

MARCO NORMATIVO DE SEGURIDADE

NOR_004 NORMATIVA DE REXISTRO DE ACTIVIDADE



CONCELLO DE RIANXO

CONTROL DE SINATURAS

ELABORADO POR:

RESPONSABLE DO SISTEMA

07/05/2026

APROBADO POR:

RESPONSABLE DOS SERVIZOS / RESPONSABLE DA INFORMACIÓN

07/05/2026

CONTROL DE VERSIÓNS

1.0 07.05.2026 Responsable do Sistema

Versión inicial do documento

1. OBXECTO

O obxecto deste documento é a definición da normativa aplicable para a xeración de rexistros de actividade das persoas usuarias dos sistemas de información, ao obxecto de reter a información necesaria para vixiar, analizar, investigar e documentar as posibles actividades indebidas ou non autorizadas, de forma que se poidan identificar en cada momento.

Este procedemento xérase en cumprimento das medidas do Esquema Nacional de Seguridade (ENS) que se indican a continuación:

- ENS Anexo II – Marco Operacional
 - Rexistro da actividade dos usuarios [op.exp.8]

Para os efectos deste documento, cando se faga referencia aos seguintes roles de seguridade, se o marco de Gobernanza para o PCE RES se estableceu por bloques de responsabilidades, entenderanse como referidos os seguintes:

- Responsable dos Servizos, Responsable da Información, Comité de Seguridade da Información: Responsable de Goberno
- Responsable da Seguridade: Responsable de Vixilancia
- Responsable do Sistema: Responsable de Operación

2. ALCANCE

Todos os sistemas de información e o persoal relacionado co Concello de Rianxo.

3. DEFINICIÓNS

Evento: Alerta ou notificación creada por un servizo de TI, elemento de configuración ou ferramenta de vixilancia.

Network Time Protocol (NTP): Protocolo da Internet para a sincronización dos reloxos dos sistemas de información. Utiliza o tempo universal coordinado (UTC).

Security Information and Event Management (SIEM): Ferramenta de recolección centralizada de eventos de seguridade e información dos rexistros de actividade (logs) dunha infraestrutura TIC, con correlación dos mesmos.

Vixilancia: Acción de observar o curso dun ou varios parámetros da actividade dun sistema de información, incluídas as persoas usuarias, co obxecto de detectar a natureza de posibles anomalías.

Log: Rexistro de información no que constan, cronoloxicamente, os acontecementos que foron

afectando a un sistema de información, así como os cambios que estes xeraron.

4. DESENVOLVEMENTO

4.1 XESTIÓN DOS REXISTROS DA ACTIVIDADE DOS USUARIOS

O Concello de Rianxo rexistrará nos servidores os eventos e actividades das persoas usuarias. O rexistro incluirá canda menos o identificador da persoa usuaria, a data e a hora, a información á que afecta o evento, o tipo de evento e o resultado (fallo ou éxito). O período de retención deste rexistro está configurado en base a unha rotación de logs con límite por espazo de almacenamento, que coa configuración establecida rolda os 24 meses de retención.

A actividade nos equipos das persoas usuarias queda asemade rexistrada nos logs de cada equipo, xestionados polo servizo Audit. de forma análoga á dos servidores.

As actividades que se deben rexistrar e o nivel de detalle quedarán determinados polo Concello de Rianxo segundo a Análise de Riscos realizada sobre cada sistema de información, que terá en conta a información mínima a recoller.

Recoméndase tamén revisar e analizar periodicamente os rexistros de actividade buscando patróns anormais de comportamento dos usuarios ou posibles accións sospeitosas ou ilícitas.

Os equipos e os servidores do Concello de Rianxo sincronizan cunha única fonte precisa de tempo os reloxos para coordinar no tempo os distintos logs xerados. A fonte de sincronización é o Network Time Protocol (NTP), que no caso dos equipos con Debian GNU/Linux están sincronizados a través do servizo timersyncd.

A continuación, descríbese a operativa a seguir pola Organización para a xestión de rexistros de actividade dos usuarios dos sistemas de información no ámbito desta normativa.

4.2 INVENTARIADO DOS REXISTROS

Antes da posta en produción dun novo sistema de información, deberáanse identificar os rexistros de actividade a recompilar e a implementar.

Recoméndase manter un inventario dos rexistros de actividade dos sistemas, que conterà, polo menos, a seguinte información:

- Sistema que os xera
- Nome do arquivo que os contén
- Tipo de rexistro: Servidores de Ficheiros, Electrónica de rede, Servidores de Aplicacións, Servidores de Base de datos

- Persoal autorizado para o acceso, modificación e eliminación
- Período de retención
- Tratamento de datos persoais
- Outra información de interese, como pode ser a súa estrutura que, no caso de aplicacións, permitirá realizar consultas ou integralos nun sistema de correlación de eventos.

O acceso ao inventario e á configuración dos rexistros de actividade estará restrinxido ás persoas usuarias debidamente autorizadas pola persoa Responsable da Seguridade, en coordinación coa persoa Responsable do Sistema, quen manterá unha relación destas autorizacións.

Calquera modificación realizada sobre a relación de persoas usuarias autorizadas deberá ser aprobada e quedar rexistrada seguindo o Procedemento de Xestión de Autorizacións: as altas, os cambios de perfil e as baixas comunicaranse en tempo e forma pola persoa Responsable da Seguridade á persoa Responsable do Sistema, quen será a responsable da debida configuración dos perfís de acceso.

As persoas administradoras dos sistemas de información non dispoñerán de permisos para o borrado ou desactivación dos rexistros que xeren as súas propias actividades.

O ficheiro do inventario de rexistros de actividade estará protexido polo seu correspondente log, co obxecto de rexistrar calquera intento de acceso non autorizado ou modificación do mesmo.

5. COMUNICACIÓN DE DEFICIENCIAS DO PROCEDIMENTO

Calquera deficiencia ou inconsistencia neste procedemento deberá de ser posta en coñecemento da persoa Responsable de Seguridade (ou na persoa na que delegue).

6. RESPONSABILIDADES. MATRIZ RACI

Actividade	R Realiza	A Responsable	C Consultado	I Informado
Elaborará e manterá a norma de elaboración e protección de rexistros de actividade dos usuarios	RSIS	RSEG	RSERV / RINFO / DPD	RSERV
Establecerá os rexistros de actividade dos sistemas de información a xerar.				
	RSIS	RSEG		
Autorizará o acceso dos usuarios aos rexistros de actividade dos sistemas de información.	RSEG	RSEG	RSIS	
Aprobará a norma e as súas actualizacións de		CSEG		

elaboración e protección de rexistros de actividade dos usuarios.				
Configurará os perfís de acceso dos usuarios autorizados aos rexistros de actividade dos sistemas de información.	ADSIS	RSIS	RSEG	
Manterá un inventario de rexistros de actividade dos sistemas de información.	ADSIS	RSIS		
Configurará os perfís de acceso dos usuarios autorizados aos rexistros de actividade do SIEM (se se dispón)	ADSIEM	RSIS		
Analizará, en tempo e forma, os eventos de potenciais incidentes de seguridade, detectados polo SIEM ou pola revisión dos rexistros de actividade dos sistemas	ADSIEM	RSIS		

COMITÉ DE SEGURIDADE DA INFORMACIÓN (CSEG)

RESPONSABLE DA INFORMACIÓN (RINFO)

RESPONSABLE DO SERVIZO (RSERV)

RESPONSABLE DA SEGURIDADE (RSEG)

RESPONSABLE DO SISTEMA (RSIS)

ADMINISTRADOR DA SEGURIDADE DO SISTEMA (ASIS)

USUARIOS (USR)

ADMINISTRADOR DE SISTEMAS DE INFORMACIÓN(ADSIS)

ADMINISTRADOR DE SIEM (ADSIEM)