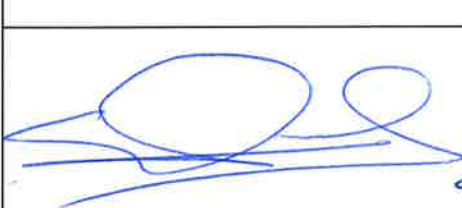


## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

### HOJA DE CONTROL DE REVISIONES

Nº Rev. / Fecha	Naturaleza de la revisión
15 febrero 2023	1º Edición de la presente política

**REVISADO Y APROBADO POR: JUAN SEVILLA DÍAZ, SEBASTIAN SEVILLA DÍAZ Y BEATRIZ SEVILLA DÍAZ**



Fecha: 15/04/23

## ÍNDICE

---

### **1.- INTRODUCCIÓN**

1.1. Prevención

1.2. Detección

1.3. Respuesta

1.4. Recuperación

### **2.- FINALIDAD**

### **3.- MARCO NORMATIVO**

### **4.- ÁMBITO DE APLICACIÓN**

### **5.- OBJETIVOS**

### **6.- PRINCIPIOS GENERALES**

### **7.- RESPONSABILIDADES**

### **8.- IMPLEMENTACIÓN**

### **9.- CONTROL Y AUDITORÍA**

### **10.- COMUNICACIÓN DE LA POLÍTICA**

### **11.- ACTUALIZACIÓN Y REVISIÓN DE LA POLÍTICA**

## 1. INTRODUCCIÓN

Construcciones Sevilla Nevado, S.A. depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones) y SSI (Sistemas de Seguridad de la Información) 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 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 previamente, supervisando la actividad diaria y reaccionando con premura 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 los departamentos dentro del alcance deben aplicar las medidas mínimas de seguridad exigidas tanto por la norma ISO 27001:2014 como 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.

Los departamentos dentro del alcance deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del Esquema Nacional de Seguridad (ENS) y con el apartado 6.1 de la norma ISO 27002: 2015.

### **1.1.- Prevención**

Toda la entidad mercantil Construcciones Sevilla Nevado, S.A. y muy en particular los departamentos que la componen deben 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 los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS y por las normas ISO 27001 e ISO 27002, 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, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos dentro del alcance deben:

- Autorizar los activos antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

### **1.2.- Detección**

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

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

### **1.3.- Respuesta**

Los departamentos dentro del alcance deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contactos para las comunicaciones con respecto a incidentes detectados en otros departamentos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

### **1.4.- Recuperación**

Para garantizar la disponibilidad de los servicios críticos, los departamentos dentro del alcance deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

## **2. FINALIDAD**

La actual Política de Seguridad de la Información establece los principios y directrices con los que Construcciones Sevilla Nevado, S.A. protegerá su información, de conformidad con la normativa aplicable y con sus valores éticos, definidos en el Código de Conducta así como con lo previsto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en cualquier otra normativa interna que resulte o pueda resultar de aplicación.

Construcciones Sevilla Nevado, S.A. velará por la protección de la información, independientemente de la forma en la que se comunique, comparta, proyecte o almacene. Esta protección afecta tanto a la información existente dentro de la entidad como a la información compartida con terceros.

En este sentido, se entiende por Seguridad de la Información, la salvaguarda y protección de la Información titularidad de la entidad mercantil, con independencia de que se encuentre en sistemas propios o de terceros; y la información titularidad de terceros, que se encuentre en sistemas de la empresa.

A los efectos de la presente Política, se entiende por Sistemas de Información el conjunto de tecnologías o medios tecnológicos, propios o de terceros que gestionen, almacenen o transmitan información (incluyendo tecnologías en la nube o similares).

### **3. MARCO NORMATIVO**

Construcciones Sevilla Nevado, S.A. se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código de Comercio, Código Civil, etc.) o específico, como por ejemplo las siguientes:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

### **4. ÁMBITO DE APLICACIÓN**

La presente Política se aplicará a toda la entidad mercantil Construcciones Sevilla Nevado, S.A. y vinculará a todo su personal, independientemente de la posición y función que desempeñe.

La aplicación de esta Política podrá hacerse extensiva, total o parcialmente, a cualquier persona física y/o jurídica vinculada a la entidad mercantil por una relación distinta de la laboral cuando ello sea posible por la naturaleza de la relación y resulte conveniente para el cumplimiento de la finalidad de aquella.

De conformidad con la Política, Construcciones Sevilla Nevado, S.A. podrá desarrollar procedimientos e instrucciones para implementar y dar cumplimiento a las obligaciones asumidas, así como para adaptar la misma a las diversas legislaciones locales aplicables a la empresa.

Asimismo, la aplicación de esta Política es complementaria a otras normas internas de obligado cumplimiento, como la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales, y aquellas otras que regulen cuestiones relacionadas con la información de la empresa.

## **5. OBJETIVOS**

La presente Política constituye el marco de referencia mediante el que Construcciones Sevilla Nevado, S.A. define las directrices de protección eficaz de la Información gestionada por la empresa y tiene los siguientes objetivos:

- Garantizar el grado de confidencialidad necesario a cada clase de Información, de conformidad con la clasificación establecida en el Procedimiento de Clasificación de la Información.
- Mantener la integridad de la información, de modo que no sufra alteraciones con respecto al momento en que haya sido generada por los propietarios o responsables de la misma.
- Asegurar la disponibilidad de la Información, en todos los soportes y siempre que sea necesaria, asegurando la continuidad del negocio y el cumplimiento de cuantas obligaciones sean exigibles a la Compañía.

## 6. PRINCIPIOS GENERALES

La consecución de los objetivos descritos en el apartado anterior se articula a través de los siguientes principios generales:

- Clasificación de la información:
  - La información se clasificará en función a su valor, importancia y criticidad para el negocio, de forma que las medidas de protección se adecúen al nivel de clasificación de cada activo de información. Del mismo modo, la clasificación de los activos de información se realizará tomando en consideración los requisitos legales, operacionales y las buenas prácticas y estándares al respecto.
  
- Uso de los sistemas de información:
  - El uso de los sistemas estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.
  
- Segregación de funciones:
  - Se deberán evitar las concentraciones de riesgos derivados de la ausencia de segregación de funciones y la dependencia unipersonal de funciones críticas para el negocio.
  - En este sentido, se deberán establecer procedimientos formales para controlar la asignación de privilegios de los Sistemas de Información, de forma que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.



- **Retención de información:**
  - Se establecerán, cuando resulte necesario o conveniente, periodos de retención de la información por categorías atendiendo a las necesidades operativas o de cumplimiento regulatorio, así como los correspondientes procedimientos de destrucción de la información.
  
- **Acceso a la Información por parte de terceros:**
  - Se desarrollarán los procedimientos de control de la puesta a disposición y acceso por terceros a la información relativa a Construcciones Sevilla Nevado, S.A.
  
- **Seguridad de la Información en los Sistemas:**
  - Los entornos de desarrollo y producción mantendrán en Sistemas independientes. Igualmente, el desarrollo y mantenimiento de los Sistemas de Información deben incluir los controles y registros necesarios para garantizar la correcta implementación de las especificaciones de seguridad.
  
- **Continuidad:**
  - Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la información crítica para la empresa en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables.
  
- **Cumplimiento:**
  - Los sistemas de información y comunicaciones de la empresa deberán estar adecuados de forma permanente a las exigencias de la legislación vigente en todas las jurisdicciones en las que opera, así como a la normativa interna de desarrollo que resulte de aplicación.

## 7. RESPONSABILIDADES

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles organizativos y funcionales de Construcciones Sevilla Nevado, S.A., cada uno en la medida que le corresponda, como se detalla a continuación.

### a) Responsabilidades de los empleados

- Todos los empleados de la entidad deberán conocer, asumir y cumplir la Política, así como la normativa interna de seguridad y uso de los Sistemas vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno laboral y debiendo comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.
- Los empleados que contraten servicios de terceros que impliquen el uso o acceso de estos últimos a la información deberán entender los riesgos derivados del proceso de externalización y asegurar una gestión eficaz de los mismos.
- El uso de los sistemas o servicios digitales por parte de los empleados, incluyendo expresamente el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

### b) Responsabilidades en relación con proveedores y otros terceros

- Los contratos con terceros que impliquen el uso o acceso de estos últimos a la información, entre los que se encuentran los de prestación de servicios o contratos de externalización, incluirán requerimientos específicos de seguridad relativos a la tecnología y las actividades de aquellos que llevan a cabo dichos servicios.
- En este sentido, deberán incluir provisiones mediante las que se garantice que los proveedores, el personal subcontratado o cualquier empresa externa que utilice o acceda, de manera potencial o real, a la información deberán conocer y cumplir la Política en lo que les sea de aplicación, estando obligados a mantener el secreto profesional y la confidencialidad de la información manejada en su relación con la sociedad.

c) Comité de Seguridad de la Información

- El Comité de Seguridad estará formado por el personal directivo de Construcciones Sevilla Nevado, S.A., que podrán estar auxiliados de manera permanente o esporádica por consultores externos.
- Este Comité, por lo que se refiere al SSI (Sistema de Seguridad de la Información) de Construcciones Sevilla y al cumplimiento de lo dispuesto en el ENS (Esquema Nacional de Seguridad), tendrá las siguientes funciones:
  - o Coordinar y aprobar las acciones en materia de seguridad de la información.
  - o Impulsar la cultura de la seguridad de la información.
  - o Participar en la categorización de los sistemas y análisis de riesgos
  - o Revisar y aprobar la documentación relacionada con la seguridad del sistema.
  - o Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.

## **8. IMPLEMENTACIÓN**

Construcciones Sevilla Nevado, S.A. se compromete a asignar recursos específicos para asegurar la implementación efectiva de la Política si fuese necesario.

## **9. CONTROL Y AUDITORÍA**

Construcciones Sevilla Nevado, S.A. se reserva expresamente el derecho a adoptar, con proporcionalidad, las medidas de vigilancia y control necesarias para comprobar la correcta utilización de los Sistemas que pone a disposición de sus empleados, incluyendo el contenido de las comunicaciones y dispositivos, respetando, en todo caso, la legislación vigente y garantizando la dignidad del empleado. La comunicación y aceptación de esta Política surtirá los efectos de notificación previa al trabajador.

La empresa, además, se someterá a revisiones y controles periódicos, así como auditorías internas y externas para evaluar el cumplimiento general de esta Política.

La valoración de un posible incumplimiento de esta Política se determinará en el procedimiento correspondiente, según las disposiciones vigentes, sin perjuicio de las responsabilidades legales, incluso de carácter sancionador en el ámbito laboral, que, en su caso, puedan resultar exigibles al incumplidor.

## **10. COMUNICACIÓN DE LA POLÍTICA**

La presente Política estará disponible tanto para todos los empleados como para todos los grupos de interés de Construcciones Sevilla Nevado, S.A en la web corporativa, siendo ésta la siguiente: [www.sevillanevado.com](http://www.sevillanevado.com).

## **11. ACTUALIZACIÓN Y REVISION DE LA POLÍTICA**

La Política será revisada y actualizada cuando proceda, con el fin de adaptarla a los cambios que puedan surgir en el modelo de negocio o en el contexto donde opere la empresa, garantizando en todo momento su efectiva implantación.