Política de Seguridad de la Información aplicable a proveedores con acceso a los sistemas informáticos de Nortegas
ET/502

Índice

Recuerde que esta Documentación en FORMATO PAPEL puede quedar obsoleta. Para consultar versiones actualizadas acuda al Web

Responsable		Fecha
Redacción	Ciberseguridad	19/08/2022
Verificación	Comité Táctico de Ciberseguridad	06/10/2022
Aprobación	Comité Estratégico de Ciberseguridad	10/10/2022

Política de Seguridad de la Información aplicable a proveedores con acceso a los sistemas informáticos de Nortegas
ET/502

1. OBJETO

En toda organización existe información confidencial, en mayor o menor grado, cuya pérdida o uso indebido puede dañar su reputación. Asimismo, el deterioro o indisponibilidad de los sistemas de información puede interrumpir el normal desarrollo de la operativa, produciendo efectos negativos en la calidad del servicio y los beneficios de la compañía.

El principal objetivo del presente documento es mitigar los riesgos asociados a los sistemas de información de Nortegas describiendo lo que se espera de todo el personal que pertenece a terceras empresas que trabajan para Nortegas y que en el desarrollo de sus funciones tenga acceso a la información, sistemas de información o recursos en general de Nortegas, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por Nortegas.

Asimismo, se pretende fomentar el uso de buenas prácticas en materia de seguridad de la información.

Para ello, las empresas proveedoras a las que se les remita este documento se responsabilizan de informar de las normas incluidas en el mismo a las personas que destinen a prestar sus servicios para Nortegas, así como de obtener su compromiso de cumplir y respetar dichas normas.

Esta Política de Seguridad refleja requerimientos legales y éticos aplicables a las actuaciones de los empleados pertenecientes a empresas proveedoras que trabajan para Nortegas. Con dicho propósito, este documento traslada, en lo que es aplicable, lo establecido en la Política de Ciberseguridad de Nortegas y las Normas que lo desarrollan, las obligaciones a las que está sujeta por la legislación vigente, y en particular por:

- el Reglamento (EU) 2016/679 del Parlamento Europeo y del consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- las exigencias de separación de actividades establecidas en la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico (LSE), en la Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos (LSH) y en sus normas de desarrollo.

2. ALCANCE

El ámbito de aplicación de este documento son todas las actividades desarrolladas por personal que pertenece a empresas proveedoras que prestan servicios a Nortegas, vinculadas a través del correspondiente contrato de provisión de servicios.

Cualquier empresa o tercero que para la prestación de servicios a Nortegas tenga que utilizar los sistemas de información o disponga de acceso a los recursos informáticos en general de Nortegas, debe tener conocimiento y comprometerse formalmente a acatar esta Política de Seguridad.

Es obligación de la empresa proveedora poner en conocimiento de su personal la presente Política de Seguridad. Para ello, los contratos o pedidos que se formalicen entre Nortegas y las empresas proveedoras de servicios recogerán de forma expresa que se conoce esta Política y se comprometen a respetarla, así como que asumen las responsabilidades en que pueden incurrir en caso de no cumplirlas.

3. DESARROLLO METODOLÓGICO

3.1. Observaciones

Esta Política de Seguridad es propiedad de Nortegas y tiene carácter de *Información Interna.* Únicamente está permitida su utilización y difusión con carácter interno a Nortegas y a terceros en régimen de subcontratación siempre que sea necesario para el desempeño de las funciones encomendadas.

3.2. Desarrollo de la Política de Seguridad

3.2.1. Política General de Seguridad de la Información

La dirección de Nortegas, como política general de la empresa, garantiza la adecuada gestión de la seguridad de la información procesada y/o albergada por los sistemas y servicios contemplados en el alcance. Para desarrollar esta política, la dirección de Nortegas se compromete a:

a) Llevar a cabo un análisis anual de riesgos de ciberseguridad que permita mantener una adecuada visión de los riesgos de seguridad de la información a los que están

expuestos los activos y desarrollar las medidas necesarias para limitar y reducir dichos riesgos, definiendo las medidas de seguridad a establecer.

b) Desarrollar una completa Normativa de seguridad que regule las condiciones en las que Nortegas, dentro del alcance establecido, debe desarrollar su actividad para respetar los requerimientos de seguridad establecidos.
c) Destinar los recursos y medios necesarios para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre coste y beneficio.
d) Establecer un plan anual de formación y concienciación en materia de ciberseguridad de la información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la seguridad de la información.
e) Desarrollar todas las medidas necesarias para garantizar la adecuada gestión de los incidentes de seguridad que puedan producirse, y que permitan la resolución tanto de las incidencias menores como de las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.
f) Establecer periódicamente un conjunto de objetivos e indicadores en materia de ciberseguridad que permitan el adecuado seguimiento de la evolución de la seguridad dentro de la empresa.
g) Establecer una metodología de revisión, auditoría y mejora continua del sistema, siguiendo un ciclo PDCA que garantice el mantenimiento continuo de los niveles de seguridad deseados. Nortegas establece los procedimientos y formas de actuación necesarias para garantizar el correcto desarrollo de esta Política, que se plasman en un sistema de seguridad, documentado y conocido por todo el personal de la compañía, y que cumple los requisitos establecidos en la norma.

3.2.2. Principios Generales

Tal y como se ha establecido en el ámbito de aplicación, todo el personal externo que desarrolle labores para Nortegas debe cumplir con la Política de Seguridad recogida en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, Nortegas se reserva el derecho de veto sobre el personal externo que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación con la empresa contratada, y que pueden llegar a la resolución de los contratos que tenga vigentes con dicha empresa.

Todo el personal que acceda a los sistemas de información de Nortegas deberá seguir las siguientes normas de actuación:

a) Proteger la información confidencial perteneciente o cedida por terceros a Nortegas de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
b) Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
c) Para obtener el acceso a los sistemas de información propios o bajo supervisión de Nortegas será necesario disponer de un acceso autorizado.
d) Será necesario conocer, aceptar y cumplir la presente Política antes de poder acceder a los sistemas de información de Nortegas. De forma adicional, todo el personal con responsabilidades específicas dentro del ámbito de actuación indicado deberá asegurarse de que se cumplen las siguientes medidas:
    - Con carácter general, todo diseño, desarrollo, implementación y operación deberá incorporar mecanismos de identificación, autenticación, control de acceso, auditoría e integridad, que se especificarán para cada caso concreto.
    - Se deberán incorporar identificaciones seguras y únicas para la autenticación de usuarios.
    - Para un correcto funcionamiento en materia de seguridad deberán compartirse las labores de seguridad entre usuarios, administradores y los encargados directos de la propia seguridad.
    - Deberán tomarse todas las precauciones posibles para proteger físicamente los sistemas y prevenirlos frente al robo, destrucción o interrupción.
    - Deberá existir un plan de recuperación del sistema para el caso en que se dé robo, destrucción o interrupción del servicio.
    - Deberá asegurarse la confidencialidad de la información almacenada, tanto en formato electrónico como no electrónico.
    - Todos los intervinientes en el plan de continuidad de negocio deberán conocer y saber aplicar cuando sea necesario dicho plan.
    - El personal del área de operación deberá tener conocimiento de los procedimientos de recuperación de datos de carácter personal, de sanitización de los soportes de

datos de carácter personal y del procedimiento de registro entrada/salida de dichos soportes.

El área de Ciberseguridad de Nortegas centraliza los esfuerzos globales de protección de los activos de la compañía, a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización. De forma genérica, los activos incluyen toda forma de información, además de las personas y la tecnología que soportan los procesos de información.

El área de Ciberseguridad dispondrá de un inventario actualizado sobre las contratas que contará con los siguientes datos:

- nombre de la contrata
- responsable de la contrata
- teléfono de contacto
- correo electrónico de contacto
- actividades desarrolladas por la contrata
- fecha de inicio de los trabajos
- fecha de finalización prevista

Por cada contrata, también deberá informarse de los usuarios y equipos corporativos utilizados. El responsable de la contrata deberá informar al área de Ciberseguridad cuando haya alteraciones de cualquiera de estos datos.

3.2.3.Confidencialidad de la Información

La confidencialidad de la información se define como la garantía de que la información no es divulgada de forma inadecuada a entidades o procesos.

Con el fin de preservarla:

a) El personal externo que tenga acceso a información de Nortegas deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información de Nortegas a la que haya tenido acceso a través de los medios de difusión pública de información.

b) Los usuarios protegerán la información confidencial a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
c) Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información confidencial en cualquier tipo de soporte, salvo que esté debidamente autorizado.
d) Se utilizará el menor número posible de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
e) En relación con la utilización de agendas de contactos dispuestas por Nortegas (por ejemplo, Outlook) el personal externo únicamente introducirá determinados datos personales que sean indispensables como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
f) Ningún colaborador externo en proyectos o trabajos puntuales deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada a Nortegas tanto ahora como en el futuro.
g) En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
h) Asimismo, el empleado de la empresa proveedora deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación de su empresa con la compañía. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento de la compañía no supondrá, en ningún caso, una modificación de este punto.
i) Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para Nortegas.
j) El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal, que puede dar derecho a exigir compensaciones.

k) Para garantizar la seguridad de los datos de carácter personal albergados en ficheros automatizados, el personal que pertenece a empresas proveedoras de servicios deberá observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:
   - El personal sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de los puestos (ordenadores personales) del personal y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
   - La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable de dicha información o fichero.
   - El propietario de la información se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
   - Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

3.2.4. Información Comercialmente Sensible (ICS)

De acuerdo con las obligaciones de separación de actividades recogidas en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, y en la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico, las sociedades que realicen actividades reguladas tienen la prohibición de compartir información comercialmente sensible con las empresas del grupo al que pertenecen, en el caso de que éstas realicen actividades liberalizadas.

Por ello, es necesario que en la ejecución del servicio contratado el proveedor guarde la confidencialidad de la información comercialmente sensible que las diferentes distribuidoras de Nortegas le proporcionen.

Así, para facilitar el cumplimiento de la regulación relativa a la separación de actividades se incluirá en el contrato una cláusula que recoja dicha obligación por parte del proveedor.

A los efectos de este punto, se considerará información comercialmente sensible cualquier información concreta referida al ejercicio de las actividades reguladas que no sea pública y que, de comunicarse o haberse comunicado a las actividades liberalizadas, podría influir, de manera apreciable, en el resultado de su negocio o suponerles una ventaja competitiva en el desarrollo de las actividades liberalizadas que realizan.

La empresa contratista deberá someterse al tratamiento que las distribuidoras tengan establecido para dicha información.

La empresa contratista se asegurará de que todos los medios humanos que intervengan en la ejecución del servicio respetan el deber de confidencialidad en los términos que han sido señalados.

En caso de incumplimiento, la compañía se reserva el derecho a resolver el contrato. En cualquier caso, la empresa contratista asumirá íntegramente la responsabilidad que derive de dicho incumplimiento y deberá indemnizar a las sociedades de Nortegas que pudieran verse perjudicadas por el mismo.

3.2.5 Control de acceso físico a instalaciones de Nortegas

Se establecen las siguientes normas:

a) El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
b) Se limitará el acceso al personal de soporte externo a las áreas especialmente protegidas.
c) Este acceso, como el de cualquier otra persona ajena que requiera acceder a áreas protegidas, se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado. El sistema de control mantendrá un registro de todos los accesos de personas ajenas.
d) Se acompañará a los visitantes en áreas protegidas y se registrará la fecha y hora de su entrada y salida. Dichas personas deberán ir provistos de la debida tarjeta de identificación o permiso correspondiente y pasar por alguno de los sistemas de control de acceso físico. Sólo se permitirá el acceso previa identificación de la persona de contacto en Nortegas.

3.2.6. Uso apropiado de los recursos

Los recursos que Nortegas pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.) están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso. Queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del servicio, o bien la extralimitación en su uso.
- La búsqueda o explotación de vulnerabilidades en cualquier aplicación o equipos.
- Los equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios de Nortegas o bajo supervisión de la compañía.
- Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), greyware, dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. El proveedor tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- Intentar acceder a áreas restringidas de los sistemas de información sin la debida autorización.
- Intentar distorsionar o falsear los registros “log” de los sistemas de información.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos. Estos actos podrían constituir un delito de daños, según la legislación vigente.

- Albergar datos de carácter personal en las unidades locales de disco de los puestos (ordenadores personales) de usuario.
- Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.
- Conectar ordenadores no corporativos a la red de comunicaciones de la compañía, excepto a la habilitada para ello (red wifi Nortegas-Guest), disponible para visitas y proveedores que necesiten de una conexión de acceso a internet.

3.2.7 Protección frente a malware

Los recursos que el proveedor utiliza para la prestación del servicio a Nortegas deberán seguir las siguientes indicaciones:

a) Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles.
b) El software antivirus se deberá instalar y usar en todos los servidores, en su caso, y en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
c) El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los ficheros de definición de virus tanto en los ordenadores personales como servidores, en su caso, así como de bloqueo frente a la detección de virus informáticos.
d) Todo el software debe estar correctamente licenciado por lo que se prohíbe expresamente el uso de software pirata, crackers, etc.
e) En caso de que sea detectado cualquier malware en uno de los equipos conectados a la red de Nortegas, dicho equipo será desconectado de dicha red sin que sea necesario aviso previo. El área de Ciberseguridad notificará con los medios disponibles el problema encontrado por lo que será responsabilidad de la contrata la eliminación del malware detectado. La conexión de nuevo a la red corporativa debe ser autorizada por el área de Ciberseguridad, la cual solicitará toda la información necesaria sobre el equipo con el fin de asegurar la limpieza de este.

3.2.8. Intercambio de información

Se establecen las siguientes normas:

a) Los usuarios no deben ocultar o manipular su identidad en ninguna circunstancia.
b) En los casos en que, excepcionalmente, Nortegas asigne un usuario genérico, será responsabilidad del proveedor mantener una relación actualizada de las personas que utilizan dicho usuario genérico en cada momento.
c) La distribución de información ya sea en formato digital o papel se realizará mediante los dispositivos facilitados por Nortegas para tal cometido y con la finalidad exclusiva de facilitar las funciones del puesto. Nortegas se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos dispositivos de difusión.
d) En relación con el intercambio de información, se considerarán no autorizadas las siguientes actividades:
   - Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
   - Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
   - Transferencia de ficheros a terceras partes no autorizadas de material de Nortegas o material que es de alguna u otra manera confidencial.
   - Transmisión o recepción de ficheros que infrinjan la Ley de Protección de Datos de Carácter Personal o directrices de Nortegas.
   - Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
   - Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el negocio.
   - Todas las actividades que puedan dañar la buena reputación de Nortegas están prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas para el propio beneficio económico del usuario o de terceras partes, y a actividades de naturaleza política.

e) Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso.
f) Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales donde está ubicado el fichero, dicho tratamiento deberá ser autorizado expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
g) La transmisión de datos de carácter personal de nivel alto a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

3.2.9. Uso del correo electrónico

La cuenta de correo electrónico tiene la consideración de herramienta que el contratista debe aportar para el desempeño de los trabajos contratados.

Se establece el siguiente criterio general:

a) Cada usuario de los sistemas informáticos de Nortegas dispondrá de una cuenta de correo electrónico específica y única, asignada exclusivamente a dicho usuario.
b) Los usuarios externos no dispondrán de una dirección de correo de Nortegas.
c) En el momento de su registro, el usuario externo debe aportar una dirección de correo del dominio de su propia empresa (preferible) o bien una dirección de correo personal.

Este criterio general es compatible con el hecho de que dichos usuarios externos pueden acceder a los buzones de correo genéricos que sean preciso para desarrollar su operativa de trabajo. El envío de correos desde estos buzones genéricos no identifica al emisor.

De forma excepcional, en consideración a las circunstancias que se justifiquen, y siempre previa autorización expresa por parte de Ciberseguridad, un usuario externo podría disponer de una dirección de correo de Nortegas. En tal caso, el responsable del servicio de Nortegas debe cursar la correspondiente solicitud que deberá ser evaluada conjuntamente por Recursos Humanos y Ciberseguridad de Nortegas.

La utilización del correo electrónico por parte de los usuarios externos estará sujeta a las siguientes normas:

a) Se considera al correo electrónico una herramienta más de trabajo provista al usuario con el fin de ser utilizada conforme al uso para el cual está destinada. Esta consideración facultará a Nortegas a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad del usuario y su derecho a la intimidad.
b) El sistema de correo electrónico de Nortegas no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
c) Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).
d) No está permitida la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
e) No está permitida la transmisión vía correo electrónico de información confidencial de la compañía salvo que la comunicación electrónica esté bien cifrada y el envío este expresamente permitido.

3.2.10. Conectividad a Internet

La utilización de internet por parte de los usuarios externos estará sujeta a las siguientes normas:

a) Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al servicio prestado a la compañía.
b) Todo el tráfico desde y hacia Internet será inspeccionado en búsqueda de amenazas. En caso de que algún equipo se encuentre accediendo a sitios clasificados como maliciosos (pornografía, juego, etc.) o ajenos al negocio podrá ser desconectado de la red sin que sea necesario aviso previo.
c) Nortegas se reserva el derecho de, en lo permitido por el marco legal, y sin aviso previo, limitar el acceso total o parcial a Internet a partir de la red informática y terminales de la compañía.
d) El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión

deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.

e) Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al de Nortegas en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
f) Únicamente se permitirá la transferencia de datos de o a Internet en conexión con las actividades del servicio prestado a la compañía. La transferencia de ficheros no relativa a estas actividades (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia) está prohibida.

3.2.11. Responsabilidades del usuario

Todo usuario externo, por el mero hecho de serlo, asume determinadas responsabilidades:

a) Cada usuario será responsable de su contraseña y todo lo que de ella se derive, por lo que es imprescindible que esta sea únicamente conocida por el propio usuario; no deberá revelarla a nadie, bajo ningún concepto, por ningún motivo.
b) El usuario será responsable de todas las acciones registradas en los sistemas informáticos de la compañía con su código de usuario y su contraseña.
c) El usuario deberá seguir las directivas definidas en relación con la gestión de las contraseñas.
d) El usuario deberá asegurar que los equipos quedan protegidos cuando estén desatendidos.
e) Se establecerán las siguientes políticas de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
   - Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
   - No dejar desatendidos los equipos asignados a funciones críticas y bloquear su acceso cuando sea estrictamente necesario.
   - Asegurar la confidencialidad de los documentos tanto en los puntos de recepción y envío de información (correo postal, máquinas de escáner y fax) como en los equipos de duplicado (fotocopiadora, fax y escáner).

- La reproducción o envío de información con este tipo de dispositivos queda bajo la responsabilidad del usuario.
- Los listados con datos de carácter personal o información confidencial deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
- Los listados con datos de carácter personal o información confidencial deberán eliminarse de manera segura una vez no sean necesarios.

f) En caso de identificarse incidentes o debilidades relacionadas con la seguridad de la información, se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar esta supuesta debilidad o incidente de seguridad.

3.2.12. Equipos de usuario

Sobre el equipamiento informático asociado al puesto del usuario se establecen los siguientes principios:

a) Todos los puestos de usuario con conectividad a recursos informáticos de Nortegas estarán controlados por Nortegas.
b) Ningún usuario intentará por ningún medio transgredir el sistema de seguridad y las autorizaciones, ni dispondrá de herramientas que puedan realizarlo.
c) Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas.
d) Cuando se desatienda un puesto durante un periodo corto de tiempo el usuario deberá activar su bloqueo.
e) Cuando se termina la jornada de trabajo se debe apagar el equipo.

3.2.13. Identificadores de usuario y contraseñas

El personal de empresas proveedoras de servicios que accede a los sistemas de información de Nortegas dentro de su ámbito de trabajo, es responsable de asegurar que los datos, las aplicaciones y los recursos informáticos sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados.

Este personal está obligado a utilizar los recursos de la compañía y los datos contenidos en ellos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales.

Para obtener el acceso a los sistemas de información este personal debe disponer de un acceso autorizado (identificador de usuario y contraseña) sobre el que, como usuarios de sistemas de información, deben observar los siguientes principios de actuación y buenas prácticas:

a) Cuando el usuario recibe su identificador de acceso a los sistemas de Nortegas se considera que acepta formalmente la Política de Seguridad vigente.
b) El usuario debe mantener sus credenciales de acceso confidenciales.
c) Todos los usuarios con acceso a un sistema de información dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
d) Los intentos de conexión sin éxito son limitados en número.
e) Todos los intentos de conexión son registrados, tanto tengan éxito o no.
f) El usuario es responsable de toda actividad relacionada con el uso de su acceso autorizado.
g) El usuario no debe utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
h) El usuario tendrá acceso autorizado únicamente a aquellos datos y recursos que precise para el desarrollo de sus funciones.
i) El usuario no debe incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
j) Las contraseñas estarán constituidas por combinación de caracteres alfabéticos (mayúsculas y minúsculas), numéricos y especiales.
k) El usuario no debe revelar bajo ningún concepto y por ningún motivo su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista ni al alcance de terceros.
l) El usuario no debe utilizar las mismas contraseñas para uso personal y profesional.
m) Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
n) En relación con los datos de carácter personal, exclusivamente el personal autorizado para ello podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.
o) Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder de inmediato a

cambiar su contraseña y contactar con el CAU de Nortegas para notificar la incidencia.

3.2.14. Software

Sobre el software se establecen los siguientes principios:

a) Nortegas facilitará al proveedor un documento que incluirá directrices a seguir en relación con el software de los equipos ("ET-501 Conexión de Empresas Colaboradoras a la red de datos").
b) Todo el personal que accede a los sistemas de información de Nortegas debe utilizar únicamente las versiones de software indicadas y siguiendo sus normas de utilización.
c) Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
d) Se prohíbe el uso de software no validado.
e) Se prohíbe el uso de software sin su respectiva licencia.
f) Se prohíbe el uso de software crackeado o pirateado.

3.2.15 . Conexión a la red

Sobre la conexión a la red se establecen los siguientes principios:

a) En caso de que el proveedor necesite acceder a la red de Nortegas para la prestación de los servicios, debe solicitar la "ET-501 Conexión de Empresas Colaboradoras a la red de datos", identificando la empresa y persona de contacto.
b) El acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación previa validación del acceso.
c) Nortegas se reserva el derecho de, sin aviso previo, bloquear, suspender, alterar o monitorizar los servicios soportados en su red informática y puestos a disposición de las entidades externas.
d) No se deberá conectar a ninguno de los recursos de la compañía ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas a la red corporativa.
e) Nadie deberá conectarse a la red corporativa de Nortegas a través de otros medios que no sean los definidos.

f) Nortegas se reserva el derecho a desconectar de la red corporativa y sin aviso previo a cualquier equipo utilizado por un proveedor cuando se detecten actividades que contravengan los principios y normas expresados en el presente documento.

3.2.16. Gestión de Accesos

Existe un proceso formal para el registro, concesión, alteración y revocación de accesos a los usuarios, aplicable a todos los sistemas de Información de Nortegas.

Se establecen los siguientes principios:

a) Existe un proceso formal para la gestión de los accesos de los usuarios a los sistemas.
b) Se debe asegurar la comunicación de las reglas y responsabilidades en el uso de los sistemas de información de Nortegas a los usuarios al atribuirles cualquier acceso a los sistemas.
c) Para cada sistema existe un conjunto de perfiles y privilegios que se atribuyen a los usuarios de acuerdo con sus necesidades.
d) Los privilegios de acceso a los sistemas se atribuyen a los usuarios considerando las necesidades efectivas para el desempeño de sus funciones, no debiendo ser atribuidos ni por exceso ni por defecto.
e) Los sistemas de Nortegas, por omisión, bloquean el acceso a los usuarios no autorizados.
f) Los privilegios de acceso a los sistemas garantizan una correcta segregación de funciones.
g) En los casos en los que no es posible garantizar la segregación de funciones, están implementados los controles compensatorios adecuados.
h) Cualquier solicitud de atribución o modificación de privilegios de acceso a los sistemas de Nortegas se debe registrar en la herramienta Jira y posteriormente debe ser aprobada.
i) Los accesos y respectivos privilegios solo se implementan en los sistemas después de obtener todas las aprobaciones necesarias.
j) Se mantiene un registro formal de todos los usuarios autorizados y respectivos privilegios de acceso a los sistemas de Nortegas.
k) Las modificaciones en las necesidades de acceso a los sistemas deben llevar aparejados los ajustes a los derechos de acceso.

l) Los privilegios de acceso a los sistemas atribuidos a los usuarios son revocados de forma automática, cuando termina su relación profesional con la compañía.
m) Se realiza una revisión periódica con el fin de eliminar o bloquear cuentas redundantes o innecesarias.
n) Los usuarios deben tener asociados, identificadores individuales (user ID), protegidos por contraseña.
o) El uso de identificadores genéricos (cuentas genéricas o de grupo) se debe permitir solo en casos excepcionales debidamente justificados, aprobados y registrados.
p) Las cuentas genéricas tienen asociado un usuario individual responsable de esa cuenta.
q) La nomenclatura utilizada en la generación de los identificadores obedece a reglas definidas por Nortegas.
r) El identificador de usuario permite reconocer su identidad, pero nunca sus niveles de privilegios.
s) El identificador debe ser personal, de uso exclusivo y único para todos los sistemas (cuando sea técnicamente viable).
t) Los identificadores de los usuarios que ya no tienen vínculo con la compañía no pueden ser atribuidos a otros usuarios, excepto en áreas de gran rotación de personas.
u) En los casos de áreas de gran rotación referidas en el punto anterior, debe existir una aprobación formal de la excepción por el responsable del área.
v) Para las excepciones debe quedar registrado y mantenido un histórico de las personas asociadas a un user ID y en qué periodo de tiempo.
w) Nortegas se reserva el derecho de, sin aviso previo, bloquear, suspender, modificar y monitorizar a los usuarios de sus sistemas y los respectivos privilegios de acceso.
x) El responsable de la contrata debe notificar al responsable del servicio en Nortegas todos los cambios habidos en cuanto a las personas, identidades y equipos que estén conectados a la red corporativa. Además, el responsable de Nortegas tiene la obligación de comunicar esta información al área de Ciberseguridad, la cual mantendrá un inventario actualizado de las conexiones realizadas a la red corporativa por las contratas.

3.2.17. Propiedad intelectual

En relación con la Propiedad Intelectual se aplicarán los siguientes principios:

a) Las entidades externas que acceden a Internet a partir de la red informática y/o terminales de Nortegas son responsables de respetar los derechos de propiedad intelectual aplicables a los contenidos accedidos.
b) Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
c) Los usuarios externos únicamente podrán utilizar material autorizado por su empresa o por Nortegas para el desarrollo de sus funciones.
d) Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia.
e) Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.
f) Nortegas únicamente autorizará el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

3.2.18. Incidencias

En el caso de detectarse alguna incidencia relacionada con los sistemas de información se seguirán las siguientes normas:

a) Ante cualquier incidencia que afecte al servicio se seguirán los procedimientos establecidos por Nortegas.
b) Todo el personal externo deberá ponerse en contacto con el servicio del centro de atención al usuario (CAU) en caso de que detecte cualquier incidencia relacionada con la información o los recursos informáticos de Nortegas.
c) Cualquier usuario podrá trasladar al responsable de Ciberseguridad sugerencias y/o debilidades, que pueda tener relación con la seguridad de la información y las directrices contempladas en la presente Política.
d) Se deberá notificar al responsable de Ciberseguridad cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.

e) El centro de atención al usuario (CAU) de Nortegas centraliza la recogida, análisis y gestión de las incidencias recibidas.

3.3. Requisitos de seguridad para la externalización

La empresa proveedora debe documentar y aplicar la sistemática adecuada para asegurar los siguientes requisitos:

a) El personal afectado debe conocer y aplicar la Política de Seguridad.
b) Deben cumplirse los requisitos reglamentarios y normativos aplicables (LOPD, LSSI, ICS).
c) Nortegas facilitará al proveedor un documento con las directrices a seguir para la conexión a su red corporativa y la instalación de los puestos de trabajo ("ET-501 Conexión de Empresas Colaboradoras a la red de datos").
d) La lista de usuarios autorizados y el registro de accesos estarán disponibles para su verificación por parte del responsable del servicio.
e) El acceso ocasional a las instalaciones de personas no autorizadas deberá quedar registrado. Estas personas estarán debidamente identificadas y acompañadas en todo momento por personal autorizado.
f) El responsable del servicio por parte de Nortegas podrá verificar estas condiciones personalmente o delegar en otra persona de la compañía o en otra empresa especializada. Deberá facilitarse el acceso para los aspectos relacionados con auditorías internas o externas cuando la compañía lo estime conveniente.
g) El proveedor notificará a Ciberseguridad si se ha producido una brecha de seguridad o cualquier cambio en el sistema de seguridad en el momento en que se detecte. Dicha brecha será tomada como una no conformidad según su sistema de calidad ISO 9000 (o procedimiento equivalente).
h) El sistema debe tener en cuenta el procedimiento de devolución/destrucción de los datos y activos una vez finalizado el servicio. En caso de detectarse algún incumplimiento de estos requisitos, será registrado en su sistema de calidad ISO 9000 (o procedimiento equivalente) donde se establecerán las acciones correctivas y preventivas pertinentes y se dará seguimiento de la misma hasta su cierre en un plazo máximo acordado con el responsable del servicio.

Nortegas se reserva el derecho de exigir:

a) La implementación de cualquier mecanismo que Nortegas considere necesario para garantizar la seguridad de acceso a sus datos y activos. Asimismo, podrá exigir las penalizaciones y/o las garantías apropiadas en función de los riesgos de incumplimiento o deterioro de los activos del servicio.
b) La presencia y colaboración de todas las empresas colaboradoras y proveedoras y su mejor ayuda en la restauración –bajo la coordinación directa de Nortegas- de la actividad normal de sus operaciones de negocio, después de que éstas hayan sido interrumpidas por una emergencia o desastre.
c) La tenencia de políticas y planes de continuidad de negocio o contingencias que permitan asegurar la continuidad de las actividades de estas compañías en el caso de que se vieran afectadas por una catástrofe o situación de desastre. De igual forma, Nortegas se reserva el derecho de auditar la existencia y grado de implantación de los mencionados planes.

3.4. Seguimiento y Control

Con el fin de velar por el correcto uso de los mencionados recursos, a través de los mecanismos formales y técnicos que se considere oportunos, Nortegas comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de dichos recursos por todos los usuarios.

En caso de apreciar que alguien utiliza incorrectamente aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, se le comunicará tal circunstancia y se le facilitará, en su caso, la formación necesaria para el correcto uso de los recursos.

En caso de apreciarse mala fe en la incorrecta utilización de las aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, Nortegas ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

Los contratos con los proveedores recogerán la posibilidad de que Nortegas lleve a cabo pruebas de penetración para evaluar los niveles de seguridad de sus sistemas, o bien que estas sean realizadas por parte de un proveedor autorizado. En ambos casos, Nortegas deberá exigir la remediación de las vulnerabilidades encontradas, en los plazos establecidos por Nortegas.

3.5. Actualización de la Política de Seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, Nortegas se reserva el derecho a modificar esta Política cuando sea necesario.

Los cambios realizados en esta Política serán divulgados a todas las empresas proveedoras de servicios a las que les aplique utilizando los medios que se consideren pertinentes.

Es responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento de la Política de Seguridad más reciente de la compañía por parte de su personal.

3.6. Otros

3.6.1 Abreviaturas, Acrónimos y Definiciones

Abreviatura/Acrónim	Descripción
LOPD	Ley Orgánica de Protección de Datos de carácter personal, Ley 15/1999, de 13 de Diciembre.
LSSI	Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, Ley 34/2002, de 11 de Julio.
ICS	Información Comercialmente Sensible.
LSE	Ley 24/2013, de 26 de diciembre, del Sector Eléctrico.
LSH	Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos.
PDCA	Plan-Do-Check-Act: el ciclo de Deming o espiral de mejora continua, es una estrategia de mejora continua de la calidad en cuatro pasos.