DOCUMENTO
GENERICO_INTERVENCION: **Ayuntamiento de Las Rozas_Seguimiento sistemas información_definitivo_Firmado**

IDENTIFICADORES

OTROS DATOS
Código para validación: **FRTNP-I1SUJ-XISHU**
Fecha de emisión: **22 de Julio de 2020 a las 7:00:01**
Página 1 de 11

FIRMAS
El documento ha sido firmado por :
1.- Interventor del AYUNTAMIENTO DE LAS ROZAS DE MADRID.Firmado 10/07/2020 12:20

ESTADO
FIRMADO
10/07/2020 12:20

GLOBAL &LOCAL AUDIT
Profesionalidad, transparencia y confianza

Informe de control financiero Área de ingresos

Informe definitivo

Ayuntamiento de Las Rozas

Seguimiento área de Sistemas de Información

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

DOCUMENTO
GENERICO_INTERVENCION: **Ayuntamiento de Las Rozas_Seguimiento sistemas información_definitivo_Firmado**

IDENTIFICADORES

OTROS DATOS
Código para validación: **FRTNP-I1SUJ-XISHU**
Fecha de emisión: **22 de Julio de 2020 a las 7:00:01**
Página 2 de 11

FIRMAS
El documento ha sido firmado por :
1.- Interventor del AYUNTAMIENTO DE LAS ROZAS DE MADRID.Firmado 10/07/2020 12:20

ESTADO
FIRMADO
10/07/2020 12:20

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

ÍNDICE

1. Introducción 1
2. Objetivos 1
3. Trámite de alegaciones 2
4. Resultados del trabajo 2
5. Conclusiones 4
6. Recomendaciones 5

Anexo I – Matriz Plan de Acción 6

Anexo II – Seguimiento Plan de Acción 8

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

1. Introducción

Con fecha 21 de diciembre de 2018 se emitió el informe definitivo del control financiero de ingresos del Ayuntamiento de Las Rozas correspondiente a la anualidad de 2017.

El control financiero actual, cuyos resultados se presentan en este Informe, tiene como objeto el seguimiento y análisis del cumplimento de las recomendaciones relacionadas en el informe definitivo del control financiero de ingresos del Ayuntamiento de Las Rozas correspondiente a la anualidad de 2017.

El alcance de los procedimientos realizados se extiende, por la propia naturaleza y esencia de la fiscalización, a los ámbitos concretos abordados por las recomendaciones cuyo cumplimiento se verifica.

2. Objetivos

Los objetivos de este control financiero son los siguientes:

1. Analizar el grado de cumplimiento de las recomendaciones realizadas en el Informe definitivo del control financiero de ingresos del Ayuntamiento de Las Rozas correspondiente a la anualidad de 2017
2. Verificar y evaluar, desde la perspectiva de los principios de buena gestión financiera, las modificaciones introducidas en los sistemas y procedimientos de control interno y de gestión económico-financiera aplicados por la Entidad al objeto de dar cumplimiento a las recomendaciones efectuadas

El control lo realiza la sociedad Global & Local Audit, S.L., en virtud del contrato de "Servicios de apoyo y colaboración con la Intervención general en las funciones de Control y Fiscalización Interna de la Gestión Económico-Financiera".

El desarrollo de los trabajos se ha realizado de acuerdo con las Normas de Auditoría del Sector Público aprobadas por Resolución de la Intervención General del Estado de 14 de febrero de 1997 y publicadas por Resolución de 1 de septiembre de 1998, que son de aplicación directa al Sector Público Local, según se establece en el artículo 220.3 del Real Decreto 2/2004, al indicar que el control financiero se realizará por procedimiento de auditoría de acuerdo con las Normas de Auditoría del Sector Público.

2.1. Limitaciones al alcance

Las áreas involucradas en la gestión de ingresos objeto de control han prestado la debida colaboración en el transcurso de los trabajos de control financiero, proporcionando toda la información y documentación que les ha sido solicitada, no habiéndose presentado limitaciones al alcance del trabajo.

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

3. Trámite de alegaciones

Con fecha 30 de abril de 2020 se emitió informe borrador para que en un plazo de 15 días se formularan las alegaciones que se estimaran pertinentes, se presentaran los documentos que tuvieran por conveniente y se justificaran o subsanaran las deficiencias o irregularidades detectadas en las actuaciones practicadas. Finalizado el mencionado plazo sin haber recibido alegaciones, más allá de los comentarios recibidos con relación a que se está trabajando sobre los aspectos de mejora relacionados en este informe y en el informe de empresa externa sobre el análisis de la seguridad informática, se eleva éste a definitivo.

4. Resultados del trabajo

En el informe definitivo del control financiero de ingresos del Ayuntamiento de Las Rozas correspondiente a la anualidad de 2017, se llevó a cabo la revisión de los sistemas de información relacionados con el área de gestión tributaria y recaudatoria como parte del control financiero del área de ingresos, por lo que no constituye un informe de auditoría informática con el alcance que éste implica.

En el mencionado informe se pusieron de manifiesto los siguientes hechos:

El Ayuntamiento dispone de las siguientes aplicaciones informáticas en las que se registran los procedimientos de gestión tributaria y recaudatoria:

- **INFAPLIC:** GIT Gestión Integral de Tributos es un sistema consolidado de Gestión Tributaria y Recaudación.
- **SICALWIN:** sistema integrado de gestión económica, financiera y presupuestaria, relacionado con la contabilización.
- **FIRMADOC:** sistema de tramitación simplificada de expedientes.

El Ayuntamiento **no dispone de una política formal de control de acceso** que establezca el procedimiento de autorización de los usuarios a las distintas aplicaciones, no obstante, no se conceden accesos a usuarios que no estén autorizados por el Jefe de Servicio correspondiente, Tesorería o Intervención en el caso del área de Ingresos. Así mismo**, no consta que se lleven a cabo auditorías sobre consultas realizadas** en las distintas aplicaciones, si bien, en las aplicaciones queda registrado quién y cuándo se realizan las distintas acciones y operaciones.

Con respecto a la Directiva de Contraseñas, el Ayuntamiento tiene establecida una **política de contraseñas** de acceso al dominio, comunicada en febrero de 2015. Sin embargo, esta política **no** afecta a las **aplicaciones relacionadas con el área de ingresos**, para las que se aplica una contraseña básica, sin exigencias de requisitos ni de vigencia.

En conclusión, el Ayuntamiento no dispone, en relación con las aplicaciones involucradas en el área de ingresos de la política de seguridad a que se refiere el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración Electrónica (ENS)[1].

[1] Artículo 11. Requisitos mínimos de seguridad

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

Seguimiento:

La aplicación INFAPLIC, en su versión web (GITWEB) sí tiene una política de seguridad de contraseñas; ésta consiste en una doble validación (existencia del usuario y validación de contraseña o acceso mediante certificado electrónico) y en la robustez de la contraseña. Así mismo, las aplicaciones de SICALWIN, FIRMADOC e INFAPLIC, esta última en su versión escritorio, permiten la configuración de políticas de contraseñas, pero no se encuentran implementadas.
No obstante, se pone de manifiesto que:

- *Los usuarios pueden no acceder a la aplicación en su versión web.*
- *No existe una política formal que, además de exigir la robustez de las contraseñas, contemple los siguientes aspectos (contemplados en la ENS):*
  - *Cambio de las contraseñas con una cierta periodicidad (al menos cada año).*
  - *Todas las contraseñas del sistema sean analizadas por un programa de descifrado de contraseñas al menos cada 30 días, anulándose las contraseñas que no superen dicha prueba.*
  - *Anulación de las contraseñas con más de un año de antigüedad.*

En relación con las auditorías sobre consultas realizadas en las aplicaciones, los responsables de INFAPLIC informan que el sistema permite hacerlas, siendo sólo necesario activar el servicio, si bien para ello es imprescindible disponer de suficiente capacidad.

Por otra parte, se está llevando a cabo una actualización de la relación de personal con acceso a las aplicaciones, pero como se ha indicado, no existe un procedimiento formal que permita la actualización continua de la base de datos de usuarios con acceso a las aplicaciones, permisos de los mismos y situación con respecto a la entidad, entre otros.

En general, se realizan copias de seguridad con una periodicidad semanal y diaria de forma diferencial, sólo de las acciones del día. En las bases de datos de INFAPLIC se realizan copias de seguridad 3 veces a la semana. Así mismo, se han realizado verificaciones de restauración con motivo de migraciones.

Seguimiento:

Se realizan 3 copias de seguridad distintas

- *1 diaria completa de la máquina, snapshot o instantánea de los servidores*
- *1 copia diaria diferencial de las BBDD a través del software de backup Commvault*
- *1 copia semanal completa con Commvault.*
- *3 copias semanales de las BBDD con los propioS Planes de Mantenimiento de Microsoft SQL SERVER*

Las copias realizadas con Commvault son a nivel de Dato y a Nivel de Máquina (Disaster Recovery)

Las **aplicaciones** INFAPLIC y SICALWIN **no están integradas entre sí**, por lo que las relaciones entre ambas se realizan de forma manual; esto lleva aparejado, entre otras, la necesidad de mayores plazos para el tratamiento de la información y, consecuentemente, para su disponibilidad, así como, el riesgo de los errores humanos, al procesar elevados volúmenes de datos.

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU) 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

Seguimiento:

De acuerdo con la información facilitada por personal de INFAPLIC, existe una conexión a través de ficheros con los que se pasa la información de ingresos a la contabilidad.

En febrero y marzo de 2020 se están procesando ficheros de ingresos para incorporarlos masivamente a Sical, no habiéndose verificado aún la integridad de dichos procesos.

Por otra parte, en el ejercicio 2018 se llevaron a cabo las siguientes actividades relacionadas con el análisis de la seguridad informática en general:

- Auditoría de vulnerabilidades
- Auditoría básica (checklist) cumplimiento ENS
- Detección de la causa raíz del ataque sufrido de RANSOMWARE GandCrab v4

Como resultado de dicho análisis se concluyó que, basándose en el modelo de madurez ISM3 (Information Security Management Maturity Model), el nivel recomendado para el Ayuntamiento es el Nivel ISM3 4, encontrándose actualmente en el Nivel ISM3 0.

En el informe emitido por la empresa externa que llevó a cabo dicho análisis se propuso un plan de acción basado en los riesgos identificados; se adjunta matriz en el anexo I.

Sobre dicho plan de acción se han llevado a cabo algunas acciones, ver anexo II – Seguimiento Plan de Acción. Para dos de ellas no se ha realizado ninguna acción:

- Pérdida de control de los sistemas / no cumplimiento y
- Robo de credenciales / intrusión /secuestro de activos / desconocimiento de uso del activo, clasificados como de riesgo medio y alto, respectivamente.

5. Conclusiones

Con base en el trabajo realizado se concluye que

1. No se dispone, en relación con las aplicaciones involucradas en el área de ingresos, de la política de seguridad a que se refiere el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración Electrónica (ENS).
    - No dispone de una política formal de control de acceso que establezca el procedimiento de autorización de los usuarios a las distintas aplicaciones.
    - No consta que se lleven a cabo auditorías sobre consultas realizadas en las distintas aplicaciones, si bien, en las aplicaciones queda registrado quién y cuándo se realizan las distintas acciones y operaciones.
    - Con respecto a la Directiva de Contraseñas y en relación con las aplicaciones relacionadas con el área de ingresos, éstas disponen de un doble control de acceso (usuario acreditado y contraseña) y a las contraseñas se les exige robustez. No obstante, no se exige caducidad a éstas.
2. Las relaciones entre las aplicaciones INFAPLIC y SICALWIN se realizan de forma manual, a pesar de existir una conexión a través de ficheros, de acuerdo con la información facilitada por personal de INFAPLIC; esto lleva aparejado, entre otras, la necesidad de mayores plazos para el tratamiento de la información y, consecuentemente, para su

Esta es una copia impresa del documento electrónico (Ref: 2447099 FRTNP-I1SUJ-XISHU 6AE3E54771A8F4BDEAA4161DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

disponibilidad, así como, el riesgo de los errores humanos, al procesar elevados volúmenes de datos. En febrero y marzo de 2020 se están procesando ficheros de ingresos para incorporarlos masivamente a Sical, no habiéndose verificado aún la integridad de dichos procesos.

3. En relación con la seguridad de la información se está trabajando en la implantación de los planes de acción propuestos para alcanzar el nivel recomendado para el Ayuntamiento, Nivel ISM3 4, con base en las recomendaciones realizadas por EINZELNET.

6. Recomendaciones

1. Deberá realizarse un control de la integridad **de la integración de la información de las aplicaciones de gestión recaudatoria, de tesorería y de contabilidad**, al objeto de reforzar la función de control de esta última. Igualmente, habría que establecer procedimientos que garanticen la conciliación periódica de la información entre los distintos órganos y servicios vinculados a la gestión recaudatoria, en particular las relativas a las liquidaciones en gestión de cobro en período voluntario y a las anulaciones de derechos por fraccionamientos y aplazamientos que impliquen un diferimiento del ejercicio de su vencimiento.
2. Debería **reforzarse la política de seguridad** a que se refiere el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración Electrónica de las aplicaciones informáticas relacionadas con el área de gestión y recaudación de ingresos.
3. Continuar implantando las recomendaciones realizadas por EINZELNET para **alcanzar el nivel de seguridad recomendado** para el Ayuntamiento.

Las Rozas, 10 de julio de 2020

GLOBAL & LOCAL AUDIT, S.L.	**AYUNTAMIENTO DE LAS ROZAS**
50160666N MARIA MAR RAMIREZ (R: B87286225) Firmado digitalmente por 50160666N MARIA MAR RAMIREZ (R: B87286225) Fecha: 2020.07.10 12:04:55 +02'00'	
María del Mar Ramírez Méndez Socio	Fernando Álvarez Rodríguez Interventor General

DOCUMENTO
GENERICO_INTERVENCION: Ayuntamiento de Las Rozas_Seguimiento sistemas información_definitivo_Firmado
IDENTIFICADORES
OTROS DATOS
Código para validación: FRTNP-I1SUJ-XISHU
Fecha de emisión: 22 de Julio de 2020 a las 7:00:01
Página 8 de 11
FIRMAS
El documento ha sido firmado por :
1.- Interventor del AYUNTAMIENTO DE LAS ROZAS DE MADRID-Firmado 10/07/2020 12:20
ESTADO
FIRMADO
10/07/2020 12:20

Anexo I – Matriz Plan de Acción

Riesgo	Nivel	Nombre del Proyecto	Coste	Esfuerzo	Plazo	Descripción
Incumplimiento Esquema Nacional Seguridad	Muy Alto	Cumplimiento ENS (Esquema Nacional Seguridad)	Medio	Alto	Inmediato	Establecimiento de un programa para el cumplimiento del Esquema Nacional de Seguridad.
Desconocimiento del estado de la seguridad	Muy Alto	Servicio Gestionado de Ciberseguridad	Medio	Bajo	Inmediato	Establecimiento de un equipo dedicado a las tareas específicas de ciberseguridad
Infección *Ransomware* (Virus) /Perdida de control de activos / Uso no adecuado	Muy Alto	Despliegue *Endpoints*	Bajo	Bajo	Corto Plazo	Despliegue de *endpoint* de seguridad en, al menos, los equipos de alto riesgo, incluyendo servidores, equipos personales y dispositivos móviles, aplicándoles la política de seguridad previamente definida.
Desconocimiento de activos	Alto	Inventario	Bajo	Bajo	Corto Plazo	Despliegue de procedimiento y tecnología que permitan gestionar el inventario de activos tecnológicos de la manera más automática posible.
Robo de credenciales / Intrusión / Secuestro de activos /Desconocimiento del uso del activo	Muy Alto	PAM *(Privileged Access Management)*	Medio	Medio	Corto Plazo	Gestión de Cuentas Privilegiadas *(Privileged Access Management)* de tal manera que se pueda gestionar de una manera sencilla y segura las cuentas con privilegios elevados
Malas prácticas de seguridad	Alto	Concienciación	Medio	Alto	Medio Plazo	Base para que cualquier cosa que se incluya alrededor de la ciberseguridad todo el mundo la conozca y la sepa usar.
Infección virus / intrusión / Secuestro de activos	Medio	Actualización / Parcheo	Medio	Medio	Medio Plazo	Definición de la política de actualizaciones de software y parches de seguridad, su desarrollo y

Esta es una copia impresa del documento electrónico (Ref: 244709 9 FRTNP-I1SUJ-XISHU 6AE3E5477 1A8F4BDEAA416DF70EF6013CA100C7) generada con la aplicación informática Firmadoc: El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

Riesgo	Nivel	Nombre del Proyecto	Coste	Esfuerzo	Plazo	Descripción
						despliegue de tecnología para soportarlo
Perdida de Información	Alto	Backup /DRP (Disaster Recovery Plan) /Plan de Continuidad	Alto	Alto	Medio Plazo	Definición de la política de backup, Disaster Recovery Plan y Plan de Continuidad, su desarrollo y despliegue de tecnología para soportarlo Política/D&R/Plan de Continuidad
Denegación de Servicio / Desconocimiento origen de ataques	Medio	WAF (Web Application Firewall)	Medio	Bajo	Largo Plazo	Despliegue de Web Application Firewall
Intrusión / Uso no aceptable de las redes	Alto	NAC (Network Access Control)	Medio	Medio	Largo Plazo	Despliegue de Network Access Control
Perdida de control de los sistemas / No cumplimiento	Medio	Respuesta ante Incidentes	Medio	Alto	Largo Plazo	Definición del proceso de Respuesta ante Incidentes y desarrollo de este
Robo de Información / No cumplimiento	Alto	Clasificación de la información / Cifrado	Medio	Alto	Largo Plazo	Definición de la política de Clasificación de la Información, su desarrollo y despliegue de tecnología para soportarlo. Proyecto de Cifrado de la Información siguiendo la política definida

DOCUMENTO
GENERICO_INTERVENCION: Ayuntamiento de Las Rozas_Seguimiento sistemas información_definitivo_Firmado

IDENTIFICADORES

FIRMAS
El documento ha sido firmado por :
1.- Interventor del AYUNTAMIENTO DE LAS ROZAS DE MADRID-Firmado 10/07/2020 12:20

ESTADO
FIRMADO
10/07/2020 12:20

OTROS DATOS
Código para validación: FRTNP-I1SUJ-XISHU
Fecha de emisión: 22 de Julio de 2020 a las 7:00:01
Página 9 de 11

Esta es una copia impresa del documento electrónico (Ref: 24470 99 FRTNP-I1SUJ-XISHU 6AE3E5477 1A8F4BDEAA416DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

DOCUMENTO
GENERICO_INTERVENCION: Ayuntamiento de Las Rozas_Seguimiento sistemas información_definitivo_Firmado
IDENTIFICADORES
OTROS DATOS
Código para validación: FRTNP-I1SUJ-XISHU
Fecha de emisión: 22 de Julio de 2020 a las 7:00:01
Página 10 de 11
FIRMAS
El documento ha sido firmado por :
1.- Interventor del AYUNTAMIENTO DE LAS ROZAS DE MADRID-Firmado 10/07/2020 12:20
ESTADO
FIRMADO
10/07/2020 12:20

Anexo II – Seguimiento Plan de Acción

Riesgo	Acción realizada	
Incumplimiento Esquema Nacional Seguridad	Se comienza con la realización de la encuesta INES (Informe Nacional del Estado de Seguridad). A los contratos que salen del departamento se exigen a los proveedores que las empresas cumplan con el ENS al menos en su nivel medio. Cuando estos puedan tener acceso a datos de nivel alto de protección de datos	
Desconocimiento del estado de la seguridad	Se ha subido a contratación un pliego técnico para adquirir una aplicación de auditoría del directorio activo y de los ficheros.	
Infección Ransomware (Virus) /Perdida de control de activos / Uso no adecuado	Se despliega un *endpoint* (SOPHOS) en todos los equipos y servidores con tecnología de detección amenazadas por comportamiento.	
Desconocimiento de activos	Se utiliza la herramienta KACE, de inventariado de *hardware* y *software*	
Robo de credenciales/Intrusión/Secuestro de activos/Desconocimiento del uso del activo	**No se ha hecho nada al respecto**	
Malas prácticas de seguridad	Junto al *endpoint* se adquiere una herramienta denominada PHISH THREAT en la que se mandan compañías ficticias por mail y si los usuarios caen, se les envía a una formación.	
Infección virus / intrusión / Secuestro de activos	Se instala servidor de actualizaciones (WINSUS) para las aplicaciones de Microsoft. Nos suscribimos a los correos electrónicos del CCN sobre ataques y vulnerabilidades en las aplicaciones y se actúa cuando existe peligro.	
Pérdida de información	Se adquiere herramienta de *backup* y se virtualizan todas las máquinas. Con un sistema de tolerancia a fallos y réplica de servidores en dos CPD's en ubicaciones distintas. Se hacen dos niveles de *backup*, a nivel de dato y a nivel de máquina completa. Se programan copias diarias con retención de 30 días para el dato y de 7 para la máquina	

Esta es una copia impresa del documento electrónico (Ref: 244709 FRTNP-I1SUJ-XISHU 6AE3E5477 1A8F4BDEAA416 1DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es

DOCUMENTO
GENERICO_INTERVENCION: Ayuntamiento de Las Rozas_Seguimiento sistemas información_definitivo_Firmado
IDENTIFICADORES
OTROS DATOS
Código para validación: FRTNP-I1SUJ-XISHU
Fecha de emisión: 22 de Julio de 2020 a las 7:00:01
Página 11 de 11
FIRMAS
El documento ha sido firmado por :
1.- Interventor del AYUNTAMIENTO DE LAS ROZAS DE MADRID-Firmado 10/07/2020 12:20
ESTADO
FIRMADO
10/07/2020 12:20

Riesgo	Acción realizada	
Denegación de Servicio / Desconocimiento origen de ataques	Se aplica mediante Firewall Fortinet de capa 7 y la herramienta SOPHOS también tiene un resumen en la red local para ver el origen de los ataques. Mediante el SIEM (*Security Information and Event Management*) se analizan todos los eventos que ocurren en la LAN Y WAN	
Intrusión / Uso no aceptable de las redes	Se realiza mediante la configuración de las bocas de red en los *switch*, activando el *security port*, sólo permite conectarse MAC (*Media Access Control*) conocidas para ese puerto. Se aíslan las redes y no se ven entre ellas. Los puertos *switchs* que están libres están apagados.	
Pérdida de control de los sistemas / No cumplimiento	**No se ha definido nada todavía**	
Robo de Información / No cumplimiento	Se están preparando dos proyectos: uno de auditoría del dato y el AD y otra de un gestor documental.	

Esta es una copia impresa del documento electrónico (Ref: 244709 9 FRTNP-I1SUJ-XISHU 6AE3E5477 1A8F4BDEAA416 1DF70EF6013CA100C7) generada con la aplicación informática Firmadoc. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://portalciudadano.lasrozas.es