POLÍTICA DE SEGURIDAD

Aprobación y Entrada en vigor el 28 octubre de 2024

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

ODIN SOLUTIONS S.L. (en adelante **OdinS**) 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. El objetivo 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 celeridad 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.

OdinS debe asegurarse que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su discontinuación 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 proyectos de TIC.

OdinS debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el 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 adscripto al Centro Nacional de Inteligencia.

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 ENS, RGPD y la LOPD, así como cualquier control adicional identificado a través de un análisis de riesgos y amenazas. 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, **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. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto periódicamente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

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:

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 no 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 asegure el origen del cual proceden los datos.

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 la 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 llegar a poner en peligro la continuidad de la organización, u ocasionar daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.

OdinS implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad, del RGPD y de la Ley Orgánica de Protección de Datos, y cumple con todos los requisitos legales aplicables.

La información y los servicios están protegidos contra pérdidas de autenticidad, confidencialidad, disponibilidad, integridad y trazabilidad.

Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.

Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.

La responsabilidad de la seguridad de la información involucrada en el alcance del ENS es de la Dirección, que otorgará los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las normativas y en los procedimientos complementarios. En el ítem “Organización de la Seguridad” de este mismo documento se describen los roles y responsabilidades del Comité de Seguridad, que gestionará la seguridad de la información, y de sus miembros.

Quienes tengan la responsabilidad de Seguridad de la Información y otras de administración relacionadas, serán quienes gestionen la seguridad.

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

Se establecerá, formalmente, un sistema de clasificación de la información, con diferentes categorías.

Se establecerán los medios necesarios y adecuados para la protección de personas, programas, datos, instalaciones, equipos, documentación y otros soportes que contengan información, y, en general, de cualquier activo de **OdinS**.

Cuestiones específicas más relacionadas con la información sobre datos personales están regulados por el conjunto de normas mencionadas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.

Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral, o bien con sanciones personalizadas si están vinculados a **OdinS** bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos en este último caso.

Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o fortalecimiento de controles.

Se promoverá la difusión de información y formación en seguridad a empleados y colaboradores, previniendo el cometido de errores, fraudes o delitos, omisiones, y tratando de detectar su posible existencia lo antes posible, y en caso que existieren, procurándose una difusión muy restringida de las indagaciones.

El personal de **OdinS** deberá conocer las normas, políticas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus responsabilidades y obligaciones, además de la segregación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.

Los incidentes de seguridad serán comunicados y tratados apropiadamente.

Marco Normativo

Según la legislación vigente, las leyes aplicables a **OdinS** en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Disposición 17238 del BOE núm. 177 de 2023. Resolución de 13 de julio de 2023, de la Dirección General de Trabajo - XVIII Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), España 5 de diciembre de 2018.

OdinS cumple con la legislación citada y con todos sus requisitos.

Organización de la seguridad

Comité de Seguridad

Funciones y Responsabilidades

El Comité de Seguridad coordina la seguridad de la información en **OdinS**.

El Comité de Seguridad 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 los requisitos del ENS.
- 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 diferentes departamentos/servicios en materia de Seguridad de la Información, para asegurar que estos sean consistentes y alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información de **OdinS**, con su dotación presupuestaria correspondiente, priorizando ésta por, sobre todo.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación.
- Realizar un seguimiento de la seguridad de la información y en específico de los principales riesgos residuales asumidos por **OdinS**, así como de los incidentes actuando de manera correctiva inmediata y proponiendo acciones para evitar recurrencias.
- Elaborar, aprobar y revisar regularmente la Política de Seguridad.
- Verificar la normativa de General de Seguridad para su aprobación e idoneidad de los procedimientos de seguridad de la información y demás documentación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de los roles y funciones de **OdinS** desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS que permitan verificar el cumplimiento de las obligaciones de **OdinS** en materia de seguridad.

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

- Establecer, implementar, mantener y mejorar continuamente el sistema general de seguridad de la información de acuerdo con los requisitos del ENS. Esto implica la definición de políticas, procedimientos, controles y medidas de seguridad necesarias para proteger la información de la organización.
- Coordinar y supervisar todas las actividades relacionadas con la seguridad de la información en la organización, asegurándose que se cumplan los requisitos del ENS y que se aborden las necesidades específicas respecto al tema.
- Identificar y evaluar los riesgos de seguridad de la información.
- Proporcionar formación y concienciación en materia de seguridad de la información a todos los empleados de la organización.
- Colaborar estrechamente con otros responsables y áreas de la organización, para garantizar una aproximación integral a la seguridad de la información.
- Participar en la gestión de los incidentes de seguridad de la información, a lo largo de todo el ciclo de vida de este. Tomando medidas de contingencia, correctivas y preventivas necesarias, así como reportar los incidentes relevantes a las autoridades competentes, en cumplimiento de los requisitos del ENS y otras regulaciones aplicables.
- Revisiones periódicas de los controles de seguridad de la información.

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

- Definir, implementar, mantener y asegurar que los servicios de Tecnología de la Información ofrecidos por la organización cumplan con los requisitos del ENS y con las necesidades de los usuarios.
- Identificar y evaluar riesgos relacionados con la prestación de servicios de TIC, y proponer medidas para mitigar estos riesgos y garantizar la continuidad del servicio.
- Garantizar la calidad y disponibilidad de los servicios.
- Realizar revisiones y evaluaciones periódicas del cumplimiento de los acuerdos de nivel de servicio (SLA), asegurando que se cumplan los compromisos establecidos con los usuarios y que se mantenga un alto nivel de calidad en la prestación de servicios de TIC.

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

- Definir, implementar y mantener los sistemas de información de la organización, asegurando que cumplan con los requisitos del ENS y con las necesidades del negocio.
- Coordinar y supervisar la gestión de los sistemas de información en la organización, asegurando que se cumplan los objetivos de seguridad y calidad establecidos y que se mantenga un alto nivel de disponibilidad y rendimiento.
- Identificar y evaluar riesgos relacionados con los sistemas de información.
- Supervisar la gestión de incidentes relacionados con los sistemas de información asegurando respuestas rápidas y efectivas a los problemas que puedan afectar la integridad, confidencialidad o disponibilidad de la información.
- Revisiones y evaluaciones del cumplimiento de políticas y estándares de seguridad.

Comité de Crisis

Funciones y Responsabilidades

Establecer un mecanismo efectivo para la gestión de crisis dentro de **OdinS.**

El Comité de Crisis reportará a la organización y estará conformado por:

- 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 (LOPD) y el Reglamento General de Protección de Datos (RGPD)[1], tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos

[1] LOPD: Ley Orgánica de protección de Datos
RGPD (Reglamento General de Protección de Datos o Reglamento 2016/679): normativa europea de protección de datos.

fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

Para garantizar dicha protección, **OdinS** ha adoptado las medidas de seguridad que se corresponden con las exigencias previstas en la legislación de aplicación.

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 **OdinS** mantienen una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o intromisión externa.

Áreas seguras

OdinS 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 **OdinS**, 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 **OdinS** 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 **OdinS** 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: 2024.11.04 12:52:19 +01'00'

X

José Trigueros Pacheco
Chief Executive Officer - CEO