#### POLITICA DE SEGURIDAD

|  |  |
| --- | --- |
| Autor | XXXXX XXXXX |
| Creación del documento | dd mm aaaa |
| Propietario del documento | XXXXXXXXX |
| Referencias | xxxxxxxxxx |
| Versión | 1.1 |
| Estado | Revisada y aprobada. |
| Última versión | XXXXXXXXXX |

Tabla de cambios:

|  |  |  |  |
| --- | --- | --- | --- |
| Version# | Fecha | Autor | Comentario |
| 1 | XXXXX | XXXXX | Version inicial |
| 1.1 | XXXXX | XXXXX | Revisada y aprobada |

Autoescuela Calderón considera que la información, en cualquier forma, es un activo de la empresa y requiere controles adecuados para proteger estos activos de todas las amenazas, ya sean internas o externas, deliberadas o accidentales.

La información es vital para el funcionamiento eficiente y efectivo de la corporación. Dicha información sólo debe utilizarse para los fines previstos, es decir, para la realización de las operaciones comerciales de Autoescuela Calderón. La política de Autoescuela Calderón es proporcionar acceso a la información únicamente en base a una base probada de "necesidad de información empresarial" y denegar el acceso a todos los demás.

Es también la política de Autoescuela Calderón garantizar la continuidad del negocio y minimizar el impacto de los incidentes de seguridad, asegurando que mantenemos los tres aspectos de la Seguridad de la Información:

* **CONFIDENCIALIDAD** - proteger información valiosa y sensible de la divulgación no autorizada.
* **INTEGRIDAD** - salvaguardar la exactitud e integridad de la información.
* **DISPONIBILIDAD** - asegurar que la información y los servicios vitales estén disponibles para los usuarios.

Para garantizar estos aspectos de la información, Autoescuela Calderón refuerza:

* **RESPONSABILIDAD** - Las acciones realizadas por un individuo a la información pueden ser rastreadas únicamente para ese individuo.
* **MENOS PRIVILEGIOS** - Cada usuario tendrá acceso a los activos de información basados en los principios de "necesidad de saber" y "necesidad de hacer" según lo requiera su rol en el trabajo.
* **SEGREGACIÓN DE LOS DEBERES** - Los deberes y el área de responsabilidad serán segregados para reducir las oportunidades de modificación no autorizada o no intencional o el uso indebido de la organización
* **ESCALABILIDAD**- Se mantendrá la arquitectura de seguridad, de manera que se puedan acomodar las diferentes necesidades de seguridad de la organización.

Esta política complementa las políticas de seguridad de AUTOESCUELA CALDERÓN , diseñadas para garantizar que AUTOESCUELA CALDERÓN opera en un entorno seguro; Que protege los intereses de los empleados, la empresa y los clientes de la empresa. Cuando los requisitos legales, regulatorios y contractuales de España son más estrictos que las políticas de seguridad corporativa o global, las políticas de seguridad de AUTOESCUELA CALDERÓN (y procedimientos) prevalecen.

### Alcance:

La política de seguridad de la información de Autoescuela Calderón **se** aplicará a:

* + Todos sus funcionarios y empleados de Autoescuela Calderón ubicados en, o trabajando desde sitios de Autoescuela Calderón.
  + En caso de teletrabajo, para profesores, los procedimientos de seguridad aplican del mismo modo, ya que las pautas para teletrabajar son similares a las de trabajo presencial, a excepción de las conexiones a la red wifi de alumnos, ver Anexo 2.
  + Todos los empleados y agentes de otras Divisiones Autoescuela Calderón que apoyan a Autoescuela Calderón
  + Todos los socios, contratistas, proveedores, sus empleados y agentes que apoyen directa o indirectamente a la Autoescuela Calderon**.**

### Objetivo:

* + Asegurar que se proporcione una adecuada protección contra las amenazas a la información de Autoescuela Calderón, garantizando así la Confidencialidad, Integridad y Disponibilidad de la información adecuada a las necesidades empresariales.
  + Asegurar que los activos de Autoescuela Calderón estén protegidos y permanezcan disponibles.
  + Asegurar que Autoescuela Calderón implemente y mantenga el estándar mínimo de seguridad definido en las políticas de seguridad global de Autoescuela Calderón o definido en cualquier Normativa, certificado o política aplicable.
  + Asegurar que la información de Autoescuela Calderón, compartida con otras partes, esté protegida contra la divulgación no autorizada y se gestiona de acuerdo con esta política.
  + Asegurar que Autoescuela Calderón implementa los requisitos de ISO 27002 - Un Código de Prácticas para la Gestión de la Seguridad de la Información, en el área de gestión de alumnado y administración, únicas áreas donde se maneja información confidencial.
  + Mantener el ISMS ISO27001 y la certificación donde se especifique.
  + Velar por que todos los alumnos, empleados y contratistas que tienen relaciones contractuales con Autoescuela Calderón conozcan y cumplan los requisitos legales y reglamentarios aplicables en materia de IT, concretamente en lo referente a la legislación española.
  + Crear y mantener la conciencia de la gestión y del personal de Autoescuela Calderón sobre la seguridad de la información, garantizando así que todos los empleados entiendan su importancia para Autoescuela Calderón y sus propias responsabilidades individuales en materia de seguridad.
  + Asegurar que sólo se utilicen equipos autorizados para procesar la información comercial de la Autoescuela Calderón ( ver Anexo 3).Asegurar que las personas que desempeñan funciones de seguridad identificadas reciban una formación especializada en consonancia con sus responsabilidades en materia de seguridad.
  + Asegurar que todas las infracciones de seguridad de la información, reales o bajo sospecha, sean reportadas e investigadas por el Departamento de Seguridad.

### Responsabilidades:

La seguridad es un problema para todos. Cada empleado, profesor o alumno debe adherirse a esta política (( ver anexo 4), directrices y procedimientos. Los empleados que no cumplan con estas directivas serán responsables de acciones disciplinarias.

Cada el propietario/usuario de cada cuenta y/o equipo conectado a la red del centro, ya sea profesor o alumno es en última instancia responsable de asegurar que los requisitos de seguridad de la información del cliente se cumplan y se implementan de acuerdo con las obligaciones contractuales y la legislación. Autoescuela Calderón proporcionará en cada caso la guía de seguridad que aplique. Cuando la cuenta es interna, esta responsabilidad recae en el Departamento de Seguridad.

Cada área funcional es responsable de:

* + Asegurarse de que cumplen con la política de gestión de información y registro de MPS 902.
  + Toda la información debe ser almacenada, identificada, inventariada y debidamente clasificada de acuerdo con su valor y las normas y directrices de la Autoescuela Calderón ( ver Anexo 5) **.**

En caso de surgir cualquier asunto relacionado con políticas de seguridad que no se haya tenido en cuenta en este documento, se asignará a en un comité formado por el Director, el personal de Gestión de la Entrega y Seguridad, para su estudio y posible modificación del procedimiento.

# Anexo 1: Información de no conformidades

Con el objetivo de establecer las pautas y la forma de trabajo en lo que respecta a la información de aquellas acciones o comportamientos que implican no conformidades con respecto a la de gestión de la seguridad de la información en la compañía, se muestran dos ejemplos sobre la forma de informar dichas no conformidades, teniendo siempre en cuenta qué cualquier no conformidad detectada deberá ser tratada e informada dentro de las reuniones de seguimiento que haya a nivel de dirección, así como su seguimiento y su numeración que debe ser incremental.

|  |  |
| --- | --- |
| **Nº no conformidad** | 3 |
| **Area:** | Seguridad física y medioambiental |
| **Tipo de no conformidad** | Menor |
| **Control incumplido:** | * + 1. - Perímetro de seguridad física     2. - Controles físicos de entrada     3. - Seguridad de oficinas, despachos y recursos     4. - Protección contra las amenazas externas y ambientales |
| **Descripción:** | No existe un perímetro de seguridad totalmente finalizado.  Aun no están instalados todas los controles físicos de seguridad, están en proceso los detectores de intrusión y todo el sistema de control de accesos. Aun no están instalados los controles de seguridad en las salas y despachos. El sistema anti-intrusion que ayuda a impedir o notifica cuando se produce alguna amenaza está en proceso de instalación. |
| **Acción correctiva:** | Revisar en unos 15 días para asegurarse de que el sistema anti-  intrusión y el sistema de control de accesos está totalmente instalado y en funcionamiento. |
| **Fecha de revisión** | 22 de Mayo de 2017 |
|  |  |
| **Nº no conformidad** | 4 |
| **Area:** | Relaciones con suministradores |
| **Tipo de no conformidad** | Menor |
| **Control incumplido:** | * + 1. - Política de información para suministradores     2. - Tratamiento del riesgo dentro de acuerdos de suministradores.     3. - Cadena de suministro en tecnologías de la información y comunicaciones. |
| **Descripción:** | No existe una política adecuada de como debe ser el tratamiento con  respecto a los proveedores externos. |
| **Acción correctiva:** | Crear una política que especifique como debe ser la relación entre la empresa y los proveedores en cuanto a seguridad de la información se refiere. |
| **Fecha de revisión** | 1 de Junio de 2017 |

# Anexo 2: Teletrabajo

# Anexo 3: Gestión de equipos autorizados

# Anexo 4: Política de subrogación de responsabilidad

Profesores

Con equipos propios

Alumnos

Con equipos propios

Terceros:

# Anexo 5: Políticas de gestión de la información confidencial