Candelita

Entidad de Utilidad Pública

Política de Seguridad de la Información
Esquema Nacional de Seguridad

Control de versiones:

Identificación	
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Revisión: 1
Ámbito: CANDELITA	Estado: Aprobada

Registro de cambios			
Revisión	Cambio	Apartado	Fecha
0	Elaboración del documento inicial	Todos los apartados.	19/01/2026
1	Revisión del documento	Apartados 5 y 8	01/04/2026

Aprobado por: Comité de Seguridad
Fecha de aprobación: 1 de abril de 2026

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la dirección de *CANDELITA*, el día 1 de abril de 2026. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y estará vigente hasta que sea reemplazada por una nueva.

La entrada en vigor de la presente Política de Seguridad de la Información supone la derogación de cualquier otra que existiera a cualquier nivel de la organización.

2. INTRODUCCIÓN

Conscientes de la importancia de adoptar marcos de referencia normalizados y reconocidos a nivel internacional en los ámbitos de la informática, las tecnologías de la información y las comunicaciones (TIC) y la ciberseguridad, CANDELITA ha alineado su Sistema de Gestión de la Seguridad de la Información (SGSI) con los requisitos establecidos en el Esquema Nacional de Seguridad.

A través de la presente Política de Seguridad, la organización establece y regula la gestión continua de la seguridad de la información. La seguridad de la información tiene como finalidad garantizar la fiabilidad de la información y la continuidad en la prestación de los servicios, mediante la adopción de medidas preventivas, la supervisión permanente de la actividad y la actuación ágil y eficaz ante la ocurrencia de **incidentes de seguridad y ciberseguridad.** Para alcanzar estos objetivos, la organización define, implanta y mantiene una política de seguridad y ciberseguridad estructurada en los siguientes pilares: **Prevención, Detección, Respuesta y Recuperación**.

CANDELITA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) 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 disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

Otro de los objetivos primordiales de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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 se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, así como realizar 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.

CANDELITA debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, 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 deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para los proyectos de TIC.

CANDELITA debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.
Esta Política de Seguridad sigue las indicaciones de la ***guía CCN-STIC-805*** del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

3. POLÍTICA DE SEGURIDAD Y CIBERSEGURIDAD BASADA EN: PREVENCIÓN, DETECCIÓN, RESPUESTA Y CONSERVACIÓN.

3.1. PREVENCIÓN:

CANDELITA 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 se implementarán las medidas mínimas de seguridad determinadas por el ENS, RGPD y la LOPD, 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, van a estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, CANDELITA 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.

3.2. DETECCIÓN

Dado que la calidad de los servicios puede verse afectada de forma rápida como consecuencia de incidentes, que pueden ir desde una disminución puntual del rendimiento hasta la interrupción total, resulta imprescindible llevar a cabo una monitorización continua del funcionamiento de los sistemas de la gestión de la información y servicios, con el fin de detectar desviaciones o anomalías en los niveles de prestación de los servicios y actuar en consecuencia, conforme a lo establecido en el artículo 9 del Esquema Nacional de Seguridad.
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, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3. RESPUESTA

CANDELITA establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos de intercambio de información sobre posibles incidentes con clientes y proveedores.

3.4. RECUPERACIÓN

Con el fin de garantizar la disponibilidad de los servicios y la resiliencia de sus sistemas de información, CANDELITA dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios esenciales.

4. MEDIDAS TRANSVERSALES DE SEGURIDAD DE LA INFORMACIÓN

En el marco del Sistema de Gestión de la Seguridad de la Información implantado, se establecen un conjunto de medidas transversales orientadas a garantizar la protección integral de los sistemas, los activos y la información gestionada. Estas medidas, de carácter global y aplicables a todos los ámbitos del sistema, complementan los controles específicos definidos en el Esquema Nacional de Seguridad, asegurando el cumplimiento de los principios básicos de seguridad —confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad—, así como la adecuada gestión de los riesgos asociados.

Mínimo privilegio: los sistemas de información han sido diseñados y configurados otorgando los mínimos privilegios necesarios para su correcto desempeño.

Seguridad física: CANDELITA aplica medidas específicas de seguridad física, garantizando que los activos de información se ubiquen en áreas seguras y estén protegidos mediante controles de acceso físicos proporcionales a su nivel de criticidad. Los sistemas y activos de información alojados en dichas áreas estarán protegidos frente a amenazas físicas o ambientales.

Protección de la información: CANDELITA garantiza la protección de la información, tanto en reposo como durante su transmisión, mediante la aplicación de medidas técnicas y organizativas adecuadas a su nivel de clasificación y criticidad. Estas medidas tienen como objetivo preservar la confidencialidad, integridad, disponibilidad y trazabilidad de la información tratada, así como de los servicios que la gestionan.

Incidentes de seguridad: gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

Prevención ante otros sistemas de información interconectados: el sistema protege el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Integridad y actualización del sistema: todos los sistemas se mantienen actualizados según los requisitos establecidos, y se articula a través de procesos de gestión del cambio y análisis de riesgos.

Protección de las instalaciones: utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones. Gestión de activos de información inventariados, categorizados y asociados a un responsable.

Adquisición de productos: adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.

Profesionalidad: la seguridad del sistema de información está atendida y es revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Se disponen determinados los requisitos de formación y experiencia necesarias del personal para el desempeño de las competencias.

Gestión de personal: mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

Mejora continua del proceso de seguridad: el proceso integral de seguridad implantado es actualizado y mejorado de forma continua. Para ello, se aplican los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

5. ALCANCE

Esta Política de Seguridad de la Información se aplicará a los sistemas de información de CANDELITA relacionados con el ejercicio de sus competencias y a todas las personas trabajadoras, personal voluntario, estudiantes en prácticas y colaboradores/as, con acceso autorizado a los mismos, con independencia de la naturaleza de su relación jurídica con la organización. Todas las personas tienen la obligación de conocer y cumplir esta Política de Seguridad y la Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue al personal afectado.

El **alcance** de esta Política de Seguridad queda establecido como:

Los sistemas de información que dan soporte a las actividades relacionadas con la gestión de los servicios sociales y de inclusión laboral de Candelita desarrollados en centros y/o en domicilios:

- Centros y servicios sociales especializados de atención a personas con discapacidad psicosocial: rehabilitación laboral, rehabilitación psicosocial, apoyo comunitario, centros de día y soporte social, programas para el apoyo a personas adultas con discapacidad psicosocial en el ejercicio de su capacidad jurídica.
- Servicios de promoción de la igualdad en nuestra sociedad con la participación de mujeres y hombres y atención integral a mujeres víctimas de violencia de género.
- Servicios de asistencia social y promoción de la autonomía personal: ayuda a domicilio y servicios de educación social en domicilio y entorno.
- Servicios de atención a la infancia, familias y personas vulnerables: apoyo socioeducativo, prevención del maltrato infantil, atención familiar (educativa y psicológica), ocio saludable, inclusión sociolaboral.
- Servicios de orientación laboral, cualificación profesional, formación ocupacional, intermediación con empresas y acompañamiento social.

Atendiendo a la declaración de aplicabilidad vigente.

Ver documento de Inventario de activos, evaluación de riesgos para más información

6. MISIÓN

CANDELITA define la presente Política de Seguridad de la Información, de carácter obligatorio para la plantilla y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve CANDELITA para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en CANDELITA serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Esta Política de Seguridad:

- Se aprobará formalmente por la organización.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.

- Se comunicará a toda la plantilla y empresas externas que trabajen con CANDELITA.

7. MARCO NORMATIVO

RD 311/2022 ESQUEMA NACIONAL DE SEGURIDAD (ENS)

La organización ha creado un repositorio de normativa y requisitos legales, que actualiza de forma periódica, disponible en su base de datos interna.

01_ ARTICULOS ART5 GUÍAS

8. ORGANIZACIÓN DE LA SEGURIDAD

8.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad coordina la seguridad de la información en CANDELITA. Este Comité dará soporte a la organización y estará formado por:

- Responsable del Servicio
- Responsable de la Información
- Responsable de Seguridad
- Responsable del Sistema

El **Comité de Seguridad** tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI).
- Elaborar la estrategia de evolución de CANDELITA en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por la organización.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de las/os responsables de área, coordinadoras/es y trabajadoras/es desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por CANDELITA y recomendar posibles actuaciones al respecto.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidentes de seguridad de la información.

- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de CANDELITA. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

8.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Serán funciones y responsabilidades del:

- **Responsable del Servicio**:
  - Establecer los requisitos del servicio en materia de seguridad.
  - Determinar los niveles de seguridad de los servicios.
  - Aprobar la categorización del sistema con respecto a los servicios.
  - Los que se vayan indicando en los documentos dentro del alcance del ENS.

- **Responsable de la Información:**
  - Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
  - Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
  - Establecer los requisitos de la información en materia de seguridad.
  - Determinar y aprobar los niveles de seguridad de la información.
  - Aprobar la categorización del sistema con respecto a la información.
  - Los que se vayan indicando en los documentos dentro del alcance del ENS.

- **Responsable de Seguridad:**
  - Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
  - Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
  - Gestionar la formación y concienciación en materia de seguridad TIC.

- Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Aprobar la declaración de aplicabilidad.
- Canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que se presta o solución que provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio (POC).
- Los que se vayan indicando en los documentos dentro del alcance del ENS.
- El Responsable de la Seguridad será el secretario del Comité de Seguridad con las funciones indicadas en la presente política.
- De conformidad con el principio de “segregación de funciones y tareas” recogido en el art. 10 del ENS, el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema.

- **Responsable del Sistema:**
  - Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
  - Definir los criterios de uso y los servicios disponibles en el Sistema.
  - Definir las políticas de acceso de usuarios al Sistema.
  - Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
  - Determinar la configuración autorizada de hardware y software a utilizar en el sistema y aprobar las modificaciones importantes de dicha configuración.
  - Realizar el análisis y gestión de riesgos en el Sistema.
  - Elaborar y aprobar la documentación de seguridad del Sistema.
  - Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
  - Implantar y controlar las medidas específicas de seguridad del Sistema.
  - Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
  - Proponer, según proceda, la suspensión del manejo de cierta información o la suspensión de la prestación de cierto servicio, si detecta deficiencias

graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

8.3. PROCEDIMIENTOS DE DESIGNACIÓN

La Dirección asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información, determinando en cada caso los motivos y el plazo de vigencia. También, se asegurará de que las y los trabajadoras/es conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen en relación con cada responsabilidad en Seguridad de la Información.

El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos.

8.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la organización y difundida para que la conozcan todas las partes afectadas.

9. DATOS DE CARÁCTER PERSONAL

La organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos, y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.
De igual forma, con la RGPD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el encargado de desempeñar las funciones relacionadas con dicha Protección de Datos.

10. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes

servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.
La gestión de riesgos quedará documentada en el informe de activos y evaluación de riesgos de la organización.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de seguridad de la información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de seguridad de la información su revisión anual y mantenimiento, proponiendo mejoras cuando sea necesario.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

- **Primer nivel normativo:** constituido por la presente Política de Seguridad de la Información, la normativa interna del uso de los medios electrónicos y las directrices generales de seguridad aplicables a los organismos o unidades de la organización a los que sean de aplicación dichos documentos.
- **Segundo nivel normativo:** constituido por las normas de seguridad derivadas de las anteriores.
- **Tercer nivel normativo:** constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Cuando resulte procedente, se deberá recabar la opinión de las y los usuarias/os, tanto internos como externos, sin perjuicio de que se adopten las medidas necesarias para proteger los intereses y el buen funcionamiento de la organización.

12. OBLIGACIONES DEL PERSONAL

Todos los miembros de CANDELITA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a las personas.

Todos los miembros de CANDELITA recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de CANDELITA, en particular a los de nueva incorporación.

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 una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

13. TERCERAS PARTES

Cuando CANDELITA preste servicios a otras organizaciones o maneje su información, se les hará partícipes de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos comités de seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando CANDELITA utilice servicios de terceros o les ceda información, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que afecte a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esta normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de estos terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la información no pueda ser satisfecho por una tercera parte, según se requiere en los párrafos anteriores, se requerirá un informe del responsable de seguridad que precise los riesgos en que se incurre y la forma de tratarlos, que se remitirá al Comité de Seguridad de la Información para su evaluación y toma de decisiones.

Compromiso con el Esquema Nacional de Seguridad en categoría ALTA

Candelita en el marco del cumplimiento del Real Decreto 311/2022,
por el que se regula el Esquema Nacional de Seguridad (ENS), aplicará las medidas
de seguridad correspondientes a la categoría ALTA, conforme a lo
establecido en el Anexo II del citado Real Decreto y su normativa de desarrollo.

En Madrid, a 1 de abril de 2026,
Firma
Representante legal y Directora de Candelita

CANDELITA
N.I.F.: G-80586696
C/ Sancho Dávila, 19 - Local
Telf.: 91 523 58 45 - Fax: 91 532 18 52
28028 MADRID

Firmado digitalmente por 50450556X PETRA GEMMA DE LA HOZ (R: G80586696)
Fecha: 2026.04.01 18:29:03 +02'00'