netZima

POLÍTICA Y DOCUMENTO DE SEGURIDAD

Sistema de gestión y seguridad de la información

Control de Documento

Datos generales

Fecha de creación del documento	*30/11/2019*
Código de documento	*PL-09 – v1.2*
Autor	*Enrique Almohalla*
Revisado por	*C.S.I.P*

Lista de distribución

Lista de distribución
Uso público a petición de cualquier parte interesada

Documentos relacionados

Título del documento
Todos documentos que integran las políticas, procedimientos, normativas, instrucciones técnicas y anexos del SGSI conforme a la Norma ISO 27001:2013, implantado en netZima.

Índice

POLÍTICA Y DOCUMENTO DE SEGURIDAD

1.- Objeto

Garantizar la seguridad de la información tiene como finalidad proteger lo que netZima entiende como uno de los activos más importantes para la organización. Es fundamental para el desempeño adecuado de las funciones y requisitos de negocio.

La información está sometida a un gran número de amenazas que pueden poner en peligro la actividad de la organización. Por eso, con el fin de garantizar que, en caso de materializar dichas amenazas, el daño que provoquen sea mínimo, y asegurar la continuidad de la actividad de la organización, se desea garantizar la seguridad de la información.

Garantizar la seguridad de la información pasa por implantar unos controles adecuados que se plasman en toda una documentación (políticas, normas, procedimientos, instrucciones técnicas, …) que establecen unos objetivos cuya finalidad última es garantizar la confidencialidad, la integridad y la disponibilidad de la información. En definitiva, además de los medios técnicos existentes, la seguridad de la información tiene que garantizarse con la definición de procesos apropiados que los trabajadores de la organización y demás personas relacionadas con ella (colaboradores, proveedores, socios, clientes y todas las partes interesadas) deben asumir.

La concienciación sobre la necesidad de proteger la seguridad de la información es una cuestión que asume la dirección de netZima. Por esa razón, desde el año 2011 se ha implantado un Sistema de Gestión de Seguridad de la Información (SGSI, en adelante) basándose en el estándar internacional ISO/IEC 27001:2013

2.- La empresa

netZima se constituyó en 2001. Es una empresa tecnológica de capital 100% español, y propiedad privada.

2.1.- Misión

¿Qué hacemos?

netZima es una compañía especializada en la generación automática y eficiente de sistemas de información para la gestión empresarial.

En 2006 demostramos la viabilidad de nuestras ideas sobre cómo crear software de gestión empresarial de forma eficiente con la primera versión comercial de icaria Lean Factory®. Hemos contribuido a llevar el concepto “lean” desde la industria al desarrollo y prueba de software. icaria 2.0 fue la fuente de ventaja competitiva de netZima® durante cinco años, tiempo en el que demostramos que crear software de forma automática es mucho más eficiente que la programación manual.

Nuestros equipos han creado numerosas soluciones importantes para el negocio de nuestros clientes. Desde 2012, otras compañías, organizaciones y equipos de trabajo que quieren mejorar radicalmente utilizan icaria Lean Factory 3.0® y nuestro proceso productivo.

En Desde 2015, usando nuestra tecnología icaria, hemos creado aplicaciones de gestión de datos de prueba y de identificación y disociación de datos sensibles: icaria TDM® y en producción el bloqueo de los datos sensibles con: icaria GDPR®, que estamos comercializando para dar servicio a compañías y organizaciones de distintos sectores.

¿Cómo lo hacemos?

netZima ha desarrollado Icaria®. Una plataforma tecnológica innovadora para la automatización del desarrollo de software de gestión empresarial. Esta tecnología permite reducir hasta en un 40% el coste total de propiedad del sistema y los plazos de ejecución de este tipo de proyectos, al tiempo que aumenta drásticamente la calidad del producto. Sustituimos horas de programación por tecnología.

¿Para quién?

Organizaciones que hacen de las Tecnologías de la Información fuente de ventaja competitiva o de excelencia en las operaciones.

¿Por qué?

Porque crea valor para nuestros clientes, proveedores, colaboradores y demás partes interesadas a través de la utilización eficiente de recursos, aumentando la calidad y reduciendo el coste de propiedad de los sistemas de información, y les permite abordar el desarrollo de nuevas capacidades de negocio basadas en la utilización de Tecnologías de la Información, completamente adaptadas a sus necesidades.

2.2.- Visión

Impulsar la competitividad de las organizaciones con las que colaboramos, automatizando sus procesos de negocio mediante la introducción de las Tecnologías de la Información, especialmente en aquellas de tamaño medio, y así contribuir al desarrollo y bienestar de la sociedad.

netZima quiere ser el socio tecnológico preferido de las organizaciones que buscan la eficiencia y la diferenciación a través de la automatización de los procesos de gestión.

Para lograrlo, continuaremos desarrollando nuestra tecnología para la automatización del proceso de producción de software de gestión, reduciendo sistemáticamente los costes y aumentando la calidad, de forma que la Tecnología de la Información más avanzada sea accesible al mayor número posible de empresas.

netZima quiere proporcionar a sus empleados y colaboradores un entorno estimulante y creativo que les permita desarrollar su potencial profesional y personal.

2.3.- Valores

Los valores de netZima son los siguientes:

- Vocación de servicio a nuestros clientes
- Orientación al trabajo en equipo
- Orientación a la innovación y la creatividad
- Búsqueda del equilibrio en el desarrollo personal y profesional
- Contribución al desarrollo de la sociedad
- Gestión de la seguridad en todos sus proyectos bajo el estándar de la ISO 27001:2013 en seguridad de la información
- En general, la búsqueda de la excelencia en todo aquello que hacemos

3.- Compromiso de la dirección y liderazgo

La Dirección de netZima es consciente de la importancia de proteger la información y los activos desde los que se trata dicha información. Los procesos de negocio de la organización dependen, en su mayoría, de la existencia de dicha información.

Con el fin de asegurar dicha protección y mantener su compromiso con la seguridad de la información y con sus clientes, proveedores, colaboradores, trabajadores y demás partes interesadas, netZima ha llevado a cabo la implantación de un SGSI basándose en el estándar internacional ISO/IEC 27001:2013.

La Dirección de netZima participa en la elaboración y aprueba este documento y toda la documentación asociada en con todas las actividades y procesos aquí descritos para el correcto desarrollo, implementación y mantenimiento del SGSI.

La ISO/IEC 27001:2013 establece la necesidad de que la Dirección sea consciente de los riesgos asociados al tratamiento y almacenamiento de la información que es utilizada en la organización.

Por este motivo, toda exclusión de controles que se considere necesaria para cumplir los criterios de aceptación del riesgo necesita ser justificada mediante evidencia de que los riesgos asociados han sido aceptados por los responsables. La exclusión de controles no deberá afectar a la capacidad y/o responsabilidad de la organización para garantizar la seguridad de la información de acuerdo con los requisitos de seguridad derivados de la evaluación de riesgos y de los requisitos legales o reglamentarios aplicables.

La Dirección de la organización, en términos generales, deberá suministrar evidencias de su compromiso para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, a través de las siguientes acciones:

- Formulando la política del SGSI.
- Velando por el establecimiento de los objetivos y planes del SGSI:
    - Servicio a clientes

Asegurar la disponibilidad del servicio a clientes
Asegurar el cumplimiento de los acuerdos de nivel de servicio

- Garantizar la continuidad del negocio
  Evitar fugas de información confidencial
  Proteger la imagen corporativa
  Ejecutar las labores necesarias para la recuperación de la actividad en caso de desastre

- Cumplimento de la normativa
  Cumplir con de la normativa GDPR y de protección de datos

- Eficiencia operativa
  Racionalización de los procedimientos internos relacionados con la seguridad de la información

- Nuevas oportunidades de negocio
  Acceder a contrataciones que exigen normativa de seguridad

- Partes interesadas
  Aplicar también el proceso a todas las partes interesadas

- Estableciendo los roles y responsabilidades en materia de seguridad de la información.
- Comunicando a la organización la importancia de cumplir los objetivos y la política de seguridad de la información, sus responsabilidades legales y la necesidad de la mejora continua.
- Proporcionando recursos suficientes para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.
- Decidiendo los criterios de aceptación de riesgos y los niveles aceptables de riesgo.
- Velando por que se realicen las auditorías internas del SGSI.
- Dirige las revisiones del SGSI.

3.1.- Gestión de los recursos

La Dirección de la organización determina y proporciona los recursos necesarios para garantizar la integridad, disponibilidad y seguridad de los recursos y activos, para ello:

- Establece, implementa, opera, supervisa, revisa, mantiene y mejora el SGSI.
- Asegura que los procedimientos de seguridad de la información responden a los requisitos empresariales.
- Identifica y cumple los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales

- Mantiene la seguridad adecuada mediante la aplicación correcta de todos los controles implantados.
- Lleva a cabo revisiones, cuando son necesarias, y reacciona en base a los resultados de estas revisiones.
- Imparte la formación necesaria para concienciar al personal de la importancia del SGSI
- Y cuando se requiera, mejorar la eficacia del SGSI.

Por otra parte, la organización se asegurará de que todo el personal al que se le hayan asignado responsabilidades definidas en el SGSI es competente para llevar a cabo las tareas requeridas, a través de:

- Determinar las competencias necesarias para el personal que lleva a cabo trabajos que afectan al SGSI.
- Impartir formación o realizar otras acciones para satisfacer estas necesidades.
- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de educación, formación, aptitudes, experiencia y cualificación.

La organización, se asegurará también de que todo el personal afectado sea consciente de la trascendencia y de la importancia de las actividades de seguridad de la información y de su contribución a los objetivos del SGSI.

3.2.- Proceso de mejora continua

La organización se compromete a mejorar de manera continua la eficacia del SGSI, garantizando la integridad, disponibilidad y seguridad, mediante el uso de la política y de los objetivos de seguridad de la información, de los resultados de las auditorías, del análisis de la monitorización de eventos, de las acciones correctivas y preventivas y de las revisiones de la Dirección.

Concretamente, la organización realizará acciones correctivas para eliminar la causa de las no conformidades con los requisitos del SGSI, a fin de evitar que vuelvan a producirse. El procedimiento documentado para las acciones correctivas define los requisitos para:

- Identificar las no conformidades.
- Determinar las causas de las no conformidades.
- Evaluar la necesidad de adoptar acciones para asegurarse de que las no conformidades no vuelvan a producirse.
- Determinar e implantar las acciones correctivas necesarias.
- Registrar los resultados de las acciones realizadas.
- Revisar las acciones correctivas realizadas.
- Verificar las auditorías

La organización también desarrollará acciones preventivas con la finalidad de eliminar la causa de las posibles no conformidades con los requisitos del SGSI y evitar que éstas vuelvan a producirse. Las acciones preventivas adoptadas deben ser apropiadas en relación a los efectos de los problemas potenciales. El procedimiento documentado para las acciones preventivas define los requisitos para:

- Identificar las posibles no conformidades y sus causas.
- Evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades.
- Determinar e implantar las acciones preventivas necesarias.
- Registrar los resultados de las acciones adoptadas.
- Revisar las acciones preventivas adoptadas.

La prioridad de las acciones preventivas se determina basándose en los resultados de la evaluación de riesgos.

4.- Política de Seguridad de la información

La actividad de netZima implica el tratamiento de información variada como forma de ejecutar procesos básicos propios de su negocio.

Los sistemas de información, aplicaciones, infraestructuras de comunicaciones, archivos y armarios, bases de datos, etc., constituyen el activo principal de netZima, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones y pueden poner en peligro la continuidad de la organización.

La política de seguridad de la información proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran para garantizar la seguridad de la información, cumpliendo el marco legal de aplicación y las directivas, políticas específicas y procedimientos definidos.

Estas actuaciones son seleccionadas e implantadas fundamentadas en el análisis de riesgos realizado. A raíz de dicho análisis de riesgos se seleccionan e implantan una serie de controles, siempre con el objetivo de lograr un equilibrio entre el riesgo que la dirección de la empresa considera aceptable sobre sus activos y el coste de las medidas que se pueden implantar para paliar dicho riesgo.

Además, en el propio informe de análisis y gestión de riesgos se identifican los criterios de evaluación de riesgos que se han tomado en consideración, así como el riesgo residual que asumen la Dirección.

Son los responsables de los activos de información, junto con el responsable del SGSI y de IT, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, de modo que los procesos más importantes y/o sensibles recibirán mayor protección.

Es responsabilidad del Comité de Seguridad y Privacidad de la Información, promover y apoyar la implantación de las medidas técnicas y organizativas necesarias para minimizar los riesgos potenciales a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos del negocio.

El objeto de esta política es alcanzar una protección adecuada de la información de netZima preservando los siguientes principios de la seguridad:

- **Confidencialidad:** garantizar que la información sea accesible sólo para quien esté autorizado a tener acceso a la misma.
- **Integridad**: garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad**: garantizar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, manual, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de netZima o fuera de ellas.

Asimismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física:** Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información.
- **Lógica:** Incluyendo los aspectos de protección de aplicaciones, redes y prototipos de comunicación electrónica y sistemas informáticos.
- **Político-corporativa:** Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal.

5.- Objetivos del SGSI

netZima desarrolla su actividad apoyándose en el tratamiento de diferentes tipos de datos e información. Dicho apoyo nos permite ejecutar procesos básicos propios del negocio.

Los sistemas, aplicaciones, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen el activo principal de netZima de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones y pueden poner en peligro la continuidad de la organización. Para que esto no suceda se ha diseñado una política de seguridad de la información con objetivos de control que se basan en:

- Proteger mediante controles y salvaguardas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Paliar los efectos de los incidentes de seguridad.

- Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información.
- Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente.
- Elaborar un conjunto de reglas, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, partes interesadas en general, etc.
- Especificar los efectos que conlleva el incumplimiento de la política de seguridad en el ámbito laboral.
- Evaluar los riesgos que afectan a los activos con el objeto de adoptar los controles y salvaguardas de seguridad oportunos.
- Verificar el funcionamiento de los controles y salvaguardas de seguridad mediante auditorías de seguridad internas realizadas por auditores independientes.
- Formar y concienciar a los usuarios en la gestión de la seguridad y en tecnologías de la información y las comunicaciones.
- Controlar el tráfico de información y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- Observar la legislación en materia de protección de datos de carácter personal, propiedad intelectual, propiedad industrial, laboral, de servicios de la sociedad de la información, penal y demás normativa aplicable, que afecte a los activos de netZima.
- Garantizar un servicio eficiente a nuestros clientes con un alto nivel de calidad, preservando así su confianza.
- Proteger el capital intelectual de la organización para que no se divulgue ni se utilice ilícitamente.
- Obtener las evidencias que permitan acreditar los incidentes de seguridad y la identificación de su autor.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la organización.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y sus efectos.

6.- Listado de requisitos legales

En la organización se observan, respetan y cumplen las leyes, la legislación actual y demás normativa legal aplicable en materia de:

- Propiedad intelectual
- Propiedad industrial
- Prevención del blanqueo de capitales y de la financiación del terrorismo,
- Administrativa
- Legal
- Contable y fiscal
- Laboral
- PRL
- LOPD
- GDPR
- Penal

7.- Política de privacidad

netZima ® respeta los derechos fundamentales, las libertades públicas y los intereses de todas las personas con las que trata y respeta todas las exigencias legales en materia de protección de datos salvaguardando, conforme a los mismos, los datos de carácter personal que recaba y trata.

7.1.- Recogida de datos

Nos basamos en no recabar más datos de los estrictamente necesarios.

Como regla general, cuando lo consientan, los datos de carácter personal que nos son facilitados por diferentes canales de comunicación, con la finalidad de atender solicitudes de información, (mediante llamada telefónica o por correo electrónico, web, etc.), así como para comunicar servicios o productos de netZima ®, no serán cedidos a terceras personas salvo a las entidades a que sea preciso para la gestión y ejecución de las relaciones comerciales que surjan.

De acuerdo con lo establecido en el régimen jurídico de protección de datos, netZima ® garantiza el derecho de los interesados a revocar el consentimiento otorgado para su uso, ejercer sobre ellos los derechos de acceso, rectificación, limitación del tratamiento, supresión, portabilidad y oposición. Para cualquiera de estas acciones, el interesado deberá enviar solicitud por escrito a dpo@netZima.com.

En lo referente a los datos conseguidos a través de la web, además de lo anterior, netZima ® indicará los tratamientos adicionales en cada caso, y la especificación para la que se tratarán los mismos, a través de formularios de recogida de datos. Además, recordará que no se puede introducir datos de terceros.

También recomendará la lectura de las cláusulas de información ubicadas al pie de cada uno de dichos formularios antes de aceptarlos y que el envío de cualquiera de los documentos supone la aceptación sin reservas de las condiciones informadas.

7.2.- Cesiones de datos

netZima ® no cede datos de carácter personal a terceros sin informar previamente a sus titulares de qué datos va a ceder, de la identidad de los cesionarios, de su actividad y de las finalidades a las que dichos cesionarios pueden destinar los datos y salvo que, en caso de ser necesario, también hemos recabado el consentimiento de los titulares de los datos.

7.3.- Tratamientos transfronterizos de datos

netZima no realiza tratamientos transfronterizos de los datos de sus clientes sin haber recibido a alguna de las circunstancias que permiten. En concreto, netZima almacena datos en servidores de Google en Estados Unidos de América bajo la autorización de la Agencia Española de Protección de Datos (vid. Expediente Google TI / 00153/2017).

7.4.- Seguridad

netZima ® ha adoptado las medidas de índole técnica y organizativa necesarias para proteger la integridad, la disponibilidad y la confidencialidad de los datos de carácter personal que trata. Así, netZima ® aplica las medidas de seguridad exigidas por el principio de seguridad y solo contrata proveedores de servicios de Internet (ISP) que tienen los más estrictos controles internacionales de gestión de la seguridad de la información.

7.5.- Política de cookies

netZima ® utiliza cookies en sus páginas web. Para más información acerca de qué son las cookies, qué datos recabamos y para qué los utilizamos existe política de cookies pública en nuestra web.

7.6.- Comunicaciones comerciales

netZima ® envía comunicaciones comerciales por medios electrónicos a las direcciones de correo electrónico y números de teléfono móvil facilitados durante la contratación de servicios si previamente han sido solicitados o consentidos por sus titulares. netZima ® le solicitará consentimiento para ello en todos los formularios de recogida de datos y dará la opción de retirar dicho consentimiento en todas y cada una de las comunicaciones que le enviará.

En todo caso, netZima ® da la opción de elegir si se quiere o no recibir este tipo de comunicaciones; permite revocar el consentimiento en todas las comunicaciones comerciales electrónicas que envía; y permite revocar el consentimiento en cualquier momento que se desee.

7.7.- Derechos de los titulares de los datos

netZima ® permite ejercer los derechos de acceso, rectificación, limitación, portabilidad, oposición y supresión en los términos recogidos en el Reglamento General de Protección de Datos y en su normativa de desarrollo. Para hacerlo es preciso dirigirse al Delegado de Protección de Datos de netZima ® bien por correo electrónico (dpo@netZima.com) bien por correo postal (netZima, S. L., C / Vivero, n.º 5 (28040 Madrid, España) bien por cualquier medio que permita acreditar el envío y recepción de la solicitud.

7.8.- Vigencia y modificación de la presente política de protección de datos

La presente política de privacidad está vigente desde el día 15 de octubre de 2018. netZima ® se reserva el derecho de modificación unilateralmente su política de privacidad en el supuesto de que exista un cambio de la legislación vigente, de la doctrina jurisprudencial o de criterios internos Cualquier cambio que se introduzca en esta política será publicado en la web y donde corresponda.

8.- Revisión de la política

La Política y normativa interna deberá ser revisada de forma periódica. Entre los supuestos que podrán originar su revisión se encuentran:

- Cambios significativos en los procesos de trabajo de netZima
- Propuestas de mejora formuladas por las auditorias efectuadas
- Cambio en la legislación vigente referente a lo que esta norma establece
- Cambios tecnológicos significativos

9.- Declaración de intenciones

La alta dirección de netZima, con Pedro Luis Primo, como presidente y Enrique Almohalla, como director general, son conscientes de la importancia que tiene para la organización la seguridad de la información con el objetivo de garantizar la continuidad de la actividad de la organización y para conseguir un grado óptimo de competitividad en el mercado actual.

Por ello, netZima ha desarrollado la presente política de seguridad y el soporte documental que la acompaña para garantizar los ámbitos de la confidencialidad, integridad y disponibilidad de la información.

La intención de la alta dirección ha sido definir los procesos más adecuados para que netZima emprenda un proceso de mejora sobre la gestión de la seguridad de su información con el

convencimiento que redundará en una mayor eficacia de sus procesos de producción y gestión. Por ello, cuando se detallen las aplicaciones o soluciones concretas a los puntos contenidos en el presente documento, se hará bajo dicha perspectiva, potenciando en lo posible aquellas soluciones que lleven seguridad a la información relevante de netZima.

La intención final de todo el sistema definido y desarrollado es la de ofrecer el mejor servicio a nuestros clientes, colaboradores, proveedores y demás partes interesadas, mejorando nuestros procesos y respetando escrupulosamente sus derechos legalmente establecidos.

Por todo ello, la alta dirección de netZima quiere dejar constancia expresa de su conocimiento y aprobación de las políticas desarrolladas en este documento, de forma que todo el personal las debe conocer y asumir como una parte de sus funciones laborales.

Para que todo esto sea posible se asignarán los recursos necesarios para el buen desarrollo y mantenimiento de lo aquí establecido,

Fdo: Pedro Luis Primo del Val

Presidente

Fdo: Enrique Almohalla Ortega

Director general

Historia

Fundada en 2001 con el objetivo de industrializar el desarrollo de software.

Tecnología

La tecnología icaria *nació en 2005.* icaria **Lean** factory ***v3.0*** *se liberó en 2011.*

Clientes & socios tecnológicos

Tecnología desplegada en operadores Telco Tier 1.

Acuerdos de licenciamiento con proveedores de TI de primer nivel.

Equipo

Profesionales experimentados.

Más de 5 años de experiencia de media en automatización.

I+D+i

Orientada a I+D+i: icaria *es una tecnología en constante evolución.*

Proyectos de innovación financiados por MINETUR a través del Plan Avanza con número de expediente: TSI-020602-2012-158. Asimismo, cuenta con la colaboración de Empresa Nacional de Innovación (ENISA).

Futuro Próximo

Nuevos productos, industrias y geografías.

Otros

Certificación ISO 27001:2013.

Metodologías ágiles de gestión de proyectos y PMBOK.

netZima

C/ del Vivero 5 - Pl1

28040 Madrid

Telf. +34 910 028 640

Fax + 34 918 269 294

sales@netzima.com