# Seguridad de la información CPS de GESNEXT
# Medidas técnicas y organizativas (TOM) para GesNext

# TOM

**TOM-GesNext**

**Versión 4.0**

**Febrero de 2021**

# Tabla de contenido



 

# 1. Introducción

En este documento (Medidas Técnicas y Organizativas o TOM) se registran los controles de seguridad implementados en los Centros de Innovación para Clientes (CIC), aplicaciones y centros de datos cloud de GESNEXT utilizados para la prestación de servicios a Clientes.

En lo sucesivo en el presente documento, el cliente de GesNext se le denominará como el Cliente.
En lo sucesivo en el presente documento, GesNext se denomina a GesNext y sus terceros contratados.

## 1.1 Ámbito

El presente documento especifica las responsabilidades entre el Cliente y GesNext en referencia a la protección de los datos del cliente.

Por favor, consulte el Apéndice E para obtener una lista de los centros de datos de GesNext, que se incluyen en el ámbito del presente documento.

| | |
|---|---|
| **Categorías de sistemas dentro del ámbito del presente Documento** | Todos los servidores, dispositivos de red, aplicaciones y estaciones de trabajo que dan soporte a los servicios empresariales de producción de Clientes de conformidad con el Apéndice E. |

Cualquier categoría de sistema no especificada en la tabla anterior se considera fuera del ámbito del presente Documento.
NOTA: Los controles para las estaciones de trabajo del usuario final se documentan en el Apéndice A.
NOTA: Los controles para las Aplicaciones se documentan en el Apéndice C.
NOTA: Es posible que no todos los tipos de sistema se dediquen a un único cliente.

Los controles estipulados en el presente documento representan los controles de seguridad mínimos que GESNEXT implementará en base a sus prácticas estándar en el entorno compartido. Si bien GESNEXT no ofrecerá controles a una calidad inferior de los especificados en el presente documento, GESNEXT se reserva el derecho a implementar prácticas de seguridad más estrictas, según considere adecuado.

# 2. Estructura del documento

El presente documento utiliza un estándar internacional, ***ISO/IEC 27002:2013, Tecnología de la información – Técnicas de seguridad – Código de prácticas para la gestión de la seguridad de la información,*** como marco para proteger la información del cliente.

A continuación se describen las catorce cláusulas, numeradas de acuerdo con su cláusula en el estándar ISO/IEC 27002:2013[1].

- **A.5** **Políticas de seguridad de la información** – La base para los estándares, los procesos y los procedimientos de seguridad
- **A.6** **Organización de la seguridad de la información** – Asignación de recursos y responsabilidades para aplicar la seguridad
- **A.7** **Seguridad de recursos humanos** – Consideraciones de seguridad antes, durante y después del empleo
- **A.8** **Gestión de activos** – Responsabilidad por las decisiones en torno a la protección de los activos
- **A.9** **Control de acceso** – Responsabilidad por el acceso a los recursos y la información
- **A.10** **Criptografía** – Controles relacionados con el cifrado y la gestión de claves
- **A.11** **Seguridad física y del entorno** – Un entorno seguro para las personas, el equipo y los datos
- **A.12** **Seguridad de las operaciones** – Procedimientos y controles para reducir los riesgos de seguridad en las operaciones diarias
- **A.13** **Seguridad de las comunicaciones** - Controles relacionados con la seguridad de las redes, la segregación y la transferencia de información
- **A.14** **Adquisición, desarrollo y mantenimiento de sistemas** – Consideraciones de seguridad en entornos de desarrollo y soporte
- **A.15** **Relaciones con los proveedores** – Controles para incluir disposiciones en materia de seguridad en los contratos con proveedores
- **A.16** **Gestión de los incidentes en torno a la seguridad de la información** – Canales de gestión para garantizar que se notifiquen los sucesos de seguridad y que se tomen medidas correctivas
- **A.17** **Aspectos de la seguridad de la información de la gestión de la continuidad del negocio** – Planes para evitar o recuperarse tras un desastre o fallo de seguridad
- **A.18** **Cumplimiento** – Comprobaciones para garantizar que los requisitos normativos y legales se cumplen y que los controles y las políticas de seguridad se aplican correctamente.

[1] Las catorce secciones de control de la seguridad en el estándar ISO empiezan en la Sección 5. Las secciones 1 a la 4 cubren el Ámbito, los Términos y Definiciones, Estructura del Estándar y Evaluación de Riesgos y Trato.

# 3. Políticas de seguridad de la información

GESNEXT se encargará de:

- Proporcionar a los Clientes estas TOM, que describen los estándares y controles de seguridad para sistemas utilizados en la prestación de servicios al Cliente
- Debatir e implementar solicitudes de cambio acordadas mutuamente en las TOM del Cliente
- Revisar las TOM con el Cliente de conformidad con el proceso de revisión acordado en el MSA

# 4. Organización de la seguridad de la información

El Cliente se encargará de:

- Proporcionar a GESNEXT un punto de enlace para las actividades relacionadas con la seguridad.

GESNEXT se encargará de:

- Proporcionar un punto de enlace de GESNEXT para las actividades relacionadas con la seguridad del Cliente.
- Disponer de una organización interna con las siguientes características:
  - Definir los roles y responsabilidades para la información de la seguridad, y asignarlos a las distintas personas.
  - Cuando proceda, separar las funciones de los distintos roles y personas para evitar conflictos de interés e impedir actividades inapropiadas.
  - Mantener contacto con las autoridades externas relevantes (como los CERT y los grupos de interés especial) sobre cuestiones relacionadas con la seguridad de la información.
- Dispositivos móviles y teletrabajo:
  - Implementar medidas de seguridad para gestionar los riesgos inherentes al uso de dispositivos móviles.
  - Implementar medidas de seguridad para proteger la información accedida, procesada o almacenada en los sitios de teletrabajo.

### 4.1 Puntos de enlace y detalles de contacto

**Tabla 1 - Información sobre los puntos de enlace**

| Puntos de enlace identificados | Detalles de contacto |
|---|---|
| Punto de enlace del cliente para las actividades relacionadas con la seguridad | - |
| Contacto secundario autorizado del Cliente | - |
| Punto de enlace de GesNext para las actividades relacionadas con la seguridad | Manuel Machuca |
| Contacto secundario autorizado de GesNext | Emilio Vázquez |

# 5. Seguridad de recursos humanos

GESNEXT se encargará de:

- Garantizar que la seguridad se aplique en los procesos de contratación, terminación y gestión de personal para el personal de GESNEXT.
- Proporcionar formación sobre reconocimiento de la seguridad al personal de GESNEXT.
- Solicitar una revisión anual de las directrices de conducta de negocio de GESNEXT por parte de los empleados de GESNEXT.
- Tomar las medidas adecuadas referentes a la gestión en caso de que se produzca un abuso de autoridad por parte del personal de GESNEXT.

Las prácticas de evaluación del personal siguen las políticas locales de recursos humanos de GESNEXT, determinadas por la legislación del país y la disponibilidad de los registros del personal.

### 5.1 Prácticas de contratación

**Tabla 2 - Prácticas de contratación**

| Prácticas de contratación | Requisito |
|---|---|
| Comprobaciones de verificación de antecedentes | N/D |
| Comunicación de los términos de confidencialidad a empleados y contratistas | Parte del proceso de nueva contratación. Los acuerdos de confidencialidad se comunican a los empleados y estos los firman. |
| Formación sobre reconocimiento de la seguridad de la información | Parte del proceso de nueva contratación y periódicamente después. |

# 6. Gestión de activos

GESNEXT se encargará de:

- Garantizar que el inventario de todos los sistemas físicos, sistemas operativos y sistemas virtuales con una dirección IP tenga un propietario o administrador, así como su mantenimiento para disponer de la información actualizada.
- Gestión de medios de almacenamiento portátiles:
    - Almacenar los medios de almacenamiento portátiles que contengan datos del Cliente en un área físicamente controlada.
    - Eliminar de forma segura los medios de almacenamiento portátiles que ya no sean necesarios, asegurándose de que sean ilegibles antes de su eliminación.
    - Implementar controles para proteger los medios durante su transporte.
- Mantener la información impresa, identificada como confidencial por el Cliente, en un contenedor cerrado con llave o un área físicamente controlada.
- Definir reglas para el uso aceptable de la información y de los activos asociados a la información y las instalaciones de procesamiento de la información.
- Garantizar que todos los empleados y subcontratados devuelvan todos los activos organizativos al cese de su empleo, contrato o acuerdo.
- Garantizar que todos los activos de información estén clasificados y etiquetados por sus propietarios, de acuerdo con la protección de seguridad necesaria, y gestionados adecuadamente.

# 7. Control de acceso

El Cliente se encargará de:

- Comunicar a GESNEXT si es necesario modificar o eliminar el acceso de algún miembro del personal del Cliente a los sistemas gestionados por GESNEXT.

GESNEXT se encargará de:

- Implementar medidas de control de acceso para proteger los activos de información.
- Implementar controles para la asignación de derechos de acceso con privilegios y la gestión segura de contraseñas.
- Autorizar y gestionar los ID y contraseñas de usuario desde su creación, provisión de acceso y hasta la eliminación de los derechos de acceso.
- Gestionar la segregación de los roles de control de acceso, es decir, la solicitud, la autorización y la administración del acceso.
- Aplicar un principio de "debe saberse" a los niveles de seguridad de la información durante la creación de los ID y eliminar los derechos de acceso cuando la necesidad de negocio finaliza de forma oportuna.
- Realizar revisiones de usuarios trimestrales para los empleados de GESNEXT.
- Revalidar la lista de los ID con privilegios anualmente.
- Aplicar reglas de contraseñas para las cuentas de usuario.
- Realizar los cambios de nivel de acceso necesarios al personal del cliente en los sistemas gestionados de GESNEXT de acuerdo con las instrucciones del cliente.
- Educar a los usuarios para mantener controles de acceso efectivos, incluyendo los requisitos para elegir contraseñas fuertes y mantener su confidencialidad.
- Restringir el acceso privilegiado y al código fuente de las aplicaciones a usuarios autorizados.

### 7.1 ID de usuario

A cada usuario se le asigna un ID de usuario exclusivo que lo identifica. La autoridad de acceso a los sistemas se basa en una necesidad de negocio actual y se controla verificando la identidad del usuario. Se proporciona acceso a usuarios, sistemas y aplicaciones solo a las zonas de red y servicios para los cuales han recibido autorización específica.

Está prohibido compartir el ID de usuario, excepto en las siguientes condiciones:

- La propiedad de un ID compartido se asigna a una persona individual.
- El propietario del ID es responsable de garantizar la responsabilidad individual cuando se comparte el id de usuario o la contraseña.
- El uso de un ID compartido no debe permitir al usuario acceder a información que el usuario no necesita conocer.

#### 7.1.1 Notificación de revocación por parte del gestor:

Cuando un usuario abandona la empresa, obtiene una excedencia y no se espera que vuelva a su empleo o bien ya no tiene una necesidad de negocio válida, el gestor del usuario debe notificarlo al administrador de ID de usuario. El administrador de ID de usuario dispone de un proceso o controles técnicos para impedir el acceso de dicho usuario al sistema tras la notificación del gestor.

- El acceso remoto a la red interna de GESNEXT se revoca en un plazo de 24 horas a partir de la fecha de separación.
- El acceso a los demás sistemas internos se revoca igualmente en un plazo de 24 horas desde su notificación por parte del gestor o el propietario del ID de usuario.

### 7.2 Contraseñas

Las reglas de contraseñas descritas en esta sección se aplican a todas las contraseñas utilizadas para verificar la identidad de los usuarios durante el inicio de sesión en los sistemas y subsistemas.

**Tabla 4 - Política de cuentas**

| Contraseñas | Requisito |
|---|---|
| Longitud mínima de la contraseña | 15 |
| Contienen como mínimo un carácter alfabético y uno no alfabético o un conjunto de al menos dos tipos de caracteres no alfabéticos | Sí |
| Contienen el ID de usuario como parte de la contraseña | No |
| Intervalo máximo de cambio (ver la nota a continuación) | 90 días |
| Número de cambios de contraseña para los cuales no se puede reutilizar la contraseña | 8 |
| Se establece una condición de expiración durante la emisión inicial o restablecimiento, si el sistema o el personal de soporte conocen el contenido de la contraseña | Sí |
| Contraseñas predeterminadas enviadas con los sistemas operativos y productos de programa para su uso durante la instalación/configuración del producto o sistema | Cambiar lo más pronto posible |
| Las contraseñas que no se hayan cambiado en el plazo de cambio arriba indicado, pero que están en condición de expiración | No infringen el requisito del plazo de cambio de contraseña. |

Notas:
Es posible que algunos ID de usuario no tengan contraseñas con plazo de expiración. Es posible que los sistemas, aplicaciones o repositorios de datos que requieran el uso de contraseñas para las comunicaciones directas, utilicen contraseñas sin plazo de expiración. No se admiten contraseñas sin plazo de expiración para sesiones de inicio de sesión interactivas (por ejemplo, personas individuales que inician sesión en el sistema o aplicación).

Cualquier modificación en estas políticas por parte del Cliente, será bajo su responsabilidad y previo acuerdo con GESNEXT, siempre que no afecte a otros posibles clientes.

#### 7.2.1 Protección de contraseñas:

**Tabla 5 - Protección de contraseñas**

| Protección de contraseñas | Recomendación |
|---|---|
| Transmisión de contraseñas | No deben transferirse en texto claro, cuando sea técnicamente posible. |
| Almacenamiento de contraseñas | Deben cifrarse, en caso posible, cuando se almacenen en archivos o bases de datos. Si no es posible cifrar, el acceso debe estar restringido a los administradores de seguridad del sistema. |

#### 7.2.2 Intentos de inicio de sesión no válidos:

**Tabla 6 - Intentos de inicio de sesión no válidos**

| Intentos de contraseña no válida | Requisito |
|---|---|
| Intentos consecutivos de inicio de sesión no válidos cuando los inicios de sesión están inhabilitados o retrasados (si es técnicamente posible) | Cinco para SAP y Meta4 |

### 7.2.3 Restablecimiento de contraseñas:

Se ha definido un proceso para restablecer contraseñas. El proceso incluye provisiones para la identificación positiva del solicitante y la nueva contraseña se envía al gestor.

### 7.3 Gestión de la autoridad administrativa de seguridad y del sistema

Se ha definido un proceso para gestionar las asignaciones de autoridad y para la eliminación puntual de la autoridad cuando finaliza la necesidad de negocio.

**Tabla 7 - Gestión de la autoridad administrativa de seguridad y del sistema**

| Gestión de la autoridad administrativa de seguridad y del sistema | Requisito |
|---|---|
| Aprobación por parte del propietario del Sistema o el Gestor de Servicios de TI para las asignaciones de autoridad administrativa | Obligatoria |
| Frecuencia de revisión de la autoridad administrativa | Anual |

### 7.4 Aislamiento de datos y aplicaciones para arrendatarios en centros de datos cloud

- Se implementan controles técnicos para aplicar el aislamiento a nivel de aplicaciones entre múltiples arrendatarios, de modo que la aplicación de un arrendatario no esté expuesta a otra y que el comportamiento de una no afecte a la otra.
- Se implementan controles técnicos (por ejemplo, cifrado) para aplicar el aislamiento a nivel de datos, de modo que los datos de un arrendatario se aíslen de otros arrendatarios.
- Se aplican políticas de control de acceso para garantizar la seguridad de los datos del cliente en entornos de múltiples arrendatarios.

## 8. Criptografía

GESNEXT se encargará de:

- Garantizar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

### 8.1 Cifrado de información confidencial

**Tabla 8 - Requisitos de cifrado**

| Cifrado | Requisito |
|---|---|
| Transmisión de datos confidenciales a través de Internet, redes públicas o dispositivos inalámbricos | Cifrar. |
| Claves criptográficas de clave secreta (también conocidas como claves compartidas o simétricas) | 128 bits de longitud como mínimo. |

| Cifrado | Requisito |
|---|---|
| Claves criptográficas de parejas de claves públicas/privadas (también conocidas como claves duales o asimétricas) | 2048 bits de longitud como mínimo. |

### 8.2 Controles de cifrado adicionales para centros de datos cloud

- Los datos sensibles se transmitirán entre aplicaciones que residen en sistemas operativos o contenedores virtuales distintos a través de canales cifrados y seguros. Algunos ejemplos de datos destinados a difusión pública y que no requieren cifrado durante su transmisión son:
  - páginas web de Internet que permiten el acceso sin autenticación, como http://www.gesnext.com,
  - información de diagnóstico como pings/trazadores de rutas de red, o
  - información en protocolos de hora de red, como NTP.
- Los flujos de datos entre subsistemas en el mismo sistema operativo o contenedor virtual no necesitan cifrado durante su transmisión. Solo deben cifrarse los datos que se transmiten entre uno o más conmutadores de red virtual o física.
- La información del cliente sensible, de acuerdo con lo indicado por el cliente y aceptado por GESNEXT, se cifra cuando se almacena (datos inactivos).

  - **8.3 Gestión de claves**
    En la política interna de seguridad de GesNext, se detalla cómo se debe transmitir y gestionar las claves de los diferentes sistemas. Las claves pueden protegerse mediante cifrado con algo que se acuerde con el usuario (por ejemplo, una clave pública o un secreto compartido como una contraseña).
  - Las claves también pueden protegerse ubicándolas en un sistema de almacenamiento separado, de manera que una vulnerabilidad técnica o una mala configuración en un sistema de almacenamiento no exponga las claves y los datos cifrados por las claves.

## 9. Seguridad física y del entorno

GESNEXT se encargará de:

- Proporcionar y gestionar la infraestructura y los controles de seguridad física en los centros de datos y las instalaciones. Se implementarán las siguientes medidas:
  - Controles de entrada física y procedimientos de trabajo, diseñados para permitir que solo el personal autorizado acceda en un área segura que contenga información crítica o sensible, oficinas, salas e instalaciones de procesamiento de la información.
  - Equipamiento para reducir los riesgos de amenazas ambientales, incluyendo averías eléctricas o daños en el cableado.
  - Designación de un propietario para gestionar la lista de accesos autorizados.
- Garantizar que los centros de datos estén protegidos ante factores ambientales como fuego, agua y calor mediante alarmas contra incendios, extintores, alarmas de humo y sistemas de supresión y extinción de incendios. Los centros de datos también están protegidos ante interrupciones o fallos del suministro eléctrico mediante sistemas de alimentación ininterrumpida (UPS) o de suministro eléctrico de emergencia (EPS), que se mantienen y prueban periódicamente.
- Garantizar que los equipos y la información no puedan desplazarse a otra ubicación, a menos que tengan la autorización pertinente y con la protección adecuada
- Implementar una política clara de pantallas y escritorios, incluyendo controles para equipos desatendidos.

### 9.1 Requisitos de control físico y de gestión para los centros de datos

Se han establecido controles en los centros de datos para limitar el acceso a los empleados cuyas tareas residen dentro del centro de datos y a otras personas con una clara necesidad de negocio de acceso. El gestor responsable del centro de datos, o la persona por él designada, aprueba todas las solicitudes de acceso permanente al centro de datos.

**Tabla 9 – Controles físicos y de gestión para los Centros de datos**

| Controles físicos en los Centros de Datos | Requisito |
|---|---|
| Acceso restringido y sólo desde el interior del edificio. | Sí |
| Propietario del área claramente identificado. | Sí |
| El área debe estar bloqueada, incluso cuando se están realizando tareas en su interior. | Sí |
| Se diseñan controles de acceso para limitar la entrada a personas autorizadas al área. Las personas que aparecen en la lista de accesos aprobados están autorizadas. | Sí |
| Las personas con acceso temporal proporcionado por una persona autorizada disponen de acceso autorizado de un solo uso. | Sí |
| Las personas con acceso autorizado deben tener un requisito de negocio actual para acceder y recibir autorización por parte del propietario del área. El propietario del área debe ser el que determine qué constituye un requisito de negocio y debe ser capaz de establecer dicha determinación. | Sí |
| Proceso definido para revocar el acceso regularmente mediante solicitud o de forma implícita al cese del empleo. | Sí |

# 10. Seguridad de las operaciones

El Cliente se encargará de:

- Instalar software antivirus y actualizaciones de software del antivirus para los servidores Windows del Cliente en las instalaciones del cliente
  - Actualizar las firmas de virus diariamente en los servidores con acceso de red al servidor de actualización de firmas de virus.
  - Responder a ataques de virus e iniciar medidas correctivas.
- Implementar parches para los sistemas bajo la gestión del Cliente de acuerdo con las políticas de seguridad del Cliente.

GESNEXT se encargará de:

- Implementar procedimientos operativos estándar para las instalaciones de procesamiento de la información.
- Separar los entornos de producción y los de no producción para impedir el acceso no autorizado o cambios en los activos de información.
- Implementar políticas y procedimientos para aplicar cambios en los sistemas de producción.
- Gestionar los sistemas y los dispositivos de red para garantizar que la capacidad cumpla con los requisitos de negocio actuales y futuros.
- Implementar procedimientos de copia de seguridad de conformidad con los requisitos de negocio.
- Recopilar registros de seguridad del sistema, cuando sea técnicamente viable, de las actividades que requieren acceso con privilegios y mantener los registros durante 90 días, así como revisarlos periódicamente.
- Aplicar medidas de control de acceso para impedir el acceso no autorizado a los archivos de registro.

- Utilizar mecanismos de protección ante código malicioso en los puntos de entrada y salida de información del sistema de herramientas y/o aplicaciones para detectar y erradicar código malicioso en correos electrónicos/archivos/archivos adjuntos.
- Instalar software antivirus y actualizaciones de software del antivirus para los servidores MS Windows
    - Actualizar las firmas de virus:
        - diariamente en los servidores con acceso de red al servidor de actualización de firmas de virus
        - semanalmente en otros servidores conectados a la red con el sistema operativo MS Windows
    - Responder a ataques de virus e iniciar medidas correctivas
- Desplegar controles automatizados para detectar y bloquear correos electrónicos sospechosos a fin de minimizar el riesgo de infección y propagación de malware, así como tomar las medidas adecuadas. Las medidas de mitigación pueden incluir la inspección del correo electrónico en el entorno de GESNEXT (o de un socio aprobado de GESNEXT) y realizar acciones correctivas, incluyendo la eliminación del malware o la supresión del correo electrónico/archivo adjunto afectado, en caso necesario.
- Restringir la instalación de software en sistemas operativos.
- Implementar parches en sistemas según el plazo indicado posteriormente de acuerdo con el proceso de gestión de cambios.
- Realizar exploraciones de vulnerabilidades TCP/IP en servidores y dispositivos según la frecuencia indicada posteriormente en la “Tabla 11- Exploración de vulnerabilidades TCP/IP”.

### 10.1 Proceso de Gestión de Parches

Se ha definido un proceso para instalar parches de aviso de seguridad dentro de los plazos especificados en la siguiente tabla. Los plazos comienzan a partir de la fecha de publicación de la corrección en el sitio web del fabricante.

**Tabla 10 - Plazos para la instalación de parches/correcciones**

| **Nivel de seguridad** | **Sistemas y dispositivos accesibles desde Internet** | **Sistemas y dispositivos no accesibles desde Internet** |
|---|---|---|
| **Gravedad crítica** | **24 horas** | **7 días** |
| **Gravedad alta** | **7 días** | **14 días** |
| **Gravedad media** | **14 días** | **45 días** |
| **Gravedad baja** | **30 días** | **90 días** |
| | | |
| | | |
| | | |
| | | |

Si no se puede instalar un parche dentro del plazo requerido, el propietario del sistema deberá iniciar el proceso de aceptación de riesgo. Sin embargo, si no se puede completar la instalación de un parche, el propietario del sistema puede o bien aceptar la existencia del riesgo y realizar medidas de control o bien proceder a apagar el sistema dentro de los siguientes 14 días naturales tras la fecha prevista original.

### 10.2 Exploración de vulnerabilidades TCP/IP

El objetivo de la exploración de vulnerabilidades TCP/IP para servidores y dispositivos de infraestructura de red es el de determinar si existen posibles vulnerabilidades o exposiciones de seguridad en los sistemas y si se toman las medidas correctivas apropiadas a tiempo.

**Tabla 11 - Exploración de vulnerabilidades TCP/IP**

| Exploración de vulnerabilidades | Requisito |
|---|---|
| Frecuencia de la exploración para interfaces conectadas a Internet desde Internet | Semanal |
| Frecuencia de la exploración para los demás sistemas de producción | Mensual |
| Prueba de realización de la exploración de vulnerabilidades | Las dos últimas iteraciones |
| Plazos de corrección | De acuerdo con la tabla 10 |

### 10.3 Activación del Servicio

Las pruebas de activación del servicio deben realizarse antes de poner los recursos a disposición general a fin de verificar que los parámetros del sistema están establecidos de acuerdo con los requisitos del presente documento.

### 10.4 Intentos de Acceso a Registros para Sistemas

Los registros que documentan el acceso a sistemas, recursos o funciones seleccionadas, cuando sea técnicamente viable, se crean y conservan, de conformidad con las siguientes especificaciones.

**Tabla 12 - Creación de registros**

| Registros | Recomendación |
|---|---|
| **Registros de Acceso al Sistema** - Intentos de inicio de sesión | Todos los satisfactorios y no satisfactorios |
| **Registros de Actividad de Usuarios con Privilegios** - Administrativo de Seguridad o Autoridad del Sistema | Acciones del registro utilizados para cambiar los Recursos del Sistema Operativo y para cambiar el estado de la seguridad |
| Retención del registro | 90 días |

# 11. Seguridad de las comunicaciones

GESNEXT se encargará de:

- Gestionar los componentes de la infraestructura de seguridad de red utilizados para la conexión de las redes del Cliente y GESNEXT.
- Definir los acuerdos de servicio de red con el proveedor de servicios de red para garantizar los niveles de servicio y seguridad adecuados, así como una gestión eficiente.
- Segregar las redes según la clasificación de seguridad de los activos de información e implementar los controles de seguridad apropiados.
- Realizar las actividades habituales en los equipos de red de forma segura, incluyendo comprobaciones de estado, gestión de ID, establecimiento de parches, exploración de vulnerabilidades y gestión de cambios.
- Inhabilitar cualquier servicio innecesario en todos los dispositivos de red
- Restringir el acceso a los usuarios generales, aparte del acceso que necesiten para proporcionar el servicio de red.
- Gestionar las Listas de Control de Acceso (ACL), si estuvieran disponibles, en todos los dispositivos de red para bloquear tráfico no deseado.
- Garantizar la transferencia segura de información a/desde terceros, incluyendo mensajería electrónica.

### 11.1 Segmentación de red

Las redes físicas y lógicas se segmentan en zonas y se asignan sistemas informáticos y de almacenamiento a las distintas zonas en función de la conectividad, el valor de los activos y criterios de gestión de riesgos. Todas las zonas requieren separación entre ellas en la capa de red.

- El acceso a las interfaces administrativas está limitado a los usuarios autorizados con privilegios
  - El acceso se basa en la autenticación del usuario individual, y solo se otorgará un usuario con privilegios, cuando haya un requisito de negocio.
  - Ningún usuario general puede acceder a las interfaces administrativas.
- Todas las zonas deben estar ubicadas en dominios de difusión separados (por ejemplo, VLAN separadas), a menos que se utilicen controles para filtrar la comunicación dentro del dominio de difusión.
- Los controles de acceso a la red, como los cortafuegos, se implementan para acceder de forma segura a una zona desde cualquier otra zona
- Se pueden utilizar pasarelas en la capa de la aplicación en lugar de controles en la capa de red.

**Tabla 13 - Controles de seguridad de red**

| Controles de seguridad de red | Requisito |
|---|---|
| Comprobaciones periódicas de estado | Sí. Consulte la sección 16.1 para conocer los requisitos de las comprobaciones de estado |
| Gestión de ID y accesos | Sí. Consulte la sección 7 para conocer los requisitos de la gestión de ID y accesos |
| Parches del sistema | Sí. Consulte la sección 10.1 para conocer los requisitos de los parches |
| Exploración de vulnerabilidades TCP/IP | Sí. Consulte la sección 10.2 para conocer los requisitos de la exploración de TCP/IP e ID |
| Registro de actividades | Sí. Consulte la sección 10.4 para conocer los requisitos del registro de actividades |

### 11.2 Requisitos de registros adicionales para dispositivos de red

Los registros que documentan el acceso a sistemas, recursos o funciones seleccionadas, cuando sea técnicamente viable, se crean y conservan, de conformidad con las siguientes especificaciones.

**Tabla 14 - Registros de red**

| Registros | Recomendación |
|---|---|
| Registrar toda asignación y publicación satisfactoria de direcciones IP de red, si el dispositivo proporciona un sistema de gestión de direcciones de red, como DHCP. | Fecha del registro, Hora, Dirección IP de Origen/Destino, protocolo IP y Servicio TCP/IP (tipo de registro o número de puerto de aplicación) |
| Registrar todos los sucesos de iniciación y finalización de sesión, satisfactorios y no satisfactorios, asociados a los flujos de tráfico entre zonas seguras. | Sí |

### 11.3 Acceso remoto

**Tabla 15 - Acceso remoto**

| Acceso remoto | Requisito |
|---|---|
| Acceso remoto a servicios del sistema IT | Permitido únicamente a través de una pasarela segura aprobada por GesNext y sólo para usuarios autorizados con una necesidad de negocio válida. |

### 11.4 Cortafuegos

#### 11.4.1 Reglas de filtro/ACL

Las reglas de filtro/ACL definen los tipos de tráfico que se permitirán a través del entorno del cortafuegos. Los detalles de estos filtros variarán para cada instalación, y podrán estar sujetos a modificaciones.
Por motivos de seguridad, las reglas del cortafuegos de un entorno compartido no se pueden personalizar en función de los requisitos específicos del cliente ni estarán disponibles para revisión.

**Tabla 16 - Requisitos de las reglas de filtrado**

| Reglas de filtro | Requisito |
|---|---|
| Revisión inicial de la regla de filtro del cortafuegos | Antes de la activación del servicio |
| Revisión posterior de la regla de filtro | Durante el proceso de comprobación del estado de la seguridad, al menos una vez al año |
| Cualquier cambio en el cortafuegos | Se seguirá un proceso de gestión de cambios formal |
| Tráfico a través del cortafuegos | Denegar todo de forma predeterminada, a menos que se permita explícitamente |
| Filtros anti-spoofing | Habilitados |

# 12. Adquisición, desarrollo y mantenimiento de sistemas

**GESNEXT se encargará de:**

- Si procede, separar los entornos de desarrollo y pruebas (incluido el uso de Datos Personales) del entorno de producción
- Crear nuevos sistemas para las especificaciones de seguridad, de acuerdo con lo definido en el presente documento
- Recopilar, analizar y documentar los requisitos de seguridad, al tiempo que se desarrollan nuevas soluciones o se mejoran las existentes
- Implementar los controles necesarios para desplegar una aplicación de forma segura
- Garantizar que las aplicaciones estén configuradas con seguridad de manera predeterminada
- Garantizar que todos los cambios en los sistemas nuevos y los cambios significativos en los sistemas existentes estén documentados, probados, aprobados e implementados de forma controlada.

# 13. Relaciones con los proveedores

GESNEXT se encargará de:

- Coordinar las actividades de seguridad con terceros contratados por GESNEXT
  - Evaluar la capacidad del Proveedor de cumplir con los requisitos de seguridad establecidos en el contrato con el Cliente.
  - Ejecutar el acuerdo de seguridad de GesNext o acordar términos y condiciones similares dentro del Acuerdo de Contratación de GESNEXT aplicable con el proveedor.
  - Si así se estipula en el contrato, transmitir los requisitos de Seguridad del Cliente al proveedor.

# 14. Gestión de los incidentes relativos a la seguridad de la información

El Cliente se encargará de:

- Proporcionar un plan de contacto para notificar los incidentes de seguridad
- Ser responsable de determinar si un incidente de seguridad ha derivado en una infracción de la privacidad
- Informar a GESNEXT sobre cualquier incidente de seguridad en los sistemas gestionados por el Cliente que podría afectar a la red o los sistemas gestionados por GESNEXT
- Tomar decisiones sobre las acciones necesarias para resolver los incidentes de seguridad relacionados con la red del Cliente, los sistemas del Cliente, el personal del Cliente o los datos del Cliente, incluyendo, si procede, la recopilación de pruebas

GESNEXT se encargará de:

- Implementar procedimientos para gestionar incidentes y vulnerabilidades de seguridad, que incluyen los requisitos para identificar, notificar, evaluar, responder y aprender de los incidentes.
- Disponer de una línea de ayuda o contacto por correo electrónico para notificar incidentes o sucesos.
- Ayudar al Cliente en la evaluación inicial del incidente.
- Informar al Cliente de cualquier incidente de seguridad importante identificado en sistemas utilizados para la prestación de servicios al Cliente.
- Tomar decisiones sobre las acciones necesarias para resolver los incidentes de seguridad relacionados con la red de GESNEXT, los sistemas de GESNEXT, el personal de GESNEXT o los datos de GESNEXT, incluyendo, si procede, la recopilación de pruebas.

# 15. Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

- GesNext evalúa sus servicios y dictamina la severidad de los mismos. De acuerdo a esta valoración, establece un plan para asegurar la continuidad del negocio. Se documentará con cada cliente una planificación propia si así se acuerda.

# 16. Cumplimiento

GESNEXT se encargará de:

- Implementar los requisitos de seguridad de la información, en relación con todos los requisitos legislativos, reglamentarios, normativos y contractuales pertinentes.
- Realizar revisiones de seguridad de los sistemas para validar el cumplimiento con las Especificaciones Técnicas de acuerdo con la frecuencia definida en la tabla 17.
- Desarrollar e implementar planes de acción para los resultados de las auditorías de seguridad de los cuales es responsable GESNEXT.

### 16.1 Comprobación del estado de la seguridad de los sistemas

Todos los sistemas se someten a comprobaciones periódicas del estado de la seguridad. Cualquier desviación de los resultados esperados o necesarios que se detecte en el proceso de comprobación del estado de la seguridad se corregirá dentro de un plazo definido.

- Salvo que se especifique lo contrarioen el contrato, las Comprobaciones de Seguridad del Sistema podrán realizarse en una muestra de sistemas
  - Las comprobaciones verificarán que:
    - Únicamente los usuarios aprobados cuenten con autoridad administrativa de seguridad o del sistema.
    - La protección anti-virus sea funcional y esté operativa en los servidores soportados.
    - Estén establecidos los controles técnicos para aplicar la política de contraseñas del sistema operativo.
    - Se recopilen los registros de acceso con privilegios y actividades de inicio y cierre de sesión, si es técnicamente viable, tal y como se define en las Especificaciones Técnicas.

**Tabla 17 - Comprobación del estado del sistema**

| Comprobación del estado del sistema | Requisito |
|---|---|
| Todos los sistemas y servicios | Se someterán a una comprobación del estado de la seguridad antes de la activación inicial del servicio |
| Pruebas de haber realizado la comprobación inicial de estado | Se conservan durante un año |
| Frecuencia de la comprobación de estado para sistemas y dispositivos de red conectados a Internet | Anual |
| Frecuencia de la comprobación de estado para los demás sistemas y dispositivos de red | Semestral |
| Pruebas de haber realizado la Comprobación de Estado | Se conservan las dos últimas iteraciones |

# A. Controles de seguridad para las estaciones de trabajo del usuario final bajo la gestión de GESNEXT

Deben activarse los siguientes controles de seguridad en todas las estaciones de trabajo para garantizar la protección ante el robo de información del cliente sensible almacenada en el dispositivo:

- Activar el cifrado de disco completo en las estaciones de trabajo del usuario final.

- Establecer un bloqueo de pantalla/teclado protegido por contraseña que se active automáticamente tras un periodo de inactividad. El periodo de inactividad establecido no debe ser superior a los 30 minutos.

  La contraseña debe:

  1. Tener una longitud de 15 posiciones
  2. Contener una combinación de caracteres alfabéticos y no alfabéticos (números, puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos
  3. No contener el ID de usuario como parte de la contraseña

- Instalar y ejecutar un programa antivirus aprobado por GesNext en la estación de trabajo.

- Instalar y ejecutar un programa de cortafuegos del Cliente aprobado por GesNext en la estación de trabajo.

- Los empleados que utilicen sistemas operativos de Microsoft Windows deben instalar los parches de alta gravedad requeridos por el CIO de GesNext en sus respectivas versiones en un plazo de 30 días desde la fecha de publicación.

- Los sistemas operativos usados en los equipos de los empleados de GesNext, se encuentran debidamente actualizados según los plazos indicados en la siguiente tabla:

| **Nivel de seguridad** | **Sistemas y dispositivos no accesibles desde Internet** |
|---|---|
| **Gravedad crítica** | **7 días** |
| Gravedad alta | 14 días |
| Gravedad media | 45 días |
| Gravedad baja | 90 días |

# B. Dispositivos móviles y teletrabajo (NO aplicable, ni acordado con el cliente)

**Controles en dispositivos móviles y teletrabajo* (solo aplicado al Teletrabajo)**

**Tabla 18: Controles en dispositivos móviles y teletrabajo**

| Requisitos del control | Valor |
|---|---|
| Registro de dispositivos móviles con sistema de inventario central | Sí |
| Requisitos para la protección física de dispositivos móviles | Sí |
| Restricción de la instalación de software (solo para dispositivos de escritorio/portátiles destinados al teletrabajo) | Sí |
| Deben ejecutar una versión de sistema operativo y una configuración de parches aprobadas por GESNEXT para cualquier dispositivo móvil | Sí |
| Deben contar con controles de complejidad de contraseña y un protector de pantalla automático protegido por contraseña | Sí |
| Instalar una solución de cifrado de disco completo o una solución de cifrado de aplicaciones aprobada | Sí |
| Instalar y ejecutar un programa antivirus aprobado por GESNEXT en el dispositivo móvil (solo para dispositivos de escritorio/portátiles destinados al teletrabajo). | Sí |

*Esta sección solo se aplicará si en el MSA se acuerda que existe una necesidad de negocio para acceder a los datos del Cliente utilizando dispositivos móviles y/o durante el teletrabajo.

# C. Controles de seguridad de las aplicaciones

## Ámbito:

| | |
|---|---|
| **Categorías de Aplicaciones dentro del ámbito del presente documento** | Aplicaciones bajo la Gestión de GesNext que dan soporte al procesamiento o almacenamiento de Datos del Cliente |

## A. Control de acceso

GESNEXT implementará los siguientes controles:

| Controles de seguridad de las aplicaciones | Valor requerido |
|---|---|
| Id de usuario | Se utiliza un identificador exclusivo asociado a cada usuario de una aplicación. |
| Supresión del id de usuario | ▪ Cuando surja la necesidad de eliminar el acceso de un usuario, se realizará dicha baja en un plazo de 24 horas desde la comunicación, no pudiendo reutilizarse dicho ID. Cuando sea un usuario del cliente, el responsable en notificar dicha baja es el propio cliente. |
| Usuarios genéricos del sistema | Asignado de forma predeterminada al responsable de GesNext de la aplicación, a menos que se asigne formalmente a otras personas autorizadas, tales como administradores de la aplicación |
| Reasignación de la propiedad de los usuarios genéricos de la aplicación | Cualquier cambio en la asignación de usuarios genéricos, debe ser notificado y aprobado por el responsable de la aplicación (o sistema). Si el responsable de la aplicación cambiase, deberán ser reasignados los usuarios genéricos al nuevo responsable.<br><br>Los usuarios genéricos de la aplicación están exentos de eliminación si dicha eliminación provocara un fallo de la aplicación. |
| Uso compartido de usuarios de la aplicación | Prohibido, salvo que se mantenga la responsabilidad individual con justificación de negocio y esté aprobado por la dirección ejecutiva. |
| Revalidación de usuarios de las aplicaciones | Trimestral |
| Pruebas de la realización de la revalidación de usuarios y registro de las medidas correctivas | Conservar la revalidación actual y la anterior |
| Verificación de la identidad de todos los usuarios (autenticación) cuando intentan iniciar sesión en la aplicación | Obligatoria |

| **Contraseñas** | **Valor requerido** |
|---|---|
| Longitud mínima de la contraseña | 15 |
| Contienen como mínimo un carácter alfabético y uno no alfabético o un conjunto de al menos dos tipos de caracteres no alfabéticos | Sí |
| Intervalo máximo de cambio | 90 días |
| Número de cambios de contraseña para los cuales no se puede reutilizar la contraseña | 8 |
| Se establece una condición de expiración durante la emisión inicial o restablecimiento, si el sistema o el personal de soporte conocen el contenido de la contraseña | Sí |
| Contraseñas predeterminadas incluidas con los sistemas operativos. Productos de programa para utilizar durante la instalación/configuración del sistema y producto | Cambiar tras el primer acceso. |
| Las contraseñas que no se hayan cambiado en el plazo de cambio arriba indicado, pero que están expiradas. | No infringen el requisito del plazo de cambio de contraseña |
| La contraseña tiene una antigüedad mínima conforme al intervalo mínimo permitido por la plataforma, pero no menos de un día | Sí |
| Transmisión de contraseñas | En la medida de lo posible, no deben transferirse en texto claro. No se deben divulgar. Cuando se deba transmitir la contraseña por un canal escrito, no se realizará la trasmisión incluyendo en el mismo correo electrónico usuario y contraseña. |
| Almacenamiento de contraseñas | Deben cifrarse, en caso posible, cuando se almacenen en archivos o bases de datos. Si no es posible cifrar, el acceso debe estar restringido a los administradores de seguridad del sistema. |

| **Contraseñas sin plazo de expiración:** | **Valor requerido** |
|---|---|
| Contraseñas sin plazo de expiración | Se utilizan solo para comunicaciones directas entre aplicaciones, se evitan en los inicios de sesiones interactivas (por ejemplo, los inicios de sesión individuales a la aplicación) y la autoridad con privilegios no |

| | |
|---|---|
| | se asigna al id de usuario, si es técnicamente posible. |

| **Certificados** | **Valor requerido** |
|---|---|
| Certificados Digitales | Los Certificados Digitales son emitidos por una Autoridad de Certificados aprobada por GesNext |
| Uso de certificados autofirmados | Restringido, solo para las comunicaciones entre aplicaciones o repositorios de datos y no se permite en Internet o para sistemas de Cliente.<br><br>Se requiere un proceso documentado y demostrable para gestionar y proteger la clave privada de la Autoridad de Certificados autogestionada. |

| **Solicitudes de acceso y necesidad de negocio** | **Autorizaciones y frecuencia de controles** |
|---|---|
| Acceso a una aplicación, que maneje Información Confidencial del Cliente o Proveedor. | A demanda. Autorización del responsable de GesNext y del contacto del cliente y en base a una necesidad de negocio. |
| Acceso a una aplicación, que no maneje Información Confidencial del l Cliente o Proveedor. | A demanda. Autorización del responsable de GesNext y en base a una necesidad de negocio |
| Revalidación de la lista de control de acceso de usuarios de las Aplicaciones para una necesidad de negocio continuada. | Anual. Realizado por el equipo de GesNext. |
| Prueba de la revalidación con registro de medidas correctivas | Año actual más la del año anterior |

| **Gestión de los usuarios privilegiados** | **Valor recomendado** |
|---|---|
| Aprobación para asignaciones de usuarios privilegiados | Obligatoria por parte del Director de sistemas y BPO d ela aplicación. Debe existir una necesidad de negocio. |
| Frecuencia de revisión de los usuarios privilegiados | Anual |
| Prueba de la revalidación de la autoridad administrativa | Año actual más la del año anterior |

## B. Gestión de Comunicaciones y Operaciones

GESNEXT implementará los siguientes controles:

| Cifrado | Valor requerido |
|---|---|
| Transmisión de Datos del Cliente y Confidenciales del Proveedor a través de Internet | Cifrados |
| Servidores web que muestran los Datos del Cliente y Confidenciales del Proveedor | TLS según esttándar de IBM |
| Claves de cifrado | Longitud mínima de clave de 128 bits para códigos de clave secreta, y 2048 bits para algoritmos de clave pública |

| Registro de actividades | Valor requerido |
|---|---|
| Registros de auditoría | Creados para los intentos de inicio de sesión satisfactorios y no satisfactorios y actividades realizadas utilizando usuarios privilegiados de seguridad |
| Periodo de retención de los registros de auditoría | 90 días |

## C. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

GESNEXT implementará los siguientes controles:

| Control | Valor recomendado |
|---|---|
| Exploración antivirus en el entorno de desarrollo de aplicaciones para garantizar que no se haya introducido ningún virus durante la fase de implementación o pruebas del desarrollo | Obligatoria |
| El propietario de la aplicación y/o sistema operativo se suscriben a los avisos de Parches del Proveedor para recibir notificaciones por correo electrónico sobre parches disponibles | Sí |
| Para productos sin soporte directo del proveedor, los propietarios de la aplicación y/o sistema operativo supervisan mensualmente los sitios web del proveedor de la aplicación y los servicios de boletines para identificar correcciones en la seguridad de la aplicación | Sí |
| El propietario de la aplicación y/o sistema operativo evalúan el riesgo y la gravedad de cualquier corrección en la seguridad de la aplicación, siempre siguiendo las indicaciones del proveedor. | Sí |
| Plazos para corregir las exposiciones de seguridad de la aplicación | i) Gravedad crítica – 24 h. para sistemas accesibles desde internet y 7 días para el resto.<br>ii) Gravedad alta – 7 días. para sistemas accesibles desde internet y 14 para el resto.<br>iii) Gravedad media - 14 días. para sistemas accesibles desde internet y 45 para el resto |

| | |
|---|---|
| | iv) Gravedad baja - 7 días. para sistemas accesibles desde internet y 90 días para el resto |
| Código de la aplicación | La codificación no contiene trampas ni puertas traseras |
| Modificaciones en la aplicación | Admitidas según el proceso de gestión de cambios de GesNext. |
| Modificaciones en los entornos de producción, aceptación y pruebas realizadas por los Desarrolladores | Restringidas |
| Pruebas de activación del servicio | Realizadas antes de poner los recursos de la aplicación a disposición general |
| El propietario de la aplicación y/o sistema operativo revisan la aplicación para verificar el cumplimiento del Estándar de Seguridad de las Aplicaciones | Antes de llevar la aplicación a producción |
| Resueltas todas las exposiciones identificadas durante las pruebas de activación inicial del servicio | Antes de añadir usuarios generales o poner el servicio a disposición general u operativo |
| Pruebas de la confirmación del proceso de activación del servicio | Se conservan durante un año |

## D. Cumplimiento

GESNEXT implementará los siguientes controles:

| **Comprobación de estado** | **Valor recomendado** |
|---|---|
| Frecuencia de la ejecución de controles. | Anual. |
| Conservación de evidencias. | Las dos últimas iteraciones. |
| Parámetros del control de acceso. | Verificar que estén establecidos de conformidad con los estándares de IBM. |
| Usuarios privilegiados de la aplicación y/o sistema operativo. | Garantizar que solo tengan estos permisos los usuarios aprobados. |
| Registros de actividades y acceso | Verificar que existen los registros, siempre que sean técnicamente viables |
| Desviaciones de las comprobaciones de estado que no se pueden corregir de acuerdo con las frecuencias de exploración establecidas | Se notifica al Cliente y al gestor del Proveedor si hubiese, que dichas desviaciones no se pueden corregir dentro del plazo especificado |
| Plazo para las medidas correctivas | Según indicado en el anterior apartado |

# D. Obligaciones del GDPR para GESNEXT

<LOS REQUISITOS DE ESTE APÉNDICE ("D. Obligaciones del GDPR para GESNEXT") SE APLICARÁN A PARTIR DEL 25 DE MAYO DE 2018.>

**GESNEXT se encargará de:**

- Almacenar y archivar la documentación relacionada con el compromiso en un repositorio seguro
- Evaluar las repercusiones de los cambios en el contrato sobre el Procesamiento de los Datos Personales del Cliente y actualizar este documento según proceda
- Realizar evaluaciones previas y disponer de Acuerdos de confidencialidad (NDA) firmados por el personal del proyecto según proceda
- Firmar acuerdos escritos con todos los Sub-procesadores para imponerles obligaciones similares a las definidas en el DPA, principalmente proporcionando suficientes garantías para implementar las medidas técnicas y organizativas adecuadas
- Realizar revisiones periódicas de los requisitos del presente documento
- Garantizar que los Datos Personales se procesen únicamente según lo acordado en el DPA
- Crear y mantener un inventario de Datos Personales del Cliente
- Almacenar y eliminar los Datos Personales del Cliente de conformidad con las medidas acordadas
- Gestionar los accesos con privilegios y los ID de usuario compartidos de acuerdo con los controles definidos en el presente documento
- Gestionar el acceso a los archivos de registro de acuerdo con los controles definidos en el presente documento
- Suprimir y devolver de forma segura todos los Datos Personales del Cliente de conformidad con los estándares acordados en el DPA
- Separar los entornos de desarrollo y pruebas (incluido el uso de Datos Personales) del entorno de producción
- Establecer y adherirse al proceso de cambios de sistemas y aplicaciones
- Implementar procesos de validación y pruebas para garantizar que solo pasen a producción los cambios autorizados.

# E. Centros de delivery y centros de datos dentro del ámbito

La siguiente lista enumera los centros de datos donde tiene alojado GesNext sus servidores que se incluyen en el ámbito del presente documento.

| Organización | País | Centro de distribución | Dirección |
|---|---|---|---|
| GesNext España | España | Madrid | Edificion Gorbea IV Avda. Bruselas 20 Alcobendas, Madrid, 28108 Madrid |
| NTT | España | Coslada | Premium Data Center NTT C\ Yécora 4, 28022 Madrid |
| Telefónica | España | Madrid | Distrito Telefónica Ronda de las Comunicaciones s/n Edificio Oeste 2, 28050 Madrid |
| NTT | Francia | París | 7-9 rue Petit 92582 Clichy Cedex Francia |

# F. Excepciones aprobadas por las TOM

La siguiente tabla muestra las adiciones, modificaciones y supresiones realizadas en el requisito de las medidas técnicas y organizativas estándar.

| Sección de las TOM | Detalles del cambio | Aprobador de Seguridad de GESNEXT | Fecha de aprobación |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# G. Control de documentos de TOM

| | |
|---|---|
| **Nombre del documento:** | TOMs - Clientes |
| **Identificación del documento:** | Version 4.0 |
| **Identificación del propietario:** | Manuel Machuca, GesNext, IT |
| **Autor:** | Manuel Machuca (manuel.machucamunoz@gesnext.com) |
| **Resumen de cambios:** | 21/03/18 – Versión incial<br>10/12/19 – Revisión anual<br>21/02/2020 – Modificaciones globales |

| | |
|---|---|
| | 18/02/2021 – Modificación Sección Cumplimiento |
| **Aprobación del documento:** | Las siguientes personas aprobarán los cambios realizados en este documento:<br>Representante del Cliente: Nombre, Organización, Departamento<br>Representante de la Oficina del Proyecto de GESNEXT: Manuel Machuca, GesNext, IT<br>Prestación de servicios: Nombre, GesNext, Departamento |
| **Plan de revisión:** | Este documento deberá ser revisado por todas las partes periódicamente, en conformidad con el plazo acordado en el MSA. Se revisarán todas las diferencias entre las especificaciones del cliente y las directrices de GESNEXT. Si todos los encargados de aprobar el documento llegan a un acuerdo, podrá omitirse la revisión.<br>La siguiente revisión será: 02/2021 |
| **Nivel más reciente:** | Dónde encontrar la documentación más actualizada:<br>Póngase en contacto con Manuel Machuca (manuel.machucamunoz@gesnext.com) para solicitar la copia más reciente. |
| **Versión anterior:** | La versión anterior del presente documento deberá conservarse hasta que se implementen todos los cambios en esta versión o tras un periodo de 12 meses, optando siempre por el periodo más largo. |
| **Distribución:** | Las copias del presente documento podrían quedar obsoletas. Es obligación del usuario verificar que está utilizando la versión más actualizada. El presente documento no deberá ser utilizado cuando esté obsoleto. |

# H. Glosario

**Personal del Cliente**
Empleados, contratistas y subcontratistas del Cliente

**Personal de GESNEXT**
Empleados, contratistas y subcontratistas de GESNEXT

**Sistemas y dispositivos de infraestructura de red**
Controladores de comunicaciones de red, puentes, pasarelas, condensadores de fluzo, repetidores, direccionadores, conmutadores, hubs de cableado, salas de cables, LAN, servidores DNS y DHCP

**Medios de almacenamiento portátiles**
Cintas magnéticas y cartuchos y discos magnéticos u ópticos extraíbles

**Información residual**
La información residual es la información procesable que permanece en medios de almacenamiento desde antes de su uso.

**Riesgo**
La combinación de la probabilidad de que se produzca un suceso y su consecuencia – el impacto potencial de un suceso en el cual una amenaza concreta explota una vulnerabilidad determinada

**Aviso de Integridad/Seguridad**
Un Aviso de Integridad/Seguridad es una advertencia de una exposición en un programa o proceso que permite a usuarios no autorizados obtener autoridad con privilegios en un sistema, eludir los controles de acceso u obtener acceso no autorizado a los datos. Debe seguirse un proceso de Aviso de Integridad/Seguridad para instalar las correcciones. Los requisitos principales para este proceso son:

- Determinación de la gravedad del riesgo en base al grado de vulnerabilidad y la categoría de la explotación.
- Notificación de la disponibilidad de la corrección.
- Procedimiento para determinar la planificación para la aplicación de las correcciones de seguridad/integridad. Solo se instalarán los avisos con correcciones disponibles.

**Controles de seguridad**
Procesos, procedimientos, estructuras organizativas o funciones de hardware y software que ofrecen medios para gestionar el riesgo

**Incidente de seguridad**
El acceso sospechado, intentado o real de terceros no autorizados o la adquisición de información confidencial.

**Política de seguridad**
Declaración de alto nivel de los objetivos, principios y responsabilidades de gestión para la seguridad

**Servicios de seguridad**
En el contexto de las medidas técnicas y organizativas, los elementos seleccionables del catálogo de servicios de GESNEXT que proporcionan uno o más tipos de controles de seguridad

**Herramientas de software**

Sistemas de software de middleware y base de datos que incluyen controles de seguridad utilizados para gestionar las funciones operativas de TI

**Sistemas**
Mainframes, servidores de rango medio y dispositivos de red

**Autoridad Administrativa de Seguridad y del Sistema**
**Autoridad del Sistema:** La autoridad otorgada a una persona individual mediante la asignación de atributos, privilegios o derechos de acceso asociados a los sistemas operativos, y que son necesarios para realizar las actividades de mantenimiento y soporte del sistema
**Autoridad Administrativa de Seguridad:** La autoridad otorgada a una persona individual mediante la asignación de atributos o privilegios asociados a los sistemas de control de acceso, y que son necesarios para establecer y administrar controles de seguridad en todos los sistemas
Nota: En algunas instancias, la misma persona puede ejercer múltiples funciones para el mismo sistema

**Especificaciones Técnicas**
Controles de seguridad para implementar estándares específicos de una plataforma tecnológica, sistema operativo o herramienta de software. Las Especificaciones Técnicas describen los parámetros de configuración que habilitan o aplican los controles acordados en las medidas técnicas y organizativas para una tecnología o implementación de arquitectura determinada

**Amenaza**
Una circunstancia o suceso con el potencial de causar daños a un recurso de TI en forma de destrucción, divulgación, modificación de datos o Denegación del Servicio (DoS)

**Vulnerabilidad**
Una debilidad en un sistema de información o sus componentes (por ejemplo, procedimientos de seguridad del sistema, diseño de hardware, controles de acceso de software, controles internos) que podría ser explotada.