netboss
COMUNICACIONES

Successful projects made with talent, technology and passion.

SGSI D51 01 Política de seguridad de la información

Santander (ES), a 25 de junio de 2026
Versión 1.11

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

www.netboss.es

Consultar Certificaciones: netboss.es/certificaciones

Control de versiones

Control de versiones			
Fecha	Autor	Versión	Cambios
29/12/2017	Dirección de sistemas de gestión	1.0	Versión inicial
08/02/2019	Dirección de sistemas de gestión	1.1	Actualización puntos 1.8, 2.5, 3.2 y 3.3
05/07/2019	Dirección de sistemas de gestión	1.2	Actualización punto 3.1
16/09/2019	Dirección de sistemas de gestión	1.3	Actualización de formato
23/07/2020	Dirección de sistemas de gestión	1.4	Actualización punto 3.1 y organigrama
04/03/2021	Dirección de sistemas de gestión	1.5	Actualización de organigrama
22/02/2022	Dirección de sistemas de gestión	1.6	Actualización y revisión
08/09/2022	Departamento de administración	1.7	Actualización punto 3.1
27/02/2024	Dirección de sistemas de gestión	1.8	Actualización de organigrama y punto 9.8
22/01/2025	Dirección de sistemas de gestión	1.9	Actualización legislación y otros
29/01/2026	Dirección de sistemas de gestión	1.10	Actualización Punto 5
25/06/2026	Dirección de sistemas de gestión	1.11	Integración NIS2

Documento revisado y aprobado por la dirección - Válido sin firma

Índice

1. INTRODUCCIÓN 7
1.1. Presentación de la Organización 7
1.2. Importancia de los sistemas TIC y la seguridad de la información 7
1.3. Conceptos Generales 8
1.4. Prevención 8
1.5. Detección 9
1.6. Respuesta 9
1.7. Recuperación 9
1.8. Normas aplicables 9
1.9. Cumplimiento de la Directiva NIS2 y enfoque de resiliencia 10
2. OBJETO Y CAMPO DE APLICACIÓN 11
2.1. Objeto 11
2.2. Alcance 11
2.3. Localización 12
2.4. Objetivos y Misión de Netboss Comunicaciones en el Marco de la Política de Seguridad de la Información 12
2.5. Plan de Mejora. Objetivos de Seguridad 14
2.6. Requisitos Legales 14
3. CONTEXTO DE LA ORGANIZACIÓN 15
3.1. Organigrama 15

3.2. Infraestructura informática 15
3.3. Partes interesadas: Relaciones internas y externas 16
3.4. Requisitos y necesidades de las partes interesadas 18
4. LIDERAZGO 18
4.1. Compromiso de la dirección 18
4.2. Requisitos de la Política de Seguridad de la Información 19
4.3. Política de Seguridad de la Información 19
4.4. Roles, responsabilidades y autoridades en la organización 19
4.4.1. Comité de Seguridad 19
4.4.2. Roles: Funciones y Responsabilidades 20
4.4.2.1. Dirección 20
4.4.2.2. Responsable de la Información 20
4.4.2.3. Responsable de los Servicios 20
4.4.2.4. Responsable de Seguridad 21
4.4.2.5. Responsable del Sistema 21
4.4.2.6. Propietario del Riesgo 22
4.4.2.7. Propietario de Activos 22
4.4.2.8. Personal 23
4.4.3. Procedimiento de Designación de responsables 23
4.4.4. Comunicación 23
4.5. Planificación 24
4.5.1. Información de entrada para la planificación 24
4.5.2. Resultado de la planificación. 24
5. APOYO 25
5.1. Recursos 25
5.1.1. Provisión de recursos 25
5.1.2. Infraestructura 25
5.2. Personas 25
5.3. Comunicación 25
5.4. Información documentada 25
5.4.1. Control de la documentación del Sistema de Gestión 26
5.4.2. Documentación del Sistema 26
5.5. Normativa 28
6. OPERACIÓN 28

6.1. Planificación y control operacional 28
6.2. Tratamiento de los riesgos de seguridad de información 28
6.2.1. Proceso Análisis de Riesgos 29
6.2.2. Proceso de Gestión de Riesgos 29
7. MONITORIZACIÓN 29
7.1. Seguimiento y medición de los procesos 29
7.2. Auditoría interna 30
7.3. Revisión por la Dirección 30
8. MEJORA CONTINUA 30
8.1. Acción correctiva y preventiva 30
9. PRINCIPIOS DE SEGURIDAD 31
9.1. Gestión de Activos 31
9.1.1. Responsabilidades asociadas a los activos 31
9.1.2. Clasificación de la información 31
9.2. Seguridad de la Gestión de los Recursos Humanos 31
9.3. Seguridad Física y del Entorno 32
9.3.1. Áreas Seguras 32
9.3.2. Seguridad de los equipos 32
9.4. Gestión de comunicaciones y operaciones 33
9.4.1. Procedimientos Operativos y Responsabilidades 33
9.4.2. Gestión de los Servicios Suministrados por Terceros 33
9.4.3. Protección frente a código malicioso y código móvil 34
9.4.4. Copias de Seguridad 34
9.4.5. Gestión de la seguridad de la red 34
9.4.6. Gestión de Soportes 34
9.4.7. Intercambio de Información 35
9.4.8. Seguimiento 35
9.5. Control de Accesos 35
9.5.1. Requisitos del negocio para el control de accesos 35
9.5.2. Gestión de accesos de los usuarios 35
9.5.3. Responsabilidades del usuario 36
9.5.4. Control de acceso a la red 36
9.6. Gestión de incidentes 36
9.7. Continuidad del negocio 36

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

Consultar Certificaciones: netboss.es/certificaciones

9.8. Política de uso aceptable..... 37

DERECHOS DE USO:

La presente documentación es propiedad de Netboss Comunicaciones S. L, y tiene el carácter de confidencial. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. En caso de cualquier duda o pregunta adicional, por favor, no dude en ponerse en contacto con nosotros en info@netboss.es.

CLÁUSULA DE GÉNERO:

Todas las referencias contenidas en este Comunicado expresadas en masculino gramatical, cuando se refieran a personas físicas, deben entenderse referidas indistintamente a hombres y mujeres y a sus correspondientes adjetivaciones masculinas o femeninas.

ACTUALIZACIÓN NORMATIVA:

Netboss Comunicaciones S.L. se reserva el derecho a actualizar y modificar estas normas. La normativa vigente se puede consultar en la dirección https://app.factorialhr.com/my-documents/company-files/list

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

www.netboss.es

Consultar Certificaciones: netboss.es/certificaciones

1. INTRODUCCIÓN

1.1. Presentación de la Organización

Netboss Comunicaciones S.L. es una de las principales compañías españolas de consultoría y outsourcing de servicios.

Contamos con tres divisiones que proporcionan a nuestros clientes una solución integral a sus necesidades operativas. Nuestra división de consultoría, especializada en reingeniería de procesos y el diseño de servicios de información y atención al cliente/ciudadano; nuestra división de BPO, especializada en el outsourcing de servicios de front y back office con contact center propio; y nuestra Software Factory, nuestra división de software, con dos productos propios en el mercado: una potente plataforma de agendamiento, reserva y cita previa multisector; y una completa plataforma de gestión de equipos en campo o "field service management".

1.2. Importancia de los sistemas TIC y la seguridad de la información

Netboss Comunicaciones S.L. depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) 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, confidencialidad, autenticidad, o trazabilidad 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 preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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 se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la legislación de protección de datos, 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.

Netboss Comunicaciones S.L. debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Netboss Comunicaciones S.L. debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Esquema Nacional de Seguridad y a la legislación de protección de datos.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

1.3. Conceptos Generales

Se contemplan las siguientes dimensiones de seguridad:

- Disponibilidad: propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran. Es necesario garantizar que los recursos del sistema se encuentren disponibles cuando se necesiten, especialmente la información crítica.
- Integridad: propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada. La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- Confidencialidad: propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados. La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- Autenticidad: propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos. El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

El ciclo PDCA es el que se utilizará durante todo el ciclo de vida del SGSI.

- ✓ P (Planificar): en esta fase se establecen las actividades, responsabilidades y recursos además de los objetivos a cumplir y cómo se van a medir estos objetivos.
- ✓ D (Desarrollar): se desarrollan los procesos y se implementan. Una vez implementados, hay que medir los resultados de la ejecución de dichos procesos.
- ✓ C (Comprobar): se analizan los resultados para comprobar si se han alcanzado los objetivos y si no es así, identificar las causas.
- ✓ A (Actuar): Se toman las acciones necesarias para corregir los fallos detectados en los procesos o para mejorarlos.

1.4. Prevención

Netboss Comunicaciones S.L. debe 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 se implementará las medidas mínimas de seguridad determinadas por el ENS, NIS2 y el RGPD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, Netboss Comunicaciones S.L debe:

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

Consultar Certificaciones: netboss.es/certificaciones

- Autorizar los sistemas 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.

1.5. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya preestablecido como normales.

1.6. Respuesta

Netboss Comunicaciones S.L.:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

1.7. Recuperación

Para garantizar la disponibilidad de los servicios críticos, Netboss Comunicaciones S.L. ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

1.8. Normas aplicables

Las normas que han servido de referencia para la elaboración de la presente Política de Seguridad de la Información son las siguientes:

- ✓ Norma UNE/ISO-IEC 27001 Tecnología de la Información. Especificaciones para los Sistemas de Gestión de Seguridad de la Información.
- ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS. Este es el marco principal que establece los principios básicos y requisitos mínimos para garantizar la protección adecuada de la información y servicios electrónicos.
- ✓ Reglamento General de Protección de Datos (RGPD) del 25/05/2018
- ✓ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda

la Unión (*Directiva NIS2*), así como la normativa nacional que la transpone en el ordenamiento jurídico español.

1.9. Cumplimiento de la Directiva NIS2 y enfoque de resiliencia

Netboss Comunicaciones S.L. apuesta por garantizar un alto nivel de seguridad de las redes y sistemas de información, alineándose con los requisitos establecidas en la Directiva (UE) 2022/2555 (NIS2) y su normativa de transposición nacional aplicable.

En este sentido, la organización adopta un enfoque basado en la gestión del riesgo de ciberseguridad y en la resiliencia operativa de los servicios prestados, especialmente aquellos considerados críticos para clientes, Administraciones Públicas y otras partes interesadas.

A tal efecto, Netboss Comunicaciones S.L. establece los siguientes principios:

Gestión de riesgos de ciberseguridad: La organización dispone de mecanismos para la detección, gestión y respuesta a incidentes de seguridad de la información. En caso de incidentes significativos, se garantizará su notificación a las autoridades competentes en materia de ciberseguridad, tales como INCIBE-CERT, CCN-CERT u otros organismos designados conforme a la normativa nacional de transposición de la Directiva NIS2, en los plazos y condiciones establecidos por la legislación aplicable.

Resiliencia y continuidad del negocio: Se implantan medidas destinadas a garantizar la continuidad de los servicios y la capacidad de respuesta y recuperación ante incidentes de ciberseguridad, incluyendo pruebas periódicas cuando sea necesario.

Gestión de incidentes de seguridad: La organización dispone de mecanismos para la detección, gestión y respuesta a incidentes de seguridad de la información. En caso de incidentes significativos, se garantizará su notificación a las autoridades competentes en los plazos y condiciones establecidos por la normativa aplicable.

Seguridad en la cadena de suministro: Se establecen criterios de evaluación, selección y seguimiento de proveedores y terceros, prestando especial atención a aquellos considerados críticos desde el punto de vista tecnológico o de prestación de servicios.

Medidas de seguridad técnicas y organizativas: La organización adopta medidas adecuadas y proporcionadas para garantizar la seguridad de los sistemas de información, incluyendo, entre otras, el control de accesos, la autenticación reforzada, la protección de la información mediante cifrado, la gestión de vulnerabilidades y la monitorización de sistemas.

Cultura de ciberseguridad y formación: Netboss promueve la concienciación y formación en materia de ciberseguridad para todo el personal, con especial énfasis en los roles con responsabilidad en la gestión y supervisión de la seguridad de la información.

Implicación de la alta dirección: La Dirección asume la responsabilidad última en materia de seguridad de la información y ciberseguridad, supervisando de forma activa el desempeño del Sistema de Gestión de Seguridad de la Información (SGSI) y la gestión de los riesgos asociados.

Mejora continua y cumplimiento normativo: El Sistema de Gestión de Seguridad de la Información se revisa y mejora de forma continua, garantizando su adecuación a los requisitos legales, regulatorios y contractuales, incluyendo los derivados de la Directiva NIS2.

El desarrollo y detalle de estas medidas se establece en los procedimientos, normas y registros del Sistema de Gestión Integrado de Netboss Comunicaciones S.L.

Los principios descritos en este apartado se desarrollan e implantan a través de los procedimientos, normas y registros del Sistema de Gestión de Seguridad de la Información (SGSI) de Netboss Comunicaciones S.L., incluyendo, entre otros, los procesos de análisis y gestión de riesgos, gestión de incidentes, continuidad del negocio y gestión de proveedores.

2. OBJETO Y CAMPO DE APLICACIÓN

2.1. Objeto

Este Documento tiene como objetivo establecer las directrices que garanticen la seguridad de la información de los servicios y productos de Netboss Comunicaciones S.L. a un nivel adecuado según el nivel de riesgo de los activos y nuestras necesidades y recursos.

La información y los procesos que la apoyan, son importantes activos para la empresa. La disponibilidad, integridad y confidencialidad de la información son esenciales para mantener los servicios y la reputación e imagen de la empresa.

2.2. Alcance

Todas las pautas descritas en el presente documento serán efectivas para el conjunto de Netboss Comunicaciones S.L., sus instalaciones y activos:

- ✓ A todos los departamentos, tanto a sus directivos como a empleados.
- ✓ A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de Netboss Comunicaciones.
- ✓ A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- ✓ A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- ✓ A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- ✓ A todos los sistemas utilizados para administrar y gestionar la información, sean propios, alquilados o licenciados.

El alcance del Sistema de Gestión de Seguridad de la Información de acuerdo con el Esquema Nacional de Seguridad se aplica a la gestión de los siguientes servicios y productos:

- ✓ Página web corporativa.
- ✓ BPO y Contact Center.
- ✓ Consultoría.

- ✓ Software de agendamiento, cita previa y reserva online.
- ✓ Software FSM (Field Service Management).

El alcance del Sistema de Gestión de Seguridad de la Información de acuerdo con la norma ISO/IEC 27001 se aplica a la gestión de los siguientes servicios y productos:

- ✓ Página web corporativa.
- ✓ BPO y Contact Center.
- ✓ Consultoría.
- ✓ Software de agendamiento, cita previa y reserva online.
- ✓ Software FSM (Field Service Management).

2.3. Localización

Netboss Comunicaciones S.L. se encuentra ubicada en Plaza Vista Bahía, 1 – 2 Bajo, 39610 Astillero. Cantabria (España).

2.4. Objetivos y Misión de Netboss Comunicaciones en el Marco de la Política de Seguridad de la Información

Misión: Nuestra misión en Netboss Comunicaciones es proporcionar soluciones de telecomunicaciones y servicios digitales confiables, seguros y de alta calidad, garantizando la confidencialidad, integridad y disponibilidad de la información. Nos comprometemos a cumplir con los estándares legales, éticos y regulatorios aplicables, protegiendo los datos de nuestros clientes, empleados y socios comerciales, al tiempo que fomentamos un entorno de innovación tecnológica y mejora continua.

Objetivos:

1. Proteger la información y los activos de la organización: Garantizar la seguridad de los datos propios y de los clientes frente a accesos no autorizados, pérdidas, alteraciones o usos indebidos.
2. Cumplir con el marco legal y regulatorio aplicable: Implementar y mantener medidas de seguridad alineadas con las leyes y normativas del sector de telecomunicaciones, incluyendo estándares internacionales y nacionales en materia de seguridad de la información.
3. Fomentar la concienciación y responsabilidad en seguridad: Desarrollar una cultura organizacional que promueva la capacitación continua y la sensibilización sobre la importancia de la seguridad de la información en todos los niveles de la organización.
4. Garantizar la continuidad del negocio: Diseñar e implementar controles y planes de gestión de riesgos que aseguren la operación ininterrumpida de los servicios críticos, incluso ante incidentes de seguridad o desastres.
5. Establecer relaciones de confianza con clientes y socios: Proteger la privacidad de los datos personales y empresariales, fortaleciendo la credibilidad y la reputación de Netboss Comunicaciones como proveedor seguro y confiable.

6. Adoptar una estrategia de mejora continua: Evaluar y actualizar periódicamente las medidas de seguridad implementadas, asegurando su efectividad frente a amenazas emergentes y cambios regulatorios.

7. Promover la innovación tecnológica segura: Integrar prácticas de seguridad desde el diseño y durante todo el ciclo de vida de los servicios y productos que ofrece Netboss Comunicaciones.

Estos objetivos reflejan nuestro compromiso con la excelencia, la seguridad y el cumplimiento normativo, asegurando que cada acción y decisión en Netboss Comunicaciones esté alineada con nuestra Política de Seguridad de la Información.

Netboss Comunicaciones S.L. define la presente Política de Seguridad, de carácter obligatorio para todos sus empleados, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Uno de los objetivos de este documento es establecer las directrices que garanticen la seguridad de la información en Netboss Comunicaciones S.L. a un nivel adecuado según el nivel de riesgo de los activos y las necesidades y recursos de esta organización.

Este documento debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve Netboss Comunicaciones para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la Información serán:

- ✓ Velar por la seguridad de la información, en sus distintas dimensiones.
- ✓ Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos, para reducir o eliminar los riesgos inherentes a nuestras actividades por medio de la mejora continua del desempeño en seguridad en nuestros procesos, productos y servicios.
- ✓ Elaborar, mantener y probar los planes de contingencia y continuidad de la actividad que se definan para los distintos servicios ofrecidos.
- ✓ Realizar una adecuada gestión de incidentes que afecten a la seguridad de la información (ciber incidentes).
- ✓ Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- ✓ Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- ✓ Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.

Esta Política de Seguridad:

- Se aprobará formalmente por la Dirección de Netboss Comunicaciones S.L.
- Se revisará de forma anual, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados.

- El responsable de seguridad será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- Cada empleado es responsable de cumplir esta política y sus procedimientos según aplique a su puesto de trabajo.
- Los responsables de cada departamento serán los encargados de implementar esta política y sus correspondientes procedimientos dentro de su área.
- Se mantendrá a disposición de las partes interesadas esta política, así como los futuros desarrollos de esta.

2.5. Plan de Mejora. Objetivos de Seguridad

El Comité de Seguridad establecerá y aprobará un Plan de Mejora con carácter anual en el que se definirán los objetivos de seguridad que se consideren necesarios en cada caso para cumplir con los objetivos indicados. Se deben establecer objetivos coherentes con las políticas de seguridad definidas, y proporcionar los recursos necesarios para su consecución, que serán definidos en el propio Plan de Mejora.

2.6. Requisitos Legales

Con el objeto de satisfacer los compromisos establecidos de cumplir con la legislación y reglamentación aplicable a las actividades, productos y servicios de Netboss Comunicaciones S.L., tiene establecido y mantiene el procedimiento SGI P613 Cumplimiento Legal para la identificación y acceso a dichos requisitos legales y otros requisitos a los que la empresa se somete (acuerdos con autoridades públicas, códigos de buenas prácticas industriales y directrices o pautas no reglamentarias).

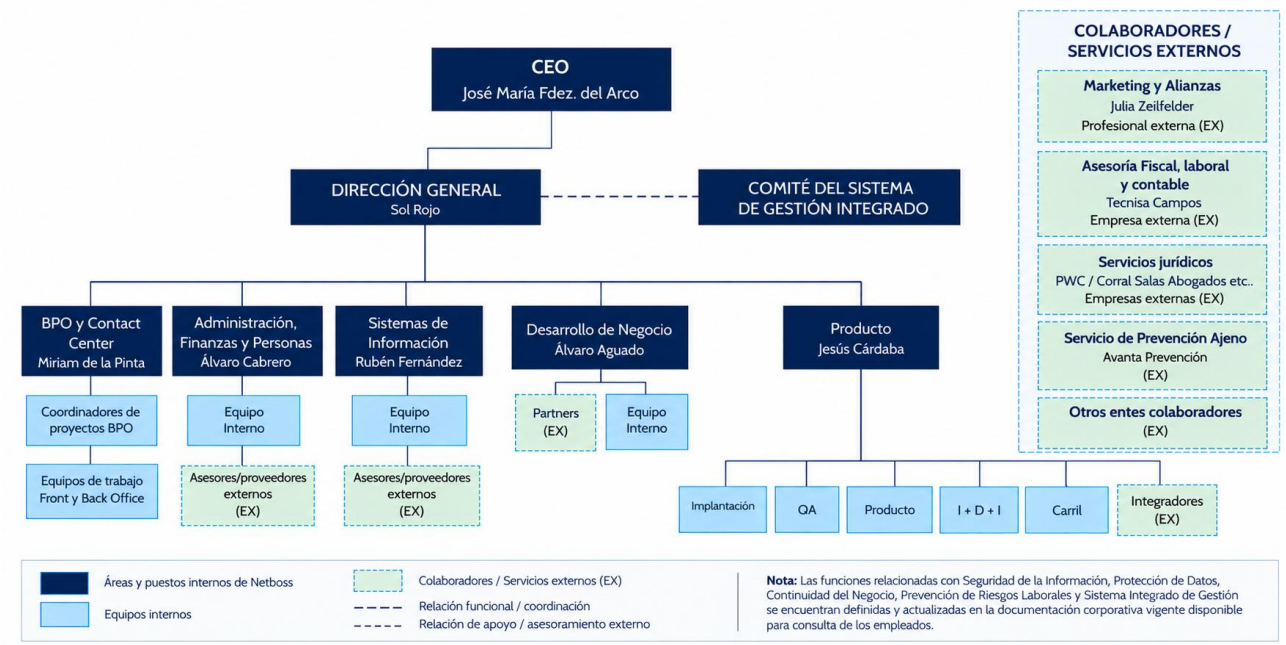
Según la legislación vigente, las leyes aplicables a Netboss Comunicaciones S.L. para las actividades dentro del alcance del Sistema de Gestión son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS. Este es el marco principal que establece los principios básicos y requisitos mínimos para garantizar la protección adecuada de la información y servicios electrónicos.
- Reglamento General de Protección de Datos (RGPD) de 25/05/2018.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley de Propiedad Industrial.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Directiva de Cookies
- Reglamento Europeo de Protección de Datos

Asimismo, la organización evalúa de forma continua su encuadre dentro del ámbito de aplicación de la Directiva (UE) 2022/2555 (NIS2) y su normativa de transposición nacional, con el objetivo de determinar su consideración como entidad esencial o importante y asegurar el cumplimiento de las obligaciones que le resulten aplicables en función de su actividad, tamaño y servicios prestados.

3. CONTEXTO DE LA ORGANIZACIÓN

3.1. Organigrama



3.2. Infraestructura informática

Netboss Comunicaciones S.L. dispone tanto de servidores como de puestos de trabajo. Los servidores están ubicados en un cuarto especifico, donde se dispone de tres armarios, uno para comunicaciones, uno dedicado solo a servidores y otro con la centralita telefónica y dos NAS de almacenamiento de archivos. También se subcontratan servicios de Cloud a proveedores con distintos usos, como la ejecución de máquinas virtuales.

Se utiliza principalmente Sistema Operativo Windows en los puestos de trabajo, en su versión Windows 11 Pro. Respecto a la estructura de servidores; se utiliza el sistema de virtualización VMware Esxi en su versión 9.0, disponiendo de servidores virtuales, con sistemas operativos tanto Windows Server 2025 como Ubuntu server o Debian.

Se dispone de acceso a internet mediante tres líneas de Fibra Óptica. El acceso a internet está filtrado mediante un cortafuegos para así garantizar la seguridad de la organización, también se garantiza la continuidad del servicio mediante el balanceo de las líneas.

Se dispone de una red organizativa con un Directorio Activo gestionado los permisos de acceso de los usuarios en los puestos de trabajos mediante grupos de usuarios. Se utilizan mecanismos de control de acceso para proteger los recursos.

La información tratada por parte de los empleados de la entidad se almacena en servidores de ficheros destinados para ello, generándose copias de seguridad periódicas de la misma.

El mantenimiento de infraestructura técnica se realiza por el personal especializado de la empresa.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es
www.netboss.es

Consultar Certificaciones: netboss.es/certificaciones

3.3. Partes interesadas: Relaciones internas y externas

El sistema de gestión definido tendrá en cuenta las diferentes partes implicadas en el sistema de información siendo estas principalmente:

Clientes: como parte fundamental del sistema, se velará por preservar la confidencialidad, integridad y disponibilidad, de la información intercambiada con los clientes, y necesaria para la prestación de los servicios señalados en el alcance, así como cualquier otra información (administrativa, de contacto…) necesaria para la prestación del servicio. Adecuación con los clientes en materia de Protección de Datos, en concreto al reglamento RGPD.

Proveedores: Debido a la relevancia de los proveedores de servicios para el tratamiento de la información, especialmente en cuanto a los servicios de TI necesarios para la prestación de los servicios de Netboss Comunicaciones S.L. (como son los proveedores de las aplicaciones informáticas, o los encargados de las tareas de mantenimiento informático), se han establecido los requisitos necesarios para garantizar la seguridad y disponibilidad de sus servicios. Se deben de tener en cuenta igualmente los envíos de información realizados a las entidades bancarias.

Administración Pública: Como destinatarios de los servicios prestados por Netboss Comunicaciones S.L., con la finalidad de cumplir con las normas y leyes de aplicación, el envío de información se realizará, bien a través de los medios que dichos organismos ponen a disposición para tal fin (servicios web) o bien mediante medios alternativos como correo electrónico (mediante firma electrónica) o soportes magnéticos.

Trabajadores: Como parte fundamental en el tratamiento de la información, los empleados deberán de conocer las normas y procedimientos de seguridad que se decidan aplicar en la organización para asegurar la confidencialidad, integridad y disponibilidad de los datos.

Competencia: Como prestador de servicios a administraciones públicas, Netboss Comunicaciones S.L. compite con otras empresas, prestadoras de servicios similares, en concursos públicos, y por la obtención de contratos menores.

Acreedores y Entidades Financieras: Cuando es necesaria financiación, Netboss Comunicaciones S.L. solicita préstamos, u otros instrumentos financieros, a entidades bancarias, otras entidades de financiación y/o empresas o personas que ofrecen financiación.

Accionariado/Propietario de la empresa: Actualmente todas las participaciones de Netboss Comunicaciones S.L. están en posesión de cuatro accionistas.

Se detalla a continuación las relaciones entre las diferentes partes interesadas que se incluyen dentro del alcance del SGSI:

Servicio	Sistema de tratamiento	Servicios subcontratados	Proveedores	Trabajadores	Clientes
Página web corporativa	Servidores Equipos de usuario Aplicaciones Equipamiento auxiliar	Internet	Proveedores de Comunicaciones	Departamento de Desarrollo Departamento de Sistemas	Administraciones publicas Empresas
Call Center	Servidores Equipos de usuario Aplicaciones Equipamiento auxiliar	Internet Red Telefónica	Proveedores de Comunicaciones	Departamento de Call Center	Administraciones publicas Empresas
Consultoría, Desarrollo e implantación de aplicaciones	Servidores Equipos de usuario Aplicaciones Equipamiento auxiliar	Internet	Proveedores de Comunicaciones	Departamento de Consultoría Departamento de Desarrollo Departamento de Sistemas	Administraciones publicas Empresas
Servicios Cloud	Servidores Equipos de usuario Aplicaciones Equipamiento auxiliar	Internet	Proveedores de Comunicaciones y Cloud	Departamento de Desarrollo Departamento de Sistemas	Administraciones publicas Empresas

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

www.netboss.es

Consultar Certificaciones: netboss.es/certificaciones

3.4. Requisitos y necesidades de las partes interesadas

Clientes: Netboss Comunicaciones S.L., debe cumplir con los requisitos contractuales establecidos con los clientes para la prestación de servicios.

Administración Pública: Netboss Comunicaciones S.L. debe cumplir con las obligaciones legales o reglamentariamente establecidas con la Administración Pública.

Proveedores: Los proveedores deberán de cumplir con las condiciones establecidas en los acuerdos de nivel de servicio formalizados en lo que la seguridad de los servicios prestados se refiere, los plazos de prestación y entrega, las incidencias, y el tratamiento de los datos de carácter personal. Por su parte Netboss Comunicaciones S.L. deberá cumplir las condiciones contractuales como contratante del servicio y en caso de tratar datos de carácter personal de los proveedores, asegurar la seguridad de estos.

Trabajadores: Los empleados deberán de conocer y cumplir las políticas, normas y procedimientos de seguridad aplicables en la organización para asegurar la confidencialidad, integridad y disponibilidad de los datos.

Acreedores y Entidades Financieras: Netboss Comunicaciones S.L. debe cumplir con las condiciones de financiación establecidas contractualmente con este tipo de entidades, principalmente, realizar los pagos de devolución del préstamo en los tiempos establecidos.

Accionariado propietario de la empresa: Netboss Comunicaciones S.L. debe cumplir con los objetivos y planes estratégicos establecidos por la Dirección, encaminados a la consecución de rentabilidad para el accionariado.

4. LIDERAZGO

4.1. Compromiso de la dirección

La presente Política de Seguridad es una línea de actuación clara, manifiesta y pública de Netboss Comunicaciones S.L., por lo que la dirección expresa su apoyo total a la misma y se compromete a mantener las directrices fijadas en el presente Documento. Asimismo, publicará y entregará a todos sus empleados y de la forma más apropiada las Políticas y Normativas, para que todos conozcan el objetivo establecido por el Comité de Seguridad, las políticas, principios y normas adoptadas y su importancia para la seguridad de la empresa, las responsabilidades generales y específicas en materia de seguridad de cada miembro de la empresa y otras referencias a documentación que puedan ser útiles.

La Dirección está comprometida en la implantación, mantenimiento y mejora del Sistema de Gestión, por lo que:

- ✓ Se implica en comunicar a la organización la importancia de satisfacer los requisitos de los clientes, así como los legales y reglamentarios.
- ✓ Establece la Política de Seguridad de la Información.

- ✓ Establece los Objetivos del sistema, así como la planificación, tal como se describe en la presente Política de Seguridad.
- ✓ Lleva a cabo revisiones del Sistema de Gestión
- ✓ Se asegura la disponibilidad de los recursos.

La Dirección asume la responsabilidad de supervisar el cumplimiento de las obligaciones en materia de ciberseguridad derivadas de la normativa aplicable, incluyendo las establecidas por la Directiva NIS2, garantizando la asignación de recursos adecuados y la integración de la ciberseguridad en la estrategia global de la organización.

4.2. Requisitos de la Política de Seguridad de la Información

Se debe asegurar que la Política de Seguridad de Netboss Comunicaciones S.L.:

- ✓ Es adecuada al propósito de la organización y a la naturaleza de las actividades, productos o servicios.
- ✓ Incluye de manera expresa un compromiso de cumplimiento con la legislación, la reglamentación aplicable y con otros requisitos que se estimen apropiados.
- ✓ Proporciona un marco de referencia para establecer y revisar los objetivos del Sistema de Gestión.
- ✓ Es comunicada y entendida por los niveles apropiados de la organización.
- ✓ Es revisada para conseguir una continua adecuación.
- ✓ La revisión se realizará de forma periódica, al menos en la Revisión por la Dirección del Sistema de Gestión (según lo establecido en la presente Política de Seguridad), y, de forma extraordinaria, siempre que la Dirección lo considere necesario.

Las Política de Seguridad estará a disposición del público que la solicite y la Dirección se asegura que esta Política es entendida, implantada y mantenida al día en la organización.

4.3. Política de Seguridad de la Información

Las políticas de seguridad de la Información se recogen en el apartado “Principios de Seguridad”.

4.4. Roles, responsabilidades y autoridades en la organización

4.4.1. Comité de Seguridad

El Comité de Seguridad coordina la seguridad de la información en Netboss Comunicaciones S.L. y está formado por:

- ✓ Dirección de la compañía.
- ✓ Responsable de la información.
- ✓ Responsable de los servicios.
- ✓ Responsable de Seguridad.
- ✓ Responsable de sistemas.

El Comité de Seguridad se reunirá al menos una vez al año.

4.4.2. Roles: Funciones y Responsabilidades

Para gestionar de forma eficiente la Seguridad de la Información, cada uno de los departamentos de Netboss Comunicaciones S.L. deberá cumplir las normas y los procedimientos que correspondan. Todas estas normas y procedimientos estarán ratificados por la Dirección.

Los miembros del Comité de Seguridad son los siguientes:

- ✓ Responsable del Servicio de la Información: Dirección de la compañía: CEO, dirección general o quien delegue. El CEO o la dirección general recae sobre Jose María Fernández de Arco o Sol Rojo Vallejo
- ✓ Responsable de la información: director de sistemas. Rubén Fernández Crespo
- ✓ Responsable de Seguridad: responsable del sistema de gestión. Sol Rojo Vallejo
- ✓ Responsable del Sistema: director de sistemas. Rubén Fernández Crespo

Las funciones y responsabilidades se detallan a continuación:

4.4.2.1. Dirección

La Dirección de Netboss Comunicaciones S.L. se compromete a responder por las obligaciones inherentes a la seguridad de la información y proteger sus activos de información implementando las medidas de seguridad más apropiadas para conseguirlo de una manera efectiva con los recursos disponibles.

4.4.2.2. Responsable de la Información

Será el responsable de:

- ✓ El riesgo de toda la Información.
- ✓ Velar por el buen uso de la información y, por tanto, de su protección.
- ✓ Cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- ✓ Establecer los requisitos de la información en materia de seguridad.
- ✓ Determinar los niveles de seguridad de la información.

4.4.2.3. Responsable de los Servicios

Será el responsable de:

- ✓ El riesgo de todos los Servicios.
- ✓ Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- ✓ Determinar los niveles de seguridad de los servicios.

4.4.2.4. Responsable de Seguridad

Es el responsable de Seguridad de la Información (incluidos los ficheros de RGPD).

- ✓ Es el Propietario del Activo de todos los activos de la empresa en lo que respecta a la norma ISO 27001. En el inventario de activos podrá especificarse un responsable del Activo, en el que el Propietario del Activo delega la toma de decisiones respecto a dicho activo.
- ✓ Es el responsable de la gestión y el mantenimiento del Sistema de Gestión.
- ✓ Asegura que los procesos del Sistema de Gestión están establecidos, implantados y mantenidos, de acuerdo con los requisitos de las normas aplicables.
- ✓ Informa a la Dirección del funcionamiento y eficacia del sistema para que ésta lleve a cabo la revisión, y como base para la mejora de la gestión de la empresa.
- ✓ Promueve el conocimiento de los requisitos de los clientes en materia de Seguridad de la Información a todos los niveles de la organización.
- ✓ Colabora con la Dirección en la definición e implantación de Políticas y Normativas de forma que sean fiel reflejo de la estrategia de la empresa.
- ✓ Planifica, programa y participa, cuando proceda, en las auditorías internas y externas.
- ✓ Controla la elaboración, actualización, aprobación y distribución de la documentación del Sistema de Gestión.
- ✓ Actúa como interlocutor con partes externas (clientes, proveedores, administración, y demás partes interesadas) sobre aspectos del sistema de gestión.
- ✓ Controla la ejecución y eficacia de las acciones emprendidas para prevenir y gestionar No Conformidades y valora las acciones a realizar tras la comunicación de una sugerencia de mejora.

4.4.2.5. Responsable del Sistema

Será el responsable de:

- ✓ El Riesgo de todos los activos, con excepción de los activos esenciales (Servicios e Información).
- ✓ Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- ✓ Definir la tipología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- ✓ Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- ✓ La administración y gestión de las cuentas de los usuarios.
- ✓ Asegurarse de que sólo las personas autorizadas a tener acceso cuentan con él.
- ✓ Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la Organización.
- ✓ Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.

4.4.2.6. Propietario del Riesgo

El propietario del riesgo, asociado a uno o varios activos de información, tendrá las siguientes responsabilidades:

- ✓ Participar en el desarrollo del análisis y evaluación de riesgos realizada al menos con carácter anual.
- ✓ Verificar la conformidad con los niveles de riesgo aceptable y colaborar en la aprobación de estos (que le afecten), así como la gestión de los riesgos asociado a los activos de información y los riesgos de los que es responsable.
- ✓ Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del riesgo deberá informar a su vez al responsable de Seguridad para tratar la incidencia.
- ✓ Informar al responsable de Seguridad cuando ocurran cambios del personal, la organización, o del resto de los activos de información, que pueda implicar una revisión o actualización del análisis de riesgos, o de los permisos de acceso asignados.

4.4.2.7. Propietario de Activos

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- ✓ Definir si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.
- ✓ Asegurarse de que el software que se utiliza tiene licencia.
- ✓ Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- ✓ Asegurarse de que el activo cuenta con el mantenimiento adecuado.
- ✓ Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al responsable de Seguridad para tratar la incidencia.
- ✓ Asegurarse de que la plantilla cuenta con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
- ✓ Asegurarse de que los soportes y equipos que contengan información son desechados según lo establecido.
- ✓ Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.
- ✓ Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
- ✓ Informar al responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.

- ✓ En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

4.4.2.8. Personal

- ✓ Conocer y comprender las políticas, normativas y los procedimientos que apliquen a su trabajo.
- ✓ Asegurarse de que sus acciones no producen ninguna infracción de seguridad.
- ✓ Informar al propietario del activo de cualquier incidencia de seguridad, real o sospechada, que detecte.

4.4.3. Procedimiento de Designación de responsables

El responsable de Seguridad será nombrado por Dirección a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

La Dirección designará también al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

4.4.4. Comunicación

Netboss Comunicaciones S.L. asegura la comunicación entre los diferentes niveles y funciones de la organización referente a los procesos del Sistema de Gestión y su efectividad. Dicha comunicación consiste en:

- ✓ Decidir y responder a las preocupaciones del personal en cuestiones relativas al Sistema de Gestión.
- ✓ Comunicación entre las diferentes áreas operativas de la organización, a fin de seguir la evolución de los procesos operativos del Sistema de Gestión y coordinar y unificar criterios de actuación.
- ✓ Comunicación a nivel de área, a fin de compartir entre sus miembros el conocimiento y las mejores prácticas adquiridas por la experiencia durante el desarrollo de los procesos correspondientes.
- ✓ Recibir, documentar y responder a las comunicaciones pertinentes de las partes interesadas de la organización, así como asegurar la comunicación interna entre los diversos niveles y funciones de la organización.

Para asegurar dicha comunicación, se procede de la siguiente manera:

- ✓ El responsable de Seguridad, mediante reuniones periódicas por departamentos con el personal, correo electrónico interno, etc., es responsable de dar a conocer las Políticas, los objetivos, las metas y la evolución del Sistema de Gestión en general y de la gestión de los requisitos del cliente en particular. Estas comunicaciones tendrán lugar siempre que dicho responsable lo considere oportuno y, en cualquier caso, tras las revisiones del sistema y las auditorías, con el fin de difundir los resultados y decisiones de carácter general y particulares derivadas de dichas actividades.
- ✓ Para asegurar que las informaciones puntuales de carácter urgente son comunicadas al personal afectado, la organización dispone herramientas de comunicación interna: correo electrónico,

Slack, Twist, teléfonos, etc., que tienen un emisor y uno o varios destinatarios, y que sirven para comunicar informaciones referentes a, por ejemplo, cambios producidos en un pedido que ya había sido transmitido al personal afectado, incorporación de una nueva persona a la organización, recepción de una visita a la organización, etc.

Se ha definido un Plan de Comunicación, detallando las vías de comunicación entre las diferentes partes interesadas, en el documento SGI D74 Plan de comunicación.

4.5. Planificación

4.5.1. Información de entrada para la planificación

La Planificación de la Gestión se realiza para establecer el marco en el que se deben desarrollar y que debe regir las actuaciones de mejora de la empresa. La Dirección de Netboss Comunicaciones S.L. a través de las disposiciones del Sistema de Gestión establecido, identifica y planifica los recursos necesarios para:

- ✓ Alcanzar los Objetivos de Seguridad.
- ✓ Garantizar que los cambios organizativos se efectúan de modo controlado y que el Sistema de Gestión mantiene su integridad durante estos cambios.
- ✓ La Planificación de la Gestión se lleva a cabo, de forma ordinaria en la Reunión de Revisión del Sistema, y de forma extraordinaria siempre que la Dirección así lo decida, quedando documentada, en cualquier caso, en las actas finales de dichas reuniones.

4.5.2. Resultado de la planificación.

Como resultado de la planificación, la Dirección, de acuerdo con las Políticas definidas, establece los objetivos de la organización en materia de gestión para cada nivel relevante de la organización, que se recogen en el Plan de Mejora e informe de análisis de riesgos, conteniendo:

- ✓ Los objetivos y metas aprobados.
- ✓ La asignación de responsabilidades en cada función y nivel relevante de la organización para el logro de los objetivos y metas.
- ✓ Los medios y el calendario en el tiempo en que han de ser alcanzados.

Los objetivos son medibles y se establecen (y revisan) considerando los requisitos de seguridad, las opciones tecnológicas y los requisitos financieros, operacionales y de la empresa, así como aquellos necesarios para satisfacer los requisitos para el producto o servicio y el compromiso de mejora continua, la opinión de los clientes y de las partes interesadas en general.

Para evaluar el grado de cumplimiento, y asegurar la adecuación y eficacia del sistema, los objetivos son revisados periódicamente, y las conclusiones de su seguimiento se tratan en las reuniones del Comité de Seguridad, tal y como se detalla en el procedimiento aplicable. El seguimiento de los objetivos es documentado, registrado y aprobado por el Comité.

5. APOYO

5.1. Recursos

El objeto de este capítulo es describir el modo en que Netboss Comunicaciones S.L. gestiona sus recursos en el marco de su Sistema de Gestión.

5.1.1. Provisión de recursos

Netboss Comunicaciones S.L. determina y proporciona, en el momento adecuado, los recursos necesarios para implantar y mejorar los procesos del Sistema de Gestión, y para lograr la satisfacción del cliente, la seguridad de la información y la entrega de los servicios.

5.1.2. Infraestructura

La Dirección está comprometida en la implantación, mantenimiento y mejora del Sistema de Gestión, por lo que identifica, proporciona y mantiene las instalaciones necesarias para lograr los objetivos de seguridad incluyendo:

- ✓ Espacio de trabajo e instalaciones asociadas.
- ✓ Equipos, hardware y software.
- ✓ Servicios de apoyo.

La infraestructura necesaria para el desarrollo de las actividades de Netboss Comunicaciones S.L. se ha identificado en el análisis de riesgos.

5.2. Personas

Netboss Comunicaciones S.L. tiene establecido, y mantiene al día, el procedimiento SGI P71 Gestión de Personal, en donde se describen los criterios y responsabilidades asociadas para asegurar que aquel personal que tenga responsabilidades definidas en el Sistema de Gestión es competente basándose en la educación aplicable, formación, sensibilización, habilidades prácticas y experiencia.

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

5.3. Comunicación

Se desarrollará un Plan de Comunicación en el que se establezcan las vías de comunicación que se producen entre las diferentes partes interesadas del sistema (ver documento SGI D74 Plan de comunicación).

5.4. Información documentada

Para desarrollar este Sistema de Gestión se dispone de una estructura documental compuesta por:

- ✓ Política de Seguridad, la presente política: documento donde se establecen las bases del Sistema de Gestión de la empresa.
- ✓ Normativa, documentación donde se definen los usos permitidos o prohibidos en la organización.

- ✓ Procedimientos: describen las actividades requeridas para implementar el Sistema de Gestión para dar cumplimiento a requisitos exigidos por alguna de las normas aplicables.
- ✓ Documentos: cualquier información en cualquier tipo de soporte del sistema de gestión integrado.

Los diferentes documentos tienen la extensión adecuada para asegurar el funcionamiento efectivo del Sistema y de la organización y el control de los procesos, en función de la complejidad del proceso, la interacción de los distintos procesos y la competencia del personal que intervenga.

5.4.1. Control de la documentación del Sistema de Gestión

Netboss Comunicaciones S.L. tiene establecido, y mantiene al día, el procedimiento de gestión del SGSI donde se describe cómo debe realizarse el control de la documentación del Sistema, donde se describen los criterios y responsabilidades asociadas al control de los documentos necesarios para el funcionamiento del Sistema de Gestión.

5.4.2. Documentación del Sistema

ISO 27001	ENS	Documento del Sistema
4. contexto de la organización	org.1 Política de seguridad	SGSI D51 01 Política de Seguridad
4.1 Comprensión de la organización y de su contexto		SGSI D51 01 Política de Seguridad SGI P61 Análisis y Gestión de Riesgos Gestión de riesgos
4.2 Comprensión de las necesidades y expectativas de las partes interesadas		SGSI D51 01 Política de Seguridad
4.3 Determinación del alcance del sistema de gestión de seguridad de la información		SGSI D51 01 Política de Seguridad SGSI D613 01 Documento de aplicabilidad
4.4 Sistema de gestión de seguridad de la información		SGSI D51 01 Política de Seguridad
5. Liderazgo		SGSI D51 01 Política de Seguridad
5.1 Liderazgo y compromiso		SGSI D51 01 Política de Seguridad SGI D3 Manual del sistema de gestión integrado
5.2 Política	org.1 Política de seguridad	SGSI D51 01 Política de Seguridad
5.3 Roles, responsabilidades y autoridades en la organización	org.1 Política de seguridad	SGSI D51 01 Política de Seguridad
6. Planificación		SGSI D613 01 Documento de aplicabilidad SGS P843 Plan de Capacidad SGI P61 Análisis y Gestión de Riesgos P61 Análisis y Gestión de Riesgos SGI P71 Gestión de Personal

ISO 27001	ENS	Documento del Sistema
6.1 Acciones para abordar riesgos y oportunidades	op.pl.1 Análisis de riesgos	SGI D10 03 Plan de Mejora SGI P61 Análisis y Gestión de Riesgos SGI P61-01 Informe de Análisis y Gestión de Riesgos
6.2 Objetivos de seguridad de la información y planificación para su consecución		SGI D10 03 Plan de Mejora
7. Soporte		
7.1 Recursos		SGSI D61 Categorización del Riesgo SGI P61 Análisis y Gestión de Riesgos SGI P61-01 Informe de Análisis y Gestión de Riesgos SGI P84 01 Gestión de proveedores
7.2 Competencia	mp.per.4 Formación	SGI P71 Gestión de Personal SGI D10 03 Plan de Mejora
7.3 Concienciación	mp.per.3 Concienciación	SGI P71 Gestión de Personal SGI D10 03 Plan de Mejora
7.4 Comunicación		SGSI D51 01 Política de Seguridad SGI D74 Plan de comunicación
7.5 Información documentada		SGSI D51 01 Política de Seguridad SGI D3 Manual del sistema de gestión integrado ISO SGI P71 Gestión de Personal
8. Operación		SGI D3 Manual del sistema de gestión integrado ISO
8.1 Planificación y control operacional		SGSI P858 Seguridad Lógica SGSI P854 Control de Accesos SGSI P861 Gestión de Incidentes SGSI P855 Seguridad Física SGI P75 02 Protección de Datos de Carácter Personal SGI P75 01 Protección de la Información SGI P83 Desarrollo de Software SGI P84 01 Gestión de proveedores
8.2 Apreciación de los riesgos de seguridad de información	op.pl.1 Análisis de riesgos	SGI P61 Análisis y Gestión de Riesgos SGI P61-01 Informe de Análisis y Gestión de Riesgos P61 Análisis y Gestión de Riesgos
8.3 Tratamiento de los riesgos de seguridad de información	op.pl.1 Análisis de riesgos	SGI P61 Análisis y Gestión de Riesgos SGI P61-01 Informe de Análisis y Gestión de Riesgos P61 Análisis y Gestión de Riesgos
9. Evaluación del desempeño	op.mon.2 Sistema de métricas	SGI D3 Manual del sistema de gestión integrado ISO
9.1 Seguimiento, medición, análisis y evaluación	op.mon.2 Sistema de métricas	SGI R91 métrica e indicadores
9.2 Auditoría interna		SGI R92 01 programa de auditorias SGI R92 02 informe de auditoría interna
9.3 Revisión por la dirección		SGI R93 revisión por la dirección

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

Consultar Certificaciones: netboss.es/certificaciones

ISO 27001	ENS	Documento del Sistema
10. Mejora		SGSI R10 control nc – ac – om - am
10.1 No conformidad y acciones correctivas		SGSI R10 control nc – ac – om - am
10.2 Mejora continua		SGSI R10 control nc – ac – om - am

5.5. Normativa

El acceso a Internet deberá realizarse a través de los mecanismos de seguridad corporativos definidos por la organización. Queda prohibido el uso de servicios web, plataformas o aplicaciones que no hayan sido previamente autorizadas cuando puedan afectar a la seguridad de la red, los sistemas de información o los servicios esenciales prestados por la organización.

Cualquier detección de sitios maliciosos, actividades sospechosas o posibles incidentes de ciberseguridad deberá notificarse inmediatamente al responsable de Seguridad.

6. OPERACIÓN

6.1. Planificación y control operacional

Durante la planificación de la prestación del servicio se determinan cuando sea apropiado, los siguientes puntos:

- ✓ Los objetivos de seguridad, y los requisitos para el servicio.
- ✓ La necesidad de establecer procesos, documentos y de proporcionar recursos específicos para la prestación del servicio.
- ✓ Las actividades requeridas de verificación, validación, seguimiento e inspección específicas para el producto / servicio, así como los criterios para la aceptación de este.
- ✓ Los registros que sean necesarios para proporcionar evidencia de que los procesos cumplen los requisitos.

6.2. Tratamiento de los riesgos de seguridad de información

Analizar los posibles riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para Netboss Comunicaciones S.L. ya que, únicamente si se conoce el estado de seguridad con evidencias racionales, podrán tomarse las decisiones adecuadas para solucionar los riesgos que surjan.

Cada activo tiene una valoración en términos de Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, que se realizará con los criterios detallados en el documento SGSI D61 categorización del riesgo.

Para la realización del análisis de riesgos se ha utilizado la metodología MAGERIT (“Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información ”) elaborada por el Consejo Superior de Administración Electrónica.

El nivel de riesgo aceptable se documentará en el documento SGI P61-01 Informe de Análisis y Gestión de Riesgos.

MAGERIT cubre las actividades de análisis y tratamiento de riesgos facilitando una gestión de riesgos informada. La gestión de esos riesgos implicará seleccionar e implantar las medidas técnicas y de organización, necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

La gestión de riesgos es el proceso integral de tratamiento de los riesgos descubiertos durante el análisis.

6.2.1. Proceso Análisis de Riesgos

- ✓ Se identificarán los activos de Netboss Comunicaciones S.L. Estos activos están expuestos a una serie de amenazas que, cuando ocurren, degradan el valor del activo, causando un cierto Impacto.
- ✓ Se identificarán una serie de amenazas que afectan directa o indirectamente al activo. Si estimamos la probabilidad de la amenaza, podemos concluir el riesgo en el sistema, o la pérdida a la cual está expuesto.
- ✓ La degradación y la probabilidad califican la vulnerabilidad del sistema frente a una amenaza.

6.2.2. Proceso de Gestión de Riesgos

La gestión de esos riesgos implicará seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Se puede elegir entre las siguientes estrategias para mitigar el riesgo:

- ✓ Asumir el riesgo: aceptar el riesgo y no implantar controles para su disminución o eliminación.
- ✓ Evitar el riesgo: eliminar la causa o la consecuencia de dicho riesgo.
- ✓ Disminuir el riesgo: limitar el riesgo implementando controles que disminuyan el impacto.
- ✓ Transferir el riesgo: pasar el riesgo a otros, como por ejemplo una aseguradora.

Se desplegarán salvaguardas para hacer frente a las amenazas. Las salvaguardas mitigan los valores de impacto y riesgo dejándolos reducidos a unos valores residuales, que serán asumidos por el responsable de la Información o el responsable del Servicio.

El Documento de Aplicabilidad correspondiente especificará para cada control de la ISO 27001 o el ENS, si se aplica o no y el motivo por el que se toma esa decisión.

Los riesgos y los controles adoptados tras el análisis de los riesgos deben ser revisados anualmente, así como siempre que las circunstancias lo aconsejen. Esto se considerará una parte más de la gestión de la seguridad.

7. MONITORIZACIÓN

7.1. Seguimiento y medición de los procesos

El seguimiento de procesos se realiza mediante la comprobación de una lista de indicadores aprobados por Dirección, que incluye la frecuencia del seguimiento, responsable de medición y responsable del análisis de los datos.

En el caso de que se detecte una desviación respecto a los resultados planificados en los indicadores, el responsable de Seguridad deberá abrir una "no conformidad" con objeto de analizar la causa de la desviación y la posible toma de acciones correctivas.

7.2. Auditoría interna

El propósito del presente capítulo es describir los procedimientos y actividades para planificar y llevar a cabo auditorías internas del Sistema de Gestión.

El responsable de Seguridad revisará las Políticas anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la Dirección. Las revisiones comprobarán la efectividad de las políticas, valorando el origen, número e impacto de las incidencias registradas desde la puesta en marcha del SGSI, el coste e impacto de los controles establecidos y las medidas de mejora adoptadas en la empresa y los efectos de los cambios tecnológicos. Estas revisiones incluirán los sistemas de información, a los proveedores de sistemas, a los propietarios de información y de activos de información, a los usuarios y también a la Dirección.

El Comité de Dirección de Netboss Comunicaciones S.L. será, en definitiva, el encargado de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a los activos evaluados originalmente y a las situaciones de riesgo establecidas.

El Sistema de Gestión de Seguridad de la Información se auditará según un plan de auditorías desarrollado por el responsable de Seguridad. El SGSI se auditará completamente cada dos años.

Este punto se desarrollará en el procedimiento de SGI D3 Manual del sistema de gestión integrado.

7.3. Revisión por la Dirección

La Dirección realiza revisiones de su Sistema de Gestión de Seguridad de la Información para asegurar su continua consistencia, adecuación y eficiencia. La revisión efectuada evalúa la necesidad de realizar cambios en el Sistema de Gestión, incluyendo la política, objetivos y otros elementos a la vista de los resultados de la auditoría del sistema, las circunstancias cambiantes y el compromiso de mejora continua. Todo esto se recoge en el Procedimiento SGI D3 Manual del sistema de gestión integrado.

Con los resultados de la Revisión se establece además el plan de gestión, que incluye los objetivos y metas para el siguiente ciclo de mejora.

8. MEJORA CONTINUA

Netboss Comunicaciones S.L. está comprometido con la mejora continua del Sistema de Gestión. Para ello se apoya en las Políticas, los objetivos, los resultados de las auditorías internas, el análisis de datos, acciones correctivas, preventivas y la revisión por la dirección para facilitar la mejora continua.

8.1. Acción correctiva y preventiva

Con el fin de establecer un proceso para reducir o eliminar las causas de no conformidad al objeto de prevenir su reaparición, se ha establecido, y mantiene al día el procedimiento SGI D3 Manual del sistema de gestión integrado, en donde se definen los criterios y responsabilidades asociados a:

- ✓ La identificación de las no conformidades, reales o potenciales.

- ✓ La determinación de las causas de no conformidad.
- ✓ La evaluación de la necesidad de adoptar acciones para asegurar que las no conformidades no vuelven a aparecer.
- ✓ El registro de los resultados de las acciones adoptadas.
- ✓ La revisión de que la acción correctiva o preventiva adoptada es eficaz.

9. PRINCIPIOS DE SEGURIDAD

9.1. Gestión de Activos

9.1.1. Responsabilidades asociadas a los activos

Para gestionar correctamente los activos el responsable de Seguridad mantendrá un inventario actualizado de los activos importantes.

En este inventario se registrará quién es el propietario del activo. Esta responsabilidad será asignada al responsable del área o departamento de Netboss Comunicaciones S.L. donde esté ubicado física o lógicamente el activo.

9.1.2. Clasificación de la información

La clasificación de la información será de acuerdo con la siguiente escala:

Confidencial	Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias serias para la organización
Uso Interno	Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
Pública	Información sin ninguna necesidad de restringir el acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización.

Existirá una relación de la información en Netboss Comunicaciones S.L. con la clasificación que le corresponde (Confidencial/Uso Interno/Pública). El personal de Netboss Comunicaciones S.L. tendrá conocimiento de esta clasificación de manera que sepan en todo momento el tipo de información que utilizan, sin necesidad de establecer un marcado de esta, no revelando así a fuentes externas la clasificación de la información. La destrucción de esta información la realizará el responsable del activo siguiendo las pautas aprobadas por el responsable de Seguridad y con su colaboración si es necesaria.

9.2. Seguridad de la Gestión de los Recursos Humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

La contratación de personal pasa por un proceso de selección en el que deben revisarse las referencias y antecedentes siempre que sea posible.

En las condiciones de la relación laboral deberán quedar reflejadas las responsabilidades del empleado en materia de seguridad de la información. Esta responsabilidad continuará durante un tiempo establecido tras la finalización del contrato.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede. Se realizarán periódicamente seminarios para que el personal conozca los procesos y tareas que deben realizar en materia de seguridad.

Los empleados que infrinjan las normas de Seguridad pueden ser sancionados por un proceso disciplinario de acuerdo con el convenio general.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones a la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

9.3. Seguridad Física y del Entorno

Para que una seguridad lógica sea efectiva es primordial que las instalaciones de Netboss Comunicaciones S.L. mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

9.3.1. Áreas Seguras

- ✓ Netboss Comunicaciones S.L. tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.
- ✓ La totalidad de las oficinas de Netboss Comunicaciones S.L. cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.
- ✓ Los lugares donde se ubican el servidor y el cableado estarán cerrados bajo llave y sólo tendrán acceso las personas autorizadas y los proveedores de servicios cuando vayan acompañados por alguien autorizado.
- ✓ Las ventanas y puertas deberán permanecer cerradas siempre.
- ✓ Las instalaciones de Netboss Comunicaciones S.L. están dotadas de dispositivos de extinción de incendios marcados por la legislación vigente en esa materia. En este sentido, se dispone de extintores y salidas de emergencia debidamente señalizados.
- ✓ Se prohíbe expresamente al personal comer y beber cerca de los servidores y equipos informáticos. Así mismo, se tendrá especial cuidado con el manejo de cualquier producto que pueda verterse sobre activos de información.
- ✓ Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

9.3.2. Seguridad de los equipos

- ✓ Los equipos informáticos son un activo importante del que depende la continuidad de las actividades de la organización, por lo que serán protegidos de manera adecuada y eficaz.

- ✓ Tanto los puestos de usuario como los servidores están protegidos contra posibles fallos de energía u otras anomalías eléctricas, para ello se han instalado equipos de alimentación ininterrumpida.
- ✓ Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el fabricante. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.
- ✓ La eliminación de equipos sólo se llevará a cabo por el responsable de Seguridad o personal en el que éste delegue.

9.4. Gestión de comunicaciones y operaciones

9.4.1. Procedimientos Operativos y Responsabilidades

Netboss Comunicaciones S.L. controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de Netboss Comunicaciones S.L. y otras redes, los mecanismos adecuados de autenticación para usuarios, equipos y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red de Netboss Comunicaciones S.L. existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los trabajadores autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema de información. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo con estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

9.4.2. Gestión de los Servicios Suministrados por Terceros

Netboss Comunicaciones S.L. al contratar un servicio externo para gestionar activos de información introduce en el proceso nuevas vulnerabilidades, ya que los recursos se exponen a posibles daños, pérdidas o filtraciones de información. Por todo ello será necesario tomar una serie de precauciones que aseguren el perfecto uso de la información de Netboss Comunicaciones S.L.

Antes de contratar un servicio externo para la gestión de la información, Netboss Comunicaciones S.L. identificará los riesgos que esta situación conlleva y elaborará un acuerdo en el que se traten las siguientes cuestiones: qué aplicaciones se mantienen en Netboss Comunicaciones S.L. por su especial criticidad, la aprobación de los propietarios de la aplicación, qué implicaciones tiene el contrato para los planes de continuidad del negocio, las normas de seguridad y cómo se medirá su eficacia, quiénes son los responsables y qué procedimientos especiales se seguirán para monitorizar las actividades importantes

de seguridad, quién y cómo manejará las incidencias de seguridad y mediante qué procedimientos se informará a Netboss Comunicaciones S.L. de esas incidencias.

9.4.3. Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de Netboss Comunicaciones S.L.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado por la Dirección.

El responsable de Seguridad supervisará la instalación de las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

9.4.4. Copias de Seguridad

Los datos deben ser guardados en un directorio de la red para asegurar que se realizan copias de seguridad habitualmente.

Habrá procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Estas copias estarán claramente identificadas y se guardarán en sitio seguro, preferiblemente fuera de las instalaciones de la organización.

También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

Si se corrompe la información en operación, hay que comprobar el software, el hardware y las comunicaciones implicadas antes de utilizar las copias de seguridad, para asegurarse de que no se pueda corromper la información contenida en ellas también.

9.4.5. Gestión de la seguridad de la red

Todos los equipos informáticos (estaciones de trabajo y el servidor…) que estén o sean conectados a la red, o aquellos que en forma autónoma se tenga y que sean propiedad de Netboss Comunicaciones S.L. deberán estar sujetos a las normas y procedimientos de instalación que emite el departamento de sistemas y que han sido ratificados previamente por la Dirección.

Los elementos de red (switch, router, etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad de del sistema.

9.4.6. Gestión de Soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

Los soportes (tanto papel como lógicos) que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando alguna persona autorizada deba utilizarla para realizar alguna gestión relacionada con las labores propias de la empresa, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto de trabajo ni los colocará en cualquier otro lugar donde una persona sin autorización pueda verlos o apropiarse de ellos.

Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas. Algunos procedimientos de destrucción que se consideran adecuados son la incineración, el triturado o vaciado de los soportes para que sean usados en otra aplicación dentro de Netboss Comunicaciones S.L.

Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una trazabilidad en caso de auditoría.

9.4.7. Intercambio de Información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

9.4.8. Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos, así como para recomendar cualquier cambio que se estime necesario.

9.5. Control de Accesos

9.5.1. Requisitos del negocio para el control de accesos

La información debe estar protegida contra accesos no autorizados.

Cada responsable de departamento o área definirá las necesidades de acceso a la información a dos niveles, para el conjunto del departamento o área y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

En el caso de que visitantes o personal no autorizado acceda a las instalaciones o a la información de Netboss Comunicaciones S.L. deberá ir siempre acompañado por un miembro responsable de Netboss Comunicaciones S.L. que controlará en todo momento que la seguridad de los recursos está garantizada.

9.5.2. Gestión de accesos de los usuarios

El responsable de Informática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo con las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

9.5.3. Responsabilidades del usuario

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado, así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

De igual forma, es necesario configurar los equipos informáticos para que éste quede bloqueado cuando el usuario no se encuentra en su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

También deben protegerse los puntos de entrada y salida de correo y las impresoras que no se encuentren atendidas por alguna persona de Netboss Comunicaciones S.L.

9.5.4. Control de acceso a la red

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con la organización para mantener el mismo nivel de seguridad que si fueran empleados de Netboss Comunicaciones S.L.

El responsable de Seguridad controlará las altas y bajas de todos los usuarios.

9.6. Gestión de incidentes

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

9.7. Continuidad del negocio

Es imprescindible para Netboss Comunicaciones S.L. establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades del negocio por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad del negocio en estos casos, Netboss Comunicaciones S.L. establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del negocio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del negocio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del negocio se incorporará a los procesos de Netboss Comunicaciones S.L. y será responsabilidad de una o varias personas dentro de la empresa.

9.8. Política de uso aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- ✓ La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- ✓ Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- ✓ No está permitido el uso de los activos para fines personales. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- ✓ Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- ✓ Malgastar los recursos de la red o los sistemas de manera premeditada.
- ✓ Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- ✓ Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- ✓ Revelar las contraseñas y los medios de acceso voluntariamente.
- ✓ Utilizar los equipos para lucro personal.
- ✓ La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar malestar u ofender.
- ✓ Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones o infringir el RGPD).
- ✓ No verificar que los correos están libres de virus.

Asimismo, los usuarios deberán de tener en cuenta las siguientes medidas de seguridad, durante el tratamiento de la información y el uso de los sistemas de TI:

- ✓ Cualquier persona que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.
- ✓ Cada equipo informático de usuario estará bajo la responsabilidad de algún usuario autorizado que tratará de proteger, en la medida de sus posibilidades, la confidencialidad de la información de la empresa y, especialmente de los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido.

- ✓ Cuando la persona responsable de un equipo informático lo abandone temporalmente deberá dejarlo en un estado que impida la visualización de los datos protegidos, bloqueando el usuario e impidiendo el uso de la estación de trabajo. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente. Si el abandono del equipo se produjera debido a la finalización de su turno de trabajo, el usuario procederá al reinicio o apagado del sistema.
- ✓ Se deben retirar de las impresoras y demás periféricos de salida todos los documentos que contengan información de la empresa conforme se vayan imprimiendo.
- ✓ Ningún usuario podrá utilizar dispositivos extraíbles (CD, DVD, USB, etc.) ni almacenar información en ellos, sin la previa autorización del responsable de Seguridad.
- ✓ Los soportes que contengan información deberán estar claramente identificados con una etiqueta externa que indique (directa o indirectamente) de qué fichero se trata y qué tipo de datos contiene.
- ✓ Se deberán guardar los soportes que contengan información en lugar seguro y bajo llave, o en salas, despachos, … con acceso restringido, cuando no sean usados, especialmente fuera de la jornada laboral.
- ✓ Ningún usuario debe instalar ni ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar cualquiera de los recursos informáticos. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente.
- ✓ Queda terminantemente prohibido la modificación de la configuración de cualquier software ya sea sistema operativo o aplicaciones, establecida, por defecto, en el equipo informático por el responsable de Seguridad, sin su previa autorización.
- ✓ El uso del correo electrónico e Internet debe limitarse a las funciones propias del puesto de trabajo.
- ✓ No se debe de responder a correos falsos, ni a cadenas de correos para evitar que la dirección de correo electrónico se difunda. Tampoco se deben abrir ficheros adjuntos sospechosos procedentes de desconocidos o que no se hayan solicitado.
- ✓ Si se detectan virus en los archivos o correos recibidos o durante la navegación por Internet, hay que ponerlo en conocimiento del responsable de Seguridad y al departamento de sistemas.
- ✓ Se asignarán contraseñas a todos los usuarios del sistema como medio de validación de su identidad. El procedimiento de asignación de contraseñas se realiza mediante la entrega personal por parte del responsable de Informática, que es el encargado de comunicar el usuario y la clave para el acceso a los sistemas. Para algunas plataformas será necesario el uso del doble factor de autenticación.
- ✓ La contraseña estará compuesta por un mínimo de 14 caracteres, (Debe tener por lo menos 3 de estas 4 características. Mayúsculas, minúsculas, números o caracteres especiales) y no se deberá revelar bajo ningún concepto, ni se deberá mantener por escrito o a la vista de terceras personas.
- ✓ Se deben cambiar las contraseñas cada dos meses. Así mismo es necesario que los equipos dispongan de protectores de pantalla que se activen a los cinco minutos de inactividad, siendo necesario una contraseña de desbloqueo.
- ✓ La contraseña no debe contener el identificador o nombre de usuario de la cuenta, o cualquier otra información personal que sea fácil de conocer (cumpleaños, nombres de hijos, cónyuges, etc.). Tampoco una serie de letras dispuestas adyacentemente en el teclado (123456, QWERTY, etc.).
- ✓ No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea. Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberán considerarse en peligro.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

Consultar Certificaciones: netboss.es/certificaciones

- ✓ No compartir las contraseñas en Internet, por correo electrónico ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que te soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla.
- ✓ Si un usuario tiene sospecha fundada de que su acceso autorizado está siendo o puede ser utilizado por otra persona, estará obligado a cambiar su contraseña para lo cual contactará con el responsable de Seguridad o Informática, para comunicar la incidencia.
- ✓ No se podrá utilizar ningún acceso autorizado de otro usuario, aunque lo autorice la persona propietaria.
- ✓ Ningún usuario debe intentar acceder a áreas restringidas de los sistemas de información propios o de terceras personas, distintos de los que le hayan sido asignados.
- ✓ Los equipos portátiles y teléfonos móviles serán asignados por Netboss Comunicaciones S.L. Existirá un inventario actualizado de los equipos portátiles y móviles. Netboss Comunicaciones S.L será la unidad encargada de gestionar dicho inventario.
- ✓ Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable de Netboss Comunicaciones S.L. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas. La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de Netboss Comunicaciones S.L. para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- ✓ Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de Netboss Comunicaciones S.L.
- ✓ Los usuarios de estos equipos se responsabilizarán de que no sean usados por terceras personas ajenas a Netboss Comunicaciones S.L. o no autorizadas para ello.
- ✓ Los dispositivos móviles requerirán la autenticación de los usuarios para el acceso a los mismos, así como a las aplicaciones instaladas.
- ✓ En general, los equipos portátiles no deberán conectarse directamente a redes externas (incluyendo la red o el acceso a Internet del usuario en su domicilio). En casos debidamente justificados y previamente autorizados por Netboss Comunicaciones S.L. se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente Normativa General que resulten de aplicación.
- ✓ Quedan prohibidas las conexiones a redes wifi-abiertas, como las proporcionadas en aeropuertos, hospitales, centros comerciales, eventos… ya que esas redes no son seguras y se puede extraer información en las comunicaciones establecidas durante la conexión.
- ✓ Se utilizará software adicional que permita la protección de los dispositivos mediante el uso de sistemas antivirus, así como acciones como la localización y borrado remoto, ante la pérdida de estos.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (ES)
+34 942010701 info@netboss.es

Consultar Certificaciones: netboss.es/certificaciones