Política de Seguridad ENS

1. MISIÓN Y ALCANCE

Desde su nacimiento, Alhambra IT tiene como objetivo convertirse en un socio tecnológico de referencia para dar respuesta a los desafíos que deben abordar las organizaciones privadas y las administraciones públicas con el fin de transformar la tecnología en palancas facilitadoras de su eficiencia y máximo rendimiento.

Tenemos como objetivo conseguir la excelencia operativa y el conocimiento técnico y de negocio más innovador que nos permita ayudar a proteger el éxito del negocio de nuestros clientes y asegurar su futuro digital.

Nuestra misión consiste en trabajar para que cualquier organización crezca, sea más innovadora, eficiente y responsable con el medio ambiente y la sociedad, gracias al buen uso seguro de la tecnología.

Teniendo en cuenta que la misión y el alcance indicados son de aplicación para las Administraciones Públicas clientes de Alhambra, y que confían en nuestro buen hacer a la hora de obtener el máximo rendimiento de sus soluciones IT, Alhambra ha decidido implantar, en el marco de sus políticas de seguridad de la información, aquellas que vienen derivadas del cumplimiento del Esquema Nacional de Seguridad, estableciendo el alcance en “Los sistemas de información que dan soporte a los servicios de cloud computing, backup, convergencia, telecomunicaciones, ciberseguridad, gestión TI, formación IT y desarrollo de software” que se desarrollan desde las oficinas centrales de Albasanz 16 en Madrid.

2. MARCO NORMATIVO

2.1 Identificación

Los servicios prestados por Alhambra se desarrollan dentro del ámbito de la informática y las telecomunicaciones, poniendo para ello a disposición de los clientes servicios IT que pueden procesar, almacenar o transmitir la información que estos depositan en nuestros sistemas, o transitan por ellos. Por este motivo, Alhambra dispone de un Observatorio de Cumplimiento que busca garantizar permanente la alineación de nuestros procedimientos y servicios con el marco normativo de aplicación en cada momento. Dicho marco normativo se encuentra referenciado en el “Anexo 1 de Cumplimiento” del Sistema Integrado de Gestión del Portal de Calidad de la compañía, debidamente actualizado y revisado periódicamente.

2.2 Datos de carácter personal

En el ámbito de aplicación de la regulación en materia de datos de carácter personal, Alhambra cumple con todos los requisitos reflejados en la Ley Orgánica 3/2018 de 5 de diciembre relativa

a la Protección de Datos Personales y Garantía de los Derechos Digitales, habiendo adaptado su normativa interna, procedimientos, contratos y otros documentos.

Además, para el caso específico de los datos de carácter personal que los clientes de Alhambra depositan en nuestros servicios, Alhambra ha adoptado voluntariamente los controles de seguridad requeridos por la norma ISO 27018 para la Gestión de Datos Personales en Servicios en Cloud y con la norma ISO 27701 de Gestión de Privacidad de Datos, certificándose en dichas normas como forma de evidenciar su elevado compromiso con la protección de los datos personales que gestiona de sus clientes en calidad de Encargado de Tratamiento a través de los servicios que presta.

2.3 Esquema Nacional de Seguridad

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad.
- Real Decreto 43/2021, de Seguridad en Redes y Sistemas de Información.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

3. PRINCIPIOS Y DIRECTRICES

Los principios básicos y requisitos que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el Capítulo V y en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan, minimizando el impacto de dichas amenazas en caso de presentarse.

3.1 Prevención

Se 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 deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. 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, los departamentos (internos o externos) deben:

- 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.

- Reducir la superficie de exposición de los sistemas frente a los riesgos y amenazadas para los mismos.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe 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 8 del ENS.

La monitorización, la vigilancia continua y la evaluación periódica son actividades especialmente relevantes cuando se establecen líneas de defensa de acuerdo con el Artículo 10 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3 Respuesta

Se 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).
- Centrar todos los esfuerzos en el restablecimiento de la información y los servicios afectados por el incidente. (recuperación).

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad y actividades de recuperación.

3.5 Conservación

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

La conservación de los mismos se realizará teniendo en cuenta aquellos requisitos de trazabilidad y reputación de los datos que sea necesaria, a fin de que los mismos puedan tener una confiabilidad elevada, caso de presentarse como evidencias futuras en los análisis que sean requeridos tras un incidente.

La conversación tendrá en cuenta los requisitos legales de aplicación, con especial atención a los derechos de los interesados de los datos, y siempre dentro de los marcos legales de aplicación.

3.6 Otros principios generales

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra para garantizar su autenticidad.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la Organización deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones) donde reside la información deben estar adecuadamente protegidos. Cada soporte de información, físico o lógico, forma parte de la cadena de custodia del dato y de las versiones de información que genera y procesa la empresa, y son vitales a fin de asegurar la trazabilidad de la información.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente relevante el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

4. ORGANIZACIÓN DE LA SEGURIDAD

4.1 Roles y responsabilidades

La estructura organizativa, roles y responsabilidades de Alhambra están definidos en los documentos “Mapa funcional” y en el “Organigrama”.

En el marco del ENS, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación con requisitos de información, requisitos del servicio y requisitos de seguridad, (art. 11).

Alhambra articula esta diferenciación en el ámbito del alcance del ENS a través de los roles (a la espera de actualización de la CCN-STIC 801 ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN):

- Gobierno: Dirección ejecutiva asesorada por el CSG.
- Supervisión: Dirección de SI.

- Operación: Departamento de sistemas.

4.2 Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno del Comité de Dirección. Podrá delegar en el Comité de Seguridad.

5. FORMACIÓN Y CONCIENCIACIÓN

Las acciones específicas de concienciación y formación relativas al ENS se gestionan, sin distinción con las del Sistema de Gestión de Seguridad de la Información, por el Departamento de Gestión de Personas y dentro del proceso de Gestión del Conocimiento.

6. GESTIÓN DE RIESGOS

Una correcta identificación y gestión de los riesgos a los que se encuentran sometidos los activos de información, que sustentan los servicios de Alhambra, es primordial para la correcta toma de decisiones de la Dirección. Esto ha motivado a basar la Metodología de Análisis y Gestión de Riesgos del ENS en MAGERIT.

Para la implementación de la metodología de Análisis y Gestión de Riesgos se ha decidido utilizar una herramienta específica que permite obtener resultados objetivos de valoración, como se establece en el procedimiento interno de "Anexo 4: Gestión de la Seguridad y la Evaluación de Riesgos".

7. DESARROLLO DE LA POLÍTICA

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.
- Segundo nivel: Normativas, manuales y procedimientos generales.
- Tercer nivel: Instrucciones Técnicas de Seguridad.
- Cuarto nivel: Informes y registros.

7.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, recogido en el presente documento y aprobado mediante Firma de la Dirección.

7.2 Segundo Nivel: Normativas y Procedimientos Generales

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en Alhambra en el marco del SGSI, en la Declaración de Aplicabilidad del ENS se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del Anexo A de ISO 27001. Realizado de acuerdo con la Guía de Seguridad (CCN-STIC 825) Esquema Nacional de Seguridad – Certificaciones 27001.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del Comité de Calidad y del Comité de Seguridad.

7.3 Tercer Nivel: Instrucciones Técnicas de Seguridad

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad, como indicamos en el apartado relativo a la Gestión de la Documentación en Alhambra dentro de la documentación de Calidad.

7.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los responsables de los Sistemas de Información y/o de Servicio en su ámbito y se define en el apartado relativo a la Gestión de los Registros en Alhambra dentro de la documentación de Calidad.

7.5 Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC actualizadas, así como las guías CCN-STIC de las diferentes series publicadas por el CCN -CERT en su página web.

8. DOCUMENTACIÓN

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema Integrado de Gestión que se recogen en el "Manual de Gestión de la Calidad" de Alhambra.

Toda la documentación corporativa sujeta a algún grado de confidencialidad deberá llevar, como mínimo en su portada, la correspondiente marca de agua, indicando el grado de clasificación conforme a la normativa de Alhambra u otra norma estándar de referencia.

9. PROCESO DE APROBACIÓN Y REVISIÓN

Esta Política de Seguridad de la Información ENS será aprobada por la Dirección y revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando circunstancias técnicas u organizativas lo requieran para evitar que quede obsoleta.

José Ramón Díaz Moya
Director General Alhambra IT

(15 de noviembre de 2023)