

# Política de Seguridad de la Información de Noventiq

## 1. ¿Qué es Noventiq?

---

Noventiq (Noventiq Holdings PLC) es un proveedor global de soluciones y servicios líder en transformación digital y ciberseguridad, con sede y cotización en Londres. La empresa permite, facilita y acelera la transformación digital de las empresas de sus clientes, conectando a más de 75 000 organizaciones de todos los sectores con cientos de los mejores proveedores de TI, junto con sus propios servicios y soluciones.

Con una facturación de 1.100 millones de dólares en el ejercicio fiscal de 2021, Noventiq es actualmente una de las empresas de más rápido crecimiento del sector. En octubre de 2021, la empresa "Noventiq Holdings PLC" obtuvo su cotización primaria en la Bolsa de Londres (LSE:NVIQ). El crecimiento de Noventiq se sustenta en su estrategia tridimensional de expansión geográfica, de cartera y de canales de venta. La estrategia se ve respaldada por el enfoque activo de Noventiq en materia de fusiones y adquisiciones, que permite a la empresa aprovechar la consolidación en curso en el sector: véanse [las empresas adquiridas por Noventiq](#).

Los 5900 empleados de Noventiq trabajan en casi 60 países de Asia, América Latina, Europa, Medio Oriente y África, mercados con un significativo potencial de crecimiento.

## 2. ¿Cuál es nuestro enfoque sobre la seguridad de la información?

---

Noventiq (sus subsidiarias, incluidas cada una de las empresas operativas de Noventiq - en conjunto, "Noventiq") se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información confiada a Noventiq. Nuestro compromiso con la seguridad de la información está en el centro de todo lo que hacemos.

## 3. ¿Cuáles son los principales componentes de nuestro programa de seguridad de la información?

---

Noventiq mantiene un completo programa de seguridad de la información basado en la Organización Internacional de Normalización (ISO) y el Instituto Nacional de Estándares y Tecnología (NIST) de Ciberseguridad. Tanto el ISO como el NIST son un conjunto de las mejores prácticas para que una organización pueda elaborar sus políticas y protocolos de seguridad en función de los riesgos identificados, los requisitos de compliance y las necesidades empresariales. Estos estándares cubren el control de acceso, la gestión de la configuración, la respuesta a incidentes, la formación en seguridad y otros ámbitos de la seguridad de la información.

### 3.1. Gobierno

El Chief Information Security Officer de Noventiq es el principal responsable del

desarrollo, mantenimiento y aplicación del programa de seguridad de la información de Noventiq. El Comité de Auditoría y Riesgos es responsable de todas las actividades de gestión de riesgos dentro de la empresa y está compuesto por miembros no ejecutivos del consejo de administración y líderes empresariales y jurídicos de la organización.

### 3.2 Política

El cumplimiento del conjunto de políticas internas de seguridad de la información es una obligación de todos los empleados de Noventiq. Noventiq lleva a cabo una serie de procedimientos de control interno para verificar el cumplimiento de las políticas internas de seguridad de la información, y todos los empleados de Noventiq reciben entrenamiento anual de manera obligatoria. Además, todas las terceras partes que entren en contacto con sistemas que puedan contener datos de Noventiq están obligados por contrato a mantener la seguridad y privacidad de los datos.

### 3.3 Acceso

El método principal de Noventiq para asignar y mantener controles de acceso y derechos de acceso será mediante la implementación del Control de Acceso Basado en Funciones (RBAC). Siempre que sea posible, los derechos y restricciones se asignan a grupos. A las cuentas de los usuarios se les podrán conceder permisos adicionales según sea necesario con la aprobación del propietario del sistema o de la parte autorizada.

### 3.4 Gestión de Activos

En Noventiq se identifican los activos asociados a la información y a las instalaciones de procesamiento de la información que almacenan, procesan o transmiten información confidencial, y se crea y mantiene un inventario de dichos activos. Los activos incluidos en el inventario son propiedad de un individuo o grupo específico de Noventiq. Las reglas por el uso aceptable de la información, activos y las instalaciones del procesamiento de información son identificadas y documentadas.

### 3.5 Encriptado

El encriptado de los datos es un elemento importante de nuestra protección de datos sensibles en reposo y en tránsito. Se revisa y actualiza anualmente según proceda, basándose en las normas y directrices más recientes publicadas por OWASP y NIST.

- *En tránsito:* Noventiq encripta los datos en tránsito a través de conexiones públicas, mediante Transport Layer Security (TLS), comúnmente conocido como SSL, utilizando protocolos, cifrados, algoritmos y tamaños de clave estándar del sector.
- *En reposo:* Noventiq cifra los datos en reposo mediante el algoritmo de cifrado AES-256 estándar del sector.

### 3.6 Terceros

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización se acordarán con el proveedor y se documentarán.

En el caso de todos los proveedores de servicios que puedan acceder a datos, sistemas o redes confidenciales de Noventiq, se lleva a cabo un Due Diligence antes de proporcionar acceso o realizar actividades de procesamiento. Se mantiene información sobre qué requisitos normativos o de certificación gestiona o afecta a cada proveedor de servicios, y cuáles gestiona Noventiq según sea necesario. Los requisitos normativos o de certificación aplicables pueden incluir ISO 27001, SOC 2, PCI DSS, CCPA, GDPR u otros marcos, normas de cumplimiento o reglamentos.

### 3.7 Seguridad de las Operaciones

Los cambios en la organización, los procesos empresariales, las instalaciones de procesamiento de la información, la producción de software y la infraestructura, y los sistemas que afectan a la seguridad de la información en el entorno de producción y los sistemas financieros se prueban, revisan y aprueban antes de su implantación en producción. Se documentan todos los cambios significativos en los sistemas y redes incluidos en el ámbito de aplicación.

El uso de los recursos de procesamiento y el almacenamiento del sistema se supervisan y ajustan para garantizar que la disponibilidad y el rendimiento del sistema cumplan los requisitos de Noventiq.

Los entornos de desarrollo y ensayo están separados de los entornos de producción para reducir los riesgos de acceso no autorizados o cambios en el entorno operativo. Los datos confidenciales de los clientes no se utilizan en entornos de desarrollo o prueba sin la aprobación expresa del Global Data Protection Officer.

Los sistemas y redes se proporcionan y mantienen de acuerdo con los estándares de configuración y refuerzo de Noventiq. Se utilizan firewalls y/o apropiados controles de acceso a la red para controlar el tráfico de red y el entorno de producción. Las normas de configuración de acceso a la red se revisan al menos una vez al año.

Para proteger la infraestructura de la empresa contra la penetración de programas maliciosos, se aplican controles de detección, prevención y recuperación de programas maliciosos, combinados con una sensibilización adecuada de los usuarios.

Se utilizan protecciones antimalware en todos los dispositivos de la empresa, excepto en los que ejecutan sistemas operativos que normalmente no son propensos al software malicioso. Además, se utiliza software de detección y respuesta a amenazas para el correo electrónico de la empresa. Las protecciones antimalware utilizadas son capaces de detectar todas las formas comunes de amenazas maliciosas y realizar la actividad de mitigación apropiada (como eliminar, bloquear o poner en

cuarentena).

Noventiq analiza todos los archivos cuando se incorporan a los sistemas y los analiza continuamente cuando se accede a ellos, se modifican o se descargan. Las actualizaciones de definiciones y motores antimalware se configuran para que se descarguen e instalen automáticamente siempre que haya nuevas actualizaciones disponibles.

La necesidad de realizar copias de seguridad de los sistemas, bases de datos, información y datos, se tiene en cuenta dentro de Noventiq y se diseñan, planifican e implementan procesos de copia de seguridad adecuados. Los procedimientos de copia de seguridad incluyen procedimientos para mantener y recuperar los datos de los clientes de acuerdo con los SLA documentados. Las medidas de protección de las copias de seguridad se diseñan y aplican de acuerdo con la confidencialidad o sensibilidad de los datos. Las copias de seguridad de la información, el software y las imágenes del sistema se realizan con regularidad para proteger contra la pérdida de datos. Las copias de seguridad y las capacidades de restauración se probarán periódicamente.

### 3.8 Gestión de Datos

Noventiq clasifica los datos y los sistemas de información de acuerdo con los requisitos legales, la sensibilidad y la criticidad empresarial para garantizar que la información recibe el nivel de protección adecuado. Los propietarios de los datos son responsables de identificar cualquier requisito adicional para datos específicos o excepciones a los requisitos de tratamiento estándar. Los sistemas de información y las aplicaciones se clasifican según la clasificación más alta de los datos que almacenan o procesan.

Los datos clasificados como restringidos o confidenciales se eliminan de forma segura cuando ya no se necesitan. Noventiq garantiza que todos los datos restringidos y confidenciales se eliminan de forma segura de los dispositivos de la empresa antes o en el momento de su eliminación. Los materiales impresos confidenciales y restringidos se trituran o eliminan de forma segura.

### 3.9 Entrenamiento en Seguridad

En Noventiq, creemos que proteger la información es responsabilidad de todos los empleados. Hemos implantado un completo programa de entrenamiento sobre seguridad de la información al que se someten todos los empleados en el momento de su contratación y que se actualiza anualmente.

### 3.10 Certificaciones

Noventiq ha certificado su principal delivery center de la siguiente manera:

ISO 27001: 2013 Information Security Management System

## ISO 22301: 2019 Business Continuity Management System

### 3.11 Privacidad

Los servicios de Noventiq están diseñados para facilitar el cumplimiento de la legislación aplicable en materia de privacidad de datos, incluido el GDPR y el GDPR del Reino Unido, en relación con la recopilación, el acceso, la revisión y la divulgación de datos personales. El [Aviso de Privacidad](#) de Noventiq describe los tipos de información recopilada, los fines, los fundamentos jurídicos, los plazos de conservación, con quién compartimos los datos, qué derechos tiene el interesado y dónde puede ponerse en contacto con nosotros. Noventiq también ha publicado en línea su [Política de Privacidad](#), en la que se expone nuestro enfoque de la privacidad.

## 4. Historial

No	Versión No	Fecha	Resumen de los cambios
1	1.0	2020	Documento Final
2	2.0	Abril 14, 2023	Documento Final