

MARCO NORMATIVO DE SEGURIDADE

NOR_002 NORMATIVA DE XESTIÓN DE ACCESO REMOTO



CONCELLO DE RIANXO

CONTROL DE SINATURAS

ELABORADO POR:

RESPONSABLE DO SISTEMA

20/01/2026

APROBADO POR:

RESPONSABLE DO GOBERNO - ALCALDE

22/01/2026

CONTROL DE VERSIÓNS

- | | | |
|-----|------------|----------------------------------|
| 1.0 | 20.01.2026 | Responsable do Sistema |
| | | Versión inicial do documento |
| 1.1 | 03.03.2026 | Responsable do Sistema |
| | | Revisión do control de sinaturas |

1. OBXECTO

O obxecto deste procedemento é recoller de forma integral os cumprimentos e controis a implementar na xestión do acceso remoto ao sistemas electrónicos do Concello de Rianxo.

Este documento réxese en definición, desenvolvemento e circuíto de aprobación pola Normativa NOR_003 de Xestión da documentación.

Calquera posible incumprimento desta normativa, estará suxeito ao disposto no apartado 9 de incumprimentos da Normativa NOR_001 de Uso de Medios Electrónicos.

2. ALCANCE

Todos os sistemas de información e persoal relacionados co Concello de Rianxo.

3. DEFINICIÓNS

VPN: Unha rede privada virtual (RPV) (en inglés, Virtual Private Network, VPN) é unha tecnoloxía de rede de computadores que permite, mediante técnicas criptográficas, unha extensión segura da rede de área local (LAN) sobre unha rede pública ou non controlada como a Internet. Permite que o computador na rede envíe e reciba datos sobre redes compartidas ou públicas con toda a funcionalidade, seguridade e políticas de xestión dunha rede privada.

Segmentación de Rede: Consiste na división dunha rede en distintas subredes máis pequenas co propósito de mellorar non só o rendemento global da rede, senón, sobre todo, as súas condicións de seguridade. A segmentación permite o control de tráfico entre as distintas subredes, en base a políticas definidas de segmentación, o que illa e mellora a seguridade.

Mitigar: Moderar, diminuír ou suavizar algún parámetro ou atributo, como pode ser o nivel de risco.

Cifrado: o cifrado é un procedemento que emprega algún mecanismo criptográfico para protexer a confidencialidade e, no seu caso, a integridade e a autenticidade da información.

Acceso: é o resultado positivo dunha autenticación.

4. DESENVOLVEMENTO

A seguinte normativa pretende regular os principios xerais de interconexión e acceso remoto aos sistemas de información da Organización, ofrecendo pautas e requirimentos mínimos que deben ser cumpridos respecto ao uso de VPNs, así como redirixindo ao procedemento adecuado respecto ás conexións LAN to LAN con outras redes propias ou alleas.

Cada vez máis, aumentan as posibilidades de poder realizar tarefas sen a necesidade de estar presente, de forma que o traballo cotiá pode ser realizado por persoas localizadas en diferentes localizacións. Isto implica necesariamente a necesidade de conceder os medios para o acceso remoto aos sistemas de información. É evidente que estas modalidades non deben descoidar a seguridade e protección da información, así como os datos das organizacións.

Considerarase acceso remoto ao realizado desde fóra do perímetro das propias instalacións da organización. Para levar a cabo a autorización de acceso remoto as organizacións necesitan establecer normas, restricións, procedementos e mecanismos operativos que doten ao acceso da necesaria seguridade.

Para realizar a solicitude do acceso remoto, a persoa interesada ou a súa responsable deberá solicitar o acceso ao Responsable do Sistema. Esta solicitude ha de ser clara e concreta, e pode referirse a un período de tempo determinado para realizar determinadas tarefas, ou ben mentres dure a vinculación coa organización, como sería o caso dunha situación contractual cun provedor, un contrato laboral con persoal interno, ou a aceptación do destino dun funcionario público nunha Organización pertencente ao devandito sector.

Tendo en conta o indicado no parágrafo anterior, o Responsable do Sistema será o encargado de cubrir o *Formulario normalizado de solicitude de Conexión remota á Rede dá Xunta de Galicia e a sistemas de EELL integrados na RCXG (VPN)*, dispoñible na sección de servizos do Portal Eido Local, e de rexistrar a solicitude. Este documento deberá ser aprobado pola Alcaldía, segundo indica o propio formulario, e recolle o apartado correspondente do *Procedemento de Xestión de Autorizacións*.

Os permisos de acceso remoto daranse de baixa unha vez rematen as causas que motivaron a solicitude.

A continuación, especifícanse as características e especificacións do acceso remoto á Rede Corporativa, xunto cunha lista de normas e recomendacións para cada unha delas.

4.1. Acceso individual por VPN

A utilización dunha VPN ou rede privada virtual permite a creación dun túnel seguro mediante o cifrado de datos durante a conexión, outorgando acceso remoto seguro entre o equipo individual e a rede da empresa.

Para asegurar a autenticidade de extremo a extremo nunha canle de comunicacións, antes de intercambiar información deberá establecerse o uso de contrasinais acordos á política da organización.

Habilitarase o rexistro de auditoría das conexións, incluíndo as direccións IP orixe e destino, data e hora de inicio e finalización da conexión VPN, así como o IDE de usuario que se conecta.

O algoritmo de cifrado empregado pola solución VPN será dos recomendados polo CCN en función da categoría do sistema.

Para o emprego de accesos remotos baseados en VPN, os usuarios deberán ter en conta:

- É responsabilidade da persoa usuaria autorizada, para acceder mediante VPN, asegurarse de que ningunha outra persoa utilice a súa conta de acceso, entendendo que é de uso persoal e intransferible para aquelas a quen lles sexa asignada.
- A utilización de múltiples conexións VPN desde un mesmo equipo de usuario non está permitida, polo que unicamente debe empregarse unha conexión activa por usuario nun momento dado.
- A conexión VPN establecida será automaticamente desconectada se non se detecta actividade. O usuario deberá autenticarse novamente para volver conectarse á rede.
- O equipo remoto desde o que se establecerá a conexión debe ser, por defecto, propiedade da Organización, polo que estará endurecido (configurado con criterios seguros) e cos programas de seguridade (antivirus e similares) actualizados.
- O acceso remoto á rede da Organización desde computadores públicos, entendendo por estes aqueles que se alugan por tempo de conexión, salas da internet de dispoñibilidade pública, cibercafés e similares, está estritamente prohibido.

Se se require realizar a conexión remota VPN desde un equipo particular (BYOD), esta requirirá autorización específica, debendo adicionalmente terse en conta as seguintes consideracións:

- O equipo deberá ter instalada e actualizada unha solución antivirus, así como ter ao día as actualizacións de seguridade do sistema operativo e as aplicacións.
- Queda prohibido deixar desatendido o equipo durante a xornada laboral, permanecendo vixentes as normas xerais da Organización orientadas ao posto de traballo, como é bloquear o equipo cando non estea atendido. Deberá liberarse a conexión VPN ante pausas que se prevexan prolongadas.
- Mentres a VPN se atope conectada á Organización non deberán estar en execución aplicacións persoais.
- Se o equipo persoal é empregado por máis dun membro da familia, deberá existir un perfil de usuario independente desde o que se realice a conexión VPN coa Organización.
- Ademais, tendo en conta que en situacións de teletraballo se atenden chamadas e videoconferencias en aberto, habitualmente falando a través do micrófono do equipo e escoitando a través dos seus altosfalantes, requirirase desactivar calquera asistente virtual (tipo Alexa, Siri, Copilot, Google Asistant ou similar) que puidese estar na

habitación onde nos atopemos, buscando con iso manter a confidencialidade o e segredo.

4.2. Acceso por LAN to LAN

Coñécese como interconexión LAN to LAN ao servizo de transmisión de datos punto a punto que permite conectar entre si dúas redes, por exemplo, as correspondentes a dúas sedes dunha mesma Organización, ou a conexión dunha sede con determinada rede dun provedor. Por cuestións de seguridade, a conexión entre sedes ha de realizarse empregando liñas corporativas integradas na Rede Corporativa da Xunta de Galicia. Noutros casos procederáse a bloquear o acceso á Rede Corporativa da Xunta naquelas sedes que dispoñan de equipos aos que se lles permita acceder a Internet mediante outra conexión

4.3. Acceso de Provedores

Cando a organización, xa sexa por acordos ou por servizos contratados, necesite garantir acceso a provedores cos que teña algunha relación, deberá verificar de maneira constante o acceso de terceiros aos sistemas da organización, levando control das contas ou accesos compartidos:

- Segmentando a rede física, limitando os accesos ás persoas usuarias, contas e procesos informáticos unicamente aos recursos absolutamente necesarios para realizar as actividades rutineiras para as que se atopan autorizadas.
- Habilitando controis de permisos específicos: a utilización de solucións de administración de accesos privilexiado para conceder unicamente os permisos necesarios e adecuados.
- Outorgando accesos remotos VPN ao persoal do provedor que o requira, se é posible con períodos finitos de vixencia, prorrogables.
- Revogando o acceso VPN ao finalizar a relación contractual, ou ao ser substituído o colaborador asignado polo provedor.
- Realizando auditorías periódicas co propósito de achar e desactivar posibles accesos remotos que xa non sexan necesarios.

Para o acceso autorizado de provedores deberán respectarse as pautas establecidas pola Xunta de Galicia e a Deputación da Coruña para o acceso aos seus sistemas e servizos.

4.4. Acceso a documentos compartidos e traballo colaborativo

Na actualidade, o Concello de Rianxo dispón dunha solución propia, baseada en sistemas NAS de

unidades de rede compartidas, para o acceso compartido a documentos, e da plataforma colaborativa Google Workspace, proporcionada por convenio coa Deputación da Coruña para o intercambio de información.

Estableceranse as seguintes medidas de protección dos documentos:

- A documentación unicamente será accesible polas persoas autorizadas, ao tempo que os usuarios da plataforma colaborativa ou de arquivos compartidos unicamente accederán aos cartafoles ou documentos autorizados, xa sexa para consulta, descarga, modificación ou supresión, como para incorporar novos documentos.
- Estableceranse permisos a nivel de usuario ou grupo de usuarios.
- Debe dispoñerse de trazabilidade respecto aos documentos.
- É recomendable establecer mecanismos que permitan coñecer se o documento se abre, ou se tenta abrir, desde unha localización descoñecida ou por unha persoa usuaria sen permisos.

5. COMUNICACIÓN DE DEFICIENCIAS DO PROCEDIMENTO

Calquera deficiencia ou inconsistencia neste procedemento deberá de ser posta en coñecemento da persoa Responsable da Seguridade.

6. DOCUMENTACIÓN COMPLEMENTARIA

- Normativa de Uso de Medios Electrónicos
- Formulario de Petición
- Procedemento de Xestión de Autorizacións
- Guía CCN-STIC-836 Seguridade en Redes Privadas Virtuais (VPN)
- Guía CCN-STIC-807 Criptoloxía de emprego no Esquema Nacional de Seguridade
- CCN-CERT BP/18 Recomendacións de seguridade para situacións de teletraballo e reforzo en vixilancia.
- Checklist CCN-CERT BP-18 Seguridade para situacións de teletraballo.xlsx
- Formulario de solicitude de conexión remota para entidades locais – Rede Corporativa dá Xunta de Galicia (RCXG).
- Política de acceso remoto corporativo a RCXG.

7. ANEXOS

7.1. RECOMENDACIÓNS

O acceso remoto aos sistemas de información corporativos debe facerse desde unha conexión a internet de confianza: unha conexión corporativa, se se dispón dela, ou a conexión persoal do fogar; nunca conexións públicas.

O acceso remoto activarase durante a xornada laboral, a condición de que sexa necesario para a realización das actividades laborais que se vaian a levar a cabo ese día. A conexión remota non pode quedar aberta fóra da xornada laboral ou cando non sexa necesario o seu uso, por motivos de seguridade e para evitar un consumo de recursos innecesario na plataforma corporativa de acceso remoto.

Recomendacións sobre o equipo informático persoal que se utilice para o acceso remoto aos sistemas de información da Rede Corporativa:

- O equipo informático que se utilice para a conexión debe ter as actualizacións de seguridade do sistema operativo instaladas, e tamén as do software ofimático, lectores de PDF e outro software de uso habitual. Debe contar tamén con algún tipo de software de seguridade, como por exemplo un antivirus, actualizado e que reciba actualizacións frecuentemente.
- No equipo persoal que se utilice para conectarse en remoto aos sistemas de información corporativos, deberanse seguir unhas pautas de navegación web segura pola rede internet que eviten comprometer a seguridade do equipo.
- O equipo debe estar protexido por un contrasinal forte ou outro medio de protección adecuado.
- Débese utilizar unha conta de usuario diferente á que se utilice para o uso persoal do equipo, destinada expresamente para o traballo remoto.
- Durante o uso dos medios de teletraballo, cómpre recordar:
 - Non se deben realizar simultaneamente co mesmo equipo actividades alleas á actividade de traballo, como por exemplo:
 - acceder a páxinas web non relacionadas coa actividade;
 - executar aplicacións non corporativas;
 - abrir documentos non corporativos ou recibidos desde fontes que non son de confianza;
 - permitir a execución de macros de documentos ofimáticos
 - É conveniente recordar que os medios de protección dun equipo fóra das

instalacións do organismo poden ser nalgúns aspectos menores que cando se está situado dentro do perímetro de seguridade do organismo, polo que cómpre extremar as precaucións.

Sempre que sexa posible, débese **evitar copiar información ao disco local** do computador que se estea utilizando na casa. A recomendación é utilizar unha conexión de escritorio remoto ao computador do traballo, almacenando toda a información nos repositorios de información corporativos.

No caso de que a información se copie de forma temporal, debe ser eliminada en canto se remate de utilizar.

É importante lembrar as recomendacións habituais sobre o uso do correo electrónico, en particular estar alerta ante calquera correo electrónico sospeitoso, e no caso de recibilo seguir as seguintes pautas:

- Non abrir ligazóns
- No caso de abrilas, comprobar que o enderezo web sexa fiable
- Non abrir os ficheiros adxuntos.

Non introducir as credenciais (usuario ou contrasinal) en páxinas web nas que se dubide sobre a lexitimidade das mesmas. Ao abrir unha páxina web, é importante verificar que é unha páxina lexítima, fixándose ben na dirección que se mostra na barra de direccións do navegador web e tamén, de usarse protocolo seguro (HTTPS), verificar o certificado asociado á páxina web.

Hai que sospeitar de correos con faltas de ortografía ou outros erros de redacción, así como calquera outro elemento sospeitoso. Ante calquera dúbida é importante verificar o campo "de" do correo electrónico e comprobar cal é a dirección de correo do remitente, máis aló do alias que empregue.

Hai que sospeitar de ligazóns curtas ou daqueles nos que, ao pasar o punteiro do rato por encima deles, apunten a unha dirección que non sexa unha dirección web coñecida ou de sitios web da organización.

Hai que ter en conta que, en ocasións, os atacantes poden utilizar unha dirección de correo lexítima da propia entidade previamente comprometida nun ataque anterior, mesmo como reenvío dun fío de correos lexítimo intercambiado entre persoas pertencentes á entidade. Nestes casos hai que extremar a atención, xa que é máis complicado darse conta do engano, polo que, en caso de dúbida, recoméndase chamar ou contactar co remitente para confirmar a lexitimidade do correo.

No caso de ser vítima dun destes correos fraudulentos ou ante calquera dúbida, deberase comunicalo canto antes ao Responsable de Seguridade da organización e contactar co Centro de Atención ao Usuario (CAU) de referencia, para que se poida minimizar calquera impacto.

Existen na actualidade páxinas web e envíos de correo electrónico fraudulentos que tentan enganar ás persoas usuarias, redirixíndoas a páxinas web con contidos maliciosos coa intención de conseguir as credenciais (usuario/contrasinal) da persoa usuaria para logo levar a cabo ataques informáticos, ou simplemente co obxectivo de difundir información falsa. É importante por tanto estar moi alerta. Se recibe chamadas, correos, mensaxes, etc., que aparentemente teñen orixe en persoal da organización, centros de atención a usuarios, etc., lembre que:

Nunca debe facilitar información de medios de acceso (usuario e contrasinal, tokens, códigos recibidos por SMS, etc.), nin sequera tratándose do persoal real de atención a usuarios, xa que o persoal de atención a usuarios debe ter mecanismos para corrixir incidencias e restablecer contrasinais sen requirir que a persoa usuaria o teña que facilitar.

O persoal de atención a usuarios dos organismos conta con medios de acceso ás infraestruturas que lles deben permitir solucionar os problemas sen requirir datos de acceso das persoas usuarias.

Se está a detectar problemas no seu acceso remoto, contacte directamente cos medios de atención a usuarios habituais. Non confíe en chamadas ou correos "proactivos" dun suposto CAU se non pode confirmar que se trata realmente do centro de atención a usuarios co que vostede contacta habitualmente.

En particular, recoméndase estremar as precaucións antes os métodos de engano máis comúns:

- Contido dos correos electrónicos que recibe: desconfiar por sistema de toda a información recibida ata comprobar que se trata dunha fonte fiable.
- Documentos e arquivos adxuntos nos correos electrónicos: non abrílos mentres non se comprobe a fiabilidade da orixe da mensaxe.
- Aplicacións que se ofrecen para descargar e instalar: non está permitida a instalación de ningunha aplicación sen a autorización previa da persoa responsable do Sistema.

No relativo á información falsa, deberase seguir as pautas:

- Non difundir información que non teña que ver coa manexada polo departamento.
- Non difundir información de temas alleos ao traballo.
- Non difundir información que non proveña de medios e fontes oficiais.
- Non contribuír á difusión de contido non contrastado.
- Non compartir mensaxes que poidan xerar alarma na poboación; son as autoridades e os medios de emerxencia quen deben deseñar as estratexias de comunicación.

Recoméndase utilizar as ferramentas corporativas postas a disposición pola organización para o traballo remoto, evitando utilizar plataformas alleas, que poderían implicar riscos de seguridade (técnicos e normativos).

O acceso remoto mediante VPN, así como as plataformas para compartir documentos e as de traballo colaborativo, sempre supoñen riscos. Con todo, son unha forma de conectividade esencial para o funcionamento actual das organizacións. Co fin de mitigar os devanditos riscos, establécense as seguintes mellores prácticas:

- **Xestión e control de hardware e sistemas operativos:** as persoas colaboradoras van acceder á rede desde diferentes dispositivos, o cal constitúe unha potencial fonte de ameazas. Por iso, os dispositivos que se utilizan para acceso remoto deben ser de confianza, deben ter sistemas operativos e aplicacións completamente actualizados e un antivirus de boa calidade. En canto ao acceso e inicio de sesión nos dispositivos de uso externo á rede corporativa, deberase facer sempre desde unha conta específica para o uso profesional, diferente ás demais contas de uso persoal do equipo.
- **Xestión da seguridade física dos dispositivos:** Ante situacións de subtracción como o roubo do dispositivo de traballo, deben tomarse medidas antes de que sucedan, como medidas de protección antirrobo, de localización do dispositivo perdido ou roubado, o cifrado do disco ríxido ou un sistema de borrado remoto de datos.
- **Xestión de roles e permisos:** dentro das organizacións hai múltiples perfís con diferentes necesidades de acceso á información. Para cada un destes perfís estableceranse os mínimos permisos requiridos que garantan o acceso á información necesaria para desempeñar os seus labores. O mesmo se aplica para os accesos remotos aos recursos municipais.
- **Vixilancia da actividade da rede:** toda a actividade dentro da rede debe ser vixiada para identificar calquera tipo de actividade sospeitosa. Os erros de acceso, a concorrencia de varios intentos errados de autenticación e calquera outro tipo de tráfico que non semelle apropiado debe ser detectado, para o que compre a vixilancia continua da información que circula pola rede.
- **Xestión de contrasinais e autenticación de dous factores:** os mecanismos de acceso e identificación, como os contrasinais, son un factor determinante á hora de manter a seguridade nas organizacións, posto que permiten establecer criterios de acceso aos recursos. Por esta razón, deben avaliarse medidas que permitan a protección ante intentos de accesos fraudulentos, como a autenticación de dobre factor ou xestores de contrasinais que permitan protexelos.
- **O factor humano:** a identificación de riscos como a explotación de vulnerabilidades deben estenderse ao capital humano que opera en contacto cos dispositivos e sistemas asociados de acceso remoto a recursos da organización. Por tanto, é de vital importancia concienciar e formar ao persoal para mitigar os riscos informáticos aos que se expón a organización.

7.2. NORMAS DE ACCESO REMOTO A TERCEIROS

Modelo de aceptación

ACEPTACIÓN E COMPROMISO DO CUMPRIMENTO DAS NORMAS DE ACCESO REMOTO AOS SISTEMAS DE INFORMACIÓN DO CONCELLO DE RIANXO

Este documento outógalle á persoa o acceso remoto aos Sistemas de Información do CONCELLO DE RIANXO, en diante o Concello, no marco da prestación do servizo e a familia de expedientes que se indica, aos recursos e coas finalidades que se indican a continuación:

Organización:	Concello de Rianxo
Nome e Apelidos:	
Documento de identidade:	
Núm. Rexistro de Persoal:	
Data:	
Sinatura:	RECIBÍN:

SERVIZO:	FAMILIA DE EXPEDIENTES:
RECURSOS:	FINALIDADE:

--	--

A utilización destes recursos implica a aceptación, por parte da persoa terceira autorizado, das seguintes normas:

O acceso outorgado é concedido exclusivamente para realizar as tarefas descritas neste documento e nos tempos e horarios especificados. Os medios informáticos utilizados para o acceso aos sistemas deberán utilizar software debidamente licenciado, contar con sistemas preventivos adecuados e contar con sistemas de protección contra *malware*. A Organización pode requirir un informe que describa as medidas de seguridade implantadas.

A persoa terceira autorizada faise responsable das credenciais de acceso e dos posibles danos que se puidesen producir nos Sistemas de Información da Organización que deriven dun mal uso das credenciais de acceso ou da negligencia no acceso e custodia da información. Cando sexa de aplicación, procederá ao cambio de contrasinal, no primeiro acceso, naqueles casos que o sistema non force ao cambio.

A persoa terceira comprométese a observar o deber de segredo profesional e manter absoluta confidencialidade sobre os procesos, sistemas, medidas de seguridade e calquera outra información relacionada ou non co Sistema de Información ao cal ten acceso.

No caso de que as tarefas para realizar impliquen o tratamento de datos de carácter persoal, comprométese ao cumprimento da normativa vixente en materia de Protección de Datos, a tratar os datos conforme as instrucións da persoa responsable do tratamentos, declarando coñecer a lexislación vixente e por tanto comprometéndose a observar os requisitos establecidos nesta lexislación.

Calquera comportamento anómalo que se poida detectar deberá ser notificado o máis axiña posible, especialmente cando existan sospeitas de que se produciu algún incidente que puidese afectar á seguridade da información. Estas notificacións deberán notificarse a través do correo electrónico **seguridade@concelloderianxo.gal**, indicando, como mínimo, os sistemas e información afectada, a hora de detección do incidente e as medidas aplicadas.

A persoa terceira comprométese a dar traslado destas normas ao persoal ao seu cargo que vaia ter acceso ao Sistema de Información da Organización. Comprométese asemade a solicitar as baixas e modificacións das credenciais en canto rematen as necesidade de acceso.

Por motivos legais, de seguridade, de calidade do servizo, e en cumprimento en todo momento do establecido para estes efectos pola lexislación vixente, o Concello poderá exercer unha auditoría e a vixilancia dos usos dos recursos postos á disposición da persoa terceira.

En proba de conformidade, as dúas partes asinan este compromiso nos termos descritos, na data e lugar indicados.