principio de seguridad en el ciclo de vida de los SSII: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

4. LIDERAZGO DE LA DIRECCIÓN

La Dirección General de la división de Ciberseguridad de ITE se compromete a liderar el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI). Para ello adopta las siguientes medidas:

- Revisión anual del estado del SGSI para garantizar que se cumple la política de la división de Ciberseguridad de ITE, sus objetivos y que éstos están alineados con la dirección estratégica de la organización.
- Exigiendo que los nuevos proyectos que afronte la división de Ciberseguridad de ITE tengan desde su nacimiento una visión global de la seguridad de la información. Para ello exige que todos los nuevos proyectos cuenten con el correspondiente informe del Responsable de Seguridad de la Información
- Estudiar la asignación de recursos económicos para la consecución de los objetivos del SGSI. Si por motivos presupuestarios esto no fuera posible, se estudiarán medidas alternativas tendentes a minimizar el riesgo. Así mismo se elevará a los organismos competentes las revisiones de seguridad que justifiquen la inversión necesaria.
- Mantener el espíritu de seguridad en la organización mediante campañas de concienciación.
- Apoyar la labor del Responsable de Seguridad de la Información y del resto de implicados en la misma.
- Garantizar el proceso de mejora continua mediante auditorías de cumplimiento y auditorías técnicas periódicas. Igualmente hará evaluaciones de los indicadores para establecer las líneas de acción necesarias.

5. SUPERVISIÓN Y EVALUACIÓN

Con una periodicidad mínima anual se revisará esta Política de Seguridad para adecuarla a los cambios en la división de Ciberseguridad de ITE, y se analizarán las incidencias y no conformidades encontradas en el sistema, estableciendo las acciones correctivas correspondientes para subsanarlas. Esta política permitirá el cumplimiento con las regulaciones actuales a las que se ve sujeta ITE, en concreto, con el Reglamento General de Protección de Datos (RGPD).

Esta Política de Seguridad y la documentación del sistema, deberán seguir un proceso de actualización periódica teniendo en cuenta:

- los cambios organizativos relevantes,
- el crecimiento de la plantilla de personal,
- los cambios en la infraestructura tecnológica,
- el desarrollo de nuevos servicios,
- los requisitos legales, reglamentarios o contractuales, y

- en general por motivos que impliquen la necesidad de hacer una evaluación del riesgo.

Los roles de auditoría de seguridad serán independientes del resto de roles de la gestión IT y Seguridad, para evitar cualquier conflicto de intereses.

Esta Política de Seguridad es difundida a todo el personal de ITE Ciberseguridad que se vea afectado por el alcance de esta.

6. OBJETIVOS DE SEGURIDAD

Anualmente, coincidiendo con la revisión por la dirección, el Comité de Seguridad establecerá los objetivos anuales en materia de seguridad que caracterizaran por:

- alineados con la política,
- serán medibles,
- basados en el análisis de riesgos,
- comunicados a los implicados.

Los objetivos quedarán recogidos en el documento REG-6.2 OBJETIVOS DE SEGURIDAD AAAA donde se indicarán:

- su descripción,
- los recursos asignados,
- el responsable de su cumplimiento,
- las fechas de inicio y finalización de los mismos, y
- la evaluación del resultado.

7. MARCO LEGAL

El marco legal incluye el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD). Ver POL-A.18 CUMPLIMIENTO.

8. DEFINICIÓN DE APETITO DEL RIESGO

El apetito de riesgo se refiere a la cantidad de exposición a impactos adversos potenciales que la empresa está dispuesta a aceptar para alcanzar sus objetivos. La política de apetito del riesgo debe de abordarse siguiendo las siguientes directrices:

1. Los gerentes, directores ejecutivos y la junta directiva deben determinar el apetito de riesgo teniendo en cuenta el nivel de exposición deseable y las interacciones entre los riesgos potenciales.
2. El apetito de riesgo es variable, pues depende de factores internos y externos. Por lo tanto, se debe revisar anualmente y abordarse de manera flexible para responder a las necesidades cambiantes del negocio.
3. Las decisiones en cuanto al apetito de riesgo siempre deben estar directamente relacionadas con la retribución y el valor que se espera obtener.
4. El apetito de riesgo no debe superar el nivel de tolerancia al riesgo de la empresa.

El apetito del riesgo está definido y aprobado en NR-6.1.2 METODOLOGIA DE GESTION DEL RIESGO.

9. NOMBRAMIENTOS

El Director General de Grupo ITE es D. Oven Martín Acedo y designa los siguientes nombramientos dentro del contexto del alcance:

Director General: Oven Martín.

Responsable de Seguridad de la Información y del SGSI: Jesús Yustas.

Punto Único de Contacto (**POC**): Amador Ortega.

Responsable de Seguridad de Sistemas de Información: Miguel Duque / Jonathan Rodrigo.

Responsable Administrador de Sistemas: Francisco Cañizares / Alfonso Martínez / Jonathan Rodrigo

Responsable Técnico: Julio César Cortés Restrepo.

Comité de Seguridad:

- Director General.
- Director del Sistema Integrado de Gestión.
- Responsable Técnico.
- Responsable de Seguridad de la Información y SGSI.
- Responsable de Gestión de Servicios y SGS.
- Responsable de Continuidad de Negocio y SGCN.
- Administrador de Sistemas.

Comité de Cambios formado por: Responsable de Gestión de Servicios, Responsable de Continuidad de Negocio, Responsable de Seguridad de la Información, Responsable Técnico y Responsable Administrador de Sistemas.

Las responsabilidades de cada cargo se detallan en NR-A.6.1 ORGANIZACION INTERNA y en NR-5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES.

El Punto único de Contacto (*PoC- Point of Contact*) será el Responsable de la Unidad de Negocio de Ciberseguridad de ITE.

10.APROBACION

La presente Política de Seguridad y toda la documentación asociada han sido aprobadas por la Dirección General, con vigencia a partir de la fecha de su firma.

Todos los firmantes asumen y aceptan plenamente el contenido de esta Política y se comprometen a aplicarla en sus respectivas áreas para conseguir el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información (SGSI).

11.USO DE APLICACIONES

El personal de ITE debe cumplir las siguientes directrices:

- No se permite el uso de aplicaciones que no dispongan de licencia.
- El borrado de aplicaciones software sólo lo podrá realizar el administrador de sistemas o en su defecto el responsable tecnológico.
- No se permite la instalación de programas software sin la previa autorización del responsable. El administrador de los sistemas es el encargado de la instalación.
- En caso de instalación de software con licencia pública, siempre se tendrán en cuenta los derechos de propiedad intelectual.

- Se restringe el acceso a redes sociales, aplicaciones de almacenamiento en la "nube" y aplicaciones de intercambio de ficheros "Punto a Punto".
- La Dirección exigirá el uso de software propietario o, en su defecto, utilización de software de licencia pública adquirido en lugares seguros cuyas páginas web sean oficiales.
- Es obligatorio realizar las actualizaciones de software que se reciban de forma automática.
- Todos los datos informáticos deberán tener una copia de seguridad que se realizará de forma diaria incremental.

12.EXENCIONES

Incumplimientos justificados por razones de negocio.

13.EXCEPCIONES

Incumplimientos no justificados.