Política de Seguridad de la Información

Clasificación Información	**Uso Interno**
Código	**PL- 001-1**
Versión	**003**
Fecha	**21/03/2024**

Tunstall, Avda. Castilla, 2. PE. San Fernando. Edif. Múnich. 2ª pl.
28830. San Fernando de Henares (Madrid). Tel. 912113720

Contenido

I. OBJETO

El presente documento constituye la Política y Normas de Seguridad de la Información en la que también se define la clasificación de la información, los puntos de control, así como la normativa aplicable. Todo esto, con el objetivo de garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información que tratamos tanto para la prestación de los servicios a sus clientes como para su propia actividad como organización.

El Comité de Seguridad de la Información, en adelante Comité de Seguridad, es consciente de la fuerte dependencia de sus servicios y productos en cuanto a las tecnologías de información y comunicaciones, con el fin de alcanzar sus objetivos y prestar los servicios de la forma más eficiente.

Los sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar la disponibilidad, integridad, confidencialidad, trazabilidad o autenticidad de la información y gestionar de manera preventiva la seguridad y actuar en su caso, previa supervisión y monitorización del sistema, ante incidentes y en su caso, eventos que pudieran generar un impacto en el sistema, minimizándolos al máximo y/o generando la continuidad del sistema y del negocio.

II. CONCIENCIACIÓN

Gran parte de la información que conocemos, manejamos o almacenamos tiene un valor para nosotros o para nuestros clientes. Utilizamos nuestra información y conocimiento para funcionar como compañía, y nuestros clientes confían en nosotros cediéndonos su información para que podamos prestarles servicios. La información es un activo clave para nosotros.

Por ello, todos y todas las profesionales y colaboradores de la compañía deben proteger la información que manejamos según las necesidades específicas de su responsable.

Como conjunto, debemos proteger la información a lo largo de todo su ciclo de vida (creación/adquisición, uso, almacenamiento y destrucción), considerando los riesgos a los que está expuesta y las necesidades específicas de su responsable para evitar que se acceda a ella o se utilice en contra de los intereses de la compañía o de quienes nos confiaron esa información.

Además, debemos proteger con especial cuidado la información que contenga datos de carácter personal, datos sensibles y confidenciales.

Debemos proteger nuestros activos de información clave, ya que:

- El talento de nuestros y nuestras profesionales es la base de nuestro negocio
- Nuestro conocimiento sobre los clientes, su negocio y la tecnología supone una ventaja diferencial para nosotros.
- Sin acceso a nuestra información y conocimiento no podemos desarrollar nuestro trabajo diario.
- Si la información que manejamos contiene errores o es incorrecta, podemos tomar decisiones erróneas que tengan un impacto negativo en **Grupo Tunstall España** y/o sobre nuestros clientes.
- Nuestros clientes pueden perder su confianza en nosotros si no cuidamos su información, al menos, con el mismo cuidado con el que ellos lo hacen.
- La información que manejamos, en manos ajenas a la compañía, puede ayudar a nuestra competencia a reforzar su posición en oportunidades que nos interesan, hacer que perdamos negocio o acarrearnos sanciones legales.
- En nuestras instalaciones se encuentra gran parte de la infraestructura que utilizamos para realizar nuestro trabajo, en ella se encuentran nuestros y nuestras profesionales y nuestra información y, en definitiva, el patrimonio de la compañía. Forman parte, además, de la imagen que la empresa proyecta a nuestros clientes y al resto de la sociedad.

- Nuestros proveedores y colaboradores nos ayudan a realizar procesos importantes que hemos delegado en ellos, y necesitamos su ayuda para focalizarnos en alcanzar el éxito en nuestro negocio.
- Garantizar la seguridad de nuestros activos más importantes es un proceso crítico para el funcionamiento de nuestro negocio, por lo que lo abordamos desde una visión completa.

III. ÁMBITO DE APLICACIÓN Y MISIÓN

3.1 Ámbito de aplicación de la Política y Normas de Seguridad de la Información

La Política y Normas de Seguridad de la Información se aplica a **todas las empresas del Grupo Tunstall en España**.

Esta Política es de aplicación, por tanto, a todos los sistemas de información, activos y personas, de todas las siguientes sociedades:

- Televida Servicios Sociosanitarios S.L.U.
- Tunstall Ibérica S.A.
- Cualquier otra empresa participada por alguna de las anteriores (ej. UTEs)

Además, será de aplicación a todo el personal que preste servicios en las anteriores **(en adelante, Grupo Tunstall España)** así como también las empresas proveedoras y colaboradores.

La Política y Normas de Seguridad de la Información del **Grupo Tunstall España** será de aplicación a todo el personal que preste servicios en las delegaciones, servicios y centros asistenciales del **Grupo Tunstall España** y sus centros de administración de servicios, así como también las empresas proveedoras de servicios relacionados.

3.2 Misión de seguridad de la información

GRUPO TUSTALL ESPAÑA gestiona su servicio con una fuerte orientación a la calidad y al alineamiento con los objetivos de sus clientes. La organización cuenta con un equipo de profesionales altamente experimentados en la gestión de servicios sociosanitarios y dispone de un fuerte respaldo tecnológico y de seguridad.

TELEVIDA SERVICIOS SOCIOSANITARIOS S.L.U. es el primer operador nacional de teleasistencia, con más de 300.000 usuarios en diversas comunidades autónomas, siendo el único operador de teleasistencia que ha logrado una auténtica flexibilidad de servicio adaptándolo a los diferentes colectivos que atiende (personas mayores, personas con discapacidad y en situación de dependencia y enfermos crónicos), y aplicando distintas tecnologías y diferentes intensidades de servicio según el grado y nivel de dependencia y de cuidados. Así, una persona puede recibir la atención más adecuada según su evolución dentro del ciclo de envejecimiento.

TUNSTALL IBERICA S.A.U. es una empresa española con matriz en Reino Unido que suministra dispositivos relacionados con el cuidado de las personas y de la salud, así como la tecnología y aplicaciones necesarias para el funcionamiento de los mismos. **TUNSTALL IBÉRICA** presta servicios de administración, mantenimiento y soporte de toda la tecnología relacionada, así mismo facilita si es necesario la infraestructura TIC necesaria a sus clientes.

Visión

Un mundo en el que las personas tienen libertad para vivir la vida al máximo en el lugar que elijan.

Misión

Proporcionar soluciones y servicios basados en datos y en tecnología para mejorar la capacidad de nuestros clientes de ofrecer nuevos modelos más eficientes y eficaces para la gestión de la salud y la atención en el entorno comunitario.

Valores

- **Enfoque en el cliente:** Apasionados por entender y satisfacer las necesidades de nuestros clientes.
- **Colaboración:** Trabajando como un único equipo, un único **Grupo Tunstall España**.
- **Innovación:** Buscando el avance continuo de nuestras y nuestros profesionales, procesos, productos y propuestas.
- **Responsabilidad:** Empoderando a nuestras y nuestros profesionales para que tengan éxito, permitiéndonos cumplir con nuestros objetivos y enorgullecernos de lo que hacemos.

Cultura

- Trabajamos en equipo con nuestros clientes, entendiendo sus necesidades particulares y aportándoles capacidades y experiencias globales.
- Somos eficientes, ágiles y nos enfocamos en crear valor para nuestras personas usuarias y nuestros clientes.
- Nuestros equipos de profesionales son artífices de la generación de valor.
- Damos un servicio integral enfocado a satisfacer las necesidades actuales y futuras de las personas usuarias, esforzándonos en exceder sus expectativas.
- Supervisamos de forma continua la calidad de los servicios que prestamos y su adecuación a la legislación vigente.

IV. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del **Grupo Tunstall España**, y, en particular, la prestación de los servicios indicados en el apartado anterior está constituido por normas jurídicas estatales orientadas a la a la seguridad de la información y los servicios que la manejan, a la seguridad en los servicios relacionados con la administración electrónica, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco se encuentran recogidas en un registro al efecto, según señala el correspondiente procedimiento de gestión de requisitos legales.

El Comité de Seguridad mantendrá dicho Marco Normativo actualizado, y en el mismo se incluirán, además, las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en la “Disposición Adicional Segunda. Desarrollo del Esquema Nacional de Seguridad” del ENS.

El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el “Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad”.

Asimismo, el Comité también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

4.1 Propiedad de los recursos y propiedad intelectual

El **Grupo Tunstall España** proporciona a cada persona empleada los medios necesarios para el desarrollo de sus funciones, responsabilizándose el profesional de su correcta utilización, y siendo estos, en todo caso, propiedad del **Grupo Tunstall España**.

Tanto la información como los medios materiales, incluyéndose los medios tecnológicos (ordenadores de sobremesa y portátiles, impresoras, fotocopiadoras, teléfonos y demás dispositivos del entorno informático y de comunicaciones) adquiridos o suministrados por el **Grupo Tunstall España** son de su propiedad. El mero hecho de conceder su uso o asignar el activo o la información a una persona, no genera derecho alguno sobre los mismos.

En todo caso, el **Grupo Tunstall España**, podrá aplicar sobre los medios corporativos mecanismos de monitorización y seguridad teniendo en cuenta la legislación vigente y los mecanismos de protección de la privacidad de las personas.

El **Grupo Tunstall España** es el propietario y cuenta con los derechos de uso de cualquier resultado del trabajo realizado por las personas empleadas, durante el desarrollo de su actividad laboral, realizado con los medios y recursos puestos a su disposición.

A todos los efectos, el **Grupo Tunstall España** dispone en exclusiva de los derechos de explotación y con el alcance necesario para el ejercicio de la actividad habitual del **Grupo Tunstall España**.

4.2 Prohibición de divulgación y secreto profesional

Todo el personal está debidamente informado de la total **prohibición de divulgar** por cualquier medio cualquier información, y en especial aquella que contiene datos de carácter personal. Su única función es la de procesar la información pertinente para el desarrollo de sus funciones. Por tanto, todas las personas deberán guardar el debido secreto y confidencialidad sobre la información y en especial en cuanto a los datos personales que conozcan en el desarrollo de su trabajo.

Como regla general, para el almacenamiento de información, se utilizarán recursos de red con restricciones de acceso a usuarios autorizados y adscritos a los procedimientos establecidos de copias de seguridad.

El personal de la organización se encuentra sujeto al deber de **secreto profesional**, continuando esta obligación aún en el caso de cese de la relación laboral o de haber cambiado de función dentro de la misma, todo ello de acuerdo con lo previsto en la legislación. La revelación de información sometida a secreto y protegida, puede ser constitutiva de delito (TÍTULO X Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio- CAPÍTULO PRIMERO - Del descubrimiento y revelación de secretos - Código Penal).

En el caso en que sea necesaria la comunicación de información se tendrá en consideración el nivel mostrado en el apartado “Clasificación de la información”. Con carácter general la información debe ser comunicada y transmitida con las correspondientes medidas de seguridad, empleando los diferentes recursos y aplicaciones que la empresa pone a disposición de cada persona empleada.

La información no debe ser transmitida a personas que no están autorizadas a conocerla.

Con carácter general, la organización dispone de procedimientos asociados a la eliminación segura de la información y el borrado seguro de los soportes que la pudieran contener información. Los documentos deberán ser destruidos empleado las destructoras o en su caso, depositando los mismo en los contenedores específicos de papel que existan en el centro. Los soportes que pudieran contener información, deben ser borrados mediante el proceso especifico definido por el Comité de Seguridad y el área de sistemas del **Grupo Tunstall España**.

V. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, en el presente apartado, se detallan las directrices fundamentales de seguridad que se deben de tener presentes en cualquier actividad relacionada con el uso de los activos de información.

- **Alcance estratégico**. La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas para conformar un todo coherente y eficaz.
- **Seguridad integral**. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.
- **Gestión de riesgos**. El análisis y gestión de riesgos será una parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos, y la eficacia y el coste de las medidas de seguridad.
- **Prevención, reacción y recuperación.** La seguridad de los sistemas del **Grupo Tunstall España** debe contemplar los aspectos de prevención, detección y corrección; para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que se maneja, o los servicios que se prestan.
- **Monitorización y Vigilancia.** La vigilancia de los sistemas de información es vital para los activos de información y de las infraestructuras del **Grupo Tunstall España**. Apostamos por la Ciber inteligencia y por una mejora continua en la monitorización del Ciberespacio con el objetivo de ir un paso por delante a los grupos que se dedican a la Ciberdelincuencia y al Ciberterrorismo.
- **Líneas de defensa.** El **Grupo Tunstall España** ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, constituidas por medidas de naturaleza organizativa, física y lógica.
- **Evaluación periódica y mejora continua**. Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad por defecto y mínimo privilegio.** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.
- **Seguridad como requisito legal.** Como requisito de seguridad, se establece el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información. Los requisitos serán identificados y organizados para su correcta gestión.
- **Seguridad basada en el liderazgo y en la organización.** Se considera la seguridad para todos los miembros de la organización, con diferentes roles y responsabilidades relacionados con la Seguridad de la Información.
- **Sensibilizar y concienciar.** Todo el personal relacionado con el sistema y con la información, deberá ser formado, concienciado e informado de sus deberes y obligaciones en materia de Seguridad de la información y Ciberseguridad.
- **Continuidad de negocio.** La continuidad formará parte del sistema de gestión, conforme a las necesidades de la organización y los controles establecidos. La organización considera el análisis de impacto y las consecuencias de la información que el mismo muestre.
- **Seguridad de áreas y entorno.** La organización prevendrá los accesos físicos no autorizados, así como los daños a la información y a los recursos mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.
- **Proteger la información**. Se contempla la protección de la información tanto interna como la relacionada con la prestación de los servicios/clientes, considerando las dimensiones de confidencialidad, integridad y disponibilidad ampliable a trazabilidad y autenticidad.

VI. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Grupo Tunstall España para lograr el cumplimiento de los artículos 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, que recogen los principios básicos y de los requisitos mínimos, así como, en general, asegurar una gestión efectiva de la seguridad de la información ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

6.1 La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en **Grupo Tunstall España** estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas

6.2 Gestión de riesgos

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

Los riesgos a los que se encuentran expuestos los elementos que manejan la información del **Grupo Tunstall España** deben analizarse. Los resultados de estos análisis deberán determinar las acciones de gestión de la seguridad más apropiadas para minimizarlos y priorizar las mismas.

El análisis de los riesgos debe realizarse de manera periódica para contemplar los cambios en los requisitos de seguridad, así como los cambios que se produzcan en los activos, amenazas, vulnerabilidades e impactos. Por su parte, la gestión del riesgo debe ser llevada a cabo de una manera metódica y capaz de generar unos resultados comparables y reproducibles.

Tras la obtención de los resultados se debe decidir cuándo un riesgo es aceptable y cuando no.

Para cada uno de los riesgos identificados, se procederá a desarrollar el tratamiento más acertado en base a la gestión de riesgos.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

6.3 Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte de **Grupo Tunstall España** permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

6.4 Cadena de suministro de seguridad

Cuando existieran proveedores en la cadena de suministro de seguridad, se les hará partícipes de esta política y Normas de Seguridad de la Información, se establecerán canales para reporte y coordinación con el **Comité de Seguridad** y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad de la cadena de suministro que tenga impacto en el **Grupo Tunstall España**.

La relación con los proveedores quedará sujeta a las obligaciones establecidas en dicha 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 los proveedores esté adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta política.

6.5 Estructura normativa de seguridad

El Sistema de Gestión de Seguridad de la información estará estructurado por diferentes niveles de forma que los objetivos planteados por el presente documento tengan un desarrollo normativo que permita definir y concretar regulaciones y restricciones que sean aplicables sobre los servicios y sistemas de información o al personal que gestiona. Esta jerarquía de documentos debe ser conexa y coherente.

El **Grupo Tunstall España** estructura su marco normativo de seguridad de la información en los siguientes tipos de documentos:

- Política y Normas de Seguridad de la Información que establece los criterios de protección en el ámbito de la organización y servirá de guía para la creación de todos los procedimientos y documentación que se genere por el Comité de Seguridad.
- Las normas, guías y procedimientos de seguridad definen los controles de que hay que proteger y los requisitos de seguridad deseados. Todo dicho conjunto debe cubrir la protección de todos los entornos de los sistemas de información de la organización.
- Las instrucciones técnicas de seguridad, en los que describirá de forma concreta, sobre cómo proteger lo definido en las normas, guías y procedimientos y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento; son documentos que describen de forma explícita y detallada las acciones técnicas a realizar en la ejecución del procedimiento o las tareas a considerar cuando se ejecute un procedimiento.

6.6 Cumplimiento de la protección de datos personales

El **Grupo Tunstall España** trata datos de carácter personal. Todos los sistemas de información se ajustarán a las exigencias de la normativa de protección de datos en vigor y a la **Política de Protección de Datos Personales**. Los datos se tratarán de manera lícita, leal, transparente, con fines determinados y explícitos, legítimos; sin ser usados para fines posteriores incompatibles. Serán datos adecuados, pertinentes y limitados, exactos y actualizados. Serán tratados durante el tiempo necesario garantizándose la seguridad de los mismos.

6.7 Formación y concienciación

Todo el personal, entidades colaboradoras y, en última instancia, los usuarios externos, deben recibir la información, formación y concienciación apropiada para el uso correcto de los servicios y sistemas que manejan información del **Grupo Tunstall España**, incluyendo requerimientos de seguridad y responsabilidades legales.

Los usuarios deben ser conscientes de la importancia de la seguridad en los sistemas de información del **Grupo Tunstall España**. La seguridad eficaz depende, en parte, de que los usuarios sepan lo que se espera de ellos y cuáles son sus responsabilidades y obligaciones.

La Dirección del **Grupo Tunstall España** tiene como objetivo lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros del grupo, y a todas sus actividades, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Todos y todas los y las profesionales de la compañía reciben formación en materia de seguridad, teniendo especial importancia del **uso apropiado de los recursos**.

6.8 Autorización y control de los accesos

Grupo Tunstall España ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

6.9 Protección de las instalaciones

Grupo Tunstall España ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

En particular, las áreas críticas para en las que se ubiquen sistemas de tratamiento de la información, dispondrán de las medidas de protección adecuadas frente a las amenazas ambientales (temperatura, humedad, climatización, fuego…).

6.10 Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad **Grupo Tunstall España** tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad, así como a las necesidades de certificación de productos y servicios requeridos por el ENS.

6.11 Protección de la información almacenada y en tránsito y continuidad de la actividad

Grupo Tunstall España prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación del ENS, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

6.12 Registro de actividad y detección de código dañino

Grupo Tunstall España con el propósito de satisfacer el objeto del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, **Grupo Tunstall España** podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

6.13 Obligaciones del personal y profesionalidad

Todo el personal que preste servicios en o para el **Grupo Tunstall España** tiene la obligación de conocer y cumplir la **Política de Protección de Datos Personales y la Política y Normas de Seguridad de la Información**.

La Política y Normas de Seguridad de la Información será de obligado cumplimiento para todo el personal y colaboradores que accedan tanto a los sistemas de información como a la propia información, con independencia de cuál sea su destino, adscripción o relación con el mismo. La política es aplicable, igualmente, en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción). Por tanto, deberá ser accesible a todos los miembros de la organización.

El incumplimiento manifiesto de la Política y Normas de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

6.14 Responsabilidades

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, con responsabilidades claramente diferenciadas, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

6.14.1 Comité de Seguridad de la Información

El comité de seguridad se ha organizado en función de la "***Política y Normas de Seguridad de la información Grupo Tunstall España"***, mediante la designación de diferentes roles con responsabilidades en materia de seguridad claramente diferenciadas, tal y como se recoge a continuación.

Se establece la siguiente estructura:

- Dirección General
- Responsable de Seguridad de la Información
- Responsable de Sistemas
- Dirección Financiera
- Dirección de Operaciones
- Dirección Jurídica y Compliance (DPO)
- Dirección de Desarrollo Estratégico Tecnología
- Dirección de Sistemas y Comunicaciones

Con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

6.14.2 Responsabilidades asociadas al Comité de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras, responsabilidades que recoge el Comité de Seguridad.

- **Funciones de el/la Responsable de la Información y de los Servicios:**
  - Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 8 de enero, previa propuesta de el/la Responsable de Seguridad ENS, y/o Comité de Seguridad.
  - Informar sobre los derechos de acceso al Servicio y a la Información.
  - Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.

- Poner en comunicación de el/la Responsable de Seguridad ENS, cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.
- Velar por la adecuada realización de sus funciones, dentro del marco de seguridad adecuado, ayudando a difundir el conocimiento y la cultura de seguridad necesarias para el correcto tratamiento de los datos.

➢ **Funciones de el/la Responsable de Seguridad ENS:**

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Promover y coordinar la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, la identificación de medidas de seguridad, determinar configuraciones necesarias, y la elaboración de la documentación del sistema.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar y aprobar la Declaración de Aplicabilidad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el/la Responsable del Sistema y el Comité de Seguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema y los procesos de certificación.
- Elevar a la Dirección y/o al Comité de seguridad la aprobación de cambios y otros requisitos del sistema.

Cuando la complejidad del sistema lo justifique el/la Responsable de Seguridad podrá designar los responsables de seguridad delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

➢ **Funciones de el/la Responsable del Sistema ENS:**

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el/la Responsable de Seguridad y/o Comité de Seguridad.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
  - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
  - Aprobar los cambios en la configuración vigente del Sistema de Información.
  - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
  - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
  - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique el/la Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

- **Funciones de Dirección General**

Aprobar la estrategia de Seguridad de la Información de la empresa. Revisar los datos e informes de seguridad aportados. Analizar los riesgos y tomar las decisiones que determinan las iniciativas y el presupuesto de seguridad de la información de la compañía.

- **Funciones de Dirección Financiera**

La Dirección Financiera es responsable de administrar las finanzas y el presupuesto de la organización. Trabaja con el comité de seguridad para asignar recursos al programa de seguridad de la información y ciberseguridad, y garantizar que sea rentable. La Dirección Financiera también puede brindar asesoramiento sobre los riesgos financieros relacionados con la seguridad de la información y asegurarse de que las pólizas de seguro de la organización cubran los incidentes de seguridad.

- **Funciones de Dirección de Operaciones**

La Dirección de Operaciones es responsable de administrar las operaciones diarias de la organización. Trabajan con el comité para garantizar que los procesos relativos a la operación y la continuidad del servicio de la organización estén alineados con las políticas y los procedimientos de seguridad de la información y

ciberseguridad. La Dirección de Operaciones también puede brindar asesoramiento sobre los riesgos operativos relacionados con la seguridad de la información y garantizar que el plan de respuesta a incidentes de la organización incluya medidas de continuidad del negocio. Además, la Dirección de Operaciones debe brindar apoyo al Comité para que los empleados reciban capacitación y concienciación sobre Seguridad de la Información.

- **Funciones de Dirección de Jurídico y Compliance**

Supervisa y asegura el cumplimiento de los marcos y políticas legales y regulatorios relacionados con la ciberseguridad y la protección de datos, estos deben estar alineados con la estrategia y los requisitos legales de la organización. Contribuye a las acciones relacionadas con la protección de datos de la organización asesorando en materia de privacidad y protección de datos y actuando como enlace con las autoridades de protección de datos.

Brinda asesoramiento legal en el desarrollo de los procesos de gobierno de la Seguridad de la Información de la organización y las estrategias/soluciones de remediación recomendadas para garantizar el cumplimiento según las políticas de la agencia de protección de datos y la normativa de seguridad de la información y ciberseguridad aplicable.

Asimismo, como Delegado de Protección de Datos del **Grupo Tunstall España**, asume las funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas de el/la responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD)
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

- **Funciones de Dirección de Desarrollo Estratégico Tecnología**

Desarrollar, operar y garantizar la seguridad en todos los sistemas desarrollados por el **Grupo Tunstall España** durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

Cerciorarse de que las medidas y metodologías de desarrollo cumplan con los requisitos establecidos en las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información.

La Dirección de Desarrollo Estratégico Tecnología puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos, previa consulta con el Comité de Seguridad y el/la Responsable de Seguridad, antes de ser ejecutada.

- **Funciones de la Dirección de Sistemas y Comunicaciones**

Supervisar y administrar la infraestructura tecnológica de la organización y garantizar que las políticas y prácticas de seguridad de la información se implementen y mantengan de acuerdo con la estrategia de seguridad de la empresa. Sirve como el principal recurso técnico para el Comité de Seguridad.

6.14.3 Funciones del Comité de Seguridad

- **Funciones del Comité de Seguridad de la Información**
  - En el ámbito de la cooperación
    - El desarrollo y el mantenimiento de un marco común normativo, organizativo y colaborativo de seguridad.
    - El desarrollo y el mantenimiento de un marco común de indicadores, métricas y analítica de datos de seguridad.
    - La aprobación y seguimiento y mejora continua de objetivos de seguridad.
    - La integración con otros marcos de gobernanza de seguridad en la cadena de suministro.
    - Atender las solicitudes, en materia de Seguridad de la Información, de la organización y de las diferentes áreas informando regularmente del estado de la Seguridad de la Información.
    - Asesorar en materia de Seguridad de la Información.
    - Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes áreas.
    - Representar frente a terceros (entidades privadas y Administraciones Públicas) la figura de Responsables de la Información ENS y Responsables de los Servicios ENS, así como el resto de responsables de la organización en el ámbito de la seguridad de la Información.
    - Promover la mejora continua del sistema de gestión de la Seguridad de la Información.
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos 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

  - En el ámbito del desarrollo de la normativa en materia de seguridad.
    - Aprobación de la Política y Normas de la Seguridad de la información.
    - La coordinación normativa con todos los departamentos de la compañía.

- La propuesta y mejora continua en el cumplimiento de la normativa de seguridad.
- La elaboración del informe anual del estado de seguridad de la compañía
- La integración con la normativa y las buenas prácticas de ámbito nacional y europeo.
- La revisión periódica de la Política de Seguridad y de la Normativa de seguridad de la compañía.

- En el ámbito de la gestión de riesgos en materia de seguridad.
  - El desarrollo y el mantenimiento de un marco común de análisis y tratamiento de amenazas y riesgos de seguridad de la información, así como para los tratamientos de datos personales.
  - La definición de los requisitos, niveles mínimos de seguridad, criterios comunes de Categorización y Declaración de Aplicabilidad para el establecimiento de un perfil de cumplimiento específico.
  - La gestión y supervisión del tratamiento de los riesgos, que se realiza mediante la operación de la seguridad de la información (arquitectura, implantación, administración y mantenimiento de los controles de seguridad que son aplicables -necesarios-, junto con su eficacia, así como si están operando o todavía no lo están).
  - El seguimiento de los controles de riesgos en materia de seguridad de la información.

- En el ámbito de la auditoría y certificación de conformidad de la seguridad de la información.
  - La constitución de una unidad de auditorías técnicas y cumplimiento.
  - Realización de revisiones de seguridad y su adecuación a las declaraciones de aplicabilidad.
  - Promover la realización de las auditorías periódicas internas y externas en el ámbito del ENS, ISO 27001 y RGPD que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la Información

- En el ámbito de la concienciación y formación en materia de seguridad.
  - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información
  - La aprobación del plan de concienciación y capacitación de seguridad de la información.

- En el ámbito de la gestión de incidentes en materia de seguridad.
  - Análisis de los resultados de ciberinteligencia.
  - Gestión y respuesta a incidentes acorde a los planes y procedimientos establecidos por el **Grupo Tunstall España**.
  - La cooperación en la gestión de incidentes con las administraciones con competencias.
  - La coordinación de actuaciones ante incidentes críticos de ámbito estatal con las autoridades competentes en materia de seguridad de las redes y sistemas de información.
  - El intercambio de información con las autoridades competentes.

XX. CONTROL DE CAMBIOS

Versión	Fecha	Cambios	Revisado	Aprobado
001	23/01/2020	Edición inicial	Comité	Consejero Delegado
002	27/02/2023	Cambio de estructura, definición de los controles	Comité de Ciberseguridad	Presidente del Comité de Ciberseguridad
003	21/ 03/2024	Actualización de la Normativa a los requisitos del nuevo ENS y a la situación actual de la organización	Comité de Seguridad	Comité de Dirección