POLÍTICA DE SEGURIDAD

Aprobación y Entrada en vigor el 21 de mayo de 2025

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación por el Comité de Seguridad, hasta que sea reemplazada por una nueva Política.

Contenido

Introducción

En **ODIN SOLUTIONS S.L.** (en adelante, **OdinS, organización**), reconocemos que los sistemas de Tecnologías de la Información y las Comunicaciones (TIC) son fundamentales para el logro de nuestros objetivos empresariales y la prestación eficaz de nuestros servicios. La correcta gestión y protección de estos sistemas es esencial para garantizar la **disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad** de la información que tratamos.

La **seguridad de la información** tiene como objetivo preservar la calidad de los datos y asegurar la continuidad de los servicios, actuando de forma preventiva, supervisando constantemente la actividad operativa y respondiendo con agilidad ante cualquier incidente.

En un entorno cada vez más digital y dinámico, las amenazas evolucionan rápidamente y pueden comprometer tanto los activos informáticos como el valor mismo de la información. Por ello, se requiere una estrategia de seguridad sólida y adaptable, alineada con los **requisitos del Esquema Nacional de Seguridad (ENS)**, la **Ley Orgánica de Protección de Datos (LOPD)**, el **Reglamento General de Protección de Datos (RGPD)** y los **estándares internacionales como la norma ISO/IEC 27001:2022**.

OdinS se compromete a:

- Aplicar de forma efectiva los principios y medidas establecidos por el **ENS**.
- Cumplir con la **ISO/IEC 27001:2022**, implantando un **Sistema de Gestión de Seguridad de la Información (SGSI)** eficaz.
- Incorporar la seguridad desde la fase de diseño hasta la retirada de los sistemas TIC.
- Identificar los requisitos de seguridad y financiación desde la planificación hasta la contratación de soluciones tecnológicas.
- Estar preparados para **prevenir, detectar, responder y recuperarse de incidentes de seguridad**, conforme a las mejores prácticas y la normativa vigente.

Esta **Política de Seguridad** sigue las directrices de la guía **CCN-STIC-805** del **Centro Criptológico Nacional (CCN)**, adscrito al **Centro Nacional de Inteligencia (CNI)**, y constituye el marco de referencia para proteger de forma proactiva y sostenible nuestros activos de información y los servicios prestados.

Prevención

OdinS 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 Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD), así como cualquier control adicional identificado a través de un análisis de riesgos y amenazas, conforme a los principios y requisitos establecidos por la norma ISO/IEC 27001:2022. Estos controles, junto con los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados como parte del Sistema de Gestión de la Seguridad de la Información (SGSI) de OdinS.

Para garantizar el cumplimiento de la política, OdinS debe:

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

Detección

Dado que los servicios se pueden deteriorar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en el Artículo 9 del ENS. La monitorización es especialmente relevante cuando se establecen líneas de defensa, de acuerdo con el Artículo 8 del ENS.

De forma complementaria, y en cumplimiento de los requisitos de ISO/IEC 27001:2022, se establecerán mecanismos de detección, análisis y reporte de eventos e incidentes de seguridad de la información, garantizando que la información llegue a los responsables pertinentes tanto de forma periódica como cuando se produzca una desviación significativa respecto a los parámetros definidos como normales. Esta capacidad de detección forma parte del sistema de control operativo y mejora continua del SGSI, permitiendo una respuesta oportuna y eficaz ante posibles amenazas o fallos.

Respuesta

OdinS:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establece protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

Recuperación
Para asegurar la disponibilidad de los servicios críticos, OdinS ha generado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

Misión
OdinS define la presente Política de Seguridad, de carácter obligatorio para empleados 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 celeridad frente a los incidentes que puedan ocurrir.

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

Autenticidad: propiedad o característica consistente en que una entidad sea quien dice ser o bien que asegure el origen del cual proceden los datos.
Confidencialidad: propiedad o característica consistente en que la información no se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
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.
Trazabilidad: propiedad o característica consistente en que los comportamientos de una entidad puedan ser atribuidas exclusivamente a dicha entidad.

Bajo estos principios los objetivos específicos de la Seguridad de la información en OdinS serán:

- Preservar la seguridad de la información, en las distintas dimensiones antes descriptas.
- 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 compañía.
- Realizar una apropiada gestión de incidencias que conciernen 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.
- Ofrecer los estándares de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Está 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 todos los empleados y empresas externas que trabajen con OdinS

Alcance
- Empleados de OdinS
- Sistemas de información que dan soporte a los procesos de diseño, desarrollo, producción, comercialización y mantenimiento de productos para la monitorización y tele gestión inteligente de infraestructuras en modalidad SaaS y On-premise.
- servicios de diseño, desarrollo, producción y comercialización de productos para la monitorización y la telegestión inteligente de infraestructuras.

- Contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información y/o los sistemas de la compañía.
- Información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas y/o administrativas.
- Información concedida dentro de un marco legal establecido, que será tenida en cuenta como propia a efectos exclusivos de su protección.

Declaración de la Política de Seguridad

El objeto de esta Política de Seguridad es proteger la información y los servicios de OdinS.

OdinS reconoce explícitamente la importancia de la información, así como la necesidad de su protección, por ser un activo vital y estratégico, hasta el grado de poder poner en peligro la continuidad de la organización u ocasionar daños significativos si se produjera una pérdida total e irreversible de determinados datos.

OdinS implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad (ENS), del Reglamento General de Protección de Datos (RGPD), de la Ley Orgánica de Protección de Datos (LOPD), y cumple con todos los requisitos legales aplicables, así como con los requisitos de la norma internacional ISO/IEC 27001:2022, mediante la implantación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

La información y los servicios están protegidos contra pérdidas de autenticidad, confidencialidad, disponibilidad, integridad y trazabilidad, tal como establece tanto el ENS como ISO/IEC 27001:2022.

Se cumple con los requisitos del servicio en materia de seguridad de la información y de los sistemas de información, aplicando controles de seguridad que serán proporcionales a la criticidad de los activos a proteger y a su clasificación, en coherencia con los principios de enfoque basado en riesgos y mejora continua establecidos por ISO 27001.

La Dirección de OdinS asume la responsabilidad última sobre la seguridad de la información incluida en el alcance del ENS y del SGSI, proporcionando los medios necesarios para su protección, sin perjuicio de que todo el personal y usuarios asuman sus responsabilidades específicas en el uso seguro de los sistemas, conforme a las normativas internas y procedimientos complementarios.

En el ítem “Organización de la Seguridad” de este mismo documento se describen los roles y responsabilidades del Comité de Seguridad, que será el órgano responsable de gestionar la seguridad de la información, conforme al ENS y a la norma ISO/IEC 27001:2022.

Quienes tengan la responsabilidad de Seguridad de la Información y otras funciones administrativas relacionadas serán los encargados de gestionar, supervisar y coordinar las medidas de seguridad del SGSI.

Se han identificado los responsables de la información, quienes deberán promover el establecimiento de controles y medidas destinadas a proteger los datos, especialmente los de carácter personal o críticos.

Se establecerá formalmente un sistema de clasificación de la información con diferentes categorías, tal como indica ISO/IEC 27001:2022 y las guías del ENS.

Se establecerán los medios necesarios y adecuados para la protección de personas, programas, datos, instalaciones, equipos, documentación y cualquier otro activo de OdinS, siguiendo criterios de análisis de riesgos y cumplimiento normativo.

Las cuestiones específicas relacionadas con datos personales estarán reguladas tanto por las normas mencionadas en este documento como por la normativa interna y otras disposiciones complementarias.

El incumplimiento de las normas y procedimientos de seguridad podrá ser objeto de sanción conforme a la legislación laboral vigente, o contractualmente, en el caso de relaciones no laborales.

Se realizarán de forma periódica evaluaciones de riesgos y, en función de las debilidades detectadas, se desarrollarán planes de acción para la implantación o fortalecimiento de controles de seguridad, en línea con el ciclo de mejora continua del SGSI según ISO 27001.

Se promoverá la difusión de información y formación en seguridad para empleados y colaboradores, con el fin de prevenir errores, fraudes, delitos u omisiones, detectarlos oportunamente, y garantizar una adecuada gestión de las investigaciones en caso de incidentes.

Todo el personal de ODIN SOLUTIONS S.L. deberá conocer las normas, políticas, procedimientos y estándares relacionados con su puesto de trabajo, así como sus responsabilidades y obligaciones, incluyendo la segregación de funciones y la revisión independiente de registros cuando corresponda, garantizando la trazabilidad de las acciones.

Los incidentes de seguridad serán comunicados y tratados de forma adecuada, conforme a lo establecido en los procedimientos internos, el ENS y el sistema de gestión ISO/IEC 27001:2022.

Marco Normativo

ODIN SOLUTIONS S.L. cumple con la legislación vigente en materia de Seguridad de la Información, siendo de aplicación, entre otras, las siguientes normas:

- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad (ENS)**.
- **Reglamento (UE) 2016/679**, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (**RGPD**).
- **Ley Orgánica 3/2018**, de 5 de diciembre, de **Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**.
- **Real Decreto Legislativo 1/1996**, de 12 de abril, por el que se aprueba el Texto Refundido de la **Ley de Propiedad Intelectual**.

ODIN SOLUTIONS S.L. cumple con la normativa legal en materia de seguridad de la información e integra el estándar internacional de calidad **ISO/IEC 27001:2022**, complementando el cumplimiento del **ENS**, **RGPD** y **LOPDGDD**. Este sistema garantiza la protección de la información, impulsa la mejora continua y refuerza la gestión del riesgo.
La Dirección lidera su implementación, asegurando recursos, formación y concienciación.

Organización de la seguridad

Comité de Seguridad

El Comité de Seguridad coordina la seguridad de la información en ODIN SOLUTIONS S.L.; reportará a la organización y estará conformado por:

- Director General
- Secretario de Comité
- Responsable de Servicio
- Responsable de la Información
- Responsable de Seguridad
- Responsable y Administrador de Sistemas

La **Dirección** nombra:

- Responsable de Seguridad, que reportará al Comité de Seguridad.
- Responsable de sistema y Administrador de sistema, que reportará al Comité de la Seguridad.
- Responsable del Servicio, que reportará al Comité de Seguridad.
- Responsable de la Información, que reportará al Comité de Seguridad.

El **Responsable de Seguridad** tendrá las siguientes responsabilidades:

- Convocar las reuniones del Comité de Seguridad.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Ejecutar directamente o delegar las decisiones del comité.
- Definir, implementar y mantener las medidas de seguridad necesarias para proteger los sistemas de información
- de la organización de acuerdo con el alcance.
- Evaluar los riesgos de seguridad y establecer controles técnicos y organizativos apropiados para mitigarlos.
- Coordinar y supervisar la gestión de la seguridad de la información desde la planificación, implementación, operación, supervisión y mejora continua del sistema.
- Garantizar la aplicación de controles de seguridad. Esto puede incluir la implementación de firewalls, antivirus, sistemas de detección de intrusiones, políticas de acceso y control de privilegios, entre otros.
- Supervisar de la gestión de incidentes de seguridad. Esto incluye la coordinación de la respuesta a incidentes y la implementación de medidas correctivas para prevenir futuros incidentes.
- Auditorías y evaluaciones del cumplimiento.

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

- Coordinar los esfuerzos de los distintos departamentos/servicios en materia de Seguridad de la Información, asegurando alineación con la estrategia organizativa, evitando duplicidades y reforzando la coherencia con el SGSI según ISO/IEC 27001:2022.

- Proponer planes de mejora de la seguridad de la información, incluyendo sus implicaciones presupuestarias, priorizando en función del análisis de riesgos.
- Garantizar que la seguridad esté considerada desde el inicio de cada proyecto hasta su operación, de acuerdo con el principio de "seguridad desde el diseño" (by design).
- Realizar seguimiento del estado de la seguridad y de los riesgos residuales, actuando ante incidentes y proponiendo acciones preventivas y correctivas, en línea con el enfoque de mejora continua de ISO 27001.
- Elaborar, revisar y mantener la Política de Seguridad de la Información.
- Validar la normativa general de seguridad, verificando la idoneidad de procedimientos y documentación asociada al SGSI.
- Diseñar e impulsar programas de formación y concienciación para todo el personal, especialmente en temas de seguridad y protección de datos.
- Establecer los requisitos de formación y competencia para los roles vinculados a la seguridad de la información.
- Promover auditorías periódicas según el ENS e ISO/IEC 27001 para verificar el cumplimiento del SGSI y de las obligaciones legales.

El **Responsable de la Información** tendrá las siguientes responsabilidades:

- Establecer, mantener y mejorar el SGSI de acuerdo con los requisitos del ENS e ISO/IEC 27001:2022.
- Supervisar la implementación de políticas, controles y procedimientos de seguridad.
- Coordinar la gestión de riesgos de seguridad de la información.
- Impulsar la formación del personal en seguridad de la información y protección de datos.
- Colaborar transversalmente con las distintas áreas de la organización para garantizar un enfoque integral.
- Gestionar el ciclo de vida de los incidentes de seguridad, incluyendo medidas de contingencia, correctivas y preventivas.
- Realizar revisiones periódicas de los controles de seguridad y su eficacia.

El **Responsable de Servicio** tendrá las siguientes responsabilidades:

- Asegurar que los servicios TIC cumplen con el ENS, ISO/IEC 27001 y las necesidades de los usuarios.
- Evaluar y gestionar los riesgos operativos, garantizando la continuidad del servicio.
- Asegurar la calidad y disponibilidad de los servicios ofrecidos.
- Realizar revisiones periódicas de cumplimiento respecto a los SLA acordados.

El **Responsable de sistema y administrador de sistema** tendrá las siguientes responsabilidades:

- Definir y mantener los sistemas de información alineados con el ENS y el SGSI de acuerdo con ISO/IEC 27001.
- Supervisar la gestión y operación segura de los sistemas.
- Identificar y tratar los riesgos asociados a los sistemas de información.
- Gestionar incidentes de seguridad tecnológica asegurando respuestas efectivas.
- Revisar periódicamente el cumplimiento de políticas y estándares técnicos de seguridad.

Comité de Crisis

Composición:

- Director de Crisis
- Asistente de Dirección
- Portavoz de Crisis
- Personal Técnico de Sistemas
- Representante de departamentos

El Comité de Crisis tendrá las siguientes responsabilidades:

- Evaluar la situación: naturaleza, alcance y gravedad de cualquier crisis dentro del alcance del ENS, que afecte a la organización.
- Tomar de decisiones rápidas y efectivas para abordar la crisis.
- Comunicar interna y externamente.
- Gestionar de recursos.
- Monitoreo y seguimiento continuo, evaluando los impactos y ajustando las estrategias y acciones según sea necesario.

- Gestionar de riesgos y contingencias.
- Apoyo y bienestar del personal: físico y emocional del personal afectado por la crisis.
- Análisis postcrisis y aprendizaje.

Datos de carácter personal

La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD) garantizan los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de sus datos personales, especialmente el derecho al honor, la intimidad personal y familiar, y la protección de su privacidad.

Estas disposiciones se aplican a todos los datos personales tratados por OdinS, tanto en soporte digital como en papel.

Para garantizar dicha protección, ODIN SOLUTIONS S.L. ha adoptado las medidas técnicas y organizativas de seguridad exigidas por esta normativa, y complementa su cumplimiento mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022.

Dicha norma establece un enfoque sistemático para la identificación de riesgos, la aplicación de controles de seguridad, y la mejora continua en la protección de la confidencialidad, integridad y disponibilidad de los datos, incluyendo aquellos de carácter personal.

Esto garantiza que el tratamiento de datos personales se realiza de forma segura, conforme tanto a la legislación nacional y europea como a los estándares internacionales más exigentes.

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.

Uso Aceptable de los SI y de la información

Los sistemas de información (SI) y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios.

No se considera aceptable:

- Generar o transmitir material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- Usar Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- Generar, utilizar o transmitir material ofensivo, obsceno o que pueda molestar u ofender.

- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).

Seguridad de la gestión de recursos humanos
La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros según aplique.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

Seguridad física y del entorno
Para una seguridad lógica efectiva, las instalaciones de ODIN SOLUTIONS S.L. mantienen una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o intromisión externa.

Áreas seguras
ODIN SOLUTIONS S.L. toma las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones. La totalidad de las instalaciones de OdinS cuentan con las barreras físicas necesarias para asegurar los recursos que éstas albergan; en concreto un control de recepción e identificación del visitante (mediante una tarjeta) y el acompañamiento del personal durante la estancia en las instalaciones.

Seguridad de los equipos
En OdinS los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz. Éstos están protegidos contra posibles fallos de energía (ordenador portátil con batería, SAIs, etc.). Adicionalmente, deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el responsable de sistemas y Administrador de sistemas. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso que los equipos deban abandonar las instalaciones para su mantenimiento.

Gestión de comunicaciones y operaciones
OdinS controlará el acceso a los servicios en redes internas y externas y se asegurará que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de OdinS y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información. Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo con estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

Protección frente a código malicioso y código móvil
Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de OdinS. Todo software adquirido por la organización sea por compra, donación o cesión es

propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias. Cualquier software nuevo que requiera ser instalado para trabajar sobre la red, el usuario que presenta la necesidad deberá solicitar autorización previamente, ésta será evaluada por responsable de área del usuario en cuestión y finalmente aprobada por el Responsable de Seguridad. El responsable de sistemas y Administrador de sistema será quien operativamente instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

Copias de seguridad
Los datos deben ser guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente.

Gestión de la seguridad de la red
Los elementos de red (switch, router, etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema. Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

Gestión de soportes
Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

Intercambio de Información
Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, etc.).

Seguimiento
Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos, así como para recomendar cualquier cambio que se estime necesario.

Control de accesos
Requisitos del servicio para el control de accesos
La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información.

Gestión de accesos de los usuarios
El responsable de información aprueba el acceso a los usuarios y luego el responsable de sistema y administrador de sistema proporciona a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario estará asociado a un perfil, de acuerdo con las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

Responsabilidades del usuario
Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado, así como otros posibles daños.

Control de acceso a la red
No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con OdinS para mantener el mismo nivel de seguridad que si fueran empleados de la propia compañía.

Informática móvil y teletrabajo

Cuando los equipos o la información propiedad de OdinS están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento según normativas y procedimientos de uso interno que establece la empresa.

Gestión de incidencias

Cualquier empleado (usuario) que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente a su supervisor directo y o responsable de seguridad para que tome las medidas oportunas. Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad. El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

Continuidad del servicio

Es imprescindible para OdinS establecer las pautas de actuación a seguir en caso que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, OdinS establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo.

La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad. La gestión de la continuidad del servicio se incorporará a los procesos de OdinS y será responsabilidad de una o varias personas dentro de la entidad.

Obligaciones del personal

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

Todos los miembros de OdinS 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 la organización, 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 o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Terceras Partes

Cuando ODIN SOLUTIONS S.L. preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad, se establecerán canales formales de actuación para la reacción ante incidentes de seguridad.

Cuando ODIN SOLUTIONS S.L. utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán metodologías específicas de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

Cuando algún aspecto de la política no pueda ser satisfecho por una tercera parte 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

52800781A JOSE TRIGUEROS (R: B73845893)

Firmado digitalmente por 52800781A JOSE TRIGUEROS (R: B73845893)
Fecha: 2025.05.22 08:11:56 +02'00'