

POLÍTICA de VELORCIOS GROUP de Calidad, Medio Ambiente, Seguridad de la Información (SGSI y ENS) y Gestión de Servicios (SGS)

La Política que inspira los sistemas de Calidad ISO 9001, Medioambiente ISO 14001; Seguridad de la Información ISO 27001, Esquema Nacional de Seguridad (ENS) y Gestión de Servicios (SGS) ISO 20000 de **Velorcios Group**, responde a la inquietud de mejora e innovación en el desarrollo y gestión con alto nivel de prestaciones acorde a los requisitos reglamentarios y legales, así como los específicos de sus clientes. La orientación y el valor para los clientes y la sociedad debe además facilitar las actividades con el menor consumo y desgaste de los valiosos y escasos recursos ambientales, así como asegurar la información soportada en las Tecnologías de la Información, y garantizar una eficaz gestión de los servicios.

Velorcios surge con el fin de aportar **soluciones tecnológicas** que mejoren la competitividad de nuestros clientes dentro de tres grandes actividades como son:

- **Infraestructuras y Equipamientos**
- **Servicios CLOUD**
- **Seguridad**

Para **Velorcios** el **CLIENTE** es lo primero, las tecnologías son un medio para aportar soluciones y nuestro mensaje es:

EL CLIENTE EN EL CENTRO

Velorcios Group establece su:

- **MISIÓN: Colaborar con las empresas en su desarrollo tecnológico**
- **VISIÓN: Ser cómplices de la transformación digital de la sociedad**
- **VALORES: Cercanía, Eficacia y Sencillez**

Esta política se aplica a todos los sistemas TIC de VELORCIOS GROUP, a todos los servicios y a todos los miembros de la organización, sin excepciones.

VELORCIOS depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas son administrados con diligencia, 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.

Se adoptan los principios básicos del Esquema Nacional de Seguridad, que tienen por objeto asegurar que una organización podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

1. Seguridad integral.
2. Gestión de riesgos.
3. Prevención, reacción y recuperación.
4. Líneas de defensa.
5. Reevaluación periódica.
6. Función diferenciada.

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 están 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 dispone de una estrategia adaptada a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, el SGSI y el SGS, 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. Los diferentes departamentos se cercioran de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación son identificadas e incluidas en la planificación y en la solicitud de ofertas TIC.

POLITICA de Calidad, Medio Ambiente, Seguridad de la Información (SGSI) y Gestión de Servicios (SGS)

La Dirección se compromete a proveer productos y servicios que satisfagan de manera consistente las necesidades y expectativas de nuestros clientes.

Todo el personal está involucrado en el cumplimiento de esta política.

Para Velorcios el CLIENTE es lo primero, las tecnologías son un medio para aportar soluciones, por tanto nuestra orientación es: EL CLIENTE EN EL CENTRO.

La gestión de la Calidad, protección del Medio Ambiente, Seguridad de la Información (SGSI) y Gestión de Servicios (SGS) es parte integrante y fundamental de nuestra organización. Esta política es marco de referencia para el establecimiento de los objetivos de calidad, ambientales, SGSI, ENS y SGS.

Para lograr el máximo nivel de calidad y seguridad en nuestros procesos y servicios, nos fundamentamos en los procesos establecidos y revisados de gestión de Calidad, Medio Ambiente, SGSI, ENS y SGS, que tienen como finalidad lograr el cumplimiento de los siguientes compromisos, propósitos y objetivos.

- Cumplir con los requisitos contemplados en la norma ISO 9001 (Sistema de Gestión de la Calidad).
- Cumplir con los requisitos contemplados en la norma ISO 14001 (Sistema de Gestión Ambiental).
- Cumplir con los requisitos contemplados en la norma ISO 27001 (Sistema de Gestión de la Seguridad de la Información).
- Cumplir los requisitos del Esquema Nacional de Seguridad (ENS) de nivel medio.
- Cumplir los requisitos contemplados en la norma ISO 20000 (Sistema de Gestión de Servicios).
- Tener identificado el marco legal regulatorio del Esquema Nacional de Seguridad y su actualización continua en cumplimiento legal.
- Cumplir con los requisitos legales, reglamentarios y estatutarios del cliente, así como otros requisitos que afecten, asegurando el cumplimiento de dichos requisitos, cuidado del medio ambiente, asegurando la seguridad de la información y una gestión de servicios eficaz.
- Mejorar continuamente la eficacia del sistema integrado de gestión según las normas ISO 9001, ISO 14001, ISO 27001, ENS e ISO 20000, la toma de medidas para la prevención de la contaminación, la mejora continua de las medidas de seguridad y garantías de la salud de los trabajadores, facilitando la participación en las decisiones que les afecta, así como el derecho a ser consultados, la mejora continua de las medidas para garantizar la seguridad de la información en base al SGSI y el ENS, y la mejora continua del SGS y los servicios.
- Analizar y maximizar la satisfacción de los clientes con nuestros productos y servicios.
- Nuestra continua orientación hacia la excelencia está fundamentada en una temprana identificación y erradicación de las fuentes de los errores. La prevención y anticipación es prioritaria frente a la corrección.
- Lograr la motivación de nuestros recursos humanos, su capacitación, cualificación y experiencia, a través de las actividades apropiadas de selección, formación y adiestramiento.
- Establecer y mantener los cauces de comunicación e información permanente con nuestros clientes, empleados, proveedores y sociedad en general.
- La Política de Calidad, Medio Ambiente, Seguridad de la Información (SGSI) y Gestión de Servicios (SGS) se pone a disposición del público y de las partes interesadas para su información y conocimiento.
- La Política de Calidad, Medio Ambiente, Seguridad de la Información (SGSI) y Gestión de Servicios (SGS) contempla la minimización del impacto de los aspectos ambientales y la prevención de la contaminación con el objetivo de mejora eficiente en la REDUCCIÓN, REUTILIZACIÓN y RECICLAJE.
- El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de **VELORCIOS GROUP** y de nuestros clientes.
- El objetivo de esta Política y de Seguridad de la Información es trabajar en un entorno seguro y controlado siendo este objetivo fundamental el marco de referencia para todas las actividades y servicios que prestamos.
- La alta dirección tiene el compromiso de cumplir los requisitos aplicables a la seguridad de la información y aportar los medios que se requieran para dicho cumplimiento.

Así mismo:

- La información está protegida contra pérdidas de Disponibilidad (D), Autenticidad (A), Integridad (I),

Confidencialidad (C) y Trazabilidad (T).

- La información está protegida contra accesos no autorizados.
- Se cumplen los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.

La Dirección dota al Sistema de Gestión de todas las herramientas precisas, documental e informáticamente establecidas, para asegurar que la Política de Calidad, Medioambiental, Seguridad de la Información y Gestión de Servicios sea: comprendida, desarrollada, aplicada y continúe vigente en todos los niveles de la organización.

Para poder cumplir con estos compromisos, la empresa establece anualmente (aprovechando la revisión y análisis del Sistema de Gestión por la Dirección, así como el análisis de Riesgos/Oportunidades con las partes interesadas y los procesos), una serie de objetivos y metas de Calidad, Ambientales, Seguridad de la Información (SGSI) y Gestión de Servicios (SGS), relacionados de forma directa con nuestro compromiso de reducción de consumos energéticos y generación de residuos, así como nuestros objetivos de gestión relacionado con el incremento y consolidación del negocio, y seguridad de la información, que pueden tener carácter cualitativo o cuantitativo, pero en cualquier caso, deben ser verificables en cuanto a cumplimiento y efectividad.

La Dirección, evalúa el avance en la consecución de estos objetivos cuando efectúa la revisión periódica del Sistema Integrado de Gestión.

Dentro de las Políticas de Seguridad de la Información, **Velorcios Group** está preparado para prevenir, detectar, reaccionar y recuperarse de incidentes.

PREVENCIÓN

VELORCIOS evita que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos tienen implementadas 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, **Velorcios**:

- 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.

DETECCIÓN

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

RESPUESTA

Se dispone de mecanismos para responder eficazmente a los incidentes de seguridad. El punto de contacto para las comunicaciones con respecto a incidentes es info@velorciosgroup.com. El protocolo para el intercambio de información relacionada con el incidente se establece por medio del proceso de gestión de No Conformidades e incidentes del SGSI. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CCCN-CERT).

RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, **Velorcios** dispone de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Principios de la Política de Seguridad de la Información. de Velorcios Group

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que esté coordinada e integrada con el resto de iniciativas estratégicas para conformar un todo coherente y eficaz; integrado con las normas ISO 9001 de Gestión de Calidad, ISO 14001 de Gestión Ambiental, ISO 27001 de Gestión de la Seguridad de la Información, el Esquema Nacional de Seguridad e ISO 20000 de Gestión de Servicios.
- Responsabilidad diferenciada: Los sistemas de información diferencian el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del

servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

- Seguridad integral: La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.
- Gestión de Riesgos: El análisis y gestión de riesgos es parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación es proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información es atendida, revisada y auditada por personal cualificado, instruido y dedicado, liderado por el CIO de **Velorcios Group**.
- Seguridad por defecto: Los sistemas se diseñan y configuran de forma que garanticen un grado suficiente de seguridad por defecto.
- Requisitos de servicio: Se tendrán en consideración los requisitos de servicio y se contará con un Plan de Gestión de Servicios, donde estén incluidos los recursos humanos, técnicos, de información y financieros necesarios para operar el SGS y los servicios de **Velorcios Group**.
- La estructura de la documentación del SGI se gestiona y mantienen en vigor por la dirección en Qualitas CLOUD, y el entorno SITE a la cual tienen acceso todos los miembros de la organización.

Políticas específicas y responsabilidades.

Estas políticas se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información acorde al ENS y el RD 3/2010 que regula el ENS y que inspiran las actuaciones de **Velorcios Group**.

1.- Protección de datos de carácter personal: **Velorcios Group** adopta las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal, cumpliendo el RGPD.

2.- Gestión de activos de información: Los activos de información de **Velorcios Group** están inventariados y categorizados y están asociados a un responsable.

3.- Seguridad ligada a las personas: se tienen implantados los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

4.- Seguridad física: Los activos de información están emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas están suficientemente protegidos frente a amenazas físicas o ambientales.

5.- Seguridad en la gestión de comunicaciones y operaciones: se tienen establecidos los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmite a través de redes de comunicaciones está adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garantizan su seguridad.

6.- Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, queda registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a las actividades de **Velorcios Group**.

7.- Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplan los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

8.- Gestión de los incidentes de seguridad: se dispone de los mecanismos apropiados para la correcta

identificación, registro y resolución de los incidentes de seguridad.

9.- Gestión de la continuidad: se dispone de los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

10.- Cumplimiento: se adoptan las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

Estructura organizativa.

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la Política de Seguridad de la Información de **Velorcios Group** está compuesta por los siguientes agentes:

El Comité de Dirección y de Seguridad de la Información está compuesto por:

- CIO de Velorcios Group con el Rol de Responsable de Seguridad
- Responsables del sistema de información
- Otros responsables técnicos

Aprobado por la Dirección General el 13 de Enero de 2021.

D. Pedro David Andueza Avero