ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto revisado el día 17 de junio de 2024 por el Responsable de Seguridad de Technology on demand y aprobado por el Comité de seguridad.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

Technology on demand es una empresa joven en el mercado pero con una dilatada y probada experiencia de todos los profesionales que la componen, en el mundo de las Tecnologías de la Información.

Nuestra propuesta es simple, Calidad , Profesionalidad y Sostenibilidad.

Calidad en todo lo que hacemos, y servimos, profesionalidad en sus proyectos y ejecuciones y sostenible porque nuestras propuestas económicas se ajustan a la realidad actual de mercado.

Proximidad con el cliente.

El objetivo de Technology on demand es ser líder en el mercado en aquellos nichos donde se requiere de una alta cualificación, experiencia, implicación y dedicación para poder abordar con éxito junto con el cliente, los proyectos solicitados. Este liderazgo obliga continuamente a que el personal este constantemente actualizado y certificado por los diferentes productos y sus fabricantes.

En Technology on demand queremos ayudar a las empresas a alcanzar sus retos de negocio, aportando soluciones diferenciales e innovadoras, crear empleo, desarrollar personas con talento, capaces de transferir conocimiento, aportar valor a sus accionistas, ser corresponsables con la sociedad.

Trasmitiendo confianza Nuestro proyecto: ser innovadores, …

Technology on demand quiere ser el Socio Tecnológico de referencia y conocida como la principal compañía de servicios profesionales de consultoría y tecnologías de la información.

Y pretendemos hacerlo gracias al carácter innovador, al talento, y la actitud positiva, de nuestros profesionales.

Technology on demand depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para prestar sus servicios. A tenor de ello los sistemas deben ser administrados tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad 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 presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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 mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Technology on demand debe estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

3. PRINCIPIOS Y DIRECTRICES

3.1. PREVENCIÓN

Technology on demand 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 implementa las medidas mínimas de seguridad determinadas por el ENS, así como

cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal están claramente definidos y documentados.
Para garantizar el cumplimiento de la política, Technology on demand:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2. DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios se monitorizan de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

Se establecen mecanismos de detección, análisis y reporte que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales alertan de ello.

3.3. RESPUESTA

Technology on demand:

- 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 para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

3.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, Technology on demand ha desarrollado un Plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4. ALCANCE

Esta Política se aplica a los sistemas de información que dan soporte a procesos de instalación y configuración de infraestructuras de servidor, almacenamiento y redes así como a los servicios de Backup de Technology on demand bajo la tecnología Synology, Azure Backup for 365, Cloud backup for 365 y Cloud backup service y a todos los miembros de la organización, sin excepciones. También se aplica sobre personal en prácticas y personal externo que puedan participar en los procesos de negocio de manera directa o indirecta.
La Política de Seguridad es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

1.Primer nivel: *Política de Seguridad de la Información.*

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto. La Política de Seguridad requiere la aprobación por parte del Responsable de Seguridad

2.Segundo nivel: *Normativa de Seguridad de la Información.*

El segundo nivel desarrolla la Política de Seguridad de la Información mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de

la información. Las Instrucciones se estructurarán en normativas y son aprobadas por el Responsable de seguridad.

3.Tercer nivel: *Procedimientos de Seguridad de la Información.*

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios.

Los procedimientos son aprobados por el Responsable de Seguridad de la Información.

El personal de Technology on demand tiene la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Normativas y los Procedimientos de Seguridad de la información están disponibles en la Intranet de la organización.

5. MISIÓN

En Technology On-Demand S.L somos conscientes que todas las empresas tienen diferentes necesidades y problemáticas a solucionar.

Es por esto que, como expertos en backup, nos apoyamos en nuestro conocimiento y bagaje profesional, para ofrecer soluciones que cubran estas necesidades rentabilizando al máximo las inversiones.

6. MARCO NORMATIVO

A continuación se detalla el marco normativo que debe cumplir la organización:

- 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 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.
- Real Decreto 311/2022, de 3 de mayo , por el que se regula el Esquema Nacional de Seguridad

7. ORGANIZACIÓN DE LA SEGURIDAD

Mediante la estructuración de nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión se base en los siguientes documentos:
Documentos Internos: los generados por el propio sistema de gestión
Documentos Externos: documentos necesarios para el correcto desarrollo del SGSI, no elaborados por la empresa. como: legislación, normas, etc.
Y además existen dos tipos de registros:
Registros internos: los generados por el propio SGSI.
Registros externos: registros recibidos del exterior (clientes, administración, proveedores, ...

8. ROLES Y RESPONSABILIDADES

8.1 COMITÉ DE SEGURIDAD

8.1.1 CONSTITUCIÓN

El Comité presenta estructura orgánica y está formado por delegados de las partes interesadas en la óptima gestión de la Seguridad de la Información. La postura oficial del Comité ante cuestiones sometidas a votación será delimitada por mayoría simple.
Los integrantes del Comité de Seguridad de la Información se detallan en la siguiente tabla.

FIGURA RESPONSABLE	**ROL**	**FUNCIONES Y RESPONSABILIDADES**
COMITÉ DE SEGURIDAD DE	Responsable de la información	Tratamiento / Protección de la información
	Responsable del servicio	Definir requisitos de seguridad de los servicios prestados

LA INFORMACIÓN		
RESPONSABLE DE SEGURIDAD	Responsable de la Seguridad	Responsable del Cumplimiento ENS
RESPONSABLE DEL SISTEMA	Responsable del sistema	Mantenimiento y continuidad de los Sistemas
	Administrador de la Seguridad	Monitorización y configuración de medidas de Seguridad

El secretario del Comité tiene como funciones del cargo:

- Convocar las reuniones del Comité.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el Acta de Reunión.
- Impulsar la ejecución directa o delegada de las decisiones del Comité.

El Presidente del Comité es responsable de presidir las reuniones. Así mismo, será responsable de revisar las Actas de Reunión y aprobarlas formalmente con su firma.

8.1.2 FUNCIONES Y RESPONSABILIDADES DEL COMITÉ

- Atender las solicitudes que, en materia de Seguridad de la Información, formulen el resto de órganos o unidades del Ayuntamiento, 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 los distintos departamentos o responsables.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información, para lo que se encargará de:

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, asegurando que sean consistentes y estén alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos 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.
- Realizar un seguimiento de los principales riesgos residuales asumidos por el Ayuntamiento y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su ulterior aprobación por el órgano competente.
- Aprobar las Normativas y Procedimientos de Seguridad de la Información.
- Aprobar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

8.2 RESPONSABLES Y MIEMBROS DEL COMITÉ

8.2.1 Responsable de la Información y de los Servicios

- Establecer y proponer para aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a los servicios y la información comprendidos en el ámbito de la Política de Seguridad de la Información de la entidad.

- Proponer para aprobación al Comité de Seguridad de la Información de los niveles de riesgo residual que afecten a los antedichos Servicios y a la Información.

8.2.2 Responsable de Seguridad

- Determinar las medidas de seguridad de naturaleza técnica que deberán ser implantadas para alcanzar las valoraciones realizadas por los Responsables de la Información y los Servicios.
- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Determinar la categoría del sistema, en colaboración con el Responsable del Sistema, para su eventual aprobación por el Comité de Seguridad de la Información.
- 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 auditorías y revisiones, externas o internas, de la seguridad del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Podrá desplegar otras funciones derivadas de otras normas jurídicas de aplicación, siempre que concurran los requisitos de conocimiento, experiencia, independencia y en su caso titulación.
- Ejercer de POC con las Administraciones Públicas con las que se trabaje.

8.2.3 Responsable del Sistema

- Detener cautelarmente la prestación de los servicios o suspender cautelarmente el acceso a la información si tiene el conocimiento de que estos presentan deficiencias graves de seguridad que pudiera ser atacadas de forma inminente, informando de ello a la presidencia del Comité de Seguridad de la Información.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar 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.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, 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, en el caso de no estar designado explícitamente dicho rol.
- 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.

8.3. PROCEDIMIENTOS DE DESIGNACIÓN

La designación de los Responsables identificados en esta Política ha sido realizada por el el Comité de Seguridad de la Información. El nombramiento será indefinido y se revisará cuando el puesto quede vacante. En este último caso será necesario realizar el nombramiento en el plazo de un mes.

La presidencia y el Secretario del comité serán nombrados por la Gerencia de la empresa.

8.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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

La difusión se practicará vía e-mail, a todos los trabajadores de la empresa, indicando la ubicación del texto definitivo de la Política en el portal WEB.

9. DATOS DE CARÁCTER PERSONAL

TECHNOLOGY ON DEMAND trata datos de carácter personal. El documento "Registro de Actividades de Tratamiento" al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados, los responsables correspondientes y las actividades de tratamiento realizadas.

Todos los sistemas de información de TECHNOLOGY ON DEMAND. se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado "Registro de Actividades de Tratamiento".

10. GESTIÓN DE RIESGOS

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

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad

• cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de TECHNOLOGY ON DEMAND aplicadas en materia de Protección de Datos de Carácter Personal.

Esta Política se desarrollará por medio de los procedimientos y políticas de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet:

En la capeta compartida ubicada en el Servidor denominada “Calidad”.

12. OBLIGACIONES DEL PERSONAL

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

Se ha establecido un programa de concienciación continua para atender a todos los miembros, 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.

13. TERCERAS PARTES

Cuando TECHNOLOGY ON DEMAND preste servicios a terceros o maneje información de otros, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte, coordinación y procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando TECHNOLOGY ON DEMAND utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte 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 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.

En Valencia a 15 de junio de 2024.