Aragonesa de Servicios Telemáticos

PROC_O14 Cuerpo Normativo de Seguridad

Documento del Sistema Integrado de Gestión de la Calidad y Seguridad de la Información

GOBIERNO DE ARAGON

IGNORANTIA LEGIS NEMINEM
EXCUSAT

(Página en blanco intencionadamente)

Ficha de control documental

Información del documento	
Archivo	PROC_O14_Cuerpo_Normativo_Seguridad.docx
Autor/es	Ignacio Pérez [AST - Resp. Seguridad]
Creado	07/02/2019
Actualizado	03/07/2019
Versión	1.0
Clasificación	Público

Registro de cambios			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	03/07/2019	Ignacio Pérez [AST - Resp. Seguridad]	Primera versión del documento

Control de revisiones			
Fecha	**Revisado por**	**Área**	**Próxima revisión**
11/06/2019	Comité de Seguridad	Dirección	11/06/2020

Distribución		
Nombre	**Área**	**Entidad**
	Todas	Todas

DURA LEX, SED LEX

(Página en blanco intencionadamente)

Contenido

1. Introducción 16
1.1. Objeto 16
1.2. Ámbito de aplicación 17
1.3. Vigencia 17
1.4. Revisión y evaluación 18
1.5. Roles y responsabilidades 18
1.6. Documentación relacionada 19
1.7. Cumplimiento de normativas y estándares 20
Leyes y normas consideradas fuera de alcance 21
1.8. Deber de denuncia de incumplimiento 21
2. Marco teórico 21
2.1. Principios básicos y requisitos mínimos definidos en el ENS 21
2.2. Líneas de defensa 22
2.3. Mejora continua del proceso de seguridad 23
2.4. Seguridad por defecto 23
N1 Organización y normativa 24
N1.1 Normativa documentada 24
N1.1.1 Política de seguridad 24
N1.1.2 Cuerpo Normativo de Seguridad 24
N1.1.3 Revisión del cuerpo normativo de seguridad 25
N1.1.4 Procedimientos e instrucciones técnicas 25
N1.2 Organización de la seguridad de la información 25
N1.2.1 Proceso de autorización 25
N1.2.2 Roles y responsabilidades en seguridad de la información 26

N1.2.3 Segregación de tareas 26
N1.2.4 Contacto con las autoridades 26
N1.2.5 Contacto con grupos de interés especial 27
N1.2.6 Seguridad de la información en la gestión de proyectos 27
N1.2.7 Divulgación 27
N2 Recursos 27
N2.1 Activos 28
N2.1.1 Inventario de activos 28
N2.1.2 Responsabilidad de los activos 28
N2.1.3 Uso aceptable de los activos 29
N2.1.4 Devolución de activos 30
N2.1.5 Retirada de materiales propiedad de AST 30
N2.2 Recursos Humanos 30
N2.2.1 Investigación de antecedentes 30
N2.2.2 Caracterización del puesto de trabajo 31
N2.2.3 Deberes y obligaciones 32
N2.2.4 Responsabilidades de gestión 33
N2.2.5 Concienciación, educación y capacitación en seguridad de la información 34
N2.2.6 Personal alternativo 35
N2.2.7 Proceso disciplinario 35
N2.2.8 Responsabilidades ante la finalización o cambio 37
N2.3 Servicios externos 38
N2.3.1 Contratación y acuerdos de nivel de servicio 38
N2.3.2 Control y revisión de la provisión de servicios del proveedor 38
N2.3.3 Gestión diaria 39
N2.3.4 Gestión de cambios en la provisión del servicio del proveedor 39

N2.3.5 Medios alternativos 39
N2.3.6 Política de seguridad de la información en las relaciones con los proveedores 39
N2.3.7 Requisitos de seguridad en contratos con terceros 40
N2.3.8 Cadena de suministro de tecnología de la información y de las comunicaciones 40
N3 Proyectos y Servicios 41
N3.1 Planificación 41
N3.1.1 Análisis de riesgos 41
N3.1.2 Análisis de requisitos y especificaciones de seguridad de la información 42
N3.1.3 Arquitectura de seguridad 42
N3.1.4 Adquisición de nuevos componentes 43
N3.1.5 Dimensionamiento / Gestión de capacidades 44
N3.1.6 Planificación de las actualizaciones y mantenimiento 44
N3.2 Servicios 45
N3.2.1 Asegurar los servicios de aplicaciones en redes públicas 45
N3.2.2 Protección de las transacciones de servicios de aplicaciones 45
N3.2.3 Componentes certificados 46
N3.2.4 Protección de servicios y aplicaciones web 46
N3.2.5 Protección frente a la denegación de servicio 47
N3.2.6 Medios alternativos 47
N4 Sistemas de Información 48
N4.1 Organización de la información 48
N4.1.1 Clasificación de la información 48
N4.1.2 Etiquetado de la información 49
N4.1.3 Manipulado de la información 49

N4.1.4 Anonimización y seudonimización de la información sensible 50

N4.2 Medidas 51

N4.2.1 Cifrado y política de uso de los controles criptográficos 51

N4.2.2 Gestión de claves 52

N4.2.3 Firma electrónica 52

N4.2.4 Sellos de tiempo 54

N4.2.5 Limpieza de documentos 54

N4.2.6 Copias de seguridad (*backup*) 55

N4.2.7 Gestión de certificados 56

N4.3 Seguridad en las comunicaciones 58

N4.3.1 Políticas y procedimientos de intercambio de información 58

N4.3.2 Acuerdos de intercambio de información 58

N4.3.3 Mensajería electrónica 59

N4.3.4 Acuerdos de confidencialidad o no revelación 59

N4.3.5 Requerimientos técnicos de notificaciones y publicaciones electrónicas 59

N4.3.6 Responsabilidad de exfiltración de la información por medios electrónicos fuera del entorno del Gobierno de Aragón 60

N4.4 Acceso 60

N4.4.1 Política de control de acceso 60

N4.4.2 Identificación 61

N4.4.3 Requisitos de acceso 63

N4.4.4 Segregación de funciones y tareas 64

N4.4.5 Registro y baja de usuario 64

N4.4.6 Provisión de acceso de usuario 65

N4.4.7 Gestión de privilegios de acceso 65

N4.4.8 Gestión de la información secreta de autenticación de los usuarios 66
N4.4.9 Revisión de los derechos de acceso de usuario 67
N4.4.10 Retirada o reasignación de los derechos de acceso 67
N4.4.11 Uso de la información secreta de autenticación 67
N4.4.12 Restricción del acceso a la información 67
N4.4.13 Mecanismo de autenticación 68
N4.4.14 Sistema de gestión de contraseñas 70
N4.4.15 Procedimiento de acceso 70
N4.4.16 Uso de utilidades con privilegios del sistema 72
N4.4.17 Control de acceso al código fuente de los programas 72
N4.4.18 Gestión de accesos con cuentas privilegiadas 72
N4.4.19 Conexiones en terminales (*log-on*) seguros 73
N4.4.20 Normativa de gestión de autorizaciones 74
N5 Soportes y puesto de trabajo 78
N5.1 Soporte físico 78
N5.1.1 Custodia 78
N5.1.2 Criptografía 78
N5.1.3 Etiquetado 79
N5.1.4 Gestión de soportes extraíbles 79
N5.1.5 Borrado y destrucción 79
N5.1.6 Reutilización 80
N5.1.7 Soportes físicos en tránsito 80
N5.1.8 Seguridad de los equipos fuera de las instalaciones 81
N5.2 Puesto de trabajo 82
N5.2.1 Equipo de usuario desatendido 82
N5.2.2 Puesto de trabajo despejado 83

N5.2.3 Política de dispositivos móviles 84
N5.2.4 Teletrabajo 85
N5.2.5 Uso del correo electrónico 89
N5.2.6 Gestión de los recursos asignados al usuario 90
N5.2.7 Copias de seguridad de la información 92
N5.2.8 Quiosco interactivo y pantallas informativas 93
N6 Infraestructuras 94
N6.1 Control de acceso físico 94
N6.1.1 Áreas separadas y con control de acceso 94
N6.1.2 Identificación de las personas 95
N6.1.3 Clasificación de ubicaciones y niveles de seguridad de acceso 96
N6.2 Procedimientos en áreas seguras 97
N6.2.1 El trabajo en áreas seguras 97
N6.2.2 Áreas de carga y descarga 97
N6.2.3 Registro de entrada y salida de equipamiento 97
N6.2.4 Mantenimiento de los equipos 98
N6.3 Protección ambiental 98
N6.3.1 Acondicionamiento de los locales 98
N6.3.2 Emplazamiento y protección de equipos 99
N6.3.3 Energía eléctrica 99
N6.3.4 Seguridad del cableado 100
N6.3.5 Protección frente a incendios 100
N6.3.6 Protección frente a inundaciones 101
N6.4 Disponibilidad del entorno 101
N6.4.1 Instalaciones alternativas 101
N6.4.2 Medios alternativos 101

N7 Telecomunicaciones 102

N7.1 Medidas comunes 102

N7.1.1 Controles de red 102

N7.1.2 Seguridad de los servicios de red 103

N7.1.3 Perímetro seguro 103

N7.1.4 Protección de la confidencialidad 104

N7.1.5 Protección de la autenticidad y de la integridad 104

N7.1.6 Segregación de redes 105

N7.1.7 Medios alternativos 106

N8 Operación y Explotación 106

N8.1 Seguridad de las operaciones 106

N8.1.1 Documentación de procedimientos de las operaciones 106

N8.1.2 Configuración de seguridad 106

N8.1.3 Gestión de la configuración 107

N8.1.4 Mantenimiento 108

N8.1.5 Gestión de cambios 108

N8.1.6 Gestión de capacidades 109

N8.1.7 Separación de los recursos de desarrollo, prueba y operación 110

N8.2 Control del software 110

N8.2.1 Controles contra el código malicioso 110

N8.2.2 Instalación del software en explotación 111

N8.2.3 Gestión de las vulnerabilidades técnicas 111

N8.2.4 Restricción en la instalación de software 111

N8.3 Monitorización y detección 112

N8.3.1 Registro de eventos 112

N8.3.2 Registros de administración y operación 112
N8.3.3 Protección de la información de registro 113
N8.3.4 Sincronización del reloj 114
N8.3.5 Detección de intrusión 115
N8.3.6 Sistema de métricas 115
N8.3.7 Controles de auditoría de sistemas de información 115
N9 Aplicaciones: desarrollo y mantenimiento 116
N9.1 Desarrollo seguro 116
N9.1.1 Política de desarrollo seguro 116
N9.1.2 Principios de ingeniería de sistemas seguros 117
N9.1.3 Entorno de desarrollo seguro 117
N9.1.4 Externalización del desarrollo de software 117
N9.1.5 Pruebas funcionales de seguridad de sistemas 118
N9.1.6 Pruebas de aceptación de sistemas 118
N9.1.7 Protección de los datos de prueba 119
N9.2 Normas particulares de desarrollo seguro 119
N9.2.1 Control de Acceso y Autenticación 119
N9.2.2 Codificación y validación de entrada/salida 120
N9.2.3 Gestión de Errores y Excepciones 121
N9.2.4 Auditoría y Registro 121
N9.2.5 Cifrado 122
N9.2.6 Gestión de Sesiones (Login/Logout) 122
N9.2.7 Gestión de cookies 123
N9.3 Mantenimiento 123
N9.3.1 Procedimiento de control de cambios en sistemas 123
N9.3.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 124

N9.3.3 Restricciones a los cambios en los paquetes de software 124

N10 Incidencias y continuidad 125

N10.1 Gestión de incidencias 125

N10.1.1 Responsabilidades y procedimientos 125

N10.1.2 Notificación de los eventos de seguridad de la información .. 126

N10.1.3 Notificación de puntos débiles de la seguridad 127

N10.1.4 Evaluación y decisión sobre los eventos de seguridad de información 127

N10.1.5 Respuesta a incidentes de seguridad de la información 127

N10.1.6 Aprendizaje de los incidentes 128

N10.1.7 Recopilación de evidencias 128

N10.2 Continuidad 128

N10.2.1 Planificación de la continuidad de la seguridad de la información 128

N10.2.2 Análisis de impacto 129

N10.2.3 Implementar la continuidad de la seguridad de la información 129

N10.2.4 Verificación, revisión y evaluación de la continuidad de la seguridad de la información 129

N10.2.5 Disponibilidad de los recursos de tratamiento de la información 130

N11 Cumplimiento 130

N11.1 Elementos fundamentales..... 130

N11.1.1 Identificación de la legislación aplicable y de los requisitos contractuales 130

N11.1.2 Derechos de propiedad intelectual (DPI)..... 131

N11.1.3 Protección de los registros de la organización 131

N11.1.4 Protección y privacidad de la información de carácter personal 131

N11.1.5 Regulación de los controles criptográficos 132

N11.1.6 Revisión independiente de la seguridad de la información.... 132

N11.1.7 Cumplimiento de las políticas y normas de seguridad 132

N11.1.8 Comprobación del cumplimiento técnico 133

Anexos 134

Anexo I. Relación entre las normas y las medidas de protección del Esquema Nacional de Seguridad..... 134

Anexo II. Relación entre las normas y los controles de la norma UNE-EN ISO/IEC 27001:2017 136

Anexo III. Listado de CMDB de proceso «O6 Gestión de la configuración» 141

Anexo IV. PLA.O14 Clausula seguridad información AST Proveedor 142

Reunidos..... 142

Exponen..... 142

Anexo V. PLA.O14 Cláusula de seguridad de la información, para la utilización por parte de terceros de la infraestructura o servicios de AST 148

Anexo VI. 02A Circular informativa RGPD y confidencialidad..... 156

Anexo VII. Solicitudes de Autorizaciones activadas 158

Anexo VIII. Cláusulas de información de uso responsable en peticiones 159

Solicitud para utilizar un acceso externo seguro a la red corporativa 160

Solicitud de acceso remoto al puesto de trabajo 160

Creación de un acceso externo seguro (VPN)..... 161

Alta de aplicación en plataforma VPN SSL..... 162

Modificación de un acceso externo seguro (VPN) 162
Solicitud de apertura de puertos del FW para housing 163
Solicitud de apertura de puertos del FW para red SARA 163
Solicitud de apertura de puertos del FW para servicios de internet 163
Solicitud de acceso seguro VPN LAN to LAN 164
Anexo IX. Glosario 165
Anexo X. Categorización de los sistemas 166
Anexo XI. Empresas asociadas a los servicios 170
Anexo XII. Área Segura: Normativa de trabajos en CPD 170
Normativa básica 170
Acceso 170
Anexo XIII. Entidades Certificadoras reconocidas en AST 172
Anexo XIV. Documentación obsoleta que abarca total o parcialmente esta instrucción técnica 172
Anexo XV. Control de versiones 173
Anexo XVI. Índice de ilustraciones 173
Anexo XVII. Índice de tablas 173

1. Introducción

1.1. Objeto

Aragonesa de Servicios Telemáticos, en adelante **AST**, es una Entidad de Derecho Público adscrita al departamento de Innovación, Investigación y Universidad cuyo régimen económico financiero se rige por el artículo 12 de la LEY 7/2001, de 31 de mayo, de creación de la entidad.

Tal y como refleja los estatutos de AST, la entidad tiene como objetivos generales:

- El cumplimiento y ejecución de las directrices estratégicas del Gobierno de Aragón en materia de servicios y sistemas corporativos de información y de telecomunicaciones, así como de la política que, en la materia, defina el Departamento de adscripción de la Entidad.
- Actuar como proveedor principal ante la Administración de la Comunidad Autónoma de Aragón, de sus organismos públicos dependientes, así como del resto de poderes adjudicadores dependiente de aquella y de éstos para la cobertura global de las necesidades de ésta en relación con las infraestructuras, servicios, sistemas y aplicaciones para la información y las telecomunicaciones, siempre que resulte compatible con la normativa vigente de contratación pública.
- La coordinación de la actuación de la Administración de la Comunidad Autónoma con las de otras Administraciones Públicas y Entidades públicas o privadas, en materia de infraestructuras, servicios y sistemas para la información y las telecomunicaciones, en el ámbito de funciones de la Entidad.
- La promoción e impulso de la oferta y demanda de servicios y sistemas de información y de telecomunicaciones en el ámbito de Aragón, así como la contribución a la ejecución de las infraestructuras y la prestación de los servicios que se consideren necesarios para impulsar el desarrollo económico y social del territorio.

El presente documento tiene como objeto establecer el Cuerpo Normativo de Seguridad, que ha de cumplir el resto de procesos y procedimientos de la entidad. Dichas normas contemplan los principios básicos y los requisitos mínimos de seguridad establecidos por el Esquema Nacional de Seguridad.

1.2. Ámbito de aplicación

Este Procedimiento es de aplicación a todo el ámbito de actuación de AST, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad de AST.

El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la entidad, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de AST.

En el ámbito de la presente normativa, se entiende por:

- **Empleado**: personal propio de AST. Hay normas cuya aplicación se circunscribe únicamente a empleados de la entidad, en ese caso se usará este término.
- **Proveedor**, o contratista: Se refiere a las entidades, o al personal perteneciente a empresas externas, con relación contractual con AST, o con algún otro organismo público, y que requiera utilizar recursos gestionados por AST para el desarrollo de su contrato. Existen normas que les aplican específicamente
- **Usuario** cualquier empleado público perteneciente o ajeno a AST, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con AST y que utilice o posea acceso a los Sistemas de Información de AST. En caso de que una norma no especifique el ámbito de aplicación se entenderá que aplica a todos los usuarios de los sistemas.

1.3. Vigencia

El presente Procedimiento ha sido aprobado por el **comité de seguridad** de AST, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que AST pone a disposición de

sus usuarios para el ejercicio de sus funciones y que, consecuentemente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de AST.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este Procedimiento.

1.4. Revisión y evaluación

La gestión de este Procedimiento corresponde al **responsable de seguridad**, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el **responsable de seguridad** revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación del **comité de seguridad** de AST. Dicha aprobación quedara reflejada o bien en Acta de reunión, o por aceptación del documento en la plataforma de gestión documental. En el caso particular tanto del **responsable de seguridad**, como de la **gerencia**, se firmará electrónicamente el documento vigente, con el fin de que no quede ninguna duda de la oficialidad del mismo cuando este se distribuya fuera de la plataforma de gestión documental.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

1.5. Roles y responsabilidades

Los siguientes roles intervienen en el proceso:

Roles	Responsabilidades
Responsable de área de Seguridad (AST)	Respecto al presente Cuerpo Normativo de Seguridad y las normas que este contiene, es obligación del responsable de seguridad: ▪ Su elaboración y mantenimiento. ▪ Adecuar el mismo a diferentes normativas o estándares que le afecten. ▪ Acompañar y asesorar, cuando se solicite esa colaboración, en los proyectos, procedimientos o mecanismos técnicos que tengan que adaptarse para cumplir las normativas del presente documento. ▪ Cumplir y hacer cumplir las normas establecidas. ▪ Vigilar activamente y buscar mecanismos para garantizar el cumplimiento del mismo por parte de todos los actores. ▪ Divulgar el conocimiento del mismo.
Comité de Seguridad	▪ Proponer correcciones al Cuerpo Normativo de Seguridad. ▪ Conocer y aprobar la versión vigente del documento. ▪ Cumplir y hacer cumplir las normas establecidas. ▪ Promover una cultura de seguridad de la información en AST.
Gerencia	▪ Conocer y firmar la versión vigente del documento. ▪ Cumplir y hacer cumplir las normas establecidas. ▪ Promover una cultura de seguridad de la información en AST.
Responsable del contrato (AST)	Personal de AST designado como responsable de un contrato. y enlace del mismo entre AST y el proveedor ▪ Proporcionar al responsable adjudicatario del contrato el Cuerpo Normativo de Seguridad ▪ Supervisar el cumplimiento por parte del proveedor de las normas que le afectan.
Responsable adjudicatario del proyecto y/o servicio (Contratista)	Personal del proveedor adjudicataria del servicio y enlace del mismo entre AST y el proveedor. Es responsable de todos los contratistas (directos o de subcontratas a su cargo) implicados en el proyecto y/o servicio. ▪ Trasladar al personal a su cargo y verificar el cumplimiento de las normas de AST. ▪ Verificar que, los contratistas (directos o de subcontratas a su cargo) disponen de toda la documentación de PRL, confidencialidad y seguridad en regla a través de la plataforma e-coordina. ▪ Supervisar el cumplimiento por parte del personal a su cargo de las normas que les afectan.
Proveedor (Contratista, Personal externo)	▪ Conocer y cumplir las normas de PRL, seguridad, confidencialidad y buenas practicas que les aplican. ▪ Realizar todas las acciones necesarias para proteger la seguridad de la información.
Todo el personal (AST)	▪ Conocer y cumplir con la normativa de seguridad. ▪ Realizar todas las acciones necesarias para proteger la seguridad de la información.

Tabla 1-1. Roles y responsabilidades.

1.6. Documentación relacionada

La implantación de un Procedimiento como el descrito requiere el examen previo de la siguiente documentación:

- *POL Política del Sistema Integrado de Gestión*
- *POL Gestión Calidad y Seguridad Información*
- *POL Seguridad del Esquema Nacional de Seguridad.*
- Proceso *PRO_O14 Gestión Seguridad*
- Declaración de aplicabilidad o SOA del ENS
- Declaración de aplicabilidad o SOA de la ISO 27001

1.7. Cumplimiento de normativas y estándares

Para la elaboración del cuerpo normativo se ha tenido en cuenta la declaración de aplicabilidad (SoA), recogida en la «*REG_E3_Declaracion_Aplicabilidad(SoA)*»

En el Cuerpo Normativo de Seguridad de AST se describen las directrices y medidas a establecer para parte de los controles de la declaración de aplicabilidad, o SOA, marcados por las siguientes normativas y estándares:

- *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad*. Y *Real Decreto 951/2015, de 23 de octubre, de modificación 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*. En adelante **ENS**
- *Norma UNE-EN ISO/IEC 27001:2017*. En adelante **ISO 27001**.
- *Reglamento (UE) 2016/679 General de Protección de Datos 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*. En adelante **RGPD**.
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. En adelante **LOPD-GDD**.
- *Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE*.

- *ORDEN PRE/690/2019, de 14 de mayo, por la que se dispone la publicación del Protocolo General de Actuación, para la colaboración en materia de ciberseguridad, entre el Centro Criptológico Nacional del Centro Nacional de Inteligencia y la Entidad Pública Aragonesa de Servicios Telemáticos*.

Leyes y normas consideradas fuera de alcance

- *Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones*. Comité de Seguridad de Aragonesa de Servicios Telemáticos del 11 de junio de 2019.

1.8. Deber de denuncia de incumplimiento

En el supuesto de que se detecte algún incumplimiento de alguna norma contenida en el presente documento, se debe comunicar al Responsable de Seguridad con la finalidad de analizar las causas (posibles fallos técnicos, de procedimiento, humanos) las consecuencias y/o repercusiones del incumplimiento (o posibles consecuencias) para estudiar e implantar las medidas necesarias que permitan evitar la repetición de esta situaciones, así como en el caso de que se considere necesario modificar la propia normativa.

2. Marco teórico

2.1. Principios básicos y requisitos mínimos definidos en el ENS

Se recomienda encarecidamente, la lectura y comprensión 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*, ya que el presente cuerpo normativo está basado en él. Tomando como referencia y asumiendo como propio el contenido del ENS, AST basara en él su cuerpo normativo de seguridad.

El ENS, en su Artículo 4, define:

> *«El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información.»*

Para ello define una serie de principios básicos y requisitos mínimos que reflejamos en la siguiente tabla, y cuya explicación viene descrita en el mencionado real decreto.

Principios básicos	Requisitos mínimos	
a) Seguridad integral.	a) Organización e implantación del proceso de seguridad.	i) Integridad y actualización del sistema.
b) Gestión de riesgos.	b) Análisis y gestión de los riesgos.	j) Protección de la información almacenada y en tránsito.
c) Prevención, reacción y recuperación.	c) Gestión de personal.	k) Prevención ante otros sistemas de información interconectados.
d) Líneas de defensa.	d) Profesionalidad.	l) Registro de actividad.
e) Reevaluación periódica.	e) Autorización y control de los accesos.	m) Incidentes de seguridad.
f) Función diferenciada.	f) Protección de las instalaciones.	n) Continuidad de la actividad.
	g) Adquisición de productos.	o) Mejora continua del proceso de seguridad.
	h) Seguridad por defecto.	

Tabla 2-1. Principios básicos y requisitos mínimos definidos en el ENS

El presente cuerpo normativo busca ser fiel a estos preceptos, teniéndolos presentes tanto en las normas específicamente escritas, como en la actuación diaria de la entidad.

A continuación, destacamos algunos de estos preceptos y se destaca la interpretación de la entidad:

2.2. Líneas de defensa

En un entorno tan amplio y diverso como el que gestiona AST, este principio básico ha de ser un pilar fundamental de toda la infraestructura. El ENS lo define como:

> *«El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:*
>
> *a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.*
>
> *b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.*
>
> *c) Minimizar el impacto final sobre el mismo.*
>
> *Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica»*

La defensa en profundidad determina que se ha de proteger un activo frente a una vulnerabilidad, pese a que ya exista una línea de protección que proteja de esa vulnerabilidad en una capa superior. A priori, no se puede confiar la seguridad a única línea.

Esto, no contradice que, en una gestión de riesgos, se considere que el riesgo residual sea menor – y por lo tanto la prioridad de los recursos a invertir sean proporcionales y ponderados a la amenaza – que si no hubiera una o varias líneas de defensa que en capas superiores proteja de la amenaza origen.

2.3. Mejora continua del proceso de seguridad

La seguridad es un proceso, no un estado.

Nunca se va a estar completamente seguro. Según avance el tiempo, una configuración que en su momento podría ser adecuada para situar la seguridad en un umbral razonable, se puede volver obsoleta.

Nuevas vulnerabilidades surgen diariamente. Toda tecnología requiere de un mantenimiento continuo y un proceso de actualización. Tanto a nivel de hardware, de software, de configuración o incluso de arquitectura.

Los procedimientos, la organización y el conocimiento, de todos los actores –implicados en el diseño, gestión y mantenimiento, de los servicios sustentados por los sistemas de información– han de actualizarse de manera continua. Con la naturalidad que lleva que lo que en su momento se consideró suficiente o adecuado, hoy puede ser visto como insuficiente o erróneo. Pasado el tiempo se han de cuestionar las decisiones y configuraciones adoptadas, con el fin de detectar brechas en las mismas que tengan que ser corregidas.

2.4. Seguridad por defecto

Ante cualquier decisión, diseño o configuración, se ha de adoptar la máxima de la seguridad por defecto. Es posible que por necesidades del negocio u otros imperativos –operatividad, etc.– se pueda tomar la decisión consciente, razonada y justificada, que rebaje la seguridad de un entorno. Esas decisiones han de quedar registradas, con un responsable nominal –no para dilucidar responsabilidades, salvo casos flagrantes, si no para facilitar la revisión de la misma pasado el tiempo– y estar acompañadas de un análisis de riesgos.

N1 Organización y normativa

N1.1 Normativa documentada

N1.1.1 Política de seguridad

AST cuenta con un conjunto de políticas escritas para la seguridad de la información. Dichas políticas han de ser, aprobadas por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Estas están publicadas en el sistema integrado de gestión, de forma que están disponibles para todos los miembros de la organización, así como otras partes interesadas.

En dichas políticas se precisa de forma clara, lo siguiente:

i. Los objetivos o misión de la organización.

ii. El marco legal y regulatorio en el que se desarrollarán las actividades.

iii. Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

iv. La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

v. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

N1.1.2 Cuerpo Normativo de Seguridad

Este documento describe:

i. El uso correcto de equipos, servicios e instalaciones.

ii. Lo que se considerará uso indebido.

iii. La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

iv. La obligación de proveedores y resto de usuarios del cumplimiento de las normas que les aplican.

En aquellos casos en los que se requiera un mayor grado de detalle para desarrollar la normativa se crearan las instrucciones técnicas, o documentación equivalente.

N1.1.3 Revisión del cuerpo normativo de seguridad

Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Dentro de la Política del SGI, *POL_Organización y Funciones AST* se especifican las funciones relativas a la aprobación de las políticas. La política está en publicada en la página web y en la plataforma de gestión documental para todo el personal. Es revisada anualmente.

Por otro lado, el presente documento es revisado anualmente por el Responsable de Seguridad de la entidad. Cualquier modificación ha de ser aprobada por el Comité de Seguridad.

N1.1.4 Procedimientos e instrucciones técnicas

Se dispondrá de una serie de documentos que detallen de forma clara y precisa:

i. Cómo llevar a cabo las tareas habituales.

ii. Quién debe hacer cada tarea.

iii. Cómo identificar y reportar comportamientos anómalos.

N1.2 Organización de la seguridad de la información

N1.2.1 Proceso de autorización

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:

i. Utilización de instalaciones, habituales y alternativas.

ii. Entrada de equipos en producción, en particular, equipos que involucren criptografía.

iii. Entrada de aplicaciones en producción.

iv. Establecimiento de enlaces de comunicaciones con otros sistemas.

v. Utilización de medios de comunicación, habituales y alternativos.

vi. Utilización de soportes de información.

vii. Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.

viii. Utilización de servicios de terceros, bajo contrato o Convenio.

N1.2.2 Roles y responsabilidades en seguridad de la información

Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.

Dichas responsabilidades se determinan los requisitos de cada puesto de trabajo. Esta información se recoge en la correspondiente Ficha del puesto de trabajo, definida y actualizada por la Dirección de Recursos.

N1.2.3 Segregación de tareas

Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

Se cuenta con una estructura organizativa dentro de AST con responsabilidades, funciones y obligaciones en materia de gestión de la seguridad de la información. Esta estructura es necesaria para la correcta implantación, gestión y mantenimiento de un Sistema de Gestión de Seguridad de la Información, extensible a toda la organización. Se determinan los requisitos de cada puesto de trabajo. Esta información se recoge en la correspondiente Ficha del puesto de trabajo.

N1.2.4 Contacto con las autoridades

Deben mantenerse los contactos apropiados con las autoridades pertinentes.

La gestión y desarrollo de las actividades cotidianas hace necesario que AST mantenga diferentes contactos, a veces de forma muy estrecha, con numerosas entidades privadas y organismos públicos.

AST mantiene puntualmente contactos con empresas profesionales en asesoría y consultoría en materia de gestión de la seguridad de la información destinando partidas de su presupuesto a cubrir de forma efectiva las necesidades existentes en esta materia.

Se ha de gestionar y mantener la relación con el Centro Criptológico Nacional (CCN), con el que hay un convenio vigente. Se cuenta con herramientas de comunicación de incidentes con el mismo (LUCIA Federada) y con sondas de monitorización

Por otro lado, se ha de ver y analizar las alertas y sugerencias provenientes de otros CERT, como el del INCIBE.

El Responsable de Seguridad tiene asignada específicamente estas tareas de contacto en su ficha de perfil de puesto.

N1.2.5 Contacto con grupos de interés especial

Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

AST mantiene contactos con foros, asociaciones profesionales, medios de comunicación y demás grupos de especial interés en materia de seguridad de la información (congreso anual de ciberseguridad CNN, administración electrónica, inscripción de alertas INCIBE). El Responsable de Seguridad, es el responsable de mantener y ser la cara visible de la Organización a la hora de establecer relaciones con estos grupos de interés incluyendo foros, asociaciones profesionales y medios de comunicación en materia de seguridad de la información.

N1.2.6 Seguridad de la información en la gestión de proyectos

La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.

PROC_O2 Gestión Proyectos

Se cuenta con un procedimiento de gestión de proyectos. También se cuenta con un proceso de gestión de la demanda donde se analiza y valida las distintas demandas que entran a Aragonesa de Servicios Telemáticos ya sean a través de los clientes, o generadas internamente. Existe un control en el cierre de proyectos.

N1.2.7 Divulgación

Como entidad pública de referencia en las TIC, AST ha de participar de forma activa en la divulgación de las ventajas de las nuevas tecnologías, las tendencias que detecta y los riesgos asociados a las mismas. Otra faceta importante para la entidad se centra en estimular la presencia de las mujeres en estudios de Ciencia, Tecnología, Ingeniería y Matemáticas (STEM).

N2 Recursos

N2.1 Activos

La información contenida en los Sistemas de Información de AST (activos) es propiedad de AST, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa del Director de la Unidad.

Se consideran por AST activos a todo soporte capaz de almacenar, procesar o transmitir información, tales como: equipos fijos, servidores, equipos de almacenamiento, etcétera; así como ordenadores portátiles, agendas personales y teléfonos móviles. Ya sean propiedad de AST, o estén disponibles en modo servicio.

N2.1.1 Inventario de activos

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

El proceso *O6 Gestión de la configuración* detalla los inventarios existentes vigentes en ese momento. Ver el Anexo III *Listado de CMDB de proceso «O6 Gestión de la configuración»* en la página 141.

N2.1.2 Responsabilidad de los activos

Todos los activos que figuran en el inventario deben tener un responsable asignado.

Es decir, en todos los registros se cuenta con responsable asignado y un mantenedor. Esta norma se trata en el proceso *A4 Gestión de infraestructura y SI*.

Por norma general la responsabilidad de los diferentes activos es ostentada por los responsables de la Dirección al que dichos activos sean destinados.

La asignación de los responsables se hace constar dentro del inventario de activos de AST (CMDB) y puede asociarse a un servicio concreto, un conjunto de actividades, una aplicación o un conjunto de datos, todo ello en función del control más o menos estricto que se necesita tener sobre los activos incluidos.

El responsable del activo tiene la obligación de:

i. Asegurar que la información y los activos que la procesan están correctamente clasificados.

ii. Definir y revisar regularmente, los permisos de acceso a dichos activos según las normas englobadas en el epígrafe *N4.4 Acceso*.

iii. Asegurar la implementación de los controles establecidos para la adquisición, tratamiento, almacenamiento y distribución de la información.

iv. De que sean etiquetados los activos de información cuando así se requiera.

v. Verificar que los activos bajo su responsabilidad se mantienen convenientemente actualizados en la CMDB y la información relativa a ellos está en vigencia.

vi. Fiscalizar el adecuado borrado o destrucción del activo

Las funciones del responsable pueden ser delegadas. Esta facultad de delegación no afecta al inventariado y clasificación de los activos que sólo puede validar su alta el responsable. Dentro del mismo inventario de activos se hará constar la identidad del responsable de cada uno de los activos, así como la de aquellas personas, cargos o entidades en quién el responsable del activo haya delegado sus funciones.

N2.1.3 Uso aceptable de los activos

Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

AST facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, aplicaciones y servicios informáticos que AST pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está prohibido.

El usuario debe ser consciente de las amenazas provocadas por software malicioso. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo. Los equipos de usuario cuentan en todo momento con sistemas de antivirus.

N2.1.4 Devolución de activos

Todos los empleados y terceras partes deben devolver todo activo de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

Cuando los medios informáticos o de comunicaciones proporcionados por AST estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función

N2.1.5 Retirada de materiales propiedad de AST

Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.

Se mantendrá un inventario donde se indican los servidores que han sido dados de baja.

Se entiende que, los medios de trabajo especialmente indicados para la movilidad como ordenadores portátiles y teléfonos no requieren de más autorización que las condiciones indicadas cuando se suministró al empleado.

Respecto a las empresas externas, se les hará firmar una cláusula de seguridad de la información para proveedores de AST, que cubra este punto. Ver el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142.

Categorización de los activos

N2.2 Recursos Humanos

N2.2.1 Investigación de antecedentes

La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.

PRO_A5_Selección, contratación y baja de empleados.

Para ocupar un puesto de trabajo, el ocupante deberá cumplir los requisitos generales previstos en el artículo 56 de RDL 5/2015, de 30 de octubre, por el que

se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público y, en su caso, los específicos contemplados en la correspondiente convocatoria. AST, evalúa el grado de educación, formación, habilidades y experiencia del personal en los procesos de selección. Parte de la evaluación se basa en el *curriculum vitae* del candidato, pero también se somete al mismo a un examen escrito y una entrevista personal. Esta información queda recogida en el archivo de datos personales del Área de Gestión de Recursos Humanos. Se evalúa que los candidatos tengan las capacidades en seguridad de la información necesaria.

Dependiendo de la importancia o sensibilidad del cargo se pueden investigar mediante; fuentes abiertas, consulta a contactos reconocidos, etc. Con el fin de asegurar la idoneidad al puesto de trabajo, y descartar los candidatos con perfiles de mayor riesgo.

En los servicios externos de larga duración, como son los acuerdos marco y otros contratos de cierta importancia, se exige en los pliegos unos niveles de experiencia y certificación a los técnicos de la contrata.

En cualquier caso, en concordancia con el primer párrafo de la norma, los niveles de exigencia son proporcionales al puesto a desempeñar.

N2.2.2 Caracterización del puesto de trabajo

Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben conocer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información.

Cada puesto de trabajo se caracterizará de la siguiente forma:

i. Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad.

ii. Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.

iii. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

Tal y como se ha descrito en la norma *N2.2.1 Investigación de antecedentes*, en la página 30, el proceso de selección recoge grado de educación, formación,

habilidades y experiencia del personal, que han de cubrir, como minino, la relación de los requisitos y obligaciones del puesto reflejado en la *REG_E6 Ficha de perfil de puesto*. Dichas fichas solo son obligatorias en los puestos de mayor nivel de responsabilidad. Y, en cualquier caso, todo el personal interno de AST, les aplica el *Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público* que en su, articulo *Artículo 52. Deberes de los empleados públicos. Código de Conducta* especifica el deber de guardar la confidencialidad.

También han le son de aplicación la *RESOLUCIÓN de 28 de julio de 2006, de la Dirección General de Trabajo e Inmigración, por la que se dispone la inscripción en el registro y publicación del VII Convenio Colectivo para el Personal Laboral de la Administración de la Comunidad Autónoma de Aragón*, en donde en su *Artículo 69.-Faltas muy graves*, se especifica como tal «La violación del sigilo profesional».

Adicionalmente se al personal interno entrega una circular informativa *02A Circular informativa RGPD y confidencialidad*, cuya firma se exige a las nuevas incorporaciones.

Todos los empleados internos de AST, están obligados a guardar confidencialidad por la Ley del Estatuto Básico del Empleado Público y por VII Convenio Colectivo para el Personal Laboral de la Administración de la Comunidad Autónoma de Aragón

---

En el caso de las empresas externas que dan servicio o realizan un proyecto, con AST; se obliga a las mismas a tener firmado una cláusula de confidencialidad del estilo al mostrado en el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142. En donde la empresa externa adquiere el deber y la responsabilidad de extender las obligaciones de confidencialidad, tanto con sus empleados directos como con las empresas y empleados subcontratados que participen del servicio/proyecto.

N2.2.3 Deberes y obligaciones

Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

i. Se especificarán las medidas disciplinarias a que haya lugar.

ii. Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.

iii. Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación. Para lo cual firmara la pertinente cláusula de confidencialidad

En caso de personal externo que realiza un proyecto o presta un servicio:

iv. Se establecerán los deberes y obligaciones de la empresa y su personal.

v. Se establecerán los deberes y obligaciones de cada parte.

vi. Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Estos últimos requisitos se establecen tanto en el pliego, en la presente normativa – que también les aplica – como en la cláusula de confidencialidad del estilo al mostrado en el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142.

N2.2.4 Responsabilidades de gestión

La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

En este sentido AST dispone de un procedimiento *PRO_A5_Selección, contratación y baja de empleados* y un *Plan de formación, concienciación y sensibilización*, *REG_E6_Programa concienciación calidad y seguridad*, presentados y validados por el Comité de Seguridad, orientados a los empleados y usuarios de sus sistemas con el objetivo de concienciar a los mismos en aspectos sobre la seguridad de la información. Todas las funciones en seguridad de la información están definidas. Además, se cuenta con las fichas de perfil de puesto.

Tal y como se indica en normas anteriores. En el caso de las empresas externas que dan servicio o realizan un proyecto, con AST; se obliga a las mismas a tener firmado una cláusula de confidencialidad del estilo al mostrado en el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142.

N2.2.5 Concienciación, educación y capacitación en seguridad de la información

Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

i. La normativa de seguridad relativa al buen uso de los sistemas.

ii. La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

iii. El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

iv. Configuración de sistemas.

v. Detección y reacción a incidentes.

vi. Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

La formación del personal de AST está justificada como consecuencia de: puntos de mejora en el desempeño del trabajo, introducción de nuevas tecnologías y cambios legales o introducción de normas. Todos los años se realiza un plan de formación en función de las necesidades anteriormente descritas. La identificación de las acciones formativas se realiza mediante el envió a los Directores de Área de *Ficha Propuesta Formación*, envió a todos los empleados de la entidad un cuestionario acerca de propuestas de formación a nivel individual y opinión

de carencias colectivas y propuestas que decide directamente la Dirección Gerencia de AST. También se cuenta con un proceso para las actividades pendientes y fuera del plan.

Adicionalmente del *Plan de formación, concienciación y sensibilización*, *REG_E6_Programa concienciación calidad y seguridad*. – presentado y validado por el Comité de Seguridad – se desarrollan acciones planteadas por el Responsable del Área de Seguridad, orientados a los usuarios de la entidad y a los administradores de los sistemas (indistintamente que sea personal propio de la entidad o externos) con el objetivo de concienciar a los usuarios en aspectos sobre la seguridad de la información.

Por último, recalcar que AST es *«[...] MEDIO propio instrumental y servicio técnico de la Administración de la Comunidad Autónoma de Aragón y de sus Organismos Públicos dependientes, así como del resto de poderes adjudicadores dependientes de aquella y de éstos, para la realización de servicios relacionados con las funciones previstas […]*», es decir que la gestión de sistemas de comunicaciones, la correcta identificación de incidentes y la gestión de los mismos es la competencia central de negocio (*core*) de la entidad.

N2.2.6 Personal alternativo

Para aquellos puestos con funciones críticas, se garantizará a existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual. El personal alternativo deberá estar sometido a las mismas garantías de seguridad que el personal habitual.

Para ello, cada dirección asignara como suplir las ausencias (habitualmente con un responsable del mismo nivel jerárquico o superior, dentro de la misma dirección).

En el caso de los servicios prestados por empresas externas, en pliego se exige un número mínimo de personal capaz de gestionar la infraestructura asumiendo bajas, vacaciones y rotación del personal externo asociado al mismo.

N2.2.7 Proceso disciplinario

El personal de AST se rige por con el régimen disciplinario de la admiración pública. Por lo que al menos les aplica las leyes:

- *Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público*.

- *RESOLUCIÓN de 28 de julio de 2006, de la Dirección General de Trabajo e Inmigración, por la que se dispone la inscripción en el registro y publicación del VII Convenio Colectivo para el Personal Laboral de la Administración de la Comunidad Autónoma de Aragón*.

En donde se recogen las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

Con el fin de potenciar la divulgación de estas normas, se reflejan algunos de los artículos que son de aplicación:

Ley del Estatuto Básico del Empleado Público

---

2. Son faltas muy graves

[…] e) La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función.

[…] e) La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función.

3. Las faltas graves serán establecidas […], atendiendo a las siguientes circunstancias

[…] c) El descrédito para la imagen pública de la Administración

---

Artículo 95. Faltas disciplinarias

.

VII Convenio Colectivo para el Personal Laboral de la Administración de la Comunidad Autónoma de Aragón

---

[…] D) Descuidos en la conservación del material, instalaciones o documentos y la falta de higiene personal.

[…] G) El retraso, negligencia o descuido en el cumplimiento de las tareas.

Artículo 67.-Faltas leves

[…] C) Abandono del puesto de trabajo o falta de atención debida al trabajo encomendado y la desobediencia a sus superiores en materia de servicio que implicase quebranto manifiesto de la disciplina o causará un perjuicio notorio al servicio.

[…] H) La no utilización de los equipos de protección individual; así como no seguir las indicaciones de seguridad.

Artículo 68.-Faltas graves

[…] E) El abandono del trabajo que cause perjuicio de importancia extraordinaria a la Administración de la Comunidad Autónoma de Aragón, a los asistidos, al público o, en general, al servicio.

[…] F) El falseamiento voluntario de datos e informaciones del servicio.

[…] I) La violación del sigilo profesional.

Artículo 69.-Faltas muy graves

N2.2.8 Responsabilidades ante la finalización o cambio

Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.

El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al Área de Gestión de Recursos Humanos de AST, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. De la misma manera, cuando los medios informáticos o de comunicaciones proporcionados por

AST estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

Los contratos de confidencialidad firmado por el personal interno y por las empresas contratistas – y los empleados directos y subcontratados de estas – exigen un deber de confidencialidad que se extiende más allá de la extinción de la relación contractual.

N2.3 Servicios externos

N2.3.1 Contratación y acuerdos de nivel de servicio

En los servicios de categoría[1] media o superior, previa a la utilización de recursos externos, se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.

N2.3.2 Control y revisión de la provisión de servicios del proveedor

AST debe controlar, revisar y auditar regularmente la provisión de servicios del proveedor.

Proceso O13 Gestión de los Niveles de Servicio

El responsable del contrato por parte de AST, junto con el responsable del adjudicatario y la Oficina Técnica de Calidad definen el informe de seguimiento del contrato, trabajando conjuntamente los criterios de medición y la presentación de los indicadores. Este informe contiene, en todos los casos, los Acuerdos de Nivel de Servicio definidos en los pliegos. Estos informes están sujetos a mejora continua. Durante la ejecución del contrato se llevarán a cabo los comités de dirección y las reuniones periódicas de seguimiento, tal y como se haya establecido en el modelo de relación de la licitación y debe quedar constancia de todas ellas levantando acta.

[1] Ver *Anexo X Categorización de los sistemas*, en la página 166.

N2.3.3 Gestión diaria

En los servicios de categoría[2] media o superior. Para la gestión diaria del sistema, se establecerán los siguientes puntos:

i. Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado (*PRO_O13 Gestión de niveles servicio*).

ii. El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo (*PRO_O4 Gestión de cambios* y *PRO_O10 Gestión de la disponibilidad*)

iii. El mecanismo y los procedimientos de coordinación en caso de incidentes y desastres (*PRO_O3 Gestión de incidencias* y *PRO_O12 Gestión de la continuidad*).

N2.3.4 Gestión de cambios en la provisión del servicio del proveedor

Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos.

Todos los cambios serán registrados y se hará seguimiento de los mismos durante las reuniones periódicas de seguimiento.

N2.3.5 Medios alternativos

En los servicios de nivel alto[3], estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo contara con las mismas garantías de seguridad que el servicio habitual.

N2.3.6 Política de seguridad de la información en las relaciones con los proveedores

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.

[2] Ver *Anexo X Categorización de los sistemas*, en la página 166.
[3] Ver *Anexo X Categorización de los sistemas*, en la página 166.

Toda subcontratación de servicios informáticos se materializa en un acuerdo contractual, en virtud del cual AST pacta la realización o la prestación de un determinado servicio con un tercero. Los contratos especifican la Calidad del Servicio prestado en base a acuerdos de niveles de servicio, el compromiso de confidencialidad por parte del proveedor, el cumplimiento de las normas de seguridad y los procedimientos operativos. Los proveedores deben acatar las responsabilidades que de ellos se derivan. Todo contrato a de contar con las clausulas con especificaciones de seguridad y RGPD.

Ver el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142.

N2.3.7 Requisitos de seguridad en contratos con terceros

Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.

Este hecho se refleja tanto en la relación con proveedores con una relación contractual directa con AST. Ver el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142.

Como en situaciones en que un tercero tenga un contrato con otro organismo y para la ejecución del mismo necesite acceder a la infraestructura gestionada por AST. En donde existen clausulas especificas *PLA.O14 Cláusula de seguridad de la información, para la utilización por parte de terceros de la infraestructura o servicios de AST*. En donde compromete con la seguridad tanto a la empresa contratada, como al organismo que encarga dicho contrato.

También existen clausulas especificas del Articulo 28 de la GDPR, *Cláusula contractual de prestación de servicios de tratamiento de datos por cuenta de tercero*.

N2.3.8 Cadena de suministro de tecnología de la información y de las comunicaciones

Los acuerdos con proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos y servicios.

Siendo obligación del proveedor transmitir la necesidad de reproducir los requisitos de seguridad de la información y velar por el cumplimiento de las mismas por parte de entidades subcontratadas que den servicio a el Gobierno de Aragón.

Así como asegurar que los productos suministrados funcionan como se espera sin ningún tipo de características inesperadas o indeseadas.

Ver el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 142.

N3 Proyectos y Servicios

N3.1 Planificación

N3.1.1 Análisis de riesgos

PRO_E3 Planificación Sistema Integrado Gestión

Categoría[4] BÁSICA

Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:

i. Identifique los activos más valiosos del sistema.
ii. Identifique las amenazas más probables.
iii. Identifique las salvaguardas que protegen de dichas amenazas.
iv. Identifique los principales riesgos residuales.

Categoría MEDIA

Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:

i. Identifique y valore cualitativamente los activos más valiosos del sistema.
ii. Identifique y cuantifique las amenazas más probables.
iii. Identifique y valore las salvaguardas que protegen de dichas amenazas.

[4] Ver *Anexo X Categorización de los sistemas*, en la página 166.

iv. Identifique y valore el riesgo residual.

Categoría ALTA

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

i. Identifique y valore cualitativamente los activos más valiosos del sistema.

ii. Identifique y cuantifique las amenazas posibles.

iii. Identifique las vulnerabilidades habilitantes de dichas amenazas.

iv. Identifique y valore las salvaguardas adecuadas.

v. Identifique y valore el riesgo residual.

N3.1.2 Análisis de requisitos y especificaciones de seguridad de la información

Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Para ello, en los pliegos de los diferentes contratos se incluyen cláusulas para la seguridad.

N3.1.3 Arquitectura de seguridad

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

Categoría[5] BÁSICA

i. Documentación de las instalaciones:

   a) Áreas.

   b) Puntos de acceso.

ii. Documentación del sistema:

   a) Equipos.

   b) Redes internas y conexiones al exterior.

[5] Ver *Anexo X Categorización de los sistemas*, en la página 166.

c) Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

iii. Esquema de líneas de defensa:

a) Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet.

b) Cortafuegos, DMZ, etc.

c) Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

iv. Sistema de identificación y autenticación de usuarios:

a) Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.

b) Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Categoría MEDIA

v. Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información

Categoría ALTA

vi. Sistema de gestión de seguridad de la información con actualización y aprobación periódica.

vii. Controles técnicos internos:

a) Validación de datos de entrada, salida y datos intermedios.

N3.1.4 Adquisición de nuevos componentes

PRO_O2 Gestión proyectos

Se establecerá un proceso formal (*PRO_O2 Gestión proyectos*) para planificar la adquisición de nuevos componentes del sistema, proceso que:

i. Atenderá a las conclusiones del análisis de riesgos (ver la norma *N3.1.1 Análisis de riesgos*, en la página 41).

ii. Será acorde a la arquitectura de seguridad escogida: (ver la norma *N3.1.2 Análisis de requisitos* y especificaciones de seguridad de la información

Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Para ello, en los pliegos de los diferentes contratos se incluyen cláusulas para la seguridad.

iii. Arquitectura de seguridad, en la página 42.

iv. Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

N3.1.5 Dimensionamiento / Gestión de capacidades

PRO_O2 Gestión proyectos

Los entornos de nivel MEDIO o superior. Con carácter previo a la puesta en explotación, se realizará un estudio previo que cubrirá los siguientes aspectos:

i. Necesidades de procesamiento (*PRO_O11 Gestión de la capacidad*).

ii. Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse (*PRO_O11 Gestión de la capacidad*).

iii. Necesidades de comunicación (*PRO_O10 Gestión de la disponibilidad*).

iv. Necesidades de personal: cantidad y cualificación profesional.

v. Necesidades de instalaciones y medios auxiliares (*PRO_O10 Gestión de la disponibilidad*, *PRO_O12 Gestión de la continuidad*).

N3.1.6 Planificación de las actualizaciones y mantenimiento

Los nuevos entornos y servicios han de diseñarse para ser actualizados y mantenidos durante todo el periodo que tengan que estar activos. Por lo que se debe definir en el diseño los procedimientos y responsabilidades, tanto para la ejecución del mantenimiento o actualización, como para el proceso de notificación previa, autorización y validación de dichas actuaciones. Esto aplica tanto a las infraestructuras contenidas en la entidad, como aquellos elementos que sin estar

gestionados por AST utilizan la infraestructura utilizada por la misma. En este último caso hay que tener en cuenta que un elemento no gestionado por AST, pero dentro de su entorno, puede comprometer a otros elementos adyacentes. En estos casos se requiere distribuir y firmar por las partes cláusulas de responsabilidad del estilo de la mostrada en el Anexo V *PLA.O14 Cláusula de seguridad de la información, para la utilización por parte de terceros de la infraestructura o servicios de AST*, descrita en la página 148.

Todas estas operaciones de mantenimiento han de cumplir las normas: *N2.3.4 Gestión de cambios en la provisión del servicio del proveedor* –página 39–, *N4.4.4 Segregación de funciones y tareas* –página 64–, *N5.1.1 Custodia* –página 78–, *N6.2.4 Mantenimiento de los equipos* –página 98–, *N8.1.4 Mantenimiento* –página 108–, *N8.3.2 Registros de administración y operación* –página 112–, y sobre todo, todas las normas descritas dentro del epígrafe *N9 Aplicaciones: desarrollo y mantenimiento*, descrito a partir de la página 116.

N3.2 Servicios

N3.2.1 Asegurar los servicios de aplicaciones en redes públicas

La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, revelación y modificación no autorizadas.

Por ello, todos los nuevos servicios han de basarse en protocolos cifrados (https, VPN, etc.). Se ha de hacer un esfuerzo por detectar y corregir servicios que no reúnan estas características y transmitir a los propietarios del servicio la necesidad de corregir dicha situación.

Se utilizan y gestionan firmas electrónicas para personas individuales como sellos de órgano y otro tipo de certificados.

N3.2.2 Protección de las transacciones de servicios de aplicaciones

La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.

Se ha de utilizar firma electrónica en aquellos servicios que lo requieran. Las rutas de comunicación han de estar cifradas y utilizando certificados según lo indicado en la norma *N4.2.7 Gestión de certificados*, pagina 56.

N3.2.3 Componentes certificados

Para aquellos sistemas de categoría[6] ALTA

Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales. Cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

Se detallará, ya sea en el pliego o en una instrucción técnica de seguridad detallará los criterios exigibles.

N3.2.4 Protección de servicios y aplicaciones web

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

i. Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:
   a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
   b) Se prevendrán ataques de manipulación de URL.
   c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies".
   d) Se prevendrán ataques de inyección de código.
ii. Se prevendrán intentos de escalado de privilegios.
iii. Se prevendrán ataques de "*cross site scripting*".

[6] Ver *Anexo X Categorización de los sistemas*, en la página 166.

iv. Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxy*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos como caché.

Nivel BAJO

Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.

Nivel ALTO

Se emplearán "certificados cualificados de autenticación del sitio web" acordes a la normativa europea en la materia.

N3.2.5 Protección frente a la denegación de servicio

Nivel MEDIO

Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (*DoS Denial of Service*). Para ello:

i. Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.

ii. Se desplegarán tecnologías para prevenir los ataques conocidos.

Nivel ALTO

iii. Se establecerá un sistema de detección de ataques de denegación de servicio.

iv. Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

v. Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

En la medida de lo posible, todos los servicios centralizados contaran con una protección anti DoS (Ver Acuerdo Marco de Telecomunicaciones).

N3.2.6 Medios alternativos

Para los servicios que lo requieran, siendo obligatorio en todos los de nivel Alto. Nivel ALTO. Se garantizará la existencia y disponibilidad de medios alternativos

para prestar los servicios en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección que los medios habituales.

Los servicios centralizados gestionados desde AST se plantean con CPD redundantes en ubicaciones geográficas separadas, al menos, 70km. Lo que garantiza la disponibilidad de los medios alternativos. El RTO es proporcional al nivel de servicio exigido.

N4 Sistemas de Información

N4.1 Organización de la información

N4.1.1 Clasificación de la información

La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

PRO_A1 Gestión de la Información Documentada

Toda la documentación está clasificada según el procedimiento de referencia[7] en público, restringido (uso interno) y confidencial. La responsabilidad de la clasificación y/o reclasificación de la información es del propietario de dicha información.

Nivel BAJO

i. Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma.

ii. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.

iii. La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido.

[7] Ver «IT_A1_Gestión Documentación Corporativa»

iv. El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

v. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Nivel MEDIO

Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

vi. Su control de acceso.

vii. Su almacenamiento.

viii. La realización de copias.

ix. El etiquetado de soportes.

x. Su transmisión telemática.

xi. Y cualquier otra actividad relacionada con dicha información.

N4.1.2 Etiquetado de la información

Toda la documentación está clasificada según el procedimiento de referencia en público, restringido (uso interno) y confidencial. La responsabilidad del etiquetado es del propietario de dicha información. El comité de seguridad es el responsable de aprobar la documentación en seguridad de la información.

PROC_A1 Gestión de la Información Documentada

En todos los documentos generados por AST se ha de identificar en su portada y en cada una de las paginas, ya sea en el pie de página, marca de agua o en donde se considere adecuado, la clasificación del mismo.

N4.1.3 Manipulado de la información

Toda la información será manipulada en función de las normativas internas de AST. Todos los empleados están sujetos a un acuerdo de confidencialidad. Todas las empresas que por la naturaleza de sus servicios o proyectos tienen acceso a

información de AST han de firmar una cláusula[8] de confidencialidad y distribuir entre sus empleados (directos o subcontratados) la responsabilidad de la misma, mediante la firma de cláusulas equivalentes.

N4.1.4 Anonimización y seudonimización de la información sensible

Para garantizar la protección de la información AST prohíbe el uso de datos Productivos en entornos no productivos a no ser que estén perfectamente anonimizados con procedimientos o herramientas garantizadas.

i. Anonimización

El objetivo de la anonimización de los datos personales es imposibilitar la identificación de una persona física en el conjunto de datos anonimizados, incluso con la ayuda de los datos originales, por lo que los datos anonimizados no se consideran datos personales. Es importante señalar que no existe un estándar prescriptivo para la anonimización dentro de los marcos legales de la UE, por lo que la elección de utilizar métodos de anonimización apropiados recae sobre el delegado de protección de datos.

AST utilizará los siguientes métodos teniendo en cuenta el grado de riesgo y el uso previsto de los datos.

- **Sustitución de directorio**: modificación del nombre de las personas físicas integradas en los datos, manteniendo la coherencia entre los valores, como "código postal + ciudad", "edad + sexo".
- **Codificación**: Implica una mezcla u ofuscación de letras. El proceso a veces puede ser reversible. Por ejemplo: Robert podría convertirse en Betror.
- **Enmascaramiento**: permite que una parte de los datos se oculte con caracteres aleatorios u otros datos.
- **Borrosidad**: una aproximación de los valores de los datos para volver obsoleto su significado y o imposibilitar la identificación de los individuos.
- **Privacidad diferencial**: este método se puede usar siempre que AST le brinde a un tercero acceso a un conjunto de datos anónimos. Una copia de los datos originales permanece en AST, y el destinatario externo solo recibe un conjunto de datos anónimos.

[8] Ver el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor* en la página 49.

- **Agregación**: un interesado se agrupa con varios otros interesados que comparten algunos o todos los datos personales.

ii. Seudonimización

La seudonimización pretende mejorar la privacidad mediante la sustitución de los campos de identificación dentro de un registro de datos por uno o más identificadores artificiales o seudónimos. Como tal, la seudonimización reduce, pero no elimina por completo, la capacidad de vincular un conjunto de datos con la identidad de un interesado.

El delegado de protección de datos establecerá los métodos apropiados de seudonimización tales como:

- **Cifrado** (utilizando una clave secreta): Los datos son cifrados con el uso de una clave secreta. El titular de la clave secreta puede volver a identificar fácilmente a los interesados descifrado el conjunto de datos.
- **Funciones hash**: Se utilizan para asignar datos de cualquier tamaño a códigos de un tamaño fijo (tenga en cuenta que existen técnicas de hash múltiples (por ejemplo, hashes salados, hashes con clave, etc.).
- **Tokenización**: es el proceso de sustitución de un elemento de datos confidenciales por un equivalente no sensible, denominado token. El token es una referencia (ej. un identificador) que se correlaciona con los datos sensibles a través de un sistema de tokenización. El sistema de tokenización proporciona a las aplicaciones de tratamiento de datos la autoridad y las interfaces para solicitar tokens o destokenizar a los datos sensibles.

N4.2 Medidas

N4.2.1 Cifrado y política de uso de los controles criptográficos

Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

En los entornos de categorizados como Alto, para el cifrado de información se estará a lo que se indica a continuación:

i. La información con un nivel ALTO en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

ii. Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en la norma N7.1.4 *Protección de la confidencialidad*, en la página 104.

iii. Para el uso de criptografía en los soportes de información, se estará a lo dispuesto en la norma N5.1.2 *Criptografía* en la página 78.

N4.2.2 Gestión de claves

Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

Se utilizarán controles criptográficos en los siguientes casos:

i. Para la protección de claves de acceso a sistemas, datos y servicios

ii. Para la transmisión de información clasificada, fuera del ámbito de la Entidad.

iii. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Responsable de Seguridad.

N4.2.3 Firma electrónica

Portafirmas corporativo del Gobierno de Aragón

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

La integridad y la autenticidad de los documentos se garantizarán por MEDIO de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.

En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que

ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del Artículo 27 del ENS.

Nivel BAJO

Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

i. Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

ii. Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

iii. Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:

iv. Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

   a. Certificados.

   b. Datos de verificación y validación.

v. El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes a) y b) del apartado *iv*.

iv. La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes *i* y *ii*.

Nivel ALTO

v. Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma.

vi. Se emplearán productos certificados conforme a lo establecido en la norma N3.2.3 *Componentes certificados*, página 46.

En este sentido, cumpliendo los requisitos de nivel ALTO del Esquema Nacional de Seguridad, AST (como el conjunto del Gobierno de Aragón) dentro de la Administración Electrónica cuenta con un portafirmas corporativo, que permite la firma y verificación de documentos gracias a los certificados de la FNMT.

N4.2.4 Sellos de tiempo

En los sistemas categorizados como nivel ALTO, los sellos de tiempo prevendrán la posibilidad del repudio posterior:

i. Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.

ii. Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.

iii. Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.

iv. Se utilizarán productos certificados (según la norma *N3.2.3 Componentes certificados*, página 46) o servicios externos admitidos (véase la norma *N8.3.3 Protección de la información de registro* en la página 113).

v. Se emplearán «sellos cualificados de tiempo electrónicos» acordes con la normativa europea en la materia.

N4.2.5 Limpieza de documentos

En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

i. Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

ii. Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.

iii. A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

N4.2.6 Copias de seguridad (*backup*)

PRO_O12 Gestión de la Continuidad

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

Las copias de seguridad deberán abarcar:

i. Información de trabajo de la organización.

ii. Aplicaciones en explotación, incluyendo los sistemas operativos.

iii. Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

iv. Claves utilizadas para preservar la confidencialidad de la información.

Los servidores cuentan con su propio sistema de copia de seguridad, con una frecuencia según el RPO marcado y una retención estipulada. Las unidades de red y otros servidores de documentación se encuentran dentro de los servidores corporativos, haciéndose copia de seguridad de todos ellos y de la información que contienen.

Por último, el sistema de copias de seguridad de la electrónica de red guarda todas las configuraciones, actuales e históricas, garantizando un RPO en estos elementos de 0.

La recuperación de información de cada uno de los sistemas e regularmente revisada y probada conforme a la *PRO_O12 Gestión de la Continuidad* y a los planes que de ella se generan. Se guardan los correspondientes registros *REG_O12_Pruebas_de_contingencia*.

N4.2.7 Gestión de certificados

AST utiliza certificados de seguridad para garantizar que la transmisión de datos entre un servidor y un usuario, o viceversa, a través de Internet, sea completamente segura. Para llevar a cabo esta tarea es necesaria que los certificados digitales utilizados en sus servidores estén bajo la gestión adecuada para poder, entre otros objetivos, tener control sobre dónde o/y quien utiliza cada certificado y el uso que se hace de cada uno de ellos.

La presente normativa engloba a todos aquellos certificados válidos utilizados en AST para asegurar las comunicaciones entre los servidores y los usuarios. Incluye tanto a los generados por entidades certificadoras como los autogenerados en AST, para su uso en las plataformas gestionadas por la propia entidad.

En el *Anexo XIII Entidades Certificadoras reconocidas en AST* –página 172– se identifican las Entidades Certificadores en las AST solicita sus certificados de confianza. También se identifica en el *Anexo XIII* las Áreas de AST que pueden generar certificados autofirmados para su uso en entornos no productivos, o para elementos internos de AST.

El ciclo de vida de los Certificados de Seguridad en AST y lo que implica su gestión se basan en su generación, custodia, despliegue, rotación y, llegado el momento, destrucción de los mismos. Sobre cada una de las fases se detalla la norma que aplica.

i. Generación de los Certificados

Solo pueden utilizarse para servidores en Producción los certificados solicitados por AST y a las empresas certificadoras indicadas en el Anexo I.

Los certificados utilizados en otros entornos de AST (preproducción e interno) serán autofirmados dentro de la Plataforma de AST creada a tal fin (PT.Generacion_Certificados). En el caso de que sea, por motivos técnicos, absolutamente necesario utilizar un certificado oficial en entornos No Productivos se debe aplicar la Normativa de Gestión de Autorizaciones para solicitarlo. En todo caso se instalará uno diferente al que haya instalado en Producción (es decir se tendrá que

solicitar uno nuevo a una entidad certificadora habilitada). El certificado debe incluir letras que indiquen el entorno al que debe prestar servicio (PRE para preproducción o INT para integración).

El procedimiento para solicitar un certificado tanto de Empresa Certificadora como autogenerado en AST es el de Gestión de Certificados de Seguridad.

ii. Custodia y monitorización de Certificados

Los certificados se encuentran en un único repositorio seguro (PTS.CUSTODIA_CERTIFICADOS). Este repositorio se encuentra cifrado y dentro de un sistema de versionado que le asegura el *backup* de la información.

En la actualidad no es posible auditar el uso de los certificados, ni el registro de las acciones llevadas a cabo por los certificados.

iii. Despliegue

Para llevar a cabo la instalación de un Certificado en un servidor es necesario hacer llegar los ficheros al personal técnico que lo debe instalar.

El Área de Seguridad que custodia el certificado facilita un fichero cifrado al técnico concreto que va a realizar la instalación. El fichero cifrado contiene la información necesaria en formato adecuado (habitualmente: *.p12*). El cifrado se realiza con la herramienta estipulada por AST y con un algoritmo de cifra actualizado.

La vía de comunicación para facilitar las claves de descifrado de fichero que contiene el certificado es bien en persona, bien telefónica. En ningún caso, se ha de proporcionar por el mismo medio por el que se facilita el certificado. Y menos aún en el mismo momento.

iv. Rotación

La vida de un certificado es limitada en el tiempo y es necesaria su renovación para poder seguir utilizándolo. Para garantizar su actualización es necesario un control sobre su vigencia y establecer la gestión pertinente para mantenerlo activo. Llegado el caso de que deje de utilizarse se debe proceder a su revocación y destrucción definitiva.

Caducidad/Expiración

Para aquellos certificados que estén bajo custodia de AST, el Área de Seguridad es la responsable de avisar al propietario del Certificado sobre su caducidad con una antelación suficiente

Se establecen dos avisos: A los 30 días y a los 15 días. El primero de ellos debe ser comunicado mediante correo electrónico. El segundo de ellos, 15 días antes del vencimiento, por teléfono y correo electrónico al contacto establecido.

Renovación

La Renovación de un Certificado se lleva a cabo a través del Procedimiento de Gestión de Certificados de Seguridad.

v. Revocación o/y destrucción

La Revocación o/y Destrucción de un Certificado se lleva a cabo a través del Procedimiento de Gestión de Certificados de Seguridad.

La tramitación de la revocación la lleva a cabo el Área de Seguridad bajo solicitud del propietario del certificado.

La destrucción de un certificado se lleva a cabo con el borrado de todos los ficheros relacionados con dicho certificado en el repositorio de certificados.

Los ficheros de certificados caducados son automáticamente destruidos.

N4.3 Seguridad en las comunicaciones

N4.3.1 Políticas y procedimientos de intercambio de información

Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

En el proceso *PRO_A1 Gestión información documentada* se incluye el procedimiento en vigor para la recepción, intercambio y distribución de documentos.

N4.3.2 Acuerdos de intercambio de información

Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.

En el proceso *PRO_A1 Gestión información documentada* se incluye el procedimiento en vigor para la recepción, intercambio y distribución de documentos. En el caso de acuerdos con terceros se incluye dentro de los contratos.

Existen cláusulas de confidencialidad para proveedores, clientes, proveedores de clientes sin relación contractual directa con AST pero que usan su infraestructura y entidades/personas colaboradoras sin relación contractual.

N4.3.3 Mensajería electrónica

La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.

El correo electrónico corporativo es una herramienta de AST, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Un uso indebido del mismo repercute de manera directa a toda la organización.

Los servidores de correo se deben encontrar dentro de la infraestructura de AST evitando accesos dichos sistemas – y la información en ellos contenida – por parte de personal no autorizado.

Dicho entorno ha de contar con las medidas de protección adecuadas, como son cortafuegos, *antispam*, etc.

N4.3.4 Acuerdos de confidencialidad o no revelación

Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación

La información contenida en los Sistemas de Información de AST es propiedad de AST, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, dentro de los parámetros indicados en el *PRO_A1 Gestión información documentada*.

Existen cláusulas de confidencialidad tanto para personal interno, proveedores, clientes, para proveedores de clientes sin relación contractual directa con AST pero que usan su infraestructura y pare entidades/personas colaboradoras sin relación contractual

N4.3.5 Requerimientos técnicos de notificaciones y publicaciones electrónicas.

Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el ENS, las siguientes exigencias técnicas:

i. Aseguren la autenticidad del organismo que lo publique.

ii. Aseguren la integridad de la información publicada.

iii. Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.

iv. Aseguren la autenticidad del destinatario de la publicación o notificación

N4.3.6 Responsabilidad de exfiltración de la información por medios electrónicos fuera del entorno del Gobierno de Aragón

El usuario será responsable de toda la información que extraiga fuera de la organización, tanto a través de dispositivos físicos, como mediante medios digitales (correo electrónico, sistemas de intercambio o almacenamiento en la nube, sistemas de mensajería instantánea u otras herramientas). Es imprescindible un uso responsable, evaluando si es imprescindible la copia de esa información fuera del entorno del Gobierno de Aragón. Cuando no quede mayor alternativa, especialmente cuando se trate información sensible, confidencial o protegida, se han de usar medidas de protección criptográfica que impida la lectura no autorizada de dicha información. No se considera suficiente la supuesta confidencialidad que pueda otorgar el proveedor de ese medio, salvo que se cuente con un contracto especifico con AST con cláusulas equivalentes a la mostrada en el *Anexo IV PLA.O14 Clausula seguridad información AST Proveedor*, página 142.

N4.4 Acceso

N4.4.1 Política de control de acceso

Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

AST implementa, a través de su herramienta IDM, un control de accesos basado en roles, RBAC, adaptado. Los usuarios disponen de una credencial compuesta por una cuenta de usuario y una contraseña. También, se les proporciona una tarjeta con certificado digital, para el acceso a alguno de los Sistemas de Información del Gobierno de Aragón.

La gestión de servidores de nivel ALTO requiere de un doble factor de autenticación

Adicionalmente el acceso físico a las ubicaciones de AST esta descrito en *IT_A4 Control acceso y visitas ubicaciones AST*, donde para las oficinas propias se requiere de una tarjeta de acceso.

En el caso de los CPD la *IT_A4 Seguridad Física y Control Acceso a los CPD de AST*, refleja todos los elementos de control de acceso al CPD (con tarjeta o control biométrico, registro de visitas y protocolo de acompañamiento).

Los racks de comunicaciones, ubicados en espacios accesibles, han de estar cerrados con llave.

N4.4.2 Identificación

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

i. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.

ii. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.

iii. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:

   a) Se puede saber quién recibe y qué derechos de acceso recibe.

   b) Se puede saber quién ha hecho algo y qué ha hecho.

iv. Las cuentas de usuario se gestionarán de la siguiente forma:

   a) Cada cuenta estará asociada a un identificador único.

   b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.

   c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.

v. En los supuestos contemplados en el Capítulo IV 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*, relativo a "Comunicaciones Electrónicas", las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el *Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE*:

   a) Si se requiere un nivel BAJO[9] en la dimensión de autenticidad: Nivel de seguridad bajo, sustancial o ALTO (artículo 8 del Reglamento n.º 910/2014)

   b) Si se requiere un nivel MEDIO[10] en la dimensión de autenticidad: Nivel de seguridad sustancial o ALTO (artículo 8 del Reglamento n.º 910/2014)

   c) Si se requiere un nivel ALTO[11] en la dimensión de autenticidad: Nivel de seguridad ALTO (artículo 8 del Reglamento n.º 910/2014).

Los usuarios disponen de una credencial compuesta por una cuenta de usuario y una contraseña. También se les proporciona una tarjeta con certificado digital, para el acceso a los Sistemas de Información de AST. Los usuarios son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. La cuenta de usuario es única para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

Aquellos usuarios con privilegios especiales emplearán el identificador que les otorga dichos privilegios únicamente durante el desarrollo de las actividades que

[9] Ver *Anexo X Categorización de los sistemas*, en la página 166.
[10] Ver *Anexo X Categorización de los sistemas*, en la página 166.
[11] Ver *Anexo X Categorización de los sistemas*, en la página 166.

requieran de los mismos. Para el resto de las actividades cotidianas emplearán un identificador diferente.

Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al CAU de AST (4100) la correspondiente incidencia de seguridad.

Si, en un momento dado, un usuario recibiera una llamada telefónica solicitándole su nombre de usuario y contraseña, **nunca facilitará dichos datos** y procederá a comunicar este hecho a la al CAU de AST (4100), de forma inmediata.

Cada vez que entre un usuario a AST se le facilitara una contraseña para acceder a los sistemas que ha de cambiar tras el primer acceso. Las contraseñas tienen que tener las siguientes características:

iv. El usuario modifica la contraseña en el primer acceso.

v. Se fuerza el cambio de contraseña cada 3 meses.

vi. La contraseña siempre debe de estar formada por al menos 8 dígitos con caracteres alga/numérico, mayúsculas, minúsculas y símbolos.

vii. Se cuenta con un registro de contraseñas.

   a. Se ocultan las contraseñas en pantalla.

viii. Todas las contraseñas se almacenan y transmiten en modo protegido.

N4.4.3 Requisitos de acceso

Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

Los requisitos de acceso se atenderán a lo que a continuación se indica:

i. Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

ii. Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

iii. Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

AST establece mecanismos de autenticación seguros para garantizar las conexiones realizadas desde redes externas, segregando sus redes de manera que se pueda restringir el acceso a los servicios proporcionados.

Los accesos remotos a la red corporativa de AST, se establecen mediante controles y mecanismos que permitan garantizar las personas que realizan dichos accesos, de acuerdo al riesgo asociado a la conexión y a los recursos empleados en dicha conexión.

Tras un periodo determinado de inactividad, se deben terminar automáticamente las sesiones establecidas en acceso remoto. Accesos por control de firewall.

N4.4.4 Segregación de funciones y tareas

En los entornos de nivel MEDIO o superior. El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.

En concreto, se separarán al menos las siguientes funciones:

i. Desarrollo de operación.

ii. Configuración y mantenimiento del sistema de operación.

iii. Auditoría o supervisión de cualquier otra función.

N4.4.5 Registro y baja de usuario

Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

PRO_A5 Gestión recursos humanos

El alta de los usuarios será comunicada al Área de Gestión de Recursos Humanos. La autorización del acceso a los recursos establecerá el perfil necesario

con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

La baja de los usuarios será comunicada al Área de Gestión de Recursos Humanos, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

Se genera el *ticket* en OTRS.

N4.4.6 Provisión de acceso de usuario

Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

PRO_A5 Gestión recursos humanos

A cada nuevo usuario que se incorpore a la organización y así lo precise, el Área de Gestión de Recursos Humanos de AST le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales asignándole un perfil de acceso.

El proceso de alta incluye la creación de una identidad digital, unificada para el acceso y uso de los recursos TIC de la organización. Esta identidad se crea en la plataforma de gestión de empleados (SIRGHA) y es distribuida de forma automática por el IDM.

El proceso de baja, se efectúa igualmente por la plataforma de gestión de empleados, deshabilitando en el IDM la identidad. Pasado un tiempo esta se elimina.

N4.4.7 Gestión de privilegios de acceso

La asignación y el uso de privilegios de acceso debe estar restringida y controlada.

Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios:

i. **Mínimo privilegio**. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada.

ii. **Necesidad de conocer**. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

iii. **Capacidad de autorizar**. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

La normativa de AST en cuanto a privilegios se basa en el acceso de mínimo privilegio o ámbito de mínimo privilegio (AMP), por lo que, para poder realizar ciertas acciones, se debe de cumplir con el proceso de solicitud de aprobación, acceso o escalonado y aprobación de la autorización. Se cuenta con un documento de Solicitudes de Autorizaciones activadas.

Los sistemas están diseñados o configurados para que las cuentas de usuario sólo accedan a las funciones permitidas, ejecutando un número limitado y controlado de actividades, las que requieran sus privilegios especiales. El Responsable de Seguridad emite un Informe anual del registro de escalado. Cuando se precise instalar dispositivos no provistos por AST o utilizar permisos superiores a los inicialmente asignados deberá solicitarse autorización previa.

AST establece las pautas para gestionar la asignación de derechos y privilegios de acceso de los usuarios a los sistemas y servicios.

N4.4.8 Gestión de la información secreta de autenticación de los usuarios

La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.

En el proceso de creación de las credenciales, se proporciona inicialmente una contraseña temporal que se ha de cambiar obligatoriamente en su primer uso. Tal y como se establece en la norma *N4.4.14 Sistema de gestión de contraseñas*.

N4.4.9 Revisión de los derechos de acceso de usuario

Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.

Con periodicidad anual se extrae un registro con las cuentas, los accesos concedidos y aquella información que pueda ser relevante para el propósito. Especial atención debe tenerse a las cuentas de usuarios duplicadas, innecesarias, obsoletas o en situación de bloqueo permanente. El registro se debe hacer llegar al Responsable de Seguridad.

N4.4.10 Retirada o reasignación de los derechos de acceso

Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.

Todos los privilegios de accesos de usuarios tanto internos como externos deben ser cancelados en el momento de la finalización de su contrato o prestación de sus servicios. Todos lo que está integrado con LDAP se dan de baja en el sistema (deshabilitación temporal).

N4.4.11 Uso de la información secreta de autenticación

Los usuarios han de seguir las prácticas de la organización en el uso de la información secreta de autenticación.

La cuenta de usuario es única para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

N4.4.12 Restricción del acceso a la información

Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

La organización restringe el acceso a la información y a los servicios proporcionados por las aplicaciones, de acuerdo a lo establecido la norma *N4.4.7 Gestión de privilegios de acceso*, página 65. Los usuarios reciben el mínimo nivel de acceso a la aplicación, según sus funciones dentro de la organización, ya que un nivel de acceso por encima de dichas necesidades podría ocasionar un riesgo para la confidencialidad e integridad de la información.

N4.4.13 Mecanismo de autenticación

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "**algo que se sabe**": contraseñas o claves concertadas.
- "**algo que se tiene**": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens).
- "**algo que se es**": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:

- Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
- De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
- De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO

i. Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.

ii. En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.

iii. Se atenderá a la seguridad de las credenciales de forma que:

   a) Las credenciales se activarán una vez estén bajo el control efectivo del usuario.

   b) Las credenciales estarán bajo el control exclusivo del usuario.

   c) El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.

   d) Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.

   e) Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

iv. Se exigirá el uso de al menos dos factores de autenticación.

v. En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.

vi. Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:

   a) Presencial.

   b) Telemático usando certificado electrónico cualificado.

   c) Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO

v. Las credenciales se suspenderán tras un periodo definido de no utilización.

vi. En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

vii. Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

N4.4.14 Sistema de gestión de contraseñas

Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.

Se establecen los siguientes requisitos:

i. Forzar el uso de identificadores de usuario y credenciales individuales.

ii. Permitir a los usuarios modificar su contraseña

iii. Forzar el cambio de contraseña, tanto inicialmente como de forma periódica

iv. Formar al usuario para cambiar la contraseña de forma temporal

v. Mantener un registro de las contraseñas utilizadas anteriormente y evitar su reutilización.

vi. Ocultar la contraseña en pantalla

vii. Almacenar y transmitir las contraseñas de un modo protegido.

N4.4.15 Procedimiento de acceso

Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por MEDIO de un procedimiento seguro de inicio de sesión.

Se considera «acceso local» al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización. Estos accesos tendrán en cuenta el nivel de las dimensiones de seguridad:

Nivel BAJO

i. Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso proporcionarán solamente la información indispensable).

ii. El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.

iii. Se registrarán los accesos con éxito, y los fallidos.

iv. El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

Nivel MEDIO

v. Se informará al usuario del último acceso efectuado con su identidad.

Nivel ALTO

vi. El acceso estará limitado por horario, fechas y lugar desde donde se accede.

vii. Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Se considera «acceso remoto» al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.

Nivel BAJO

viii. Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (según lo indicado en los apartados *i*, *ii*, *iii* y *iv*) como el canal de acceso remoto (ver normas *N7.1.4 Protección de la confidencialidad*, página 104, y *N7.1.5 Protección de la autenticidad y de la integridad*, página 104).

Nivel MEDIO

ix. Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.

Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el «salvapantallas», para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 15 minutos.

N4.4.16 Uso de utilidades con privilegios del sistema

Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

Se establece el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Los usuarios no trabajan con el perfil de administrador de su máquina.

N4.4.17 Control de acceso al código fuente de los programas

Se debe restringir el acceso al código fuente de los programas.

El acceso al código fuente está solo limitado a las áreas de la Dirección de Tecnología y Sistemas que lo requieren. De igual forma, también está disponible a las empresas y desarrolladores que lo necesitan para cumplir con sus obligaciones contractuales con el Gobierno de Aragón.

N4.4.18 Gestión de accesos con cuentas privilegiadas

Los accesos lógicos a la administración de los equipos se hacen a través de lo que en AST se llama “Zonas de Salto” donde se accede con los usuarios nominales y se cambia a los usuarios de administración de los equipos

La Zona de Salto (Zona DS o ZDS) son en realidad servidores bastionados que permite acceder a las distintas redes donde se ubican los servidores a administrar. En todo momento se generan *logs* de trazabilidad que permiten hacer un seguimiento de la actividad de las cuentas privilegiadas.

Tanto la Zona DS como los servidores administrados comparten servidor NTP para poder hacer un correcto seguimiento de las actividades.

El acceso al Zona DS se puede realizar desde la red interna únicamente y con el usuario personal. Desde el exterior es necesario acceder por VPN y también con el usuario personal. En ambos casos esta gestionado por las herramientas de control de identidades de AST (IDM y LDAP)

N4.4.19 Conexiones en terminales (*log-on*) seguros

El acceso a los sistemas operativos de la organización estará controlado por un proceso de inicio de sesión diseñado para minimizar los intentos de accesos no autorizados.

Con este fin el proceso de inicio de sesión contará con las siguientes características:

i. El proceso de inicio de sesión no deberá mostrar ninguna información sobre el sistema o aplicaciones hasta que haya sido completado con éxito y el tiempo permitido para establecer el proceso de conexión estará limitado.

ii. Tras un intento fallido existe un retardo hasta que el siguiente intento sea posible.

iii. El número de intentos de log-on en los sistemas estará limitado a 5 intentos y se considerarán los siguientes aspectos.

iv. La cuenta permanecerá bloqueada al menos entre 15 y 30 segundos desde el último intento fallido (en función de la criticidad del sistema).

v. Deberá limitarse el tiempo mínimo y máximo permitido para el proceso de log-on a los sistemas. Si se excede el sistema debe finalizar el proceso de log-on.

vi. En caso de superar el número máximo de intentos se requerirá autorización del superior jerárquico para restablecer una cuenta bloqueada.

vii. Solo se solicita la mínima información imprescindible para conectarse. No se ofrecen mensaje de ayuda durante la conexión y solo se presenta la mínima información imprescindible durante el proceso de conexión.

viii. Solo se validará el acceso cuando los datos insertados en el inicio de sesión sean completos. En caso de error no se informará sobre que parte de los datos son incorrectos.

ix. Se presenta un mensaje indicando que toda actividad podrá ser supervisada y que queda prohibido todo uso no autorizado.

x. Mostrar la siguiente información cuando se haya completado con éxito el procedimiento de inicio de sesión:

   a. Fecha y hora del último log-on completado con éxito, mostrando los intentos fallidos desde entonces.

   b. Detalles de cualquier intento de inicio de sesión fallido desde el ultimo que se completó con éxito.

   c. Mostrar mensaje indicando el uso debido del sistema, quedando prohibido todo uso no autorizado y que toda actividad podrá ser registrada y supervisada.

xi. Durante el proceso de inicio de sesión la contraseña permanecerá oculta mientras es introducida o estará oculta por asteriscos y no podrá ser almacenada en ningún proceso automático (macros, teclas de función…)

xii. Las claves que vayan a viajar por la red para su validación durante el proceso de inicio de sesión irán ocultas y protegidas durante su transmisión.

N4.4.20 Normativa de gestión de autorizaciones

El ámbito de un acceso de mínimo privilegio, o ámbito de mínimo privilegio (AMP), de una credencial está constituido, por una parte, por aquellas Plataformas Tecnológicas a las que se puede acceder con esa credencial y, por otra, por aquellos privilegios mínimos dentro de las plataformas que la credencial necesita para que el propietario de ésta pueda desarrollar toda su actividad.

La autorización es un procedimiento para que una credencial acceda a recursos de manera temporal que están fuera de su ámbito de mínimo privilegio (AMP). Es por este motivo que la Gestión de Autorizaciones debe tomarse como la gestión de excepciones.

La autorización se solicita a través de un procedimiento de Solicitud de Autorización al CAU de AST que debe llegar al Área de Seguridad que la tramita.

Ese procedimiento de autorización debe activarse a través del CAU de AST y en ella debe constar el Responsable de Área solicitante, la plataforma o servicio sobre el que solicita el acceso o escalado. El Responsable de la Plataforma, o en su defecto el Responsable de Seguridad, es la persona que debe validar el acceso o escalado.

Las plataformas tecnológicas están detalladas en el Catálogo de Servicios de AST.

La presente normativa se complementa con la Gestión de Accesos Lógicos y las Normativas de Seguridad Física y del Entorno (*IT_A4_Control_acceso_y_visitas_ubicaciones_AST* y *IT_A4_Seguridad_Fisica_y_Control_Acceso_CPD_AST*).

i. Credenciales de personas, de sistemas y de aplicaciones

La credencial, según Normativa de Gestión de Usuarios está compuestas de un par identificador-clave, es única e intransferible.

Todas las credenciales del personal de AST, o del personal que trabaja para AST, tienen un AMP inicial que está configurado en la Plataforma de Tecnológica de Gestión de Identidades (PT.IDM) y del que se puede extraer un registro.

El uso de una credencial, sea de persona, de sistemas, aplicaciones o cuenta genérica (CUG), para accesos a plataformas, servicios o aplicaciones…, fuera de su AMP requiere obligatoriamente una autorización.

Las autorizaciones a credenciales personales, de aplicaciones, de sistemas o cuentas genéricas son siempre temporales. En AST no hay autorizaciones permanentes para credenciales.

Queda particularmente incluida en esta norma la autorización de accesos entre plataformas, sistemas, servicios y aplicaciones (con todas sus combinaciones), es decir aquellas interactuaciones en las que no intervengan personas. La razón principal es tener un mecanismo de control que permita conocer la interrelación de sistemas y quien se responsabiliza de si es necesario mantener ese intercambio de información habilitado.

ii. Ámbito de Mínimo Privilegio

La definición del Ámbito de Mínimo Privilegio para las credenciales debe realizarse dentro de cada Área de AST. El Responsable de Área debe tener el AMP correctamente definido para las credenciales (personas, sistemas, servicios, aplicaciones…) bajo su alcance para evitar, en lo posible, tener que solicitar autorizaciones.

La solicitud constante de autorizaciones puede ser un indicador de una deficiente definición de los AMP de un área o de una generación de excepciones que merece la pena tener en consideración.

La modificación y validación de los AMP de un Área es potestad del director de esa área. La modificación y validación de los AMP deben ponerse con conocimiento del Responsable de Sistemas y el Responsable de Seguridad.

iii. Solicitud de Autorización

Las Autorizaciones deben ser solicitadas y quedar registradas para su consulta. En AST la solicitud se realizada a través de la herramienta de *ticketing* (PT.OTRS), quedando registro de su solicitud y tramitación.

En el *Anexo VII Solicitudes de Autorizaciones activadas*, mostrado en la página 158 del presente documento, se detallan aquellas autorizaciones que están a priori comprendidas en esta normativa. Del análisis de las autorizaciones solicitadas, el Responsable de Seguridad debe proponer los tipos de autorizaciones que deben ser incluidas o extraídas del Anexo.

El anexo se convierte así en un indicador de las excepciones y en consecuencia un indicador potencial de los riesgos que se asumen en la gestión de las autorizaciones.

iv. Autorización de Acceso o Autorización de Escalado

La solicitud de una autorización se debe dar, bien cuando la credencial necesita escalar privilegios dentro de la plataforma a la que ya puede acceder, bien porque necesita acceder a plataformas y/o servicios para las que no tiene acceso.

En el caso de la escalar privilegios sobre la misma plataforma, sobrepasar el AMP debe generar una petición de autorización de escalado. Si fuera necesario otro escalado sobre uno anterior que ya estuviera fuera del AMP, se debería solicitar de nuevo otra autorización.

El acceso a una plataforma fuera del AMP da lugar a una solicitud de Autorización de Acceso que solo puede conceder un privilegio mínimo sobre esa plataforma. Un escalado sobre ese mínimo privilegio para que la credencial pueda desarrollar su labor requiere una Autorización de Escalado de privilegio.

v. Aprobación de la Autorización

La solicitud de la Autorización debe llegar al Responsable de la Plataforma que es el rol adecuado para poder valorar convenientemente el nuevo AMP

(ámbito de mínimo privilegio) temporal que se le está permitiendo a esa credencial.

vi. Caducidad de las Autorizaciones

Todas las autorizaciones sin excepción son por defecto temporales.

vii. Modificación del Ámbito de Mínimo Privilegio

Dado que las autorizaciones son por definición temporales y para evitar la demanda reiterada y periódica de ellas, se puede solicitar una autorización de ampliación del Ámbito de Mínimo Privilegio con el fin de proponer, justificándolo, un alcance mínimo mayor para esas credenciales.

La solicitud debe ser propuesta por el Responsable de Área a través del al CAU de AST que llega al Responsable de Seguridad. La solicitud se elevará al Director del Área para su validación y se pondrá en conocimiento de los Responsables de las Plataformas afectadas.

viii. Informe periódico

La revisión de las Autorizaciones queda estipulada en Plan de Revisión de Autorizaciones (PLAN_RevisiónAutorizaciones) que aprueba el Comité de Seguridad.

De resultas del Plan de Revisión de Autorizaciones, el Responsable de Seguridad genera un Informe periódico de las autorizaciones recabadas. De su análisis se puede extraer nuevos requisitos de acceso que permiten incrementar el nivel de “mínimo privilegio”

Se trata de tener control sobre los AMP sobrepasados y también información valiosa para establecer nuevos ámbitos de Mínimo Privilegio, tanto por ampliación como por reducción.

Así, que un tipo de perfiles demanden reiteradamente un mayor AMP, debe implicar un estudio de la ampliación de su zona de Mínimo Privilegio por si fuera necesario extenderla para evitar incomodidades y retrasos en las labores encomendadas.

El Responsable de Seguridad se encarga de recabar esa información a través de los registros de las peticiones de autorizaciones y elaborar ese informe proponiendo las mejoras que considere oportunas.

ix. **Solicitud de autorizaciones para usuarios sin credencial**

Las solicitudes de autorizaciones para personal sin credencial de AST (o de Gobierno de Aragón) deben ser igualmente solicitadas por los responsables de Área al CAU de AST utilizando el mismo procedimiento para ello indicando el acceso necesario.

N5 Soportes y puesto de trabajo

N5.1 Soporte físico

N5.1.1 Custodia

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

i. Garantizando el control de acceso con medidas físicas (Ver normas *N6.1.1 Áreas separadas y con control de acceso*, página 94 y *N6.2.3 Registro de entrada y salida de equipamiento*, página 97) o lógicas (*N5.1.2 Criptografía* página 78), o ambas.

ii. Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

N5.1.2 Criptografía

Esta medida se aplica, en particular, a todos los dispositivos removibles. Se entenderán por dispositivos removibles, los CD, DVD, discos USB, u otros de naturaleza análoga. Así como los ordenadores portátiles, teléfonos inteligentes, tabletas o cualquier otro dispositivo que bien almacene en su interior información de nivel MEDIO o superior. O que guarde una configuración que permita el acceso a dicha información (VPN, aplicaciones con parte de la credencial guardada, etc.).

Nivel MEDIO

i. Se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

Nivel ALTO

ii. Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

iii. Se emplearán productos certificados conforme a lo establecido en la norma *N3.2.3 Componentes certificados*, página 46.

N5.1.3 Etiquetado

Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.

N5.1.4 Gestión de soportes extraíbles

Durante el transporte fuera de los límites físicos de la organización, los soportes (USB, discos duros, tarjetas de memoria, CD/DVD, ordenadores portátiles, teléfonos, etc.) que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro. Es responsabilidad del usuario aplicar dichas medidas de seguridad si estas no vienen activadas en dicho soporte.

Para ello se ha de seguir en estos soportes la norma *N5.1.2 Criptografía*, página 78.

Por otro lado, los empleados de la entidad firman una cláusula de uso responsable de los medios que la misma pone a su disposición para la ejecución de su trabajo. Siendo responsabilidad de cada empleado la custodia, cuidado y garante del buen uso de estos medios fuera de la entidad.

En el caso de tener que enviar documentación escrita o trasladar algún soporte se utiliza el sistema de mensajería interna del Gobierno de Aragón con todas las garantías que la misma proporciona.

N5.1.5 Borrado y destrucción

Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

i. Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO

ii. Se destruirán de forma segura los soportes, en los siguientes casos:

a) Cuando la naturaleza del soporte no permita un borrado seguro.

b) Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,

iii. Se emplearán productos certificados conforme a lo establecido en la norma *N3.2.3 Componentes certificados*, página 46.

Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deben ser eliminados de forma segura para evitar accesos ulteriores a dicha información.

Existe un procedimiento escrito y una empresa contratada para la eliminación de equipos informáticos. Los servidores, discos duros, y PC se eliminan por una empresa externa certificada, cuya contratación y registro se efectúa dentro del proceso *PRO_A3 Gestión de contratación*. Dicha empresa emite un certificado de la destrucción la realizada.

N5.1.6 Reutilización

Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

Todo sistema de información que contenga información privada y confidencial, que se haya decidido reutilizar, en lugar de seguir la norma N5.1.5 Borrado y destrucción deberá realizarse un borrado seguro, conforme al procedimiento de reutilización y desechado de soportes de información de AST.

N5.1.7 Soportes físicos en tránsito

El usuario será responsable de toda la información que extraiga fuera de la organización a través de dispositivos tanto físicos, tales como memorias USB, dis-

cos duros portátiles, tarjetas SSD CD, DVD, etc. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida

Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información **deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro**.

Para ello sería de aplicación la norma *N5.1.4 Gestión de soportes extraíbles*, descrita en la página 79.

En el caso de sistemas especiales que así lo requieran, el responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

Para ello:

i. Se dispondrá de un registro de salida que identifique al transportista que recibe el soporte para su traslado.

ii. Se dispondrá de un registro de entrada que identifique al transportista que lo entrega.

iii. Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.

iv. Se utilizarán los medios de protección criptográfica indicados en la norma *N5.1.2 Criptografía* correspondientes al nivel de calificación de la información contenida de mayor nivel.

v. Se gestionarán las claves según la norma *N4.2.2 Gestión de claves*, descrita en la página 52.

N5.1.8 Seguridad de los equipos fuera de las instalaciones

Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

Categoría[12] BÁSICA

[12] Ver *Anexo X Categorización de los sistemas*, en la página 166.

Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

i. Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

ii. Se establecerá un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.

iii. Cuando un equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de Internet y otras redes que no sean de confianza.

iv. Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

Categoría ALTA

v. Se dotará al dispositivo de detectores de violación que permitan saber el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente.

vi. La información de nivel ALTO almacenada en el disco se protegerá mediante cifrado.

N5.2 Puesto de trabajo

N5.2.1 Equipo de usuario desatendido

Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.

Nivel MEDIO

i. El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Nivel ALTO

ii. Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

El usuario debe cerrar su cuenta al terminar la sesión y/o bloquear el equipo cuando lo deje desatendido. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 15 minutos.

N5.2.2 Puesto de trabajo despejado

Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información

Categoría[13] BÁSICA

i. Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento

Categoría MEDIA

ii. Este material se guardará en lugar cerrado cuando no se esté utilizando.

Es crucial proteger la información confidencial de que sea publicada. Las oficinas pueden ser visitadas por proveedores, clientes, personal de limpieza y otros compañeros de trabajo.

La política de escritorio limpio afecta a información en cualquier formato y su fin es el de evitar que recaiga en manos no autorizadas, lo que podría dañar la imagen y reputación de la organización.

[13] Ver *Anexo X Categorización de los sistemas*, en la página 166.

Para ello, todos los escritorios o mesas de trabajo deben permanecer limpios de documentos en papel y dispositivos de almacenamiento digitales, siempre que no estén bajo custodia durante el horario normal de trabajo y especialmente fuera del mismo. En este sentido, además, habrá que ser cauto con los documentos en impresoras y faxes, o el desecho físico de documentación.

Se considera una buena práctica que los empleados mantengan su escritorio lo más limpio y organizado posible. En todo momento:

- Almacenar los documentos que contengan información personal y confidencial en cajones bajo llave, usándolos exclusivamente cuando sea necesario para la labor que desempeñan.
- Bloquear y/o apagar el ordenador cada vez que se alejen físicamente del mismo (*Crtl+Alt+Delete*) o tecla Windows + L.
- No publicar información confidencial como, por ejemplo: nombre de usuario y *passwords*; direcciones IP; contratos; números de cuenta; listas de clientes; propiedad intelectual, datos de empleados, etc.

Al terminar la jornada laboral el empleado:

- Recopilar y asegurar el material confidencial.
- Cerrar bajo llave cajoneras y despachos/oficinas.
- Asegurar que los equipos informáticos, así como cualquier otro equipamiento que esté bajo su responsabilidad, están debidamente apagados.

Se envía anualmente un recordatorio para el cumplimiento del requisito mesa limpia y ordenada a todos el personal y concienciación al respecto.

N5.2.3 Política de dispositivos móviles

Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

Los equipos portátiles pertenecientes a AST, deben disponer de medidas específicas que garanticen la seguridad de la información que contienen, considerando como tales equipos aquellos ordenadores portátiles, agendas personales y teléfonos móviles avanzados, utilizados por los usuarios para almacenar, procesar o acceder a la información relativa a la organización. AST facilita a los

usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, aplicaciones y servicios informáticos que AST pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está prohibido.

Se ha de tener un inventario de activos (equipos portátiles y móviles) que incluya el empleado encargado del buen uso y custodia de los mismos.

N5.2.4 Teletrabajo

Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

Se debe tener especial cuidado cuando se utilicen sistemas de información de AST en lugares públicos, salas de reuniones y otras áreas desprotegidas. En estas situaciones, los usuarios deben tener en cuenta las recomendaciones de buen uso de los sistemas de información referentes a uso de equipos móviles y teletrabajo. Existen registros para la petición en función de la situación.

Existen dos modalidades de teletrabajo aceptada:

i. Con un equipo portátil corporativo. En este caso cuenta con la protección *endpoint* asociada. Y la conexión con el entorno corporativo es mediante uso de canales cifrados (VPN, https, etc.)

ii. Mediante un equipo personal. En este caso, la VPN solo permite establecer un escritorio remoto al puesto fijo del empleado, y a partir de ese punto trabaja con todas las medidas de seguridad corporativas, incluyendo el filtrado y protección en la navegación.

El trabajo fuera de las instalaciones de AST comprende tanto el teletrabajo habitual y permanente de los usuarios desplazados, como el trabajo ocasional, usando, en ambos casos, dispositivos de computación y comunicación (usualmente: ordenador portátil, *tablet*, teléfono móvil, etc.). Este modo de trabajo comprende también las conexiones remotas realizadas desde Congresos o sesiones de formación, alojamientos o, incluso, llamadas telefónicas de contenido profesional que sean realizadas o atendidas en áreas públicas.

El trabajo fuera de las instalaciones de AST conlleva el riesgo de trabajar en lugares desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en sus instalaciones. Fuera de este perímetro de seguridad aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, lo que hace necesario adoptar medidas de seguridad adicionales.

Se incluyen seguidamente un conjunto de normas de obligado cumplimiento, que tienen como objetivo el reducir el riesgo cuando se trabaja fuera de las instalaciones del Gobierno de Aragón.

i. Uso personal y profesional. Los dispositivos móviles de computación y comunicación asignados al usuario del Gobierno de Aragón son para su uso exclusivo y solamente pueden ser utilizados para fines profesionales. No pueden prestarse a terceros salvo autorización expresa de AST, que incluirá en todo caso la definición de las condiciones de uso.

ii. Necesidad de Autorización. La salida fuera de las dependencias del Gobierno de Aragón de documentación, equipos y dispositivos informáticos y de comunicaciones precisa autorización previa de AST. Asimismo, es necesaria la correspondiente autorización para utilizar equipos personales del usuario en el tratamiento de la información de la organización o en el acceso a recursos o sistemas de información del Gobierno de Aragón.

iii. Copias de seguridad. AST no hace por defecto copias de seguridad de los puestos de trabajo. Siendo responsabilidad del usuario utilizar los servidores corporativos para almacenar la información y que esta se pueda recuperar en caso de desastre.

iv. Uso de los canales de comunicación establecidos. La transmisión de información y el acceso remoto se realizará únicamente a través de los canales establecidos, siguiendo los procedimientos y requisitos definidos para ello y adoptando las siguientes precauciones:

    a. En caso de utilizar contraseñas en la autenticación, estas deben ser robustas.

    b. Cerrar siempre la sesión al terminar el trabajo.

c. Cifrar la información sensible, confidencial o protegida que vaya a ser transmitida a través de correo electrónico o cualquier otro canal que no proporcione la confidencialidad adecuada.

v. Vigilancia permanente. La documentación y los dispositivos móviles deben estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada en ellos o que pueda extraerse de ellos. En los desplazamientos en avión, este tipo de equipamiento no debe facturarse y deberá viajar siempre con el usuario.

vi. Evitar el acceso no autorizado. El trabajo en lugares públicos debe realizarse con la mayor cautela y precaución, evitando que personas no autorizadas vean o escuchen información interna a la organización.

vii. En relación con el acceso remoto (vía web), deben adoptarse las siguientes cautelas:

a. Los navegadores utilizados para el acceso vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

b. Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.

c. Desactivar las características de recordar contraseñas en el navegador.

d. Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.

e. Salvo autorización expresa, está prohibida la instalación de addons para el navegador.

viii. Transporte seguro. La documentación y equipos que salgan de las instalaciones del Gobierno de Aragón se deberá transportar de manera segura, evitando proporcionar información sobre el contenido en los mismos y utilizando, en su caso, maletines de seguridad que eviten el acceso

no autorizado. En el caso de información digital esta debe estar cifrada (o en un contenedor cifrado).

ix. Utilización de candados. Es obligatorio el uso de candados y/o cables de seguridad para los dispositivos de computación que deban permanecer desatendidos fuera de las instalaciones del Gobierno de Aragón.

x. Mantenimiento de los equipos. Los equipos se mantendrán de acuerdo con las especificaciones técnicas de uso, almacenamiento, transporte, etc., proporcionadas por el fabricante. En particular, se evitará su uso en condiciones de temperatura o humedad inadecuadas, o en entornos que lo desaconsejen (mesas con alimentos y líquidos, entornos sucios, etc.).

xi. Revisión periódica de los equipos. Al menos, dos veces al año, para verificar la ausencia de software dañino. Esta revisión se hará mediante el gestor centralizado de protección *endpoint*.

xii. Normativa interna. Durante la actividad profesional fuera de las instalaciones del Gobierno de Aragón se seguirán las normas, procedimientos y recomendaciones internas existentes, atendiendo de manera especial a las siguientes:

   a. Las contraseñas deberán ser robustas y renovarse periódicamente o cuando se sospeche que pueden estar comprometidas.

   b. El almacenamiento de la información en soportes electrónicos (CD, DVD, memorias USB, etc.), debe caracterizarse por no ser accesible para usuarios no autorizados. Para ello, es necesario aplicar claves de acceso o algoritmos de cifrado cuando la naturaleza de la información así lo aconseje.

   c. No desactivar las herramientas de seguridad habilitadas en los dispositivos móviles (ordenadores portátiles, móviles, *tablets*, etc.) y comprobar que se mantienen actualizadas.

   d. No descargar ni instalar contenidos no autorizados en los equipos (tonos de teléfono, aplicaciones para *tablets* o móviles, etc.).

N5.2.5 Uso del correo electrónico

El correo electrónico corporativo es una herramienta de AST, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Un uso indebido del mismo repercute de manera directa a toda la organización. Se tienen que cumplir las siguientes directrices:

i. Sólo se permite el empleo de buzones de correo proporcionados por la organización, y su uso será estrictamente laboral.

ii. Los usuarios son responsables de las actividades realizadas con su cuenta/buzón de correo proporcionados por AST.

iii. No facilitar y/o permitir la utilización de la cuenta y/o buzón a personas no autorizadas.

iv. Se prohíbe la utilización de otras cuentas que no sean las puestas a disposición por la organización, el envío de mensajes con direcciones no asignadas por los responsables de la institución y la manipulación de las cabeceras de correo electrónico saliente.

v. El correo electrónico es una herramienta para el intercambio de información y no de difusión.

vi. Es responsabilidad del usuario comunicar cualquier anomalía.

vii. Queda prohibido enviar, almacenar o distribuir mensajes cuyo contenido atente contra los derechos reconocidos en las Leyes españolas y Tratados Internacionales suscritos por España o promueva actuaciones contrarias a la ley.

Así mismo, **se prohíbe el uso del correo para**: propagar cartas encadenadas, esquemas piramidales o similares; enviar correos a quien no desee recibirlo; enviar correo propio desde una cuenta ajena sin consentimiento; atacar para imposibilitar u obstruir sistemas (cuyo único propósito sea el de sobrecargar, paralizar o, de cualquier otro modo, perjudicar el normal uso de este servicio o los equipos informáticos de otros usuarios de Internet); enviar mensajes a foros, *newsgroups* o listas de distribución que comprometan la reputación de la compañía.

Desde el momento en que Aragonesa de Servicios Telemáticos detecte que dichas actividades perjudican el correcto funcionamiento de los servicios y/o provoquen retrasos en las entregas de correo de los demás usuarios de los sistemas, adoptará

las medidas que considere necesarias, ya sea bloqueando direcciones IP, dominios, usuarios u otras medidas, pudiendo incluso procederse a la suspensión inmediata y sin previo aviso del servicio.

Asimismo, el usuario del correo electrónico de AST por el mero hecho de hacer uso del servicio se entiende que acepta los principios enunciados en esta norma, que se conforma como la principal herramienta de AST para la lucha contra esta práctica tan perniciosa para el uso responsable de los recursos de Internet y que se materializa en la Plataforma Tecnológica de AntiSpam (PT.ANTISPAM) de AST.

N5.2.6 Gestión de los recursos asignados al usuario

Los equipos informáticos son asignados el Área de Gestión de Recursos Humanos de AST

Existe un inventario actualizado de los equipos informáticos que están incluidos dentro de la CMDB de AST y regidos por la normativa de Gestión de Activos. Es el Área de Gestión de Recursos Humanos de AST la unidad encargada de gestionar dicho inventario.

A cada nuevo usuario que se incorpore a la organización y así lo precise, el Área de Gestión de Recursos Humanos de AST le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales asignándole un perfil de acceso a los sistemas como “usuario de mínimo privilegio” y siguiendo el procedimiento de Gestión de Usuarios.

Únicamente el personal autorizado según puede distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de AST. Cuando se precise instalar dispositivos no provistos por AST o utilizar permisos superiores a los inicialmente asignados deberá solicitarse autorización previa según Normativa de Gestión de Autorizaciones. En tal caso el usuario tendrá la calificación de ‘Usuario de Acceso Privilegiado’ y tendrá que renovar periódicamente ese status. Los privilegios de administración del PC han de gestionarse mediante una credencial independiente de la usada por el usuario en su trabajo diario. Tal y como refleja la norma *N4.4.20 Normativa de gestión de autorizaciones*, página 74

Los usuarios no tendrán privilegio de administración sobre los equipos con lo que también queda prohibido alterar cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.

Los usuarios deben facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limita únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finaliza completado el mantenimiento o una vez resueltos aquellos.

Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento al Responsable de Seguridad, que tomará las oportunas medidas correctoras y dará traslado de la incidencia a la CAU para su resolución.

Los ordenadores personales de la organización deben mantener actualizados los parches de seguridad de todos los programas que tengan instalados con lo que no se puede desactivar la actualización automática configurada por defecto en la Política de Configuración del Puesto de Trabajo. Se debe prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus.

Los usuarios deberán notificar al CAU de AST (4100), a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

Salvo aquellos ordenadores instalados en las zonas comunes de acceso a Internet (ver norma *N5.2.8 Quiosco interactivo y pantallas informativas*, página 93), cada equipo deberá estar asignado a un usuario. Tales usuarios son responsables de su correcto uso.

El usuario debe participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta al CAU de AST (4100) de tales circunstancias.

El usuario debe ser consciente de las amenazas provocadas por software malicioso. Gran parte del malware (troyanos,) requieren la participación de los usuarios para propagarse, teniendo como vectores de entrada, memorias USB (u otros dispositivos físicos como tarjetas SSD, CD, DVD), mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.

El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata a la Área de Gestión de Recursos Humanos de AST, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. De la misma manera, cuando los medios informáticos o de comunicaciones proporcionados por AST estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

N5.2.7 Copias de seguridad de la información

Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no es objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios subir la información a las plataformas corporativas correspondientes.

En caso de que el usuario decida realizar una copia de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional, fuera de las plataformas corporativas, esta copia deberá de ser en un sistema cifrado con las mismas garantías de confidencialidad que el dispositivo copiado.

AST puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso limitado y compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.

No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales

Mantener copias de seguridad es una cautela esencial de protección de la información. Los datos generados por el usuario en el desempeño de sus competencias profesionales deben mantenerse en un sistema de gestión documental corporativa.

De forma programada, se realizan copias de seguridad, tanto completas como incrementales, de los servidores de AST donde se almacene la información del usuario. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse al CAU de AST (4100).

N5.2.8 Quiosco interactivo y pantallas informativas

Los quioscos interactivos y pantallas informativas; o cualquier otro dispositivo análogo, tiene por definición un acceso público. No teniendo sentido que cuenten con una credencial de acceso nominal, ni bloqueo de pantalla.

Sin embargo, son entornos tremendamente vulnerables, por lo que se ha de tener en cuenta:

i. Las credenciales de administrador del dispositivo han de estar debidamente protegidas por un mecanismo de autenticación que cumpla la norma *N4.4.13 Mecanismo de autenticación*, página 68.

ii. La sesión de información, accesible para el público ha de ser otra que la sesión de administración. La configuración de esta sesión ha de ser tal que mantenga el principio de mínimo privilegio. Permitiendo acceder únicamente a aquellas funciones, programas y sitios lógicos (web, etc) imprescindibles para ejecutar su cometido.

iii. Estos puestos han de estar protegidos contra código malicioso. Y aplicar cualquier otra configuración que disminuya la posibilidad de ser usado en el tiempo de forma perniciosa (congelación de sistema operativo, etc).

iv. Las sesiones de información no han de tener permiso de escritura sobre el propio dispositivo, ni sobre ningún componente que no esté especialmente diseñado para esa escritura.

v. Los campos accesibles desde esos quioscos han de estar protegidos frente la inyección de comando no autorizados.

vi. Salvo necesidad explicita para su función, los puertos de acceso (USB, serial, etc.) han de estar protegidos físicamente, o deshabilitados lógicamente. Se entiende que los quioscos requieren de panel táctil o teclado y ratón para realizar su cometido. En las pantallas de información, se ha de quitar, y bloquear, la posibilidad de acceso y manipulación, al menos en aquellas zonas expuestas al público.

vii. Se ha de aplicar la defensa en profundidad. Al poner un elemento de esta naturaleza, se ha de contemplar la idea de que puede terminar comprometido. Por lo que se debe aislar dentro de la red de otros activos de mayor sensibilidad. En caso de que por funcionamiento estos quiscos requieran acceso a información contenida dentro de la red corporativa, estos deberán tratarse como un elemento externo a la organización, es decir deberán filtrarse su acceso mediante firewall y medidas similares.

N6 Infraestructuras

Todas las normativas que afectan a las infraestructuras quedan reflejadas en el proceso *PRO_A4 Gestión de Infraestructura y SI*, donde sus procedimientos e instrucciones técnicas desarrollan la aplicación de muchas de las normativas situadas bajo este epígrafe.

PRO_A4 Gestión de Infraestructura y SI

N6.1 Control de acceso físico

N6.1.1 Áreas separadas y con control de acceso

Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información. El equipamiento de instalará en áreas separadas específicas para su función.

Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves. Siguiendo una política de puerta cerrada.

AST contempla cuatro tipos de áreas:

i. Oficinas. Centro de trabajo propio o compartido, donde se tiene acceso a los recursos corporativos.

   a. Si el centro de trabajo pertenece, y es compartido, por otro organismo del Gobierno de Aragón el control de acceso será responsabilidad de este último. Siendo obligación de todos los empleados de AST y de las empresas contratadas por AST, seguir las normativas de control de accesos de que se haya establecido en esa ubicación.

   b. En los centros bajo control de AST la normativa de control de acceso está desarrollada en la instrucción técnica *IT A4 Control de acceso y visitas a ubicaciones de AST*.

ii. Cuartos de técnicos de Telecomunicaciones y CPD de terceros. El control de acceso a los mismos es responsabilidad exclusiva del edificio donde están situados o del organismo del que dependa.

iii. Centros de Telecomunicaciones (Emisores). Se encuentran cerrados con un sistema centralizado y el acceso se encuentra fiscalizado.

iv. Centros de Proceso de Datos. Cuentan con una protección de acceso independiente y adicional al edificio donde se encuentra. Una descripción detallada de la norma se encuentra en la instrucción técnica *IT A4 Seguridad Física y Control Acceso a los CPD de AST*.

N6.1.2 Identificación de las personas

Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

El mecanismo de control de acceso se atendrá a lo que se dispone a continuación:

i. Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.

ii. Se registrarán las entradas y salidas de personas.

AST contempla cuatro tipos de áreas:

i. Oficinas. Centro de trabajo propio o compartido, donde se tiene acceso a los recursos corporativos.

a. Si el centro de trabajo pertenece, y es compartido, por otro organismo del Gobierno de Aragón el control de acceso será responsabilidad de este último. AST en esta situación no realiza ningún control de acceso adicional.

b. En los centros bajo control de AST, es obligatorio identificarse y registrase en recepción, salvo que se cuente con un MEDIO de acceso a la oficina (tarjeta de proximidad). El sistema de acceso es fiscalizado y deja un registro telemático que se puede consultar en caso de ser necesario. La normativa de control de acceso está desarrollada en la instrucción técnica *IT A4 Control de acceso y visitas a ubicaciones de AST*.

ii. Cuartos de técnicos de Telecomunicaciones y CPD de terceros. El control de acceso a los mismos es responsabilidad exclusiva del edificio donde están situados o del organismo del que dependa.

iii. Centros de Telecomunicaciones (Emisores). Se encuentran cerrados con un sistema centralizado y el acceso se encuentra fiscalizado electrónicamente.

iv. Centros de Proceso de Datos. Cuentan con una protección de acceso independiente y adicional al edificio donde se encuentra. Se puede acceder por diversos medios (tarjeta de proximidad o control biométrico), estos medios dejan un registro electrónico que se puede consultar. En caso de no disponer de ese medio, la visita ha de contar con una autorización previa por parte de un responsable de AST. En ese caso, se registra manualmente el acceso, se revisa tanto la autorización, como – en el caso de que se vaya a realizar algún trabajo en el interior – la vigencia de la documentación en materia de prevención de riesgos laborales. Una descripción detallada de la norma se encuentra en la instrucción técnica *IT A4 Seguridad Física y Control Acceso a los CPD de AST*.

N6.1.3 Clasificación de ubicaciones y niveles de seguridad de acceso

Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.

En este caso se sigue una política de puertas cerradas. El acceso a la misma se hace mediante tarjeta o registrándose en recepción siguiendo lo establecido en la norma *N6.1.2 Identificación de las personas*, página 95.

N6.2 Procedimientos en áreas seguras

N6.2.1 El trabajo en áreas seguras

Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.

Este procedimiento se encuentra detallado en la *IT A4 Área Segura: Normativa de trabajos en CPD y Centros de Telecomunicaciones*. Se puede ver una copia del misma – que puede estar desactualizada – en el Anexo XII *Área Segura: Normativa de trabajos en CPD*, en la página 170.

N6.2.2 Áreas de carga y descarga

Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.

Existe un entorno de carga y descarga en el edificio de Walqa, permanentemente cerrado y monitorizado mediante alarma. La apertura de la misma se hace exclusivamente bajo supervisión y por estricta necesidad del trabajo que lo requiera.

Los servicios de mensajería, que no son la interna del Gobierno de Aragón, no acceden nunca más allá de la recepción de cada sede.

En los edificios compartidos es responsabilidad del organismo titular de la explotación del edificio.

N6.2.3 Registro de entrada y salida de equipamiento

Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento. Siguiendo el siguiente cuadrante:

i. Oficinas: no aplica.

ii. Cuartos de técnicos de Telecomunicaciones y CPD de terceros. El cambio de cualquier elemento de la electrónica de red ha de estar supervisado por AST. Registrando los cambios en su correspondiente CMDB.

De igual forma, cualquier cambio que afecte a un servidor gestionado por AST se ha de autorizar, controlar y registrar cualquier cambio en el mismo.

iii. Centros de Telecomunicaciones (Emisores). El cambio de cualquier elemento de la electrónica de las redes del Gobierno de Aragón ha de estar supervisado por AST. No hay equipos que almacén o procesen información en estas instalaciones. Solo elementos de recepción y transmisión.

iv. Centros de Proceso de Datos. El cambio de cualquier elemento de hardware – electrónica de red, host, cabina, disco duro, etc. – ha de estar supervisado por AST

N6.2.4 Mantenimiento de los equipos

Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

El mantenimiento de los sistemas informáticos de AST se realiza de conformidad con las recomendaciones de sus respectivos fabricantes y solo el personal de mantenimiento debidamente autorizado debe realizar la reparación de los servicios y equipos.

N6.3 Protección ambiental

N6.3.1 Acondicionamiento de los locales

Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

Los locales donde se ubiquen los sistemas de información y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial:

i. Condiciones de temperatura y humedad.

ii. Protección frente a las amenazas identificadas en el análisis de riesgos.

iii. Protección del cableado frente a incidentes fortuitos o deliberados.

Los sistemas de información y comunicación de AST son protegidos e instalados en lugares que reducen los riesgos de acceso no autorizado o peligros o amenazas ambientales.

En general, para facilitar la gestión y control de dichos accesos, AST ha optado por agrupar estos equipos en salas específicas. En este sentido, los Centros de Proceso de Datos principales son los lugares en donde se almacenan los sistemas ofimáticos (servidores de ficheros, dominio, correo, etc.) y los sistemas centrales de AST. En este último grupo se incluyen los servidores de aplicaciones, bases de datos, sistemas de comunicaciones, etc.

Estas salas han sido consideradas como área segura dentro de la organización, de modo que se han establecido las correspondientes medidas asociadas a la protección de los activos que se encuentran en las áreas seguras.

Las áreas donde se ubican estos equipos incluyen las medidas de seguridad específicas que garantizan la integridad, confidencialidad y disponibilidad inherentes a los sistemas de información ubicados en las salas:

i. Suelo técnico.

ii. Sistema de Control de Acceso basado en tarjetas.

iii. Sistemas automáticos de protección contra incendios y equipos de climatización.

iv. Sistemas de protección contra fallos de suministro eléctrico (Sistemas de Alimentación Interrumpida y Grupo Electrógeno).

Una descripción detallada de esta norma se desarrolla en la instrucción técnica *IT A4 Seguridad Física y Ambiental en los CPD de AST*.

N6.3.2 Emplazamiento y protección de equipos

Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados. Por ello no debe haber equipos sensibles fuera de un entorno de CPD que no cumpla la norma *N6.3.1 Acondicionamiento de los locales*.

N6.3.3 Energía eléctrica

Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

Nivel BAJO

i. Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos:

   a. Se garantizará el suministro de potencia eléctrica.

   b. Se garantizará el correcto funcionamiento de las luces de emergencia.

Nivel MEDIO

ii. Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.

Particularmente, en los CPD principales, AST dispone de un sistema de control del suministro eléctrico conectado al puesto de control. Se cuenta con sistemas (SAI y Grupo Electrógeno) que controlan el suministro de energía a los equipos de forma que se pueda seguir con la continuación de sus actividades en caso de fallo de suministro eléctrico.

N6.3.4 Seguridad del cableado

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.

AST ha diseñado una infraestructura de cableado adecuada a las necesidades de la Organización y protegida de manera que se garantiza tanto la seguridad del cableado eléctrico, como el cableado de comunicaciones (voz y datos). Por ello, dentro de los CPD y Centros de Telecomunicaciones, solo se podrá utilizar cableado debidamente certificado.

N6.3.5 Protección frente a incendios

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.

Una descripción detallada de esta norma se desarrolla en la instrucción técnica *IT A4 Seguridad Física y Ambiental en los CPD de AST*.

N6.3.6 Protección frente a inundaciones

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.

Una descripción detallada de esta norma se desarrolla en la instrucción técnica *IT A4 Seguridad Física y Ambiental en los CPD de AST*.

N6.4 Disponibilidad del entorno

N6.4.1 Instalaciones alternativas

Nivel ALTO

Se garantizará la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles. Las instalaciones alternativas disfrutarán de las mismas garantías de seguridad que las instalaciones habituales.

En este sentido, debe existir redundancia entre los Centros de Proceso de Datos principales, permitiendo que, en caso de caída de uno de ellos, el resto pueda absorber y proveer de los servicios que este prestara – y que se hayan considerado necesarios – dentro de los parámetros que cada servicio tenga estipulados, incluidos los RTO correspondientes.

De igual forma, AST tiene a su disposición diversas oficinas donde trasladar al personal fundamental para el mantenimiento de sus servicios, en caso de que una de ellas no estuviera disponible.

N6.4.2 Medios alternativos

Nivel MEDIO

Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.

Igualmente, se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento.

Se potenciará que la redundancia se plante dentro de cada plataforma tecnología, permitiendo añadir capas de abstracción entre el servicio y el hardware que lo sustenta. A modo de ejemplo:

i. El almacenamiento de la información se haga dentro de cabinas (con replicación) basadas en sistemas RAID que permiten distribuir la información entre múltiples discos duros permitiendo que la indisponibilidad de uno de ellos no afecte a la indisponibilidad del servicio

ii. Virtualización de servidores, que permita ejecutar los sistemas operativos indistintamente del *host* físico donde se esté procesando. La indisponibilidad de un *host* físico concreto no debe afectar al servicio de las máquinas virtuales que habitualmente sustenta.

Cuando no exista esta capacidad de abstracción se habrá de poner los medios técnicos suficientes y la configuración adecuada para que la caída de un elemento de *hardware* (como los elementos de electrónica de red) no afecte a la disponibilidad del servicio que sustenta

En este sentido, debe existir redundancia entre los Centros de Proceso de Datos principales. Permitiendo que, en caso de caída de uno de ellos, el resto pueda absorber y proveer de los servicios que este prestara – y que se hayan considerado necesarios – dentro de los parámetros que cada servicio tenga estipulados. Incluido los RTO correspondientes.

N7 Telecomunicaciones

N7.1 Medidas comunes

N7.1.1 Controles de red

Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

Se realizan controles de acceso a las redes mediante la autenticación de usuarios desde redes externas, la identificación de los equipos dentro de la red, el diagnostico remoto y la protección de los puertos de configuración, control de conexiones a Internet y a Correo, controles de encaminamiento de Red, control de acceso a las aplicaciones. AST gestiona y controla sus redes para la protección contra posibles amenazas tanto de las propias redes, como contra los sistemas y aplicaciones soportadas en ellas, a través de controles que buscan garantizar la confianza en la información que se encuentra dentro del Gobierno de Aragón. AST controla las redes internas de la entidad, así como las redes de acceso a la propia red interna. Las redes de acceso se considerarán redes de

ALTO riesgo, especialmente las redes de acceso externas, directamente expuestas a intentos de intrusión desde el exterior de AST. Por esta razón, se minimizará el número de redes de acceso externas, con el fin de reducir la superficie de exposición y poder centrar los esfuerzos en los mecanismos defensivos. Como norma general, desde entidades conectadas a través de redes de acceso externas únicamente se podrá acceder a servicios situados en redes DMZ. Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio Dominio de Seguridad utilizando, preferentemente, dispositivos *hardware* para el establecimiento y utilización de red privada virtual. Existe un Registro de las Redes de comunicaciones gestionadas por AST (CMDB Comunicaciones) que se revisa continuamente. Periódicamente se crea un Acuerdo Marco de Telecomunicaciones que permite una planificación, actualización y mejora de todas las redes de AST a MEDIO plazo (de cuatro a seis años), evitando los problemas derivados de la obsolescencia tecnológica y permitiendo adecuar globalmente la infraestructura a los diseños más óptimos, escalables y seguros.

N7.1.2 Seguridad de los servicios de red

Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

Las características de seguridad, los niveles de servicio, y los requisitos de gestión para los servicios de red estarán identificados e incluidos en los acuerdos de servicio de red detallados en el Catálogo de Servicios de AST. También hay normas sobre la red inalámbrica corporativa.

N7.1.3 Perímetro seguro

Categoría[14] BÁSICA

i. Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados

Categoría ALTA

[14] Ver *Anexo X Categorización de los sistemas*, en la página 166.

ii. El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.

iii. Se dispondrán sistemas redundantes.

N7.1.4 Protección de la confidencialidad

Nivel MEDIO

i. Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

ii. Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Nivel ALTO

iii. Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

iv. Se emplearán productos certificados conforme a lo establecido en la norma *N3.2.3 Componentes certificados*, descrita en la página 46.

N7.1.5 Protección de la autenticidad y de la integridad

Nivel BAJO

i. Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver norma *N4.4.13 Mecanismo de autenticación*, página 68).

ii. Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos:

   a. La alteración de la información en transito

   b. La inyección de información espuria

   c. El secuestro de la sesión por una tercera parte

iii. Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.

Nivel MEDIO

iv. Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

v. Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

vi. Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

Nivel ALTO

vii. Se valorará positivamente el empleo de dispositivos *hardware* en el establecimiento y utilización de la red privada virtual.

viii. Se emplearán productos certificados conforme a lo establecido en establecido en la norma *N3.2.3 Componentes certificados*, descrita en la página 46.

ix. Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

N7.1.6 Segregación de redes

Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.

La segregación de redes acota el acceso a la información y, en consecuencia, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren. Las redes de AST está segmentada bien por dispositivos físicos y/o lógicos, y los puntos de interconexión están particularmente asegurados, mantenidos y monitorizados.

Categoría[15] ALTA.

La red se segmentará en segmentos de forma que haya:

i. Control de entrada de los usuarios que llegan a cada segmento.

ii. Control de salida de la información disponible en cada segmento.

iii. Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado (como lo descrito en la norma *N7.1.3 Perímetro seguro*, página 103).

[15] Ver *Anexo X Categorización de los sistemas*, en la página 166.

En esta categoría se engloban, entre otras, las redes de gestión. Estas deben estar separadas de las de servicio, con un control de acceso a las mismas mediante algún tipo de entorno bastionado. Con el fin de impedir modificaciones no autorizadas en su configuración.

N7.1.7 Medios alternativos

En los dispositivos de Nivel Alto, como lo son nodos centrales de red (*core*, perimetrales, enlaces, etc). Se garantizará la existencia y disponibilidad de medios alternativos de comunicación para el caso de que fallen los medios habituales. Los medios alternativos de comunicación:

i. Estarán sujetos y proporcionar las mismas garantías de protección que el MEDIO habitual.

ii. Garantizarán un tiempo máximo de entrada en funcionamiento.

N8 Operación y Explotación

N8.1 Seguridad de las operaciones

N8.1.1 Documentación de procedimientos de las operaciones

Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

Dentro del repositorio documental se disponen de *procedimientos* e *instrucciones técnicas* de *operaciones*. Estos procedimientos operativos están asignados a los elementos monitorizados con Nagios. Se actualizarán los mismos cuando: se producen cambios en los sistemas que así lo requieran, se detecten deficiencias en la ejecución de *procedimientos* o *instrucciones técnicas* concretos o cualquier otro tipo de razón que induzca a los validadores de los Procedimientos e Instrucciones a solicitar su revisión.

Cada grupo de trabajo es responsable de redactar y mantener las *instrucciones técnicas de operaciones* que reflejen sus procedimientos. Los responsables de Área – de forma directa o delegada –, han de validar, garantizar la custodia y guardar un índice de la documentación, según lo marcado en el procedimiento *PRO_A1 Gestión información documentada*.

N8.1.2 Configuración de seguridad

Se configurarán los equipos previamente a su entrada en operación, de forma que:

i. Se retiren cuentas y contraseñas estándar.

ii. Se aplicará la regla de "mínima funcionalidad":

a) El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,

b) No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.

c) Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.

iii. Se aplicará la regla de "seguridad por defecto":

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.

b) Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.

c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

N8.1.3 Gestión de la configuración

Categoría[16] MEDIA

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

i. Se mantenga en todo momento la regla de “funcionalidad mínima” (ver norma *N8.1.2 Configuración de seguridad*, página 106).

ii. Se mantenga en todo momento la regla de “seguridad por defecto” (ver norma *N8.1.2 Configuración de seguridad*, página 106).

[16] Ver *Anexo X Categorización de los sistemas*, en la página 166.

iii. El sistema se adapte a las nuevas necesidades, previamente autorizadas (ver norma *N4.4.7 Gestión de privilegios de acceso*, página 65).

iv. El sistema reaccione a vulnerabilidades reportadas (ver norma *N8.1.4 Mantenimiento*, página 108).

v. El sistema reaccione a incidentes (ver norma *N10.1.1 Responsabilidades y procedimientos*, página 125).

N8.1.4 Mantenimiento

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

i. Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

ii. Se efectuará un seguimiento continuo de los anuncios de defectos.

iii. Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

N8.1.5 Gestión de cambios

Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.

PRO_O4 Gestión Cambios

Categoría[17] MEDIA

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

i. Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.

ii. Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la

[17] Ver *Anexo X Categorización de los sistemas*, en la página 166.

nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.

iii. Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.

iv. Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel ALTO serán aprobados explícitamente de forma previa a su implantación.

AST garantiza el control satisfactorio de todos los cambios en los equipos, en el software o en los procedimientos. Se tiene un proceso específico para este ámbito: *PRO_O4 Gestión Cambios*. Existe registro de cambios en OTRS. Se requiere especificar, al menos, los campos:

- Nombre del cambio
- Proyecto asociado
- Fecha propuesta
- Tipo de cambio (Urgencia / Estándar)
- Ventana de corte
- Servicios afectados
- Afección de los servicios
- Responsable cambio Observaciones

N8.1.6 Gestión de capacidades

Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

PRO_O11 Gestión de la capacidad

Se cuenta con un proceso de gestión de la capacidad. AST busca asegurar que la capacidad de las infraestructuras TI se correspondan con las necesidades del negocio de una forma efectiva en términos de costes y de tiempo. Es necesario un equilibrio entre coste y capacidad y entre provisión y demanda. El Plan de Capacidad tiene una vigencia anual y se monitoriza su cumplimiento para adoptar medidas correctivas en cuanto se detecten desviaciones importantes del mismo. Esa revisión es semestral y se coteja con los datos reales extraídos de la monitorización del sistema y de las previsiones de negocio.

También se cuenta con el procedimiento de gestión de la demanda, el objetivo de este proceso es analizar y validar las distintas demandas que entran a Aragonesa de Servicios Telemáticos ya sean de los clientes, o generadas internamente. Una vez validadas también se procede a su valoración económica bien contra presupuesto interno, o a través de la aceptación del departamento que lo solicita. Por último, se redirige al proceso que convertirá la demanda realizada en el producto solicitado, es decir, en un proyecto. Una vez finalizado y puesto en producción, la gestión de la demanda procederá al cierre de la misma.

N8.1.7 Separación de los recursos de desarrollo, prueba y operación

Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

Esta separación queda definida en los procesos: *PRO_06 Gestión de la configuración* y *PRO_08 Gestión de versiones y despliegues*

N8.2 Control del software

N8.2.1 Controles contra el código malicioso

Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como “spyware”, y en general, todo lo conocido como “malware”.

Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

A este respecto y derivado de la enorme superficie de exposición, se requiere una distribución de seguridad *endpoint* centralizada. Adicionalmente, se escanearán y analizarán los comportamientos sospechosos en puntos estratégicos de la red que puedan revelar un entorno comprometido.

Por último, se realizarán campañas de concienciación de cara a los usuarios. Instalación del software en explotación

N8.2.2 Instalación del software en explotación

Se deben implementar procedimientos para controlar la instalación del software en explotación.

En el entorno de servidores esta instalación queda definida en los procesos: *PRO_06 Gestión de la configuración* y *PRO_08 Gestión de versiones y despliegues*

Respecto a los puestos de trabajo digital (PC y Portátiles) de AST se entregan normalizados, y los usuarios que los utilizan no tienen privilegios de administrador con lo que queda restringida la posibilidad de la instalación de software.

Se controlará el número de usuarios con privilegios de administración sobre su propio puesto de trabajo y para aquellos que tengan dichos privilegios, se les dará una credencial específica, diferente a la que usen en su día a día, de tal forma que se dificulte la ejecución o instalación de malware.

N8.2.3 Gestión de las vulnerabilidades técnicas

Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

AST realiza una gestión de vulnerabilidades, tanto técnica como no técnica. Se cuenta un proceso de gestión de vulnerabilidades. Las herramientas son PT.OWASP Vulnerabilidades de la capa de presentación, PT.NESSUS y PT.SIEM para vulnerabilidades de los sistemas operativos.

N8.2.4 Restricción en la instalación de software

Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

Únicamente el personal autorizado puede distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de AST.

N8.3 Monitorización y detección

N8.3.1 Registro de eventos

Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

Con ese fin existe una plataforma tecnológica SIEM dentro de AST donde se ingesta los *logs* de los principales servidores y elementos claves de la electrónica de red. Hay un equipo técnico encargado de buscar nuevos patrones, detectar e investigar nuevas ofensas.

Para el resto de equipos de soporte técnico, se cuenta con unas directrices que marcan la gestión y control de los *logs* generados por los equipos y aplicaciones de AST, como parte de la labor de gestión de los Sistemas de información y la protección de los datos que ejerce en el cumplimiento de sus funciones. Los sistemas de información y comunicaciones AST son monitorizados con la finalidad de identificar comportamientos anómalos o sospechosos. Toda actividad relevante del sistema queda registrada para su análisis posterior. Asimismo, se emplean sistemas de monitorización para inspeccionar eventos que ocurran en tiempo real, como, por ejemplo, la actividad en la red o el uso de los recursos.

N8.3.2 Registros de administración y operación

Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.

Se registrarán las actividades de los usuarios en el sistema, de forma que:

i. El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.

ii. Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

iii. Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.

iv. La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema (ver norma *N3.1.1 Análisis de riesgos*, página 41]).

Nivel BAJO

v. Se activarán los registros de actividad en los servidores.

Nivel MEDIO

vi. Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO

vii. Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.

El ámbito de un acceso de mínimo privilegio, o ámbito de mínimo privilegio (AMP), de una credencial está constituido, por una parte, por aquellas Plataformas Tecnológicas a las que se puede acceder con esa credencial y, por otra, por aquellos privilegios mínimos dentro de las plataformas que la credencial necesita para que el propietario de ésta pueda desarrollar toda su actividad. La autorización se solicita a través de un procedimiento de Solicitud de Autorización al CAU de AST que debe llegar al Área de Seguridad que la tramita. Se guarda un histórico de cada sesión de administración en la propia máquina que hace de pasarela.

Para el apartado vii se cuenta con una herramienta SIEM, cuya administración la llevan a cabo técnicos independientes de otros servicios o funciones.

N8.3.3 Protección de la información de registro

Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.

Nivel ALTO

Se protegerán los registros del sistema, de forma que:

i. Se determinará el periodo de retención de los registros.

ii. Se asegurará la fecha y hora. (Ver norma *N4.2.4 Sellos de tiempo*, página 54).

iii. Los registros no podrán ser modificados ni eliminados por personal no autorizado.

iv. Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

Está prohibido el acceso de personas no autorizadas, con el fin de evitar que puedan ver, alterar o eliminar registros. Para ello los registros son custodiados por la herramienta SIEM (plataforma tecnológica que ingesta, córrela y almacena estos registros). Se establecen dos niveles de permisos:

i. Permiso de lectura, para aquellos que pueden visualizar los datos proporcionados por la herramienta SIEM (plataforma tecnológica que ingesta, córrela y almacena estos registros). Este permiso está extendido entre administradores de otras plataformas tecnológicas, donde la consulta de estos registros permite facilitar la investigación (*Troubleshooting*) de incidentes o problemas en las mismas.

ii. Permiso de administración. Este último se concede únicamente a técnicos independientes de otros servicios o funciones.

El acceso a los registros está restringido a las personas designadas explícitamente por el Responsable de Seguridad y sólo tienen acceso al ámbito necesario para desarrollar las tareas relacionadas. Para ello es necesaria la autorización expresa según las normas *N1.2.1 Proceso de autorización* y *N4.4.7 Gestión de privilegios de acceso*; páginas 25 y 65 respectivamente. Los permisos de los Administradores para acceder a este tipo de información caduca con periodicidad anual y debe ser renovada explícitamente por el Responsable de Seguridad de AST.

N8.3.4 Sincronización del reloj

Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.

Salvo por impedimento técnico justificado, todos los sistemas y equipos de red de AST han de tener configurados los servidores de tiempo corporativos (NTP). Esto es especialmente relevante y debe cumplirse con exactitud para aquellos Sistemas y Equipos de Red que vuelcan sus eventos/*logs* en la Plataforma de Gestión de *Logs* (SIEM) para garantizar la precisión de los sucesos registrados y permitir la correlación de los diferentes eventos.

N8.3.5 Detección de intrusión

Categoría[18] MEDIA

Se dispondrán de herramientas de detección o de prevención de intrusión.

A este respecto AST utiliza las sondas SAT-INET del CCN. La herramienta SIEM también se utiliza para detectar ofensas dentro de la infraestructura.

N8.3.6 Sistema de métricas

Categoría[19] BÁSICA:

i. Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II del Esquema Nacional de Seguridad y, en su caso, para proveer el informe anual requerido por el artículo 35 de dicha ley, el conocido como INES (Informe Nacional del Estado de Seguridad).

Categoría MEDIA:

ii. Además, se recopilarán datos para valorar el sistema de gestión de incidentes, permitiendo conocer

   a. Número de incidentes de seguridad tratados.
   b. Tiempo empleado para cerrar el 50% de los incidentes.
   c. Tiempo empleado para cerrar el 90% de los incidentes.

Categoría ALTA

iii. Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC:

   a. Recursos consumidos: horas y presupuesto.

N8.3.7 Controles de auditoría de sistemas de información

Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.

[18] Ver *Anexo X Categorización de los sistemas*, en la página 166.
[19] Ver *Anexo X Categorización de los sistemas*, en la página 166.

Se cuentan con instrucciones de operaciones para comprobación de los sistemas. Periódicamente se realizarán auditorías técnicas, y se testea la seguridad del entorno. En cualquier caso, siempre se hace bajo las líneas indicadas en el procedimiento *PRO_O10 Gestión de la disponibilidad*.

N9 Aplicaciones: desarrollo y mantenimiento

N9.1 Desarrollo seguro

N9.1.1 Política de desarrollo seguro

Están establecidas y se deben aplicar las reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.

Categoría[20] MEDIA

i. El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.

ii. Se aplicará una metodología de desarrollo reconocida que:

   a) Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.

   b) Trate específicamente los datos usados en pruebas.

   c) Permita la inspección del código fuente.

   d) Incluya normas de programación segura.

iii. Los siguientes elementos serán parte integral del diseño del sistema:

   a) Los mecanismos de identificación y autenticación.

   b) Los mecanismos de protección de la información tratada.

   c) La generación y tratamiento de pistas de auditoría.

iv. Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Se cuenta con un documento que define la *IT_ O12 Normativa de Desarrollo de Aplicaciones Web* para tener un marco común de desarrollo seguro en el diseño

[20] Ver *Anexo X Categorización de los sistemas*, en la página 166.

y codificación de aplicaciones web con el objetivo de que se garantice su disponibilidad asegurando las transacciones de manera eficiente y garantizando la identidad y privilegios en la utilización de estos servicios.

N9.1.2 Principios de ingeniería de sistemas seguros

Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.

Las políticas de AST están basadas principios de ingeniería seguros.

N9.1.3 Entorno de desarrollo seguro

AST establece y protege adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.

El desarrollo de aplicaciones se realiza en un sistema diferente y totalmente separado del de producción, sin que haya herramientas o datos de desarrollo en el entorno de producción. Tal y como se indica en la norma *N8.1.7 Separación de los recursos de desarrollo, prueba y operación*, página 110.

N9.1.4 Externalización del desarrollo de software

El desarrollo de software externalizado debe ser supervisado y controlado por la organización.

Cuando el desarrollo el software este externalizado se deberá seguir la normativa establecida en AST para el desarrollo seguro, que considera entre otros puntos:

i. Acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual
ii. Certificación de la calidad
iii. Reserva de la potestad auditora sobre la calidad y exactitud del trabajo realizado
iv. Requisitos contractuales sobre la calidad y seguridad funcional del código desarrollado
v. Pruebas previas a la instalación del software para la verificación de la inexistencia de troyanos u otro código malicioso

N9.1.5 Pruebas funcionales de seguridad de sistemas

Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo. Estas pruebas han de cumplir lo estipulado en la norma N9.1.7 *Protección de los datos de prueba*, descrita en la página 119.

Categoría[21] BÁSICA

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

i. Se comprobará que:

   a) Se cumplen los criterios de aceptación en materia de seguridad.

   b) No se deteriora la seguridad de otros componentes del servicio.

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

ii. Análisis de vulnerabilidades.

iii. Pruebas de penetración.

Categoría ALTA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

iv. Análisis de coherencia en la integración en los procesos.

v. Se considerará la oportunidad de realizar una auditoría de código fuente. deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.

Actualmente se utilizan herramientas de análisis de código bajo criterios OWASP. Ver *IT_ O12 Normativa de Desarrollo de Aplicaciones Web*

N9.1.6 Pruebas de aceptación de sistemas

Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

PRO_O4 Gestión Cambios

[21] Ver *Anexo X Categorización de los sistemas*, en la página 166.

PRO_O8 Gestión de versiones y despliegues

N9.1.7 Protección de los datos de prueba

Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.

i. Las pruebas se realizarán en un entorno aislado (pre-producción).

ii. Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

En concordancia con lo indicado en las normas *N8.1.7 Separación de los recursos de desarrollo, prueba y operación* y *N9.1.1 Política de desarrollo seguro*; páginas 110.y 116 respectivamente.

N9.2 Normas particulares de desarrollo seguro

N9.2.1 Control de Acceso y Autenticación

Se deben analizar las vulnerabilidades que pueden darse en las aplicaciones a la hora de identificar sus usuarios y los permisos que estos poseen recogiendo una serie de recomendaciones para el desarrollo de aplicaciones que ayuden a mitigar los riesgos de producirse situaciones como el escalado de privilegios o la suplantación de identidad.

Los objetivos a alcanzar son asegurar la identidad de los usuarios que acceden a las aplicaciones y controlar el acceso a recursos protegidos.

i. Autenticación

a. Asegurar que todas las peticiones pasan por un formulario de autenticación, y que éste no se puede saltar (con especial atención a las URLs de acceso directo, que deberemos asegurar que pasan por una autenticación)

b. Asegurar que todas las páginas cumplen el requisito de autenticación.

c. Asegurar que siempre que se pasen credenciales de autenticación (o cualquier información sensible), sólo se aceptará la información vía HTTP POST y nunca con GET.

d. Cualquier página para la que se descarte el mecanismo de autenticación debe ser revisada para asegurarse de que no tiene brechas de seguridad.

e. Asegurar que las credenciales de autenticación no se transfieren en claro.

f. Asegurar que no hay “puertas traseras” en el código en producción.

ii. Autorización

a. Asegurar que tenemos mecanismos de autorización (control de acceso y gestión de roles).

b. Asegurar que la aplicación tiene claramente definidos los tipos de usuario y sus privilegios.

c. Asegurar que asignamos los mínimos privilegios necesarios.

d. Asegurar que los mecanismos de autorización funcionan bien y no pueden saltarse.

e. Asegurarse de chequear la autorización en todas las peticiones.

f. Asegurar que no hay “puertas traseras” en el código en producción.

N9.2.2 Codificación y validación de entrada/salida

La debilidad de seguridad más común en aplicaciones web es la falta de validación apropiada de las entradas del cliente o del entorno. Teniendo en cuenta una serie de indicaciones y consejos a la hora de codificar nuestras aplicaciones podremos evitar problemas como la inyección de código SQL, de comandos, LDAP, XPath, XML o por XSS.

i. Asegurarse de tener mecanismos de validación de datos.

ii. Asegurarse de validar todas las entradas que pueden ser modificadas por un usuario malicioso: cabeceras HTTP, Input fields, hidden fields, drop down lists, etc.

iii. Asegurarse de comprobar las longitudes de todas las entradas.

iv. Asegurarse de validar todos los campos, cookies, http headers/bodies y form fields.

v. Asegurarse de formatear los datos convenientemente y que sólo contienen caracteres conocidos como buenos.

vi. Asegurarse de validar los datos en el servidor.

vii. Asegurar que no hay “puertas traseras” en el modelo de validación.

REGLA DE ORO: Cualquier entrada externa, sea cual sea, será examinada y validada

N9.2.3 Gestión de Errores y Excepciones

Uno de los focos que originan vulnerabilidades en nuestras aplicaciones es la falta de control sobre los errores que se producen en su ejecución y el tratamiento correcto de las excepciones. Veremos cómo disminuir los riesgos de ser atacado a partir de la generación de un error o excepción en la aplicación.

El objetivo es asegurar la gestión de errores y excepciones en las aplicaciones desarrolladas, para ello:

i. Asegurar que todas las llamadas a métodos/funciones que devuelven un valor tienen su control de errores y además se comprueba el valor devuelto.

ii. Asegurarse de gestionar adecuadamente las excepciones y los errores.

iii. Asegurar que al usuario no le devolvemos errores del sistema.

iv. Asegurar que la aplicación falla de un modo seguro.

v. Asegurarse de liberar los recursos en caso de error.

N9.2.4 Auditoría y Registro

La auditoría y el registro de los eventos que suceden al ejecutar nuestras aplicaciones nos permite monitorizarlas y detectar posibles intentos de ataques o intrusiones. Además, veremos cómo mejorar la gestión de los archivos de log para que sean más seguros.

Los objetivos son garantizar la monitorización de los eventos que se producen en la aplicación y asegurar la información de los ficheros de registro, para ello:

i. Asegurar que no se registra información sensible en el log en caso de error.

ii. Asegurarse de definir y controlar la longitud máxima de una entrada de log.

iii. Asegurar que no se registra datos sensibles en el log: cookies, método HTTP “GET”, credenciales de autenticación.

iv. Determinar si la aplicación auditará las operaciones lanzadas desde el cliente, sobre todo la manipulación de datos: Create, Update, Delete (operaciones CUD).

v. Asegurarse de registrar en el log las operaciones de autenticación (fallidas o exitosas).

vi. Asegurarse de registrar en el log los errores de la aplicación.

vii. Determinar si al hacer *debug* estamos registrando en el log datos sensibles.

N9.2.5 Cifrado

Una de las principales medidas para asegurar la integridad y la confidencialidad de la información que se transmite a través de la red es el cifrado o codificación de los mensajes, evitando que sea posible su entendimiento aún interceptando nuestra comunicación. Para ello, se resumen diversas situaciones en las que se debe cifrar la información y los algoritmos que se deben utilizar.

El objetivo es asegurar la confidencialidad e integridad de la información, para ello:

i. Asegurar que no se transmiten datos sensibles en claro, interna o externamente.

ii. Asegurar que la aplicación implementa buenos y conocidos métodos criptográficos.

N9.2.6 Gestión de Sesiones (Login/Logout)

El manejo de la sesión es uno de los aspectos críticos de la seguridad web. Veremos cómo se puede mejorar la seguridad en el control de acceso y la autenticación a través del manejo de las sesiones y de la información de los usuarios de nuestras aplicaciones.

Los objetivos son que los usuarios autenticados tengan una asociación con sus sesiones, robusta y criptográficamente segura, que se cumplan los controles de autorización y prevenir los típicos ataques web, tales como la reutilización, falsificación e intercepción de sesiones, para ello:

i. Comprobar cómo y cuándo se crean las sesiones de usuario, ya sean autenticadas o no.

ii. Comprobar el ID de sesión y verificar que tiene la complejidad necesaria para “ser fuerte”.

iii. Comprobar cómo se almacenan las sesiones: en base de datos, en memoria, etc.

iv. Comprobar cómo hace la aplicación el seguimiento de las sesiones (track sessions).

v. Determinar qué hace la aplicación en caso de encontrar un ID de sesión inválido.

vi. Comprobar la invalidación de sesiones.

vii. Determinar cómo se gestionan las sesiones multithreaded/multi-user.

viii. Determinar cómo funciona el *log-out*.

N9.2.7 Gestión de cookies

La gestión de las cookies toma mucha relevancia en tanto en cuanto ubicar información externa en los sistemas del cliente es una de los sistemas más utilizados para atacar la seguridad de éstos. Para incrementar la seguridad debemos:

i. Asegurarse de no comprometer información sensible.

ii. Asegurar que no se puedan hacer operaciones no autorizadas manipulando cookies.

iii. Asegurarse de usar cifrado.

iv. Determinar si todas las transiciones de estados en el código de la aplicación, verifican el uso seguro de cookies.

v. Asegurarse de validar los datos de la sesión.

vi. Asegurarse de que las cookies contienen la mínima información privada posible.

vii. Asegurarse de cifrar una cookie completa si contiene información sensible.

Definir todas las cookies que usa la aplicación, sus nombres y para qué son necesarias.

N9.3 Mantenimiento

N9.3.1 Procedimiento de control de cambios en sistemas

La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.

AST refleja estos procedimientos, dentro de los procesos *PRO_O4 Gestión Cambios* y *PRO_O8 Gestión de versiones y despliegues*.

N9.3.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.

PRO_O4 Gestión Cambios

Cuando se realicen cambios sobre los sistemas de la Organización, las aplicaciones críticas del negocio deberán ser revisadas y probadas para garantizar que no se ha comprometido la seguridad de estas aplicaciones. En particular, si los cambios afectan al software base de AST (sistemas operativos, directorio activo, etc.), éstos serán analizados, revisados y probados para asegurar que no impactan en la seguridad de la información. Los cambios a realizar deberán notificarse a tiempo para asegurar que pueden realizarse las revisiones y pruebas necesarias dentro de estas aplicaciones, previamente a su implementación.

N9.3.3 Restricciones a los cambios en los paquetes de software

Se ha de evitar, en la medida de lo posible, las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.

Los cambios en el software estándar solo deberían ser realizados cuando haya razones de negocio suficientes para ello, tales como un incremento en los riesgos para el sistema, mejoras sustanciales del aplicativo, motivos de escalabilidad, adaptación a normativas o estándares, etc.

Cuando estos paquetes de software necesiten ser modificados los siguientes elementos deben ser considerados:

i. Los riesgos de debilitar los controles incorporados,

ii. La obtención del consentimiento del vendedor

iii. La posibilidad de obtener los cambios requeridos a través de actualizaciones normales del programa del vendedor.

iv. El impacto causado si la organización toma la responsabilidad de mantener el programa como consecuencia de los cambios realizados.

PRO_O8 Gestión de versiones y despliegues

En estos casos, se deberá guardar una copia del software original y los cambios deben realizarse sobre una copia que este claramente identificada como tal. Es aconsejable emplear un sistema para el control de versiones del software. Todos los cambios deben ser totalmente probados y documentados. En caso de que sea necesario las modificaciones serán chequeadas por un equipo independiente de evaluación.

N10 Incidencias y continuidad

N10.1 Gestión de incidencias

N10.1.1 Responsabilidades y procedimientos

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

Categoría[22] MEDIA

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

i. Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

ii. Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

iii. Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

iv. Procedimientos para informar a las partes interesadas, internas y externas.

[22] Ver *Anexo X Categorización de los sistemas*, en la página 166.

v. Procedimientos para:

   a. Prevenir que se repita el incidente.

   b. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

   c. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.

PRO_O3 Gestión incidencias

La gestión de incidencias se realiza a través de CAU DE AST (4100), siguiendo el proceso *PRO_O3 Gestión incidencias*.

N10.1.2 Notificación de los eventos de seguridad de la información

Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible.

Categoría[23] MEDIA

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

i. Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

ii. Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

[23] Ver *Anexo X Categorización de los sistemas*, en la página 166.

iii. Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de AST o su imagen, deberá informar inmediatamente al CAU DE AST (4100) mediante el empleo de los cauces reglamentados.

N10.1.3 Notificación de puntos débiles de la seguridad

Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.

Se firma el código ético de sistemas en el que se especifica que el empleado reportará inmediatamente cualquier incidente de incumplimiento de los términos del propio acuerdo a un supervisor o al administrados apropiado. Mientras que, tal y como refleja el Anexo IV *PLA.O14 Clausula seguridad información AST Proveedor*,: en la página 145, los proveedores están obligados contractualmente a:

> «[…] El PROVEEDOR ha de notificar a AST de cualquier punto débil – vulnerabilidad, riesgo, etc. – que observen o que sospechen que exista, en los sistemas o servicios; indistintamente de que PROVEEDOR opere o despliegue dichos sistemas o no. […]»

N10.1.4 Evaluación y decisión sobre los eventos de seguridad de información

Los eventos de seguridad de la información deben ser evaluados y debería decidirse si se clasifican como incidentes de seguridad de la información.

Desde la herramienta SIEM se inician investigaciones de ofensas (eventos) y dependiendo del resultado de la investigación se registra como incidente en el sistema de gestión de *tickets*.

N10.1.5 Respuesta a incidentes de seguridad de la información

Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.

AST desarrolla Planes anuales para la mejora de en la respuesta ante ciber-incidencias para dar adecuada respuesta al reto que supone la especialización y el crecimiento de éstas.

N10.1.6 Aprendizaje de los incidentes

El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.

Habitualmente un incidente de seguridad utilizara uno o varios vectores derivados de vulnerabilidades del entorno. Se requiere analizar esas vulnerabilidades y tratarlas como riesgos, con el fin de eliminar, mitigar, trasladar – y en caso de que no haya más alternativa–, aceptar esos riesgos derivados.

El Responsable de Seguridad puede emitir Informes puntuales sobre ciberincidentes especialmente relevantes que haya sufrido la organización y que se deben considerar también en el Informe anual.

N10.1.7 Recopilación de evidencias

La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.

Las propias herramientas de *ticketing* y las incidencias creadas sirven de registro de actuaciones a efectos de auditoría. Por otro lado, la plataforma SIEM custodia los *logs* del resto de plataformas tecnológicas. El acceso administrativo a dicha herramienta, y por lo tanto, la capacidad de alterar o eliminar esos *logs*, se encuentra restringido y regulado por la norma *N8.3.3 Protección de la información de registro*, descrita en la página 91.

N10.2 Continuidad

N10.2.1 Planificación de la continuidad de la seguridad de la información

Para cada servicio, se debe determinar las necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

PRO_O12 Gestión de la continuidad

Todo el proceso se lleva a cabo a través de la gestión de la continuidad. En donde se prueba la capacidad de proporcionar servicio, desde medios alternativos, las diferentes plataformas tecnológicas y sistemas de AST.

N10.2.2 Análisis de impacto

Nivel MEDIO

Se realizará un análisis de impacto que permita determinar:

i. Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.

ii. Los elementos que son críticos para la prestación de cada servicio.

N10.2.3 Implementar la continuidad de la seguridad de la información

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

Nivel ALTO

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos:

i. Se identificarán funciones, responsabilidades y actividades a realizar.

ii. Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.

iii. Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.

iv. Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.

v. El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Se lleva a cabo a través del proceso *PRO_O12 Gestión de la continuidad*.

N10.2.4 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Se debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas

En los sistemas clasificados como nivel ALTO, se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad

Dentro del proceso *PRO_O12 Gestión de la continuidad*, se ejecuta anualmente un plan de *pruebas técnicas de recuperación, contingencia y continuidad*, donde realizan pruebas sobre el entorno de. Se han de guardar evidencias de todas las pruebas realizadas. Con los resultados de esas pruebas se debe evaluar los resultados de las mismas.

N10.2.5 Disponibilidad de los recursos de tratamiento de la información

Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

Tal y como se especifica en las normas: *N2.3.5 Medios alternativos* – página 39–, *N3.2.6 Medios alternativos* – página 47 –, *N6.4.2 Medios alternativos* – página 101 – y *N7.1.7 Medios alternativos* – página 106–.

N11 Cumplimiento

N11.1 Elementos fundamentales

N11.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de AST para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para sistema de información de la organización.

El registro de legislación que aplica a AST queda recogido en el documento *REG_E1_Listado Legislación*. En lo que respecta a los sistemas de información, las leyes recogidas en el apartado *1.7 Cumplimiento de normativas y estándares* – página 20 – son tratadas en el presente cuerpo normativo de seguridad.

La Dirección de Recursos controla los cumplimientos legales y contractuales.

N11.1.2 Derechos de propiedad intelectual (DPI)

Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

A la hora de regular la propiedad industrial e intelectual se debe incluir una cláusula en los contratos laborales y convenios de becas o prácticas formativas; en los contratos ya suscritos se debe incluir un anexo. Sirva como ejemplo el *Clausula propiedad intelectual en relaciones laborales*.

En los contratos suscritos con proveedores, que tengan por objeto el desarrollo y la puesta a disposición de productos protegidos por derechos de propiedad industrial y/o intelectual debe llevar aparejados la cesión de los correspondientes derechos de explotación a las sociedades por el tiempo y en el ámbito necesario para su explotación prevista. Tal y como reflejan el apartado *VII* – Ver página 145 del *Anexo IV PLA.O14 Clausula seguridad información AST Proveedor*.

En los entornos de acceso público, como páginas web corporativas, también han de contar con el pertinente aviso legal.

Para el control del software AST dispone de un inventario de las licencias disponibles. el inventario está incluido en la CMDB de AST y se revisa periódicamente para su actualización.

N11.1.3 Protección de los registros de la organización

Los registros deberían estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

El personal de AST no compartirá, grabará, copiará, borrará y alterará de ninguna manera la información en los sistemas excepto que sea necesario para realizar las funciones asignadas. Estas limitaciones se extienden de igual modo los proveedores y contratistas, tal y como se indica en el *Anexo IV PLA.O14 Clausula seguridad información AST Proveedor*, página 142.

N11.1.4 Protección y privacidad de la información de carácter personal

Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

Dicha legislación está identificada siguiendo la norma *N11.1.1 Identificación de la legislación aplicable y de los requisitos contractuales*, página 130.

N11.1.5 Regulación de los controles criptográficos

Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

Tal y como se refleja en las normas: *N4.2.1 Cifrado y política de uso de los controles criptográficos*, *N4.2.2 Gestión de claves*, *N4.2.3 Firma electrónica*, *N4.2.4 Sellos de tiempo* –páginas de la 51 a la 54–, *N5.1.2 Criptografía* –página 78–, *N5.1.7 Soportes físicos en tránsito*, *N5.1.8 Seguridad de los equipos fuera de las instalaciones* –página 81–, *N5.2.4 Teletrabajo* –página 87– y *N7.1.4 Protección de la confidencialidad* –página 104–.

N11.1.6 Revisión independiente de la seguridad de la información

El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debería someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

Periódicamente, el modelo de gestión de seguridad de la información incluidos sus objetivos, políticas, normas, procedimientos y la implementación de todos ellos debe ser revisado por auditores externos independientes, quiénes emitirán una valoración del estado de la gestión de los sistemas de información y las recomendaciones pertinentes para AST. Para ello se aprovecharán las auditorias asociadas al ENS, ISO 2001 y otras similares que pudieran surgir. El Responsable de Seguridad es el encargado de recoger las recomendaciones realizadas por los auditores que estén referidas a materia de seguridad de la información y proponer los cambios y actividades a realizar para su posterior aprobación por el Comité de Seguridad.

N11.1.7 Cumplimiento de las políticas y normas de seguridad

Los directivos deberían asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

La revisión del Cuerpo Normativo de Seguridad se hace con carácter periódico (mínimo anual) con el objetivo de mantenerlo actualizado. En esa revisión se deben dar de baja aquellas normas y documentos que pierdan vigencia por el cambio tecnológico o por los procesos internos de la entidad y se darán de alta aquellas nuevas normativas que regulen tecnologías emergentes.

N11.1.8 Comprobación del cumplimiento técnico

Debería comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

AST realiza de forma periódica una auditoría interna de su modelo de gestión de seguridad de la información para la verificación de la idoneidad, adecuación y efectividad de los controles implementados. Los resultados de todas estas revisiones deben ser entregados al Comité de Seguridad y a la Oficina de Seguridad. Es por cuenta del Responsable de Seguridad, tras la aprobación del Comité de Seguridad, el coordinar la implementación de dichas recomendaciones y proponiendo en su caso al Comité de Seguridad los cambios que sea necesario realizar en la políticas, normativa u procedimientos para su aprobación.

Fin del apartado

Anexos

Anexo I. Relación entre las normas y las medidas de protección del Esquema Nacional de Seguridad

Medida	ENS	Código	Norma
org.1	Política de seguridad	N1.1.1	Política de seguridad
org.2	Normativa de seguridad	N1.1.2	Cuerpo Normativo de seguridad
org.3	Procedimientos operativos de seguridad	N1.1.4	Procedimientos e instrucciones técnicas
org.4	Proceso de autorización	N1.2.1	Proceso de autorización
op.pl.1	Análisis de riesgos	N3.1.1	Análisis de riesgos
op.pl.2	Arquitectura de seguridad	N3.1.3	Arquitectura de seguridad
op.pl.3	Adquisición de nuevos componentes	N3.1.4	Adquisición de nuevos componentes
op.pl.4	Dimensionamiento / Gestión de capacidades	N3.1.5	Dimensionamiento / Gestión de capacidades
op.pl.5	Componentes certificados	N3.2.3	Componentes certificados
op.acc.1	Identificación	N4.4.2	Identificación
op.acc.2	Requisitos de acceso	N4.4.3	Requisitos de acceso
op.acc.3	Segregación de funciones y tareas	N4.4.4	Segregación de funciones y tareas
op.acc.4	Proceso de gestión de derechos de acceso	N4.4.7	Gestión de privilegios de acceso
op.acc.5	Mecanismo de autenticación	N4.4.13	Mecanismo de autenticación
op.acc.6	Acceso local (local logon)	N4.4.15	Procedimiento de acceso
op.acc.7	Acceso remoto (remote login)	N4.4.15	Procedimiento de acceso
op.exp.1	Inventario de activos	N2.1.1	Inventario de activos
op.exp.2	Configuración de seguridad	N8.1.2	Configuración de seguridad
op.exp.3	Gestión de la configuración	N8.1.3	Gestión de la configuración
op.exp.4	Mantenimiento	N8.1.4	Mantenimiento
op.exp.5	Gestión de cambios	N8.1.5	Gestión de cambios
op.exp.6	Protección frente a código dañino	N8.2.1	Controles contra el código malicioso
op.exp.7	Gestión de incidencias	N10.1.1	Responsabilidades y procedimientos
op.exp.8	Registro de la actividad de los usuarios	N8.3.2	Registros de administración y operación
op.exp.9	Registro de la gestión de incidencias	N10.1.2	Notificación de los eventos de seguridad de la información
op.exp.10	Protección de los registros de actividad	N8.3.3	Protección de la información de registro
op.exp.11	Protección de claves criptográficas	N4.2.2	Gestión de claves
op.ext.1	Contratación y acuerdos de nivel de servicio	N2.3.1	Contratación y acuerdos de nivel de servicio
op.ext.2	Gestión diaria	N2.3.3	Gestión diaria
op.ext.9	Medios alternativos	N2.3.5	Medios alternativos
op.cont.1	Análisis de impacto	N10.2.2	Análisis de impacto
op.cont.2	Plan de continuidad	N10.2.3	Implementar la continuidad de la seguridad de la información
op.cont.3	Pruebas periódicas	N10.2.4	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
op.mon.1	Detección de intrusión	N8.3.5	Detección de intrusión

Medida	ENS	Código	Norma
op.mon.2	Sistema de métricas	N8.3.6	Sistema de métricas
mp.if.1	Áreas separadas y con control de acceso	N6.1.1	Áreas separadas y con control de acceso
mp.if.2	Identificación de las personas	N6.1.2	Identificación de las personas
mp.if.3	Acondicionamiento de los locales	N6.3.1	Acondicionamiento de los locales
mp.if.4	Energía eléctrica	N6.3.3	Energía eléctrica
mp.if.5	Protección frente a incendios	N6.3.5	Protección frente a incendios
mp.if.6	Protección frente a inundaciones	N6.3.6	Protección frente a inundaciones
mp.if.7	Registro de entrada y salida de equipamiento	N6.2.3	Registro de entrada y salida de equipamiento
mp.if.9	Instalaciones alternativas	N6.4.1	Instalaciones alternativas
mp.per.1	Caracterización del puesto de trabajo	N2.2.2	Caracterización del puesto de trabajo
mp.per.2	Deberes y obligaciones	N2.2.3	Deberes y obligaciones
mp.per.3	Concienciación	N2.2.5	Concienciación, educación y capacitación en seguridad de la información
mp.per.4	Formación	N2.2.5	Concienciación, educación y capacitación en seguridad de la información
mp.per.9	Personal alternativo	N2.2.6	Personal alternativo
mp.eq.1	Puesto de trabajo despejado	N5.2.2	Puesto de trabajo despejado
mp.eq.2	Bloqueo de puesto de trabajo	N5.2.1	Equipo de usuario desatendido
mp.eq.3	Protección de equipos portátiles	N5.1.8	Seguridad de los equipos fuera de las instalaciones
mp.eq.9	Medios alternativos	N6.4.2	Medios alternativos
mp.com.1	Perímetro seguro	N7.1.3	Perímetro seguro
mp.com.2	Protección de la confidencialidad	N7.1.4	Protección de la confidencialidad
mp.com.3	Protección de la autenticidad y de la integridad	N7.1.5	Protección de la autenticidad y de la integridad
mp.com.4	Segregación de redes	N7.1.6	Segregación de redes
mp.com.9	Medios alternativos	N7.1.7	Medios alternativos
mp.si.1	Etiquetado	N5.1.3	Etiquetado
mp.si.2	Criptografía	N5.1.2	Criptografía
mp.si.3	Custodia	N5.1.1	Custodia
mp.si.4	Transporte	N5.1.7	Soportes físicos en tránsito
mp.si.5	Borrado y destrucción	N5.1.5	Borrado y destrucción
mp.sw.1	Desarrollo	N9.1.1	Política de desarrollo seguro
mp.sw.2	Aceptación y puesta en servicio	N9.1.5	Pruebas funcionales de seguridad de sistemas
mp.info.1	Datos de carácter personal	N11.1.4	Protección y privacidad de la información de carácter personal
mp.info.2	Calificación de la información	N4.1.1	Clasificación de la información
mp.info.3	Cifrado	N4.2.1	Cifrado y política de uso de los controles criptográficos
mp.info.4	Firma electrónica	N4.2.3	Firma electrónica
mp.info.5	Sellos de tiempo	N4.2.4	Sellos de tiempo
mp.info.6	Limpieza de documentos	N4.2.5	Limpieza de documentos
mp.info.9	Copias de seguridad (backup)	N4.2.6	Copias de seguridad (backup)
mp.s.1	Protección del correo electrónico	N4.3.3	Mensajería electrónica
mp.s.2	Protección de servicios y aplicaciones web	N3.2.4	Protección de servicios y aplicaciones web

Medida	ENS	Código	Norma
mp.s.8	Protección frente a la denegación de servicio	N3.2.5	Protección frente a la denegación de servicio
mp.s.9	Medios alternativos	N3.2.6	Medios alternativos

Tabla 0-1. Anexo I. Relación entre las normas y las medidas de protección del Esquema Nacional de Seguridad

Anexo II. Relación entre las normas y los controles de la norma UNE-EN ISO/IEC 27001:2017

Control	ISO 27001	Código	Norma
5.1.1	Políticas para la seguridad de la información	N1.1.1	Política de seguridad
5.1.2	Revisión de las políticas para la seguridad de la información	N1.1.3	Revisión del cuerpo normativo de seguridad
6.1.1	Roles y responsabilidades en seguridad de la información	N1.2.2	Roles y responsabilidades en seguridad de la información
6.1.2	Segregación de tareas	N1.2.3	Segregación de tareas
6.1.3	Contacto con las autoridades	N1.2.4	Contacto con las autoridades
6.1.4	Contacto con grupos de interés especial	N1.2.5	Contacto con grupos de interés especial
6.1.5	Seguridad de la información en la gestión de proyectos	N1.2.6	Seguridad de la información en la gestión de proyectos
6.2.1	Política de dispositivos móviles	N5.2.3	Política de dispositivos móviles
6.2.2	Teletrabajo	N5.2.4	Teletrabajo
7.1.1	Investigación de antecedentes	N2.2.1	Investigación de antecedentes
7.1.2	Términos y condiciones del empleo	N2.2.2	Caracterización del puesto de trabajo
7.2.1	Responsabilidades de gestión	N2.2.4	Responsabilidades de gestión
7.2.2	Concienciación, educación y capacitación en seguridad de la información	N2.2.5	Concienciación, educación y capacitación en seguridad de la información
7.2.3	Proceso disciplinario	N2.2.7	Proceso disciplinario
7.3.1	Responsabilidades ante la finalización o cambio	N2.2.8	Responsabilidades ante la finalización o cambio
8.1.1	Inventario de activos	N2.1.1	Inventario de activos
8.1.2	Propiedad de los activos	N2.1.2	Responsabilidad de los activos
8.1.3	Uso aceptable de los activos	N2.1.3	Uso aceptable de los activos
8.1.4	Devolución de activos	N2.1.4	Devolución de activos
8.2.1	Clasificación de la información	N4.1.1	Clasificación de la información
8.2.2	Etiquetado de la información	N4.1.2	Etiquetado de la información
8.2.3	Manipulado de la información	N4.1.3	Manipulado de la información
8.3.1	Gestión de soportes extraíbles	N5.1.4	Gestión de soportes extraíbles
8.3.2	Eliminación de soportes	N5.1.5	Borrado y destrucción

Control	ISO 27001	Código	Norma
8.3.3	Soportes físicos en tránsito	N5.1.7	Soportes físicos en tránsito
9.1.1	Política de control de acceso	N4.4.1	Política de control de acceso
9.1.2	Acceso a las redes y a los servicios de red	N4.4.3	Requisitos de acceso
9.2.1	Registro y baja de usuario	N4.4.5	Registro y baja de usuario
9.2.2	Provisión de acceso de usuario	N4.4.6	Provisión de acceso de usuario
9.2.3	Gestión de privilegios de acceso	N4.4.7	Gestión de privilegios de acceso
9.2.4	Gestión de la información secreta de autenticación de los usuarios	N4.4.8	Gestión de la información secreta de autenticación de los usuarios
9.2.5	Revisión de los derechos de acceso de usuario	N4.4.9	Revisión de los derechos de acceso de usuario
9.2.6	Retirada o reasignación de los derechos de acceso	N4.4.10	Retirada o reasignación de los derechos de acceso
9.3.1	Uso de la información secreta de autenticación	N4.4.11	Uso de la información secreta de autenticación
9.4.1	Restricción del acceso a la información	N4.4.12	Restricción del acceso a la información
9.4.2	Procedimientos seguros de inicio de sesión	N4.4.15	Procedimiento de acceso
9.4.3	Sistema de gestión de contraseñas	N4.4.14	Sistema de gestión de contraseñas
9.4.4	Uso de utilidades con privilegios del sistema	N4.4.16	Uso de utilidades con privilegios del sistema
9.4.5	Control de acceso al código fuente de los programas	N4.4.17	Control de acceso al código fuente de los programas
10.1.1	Política de uso de los controles criptográficos	N4.2.1	Cifrado y política de uso de los controles criptográficos
10.1.2	Gestión de claves	N4.2.2	Gestión de claves
11.1.1	Perímetro de seguridad física	N6.1.1	Áreas separadas y con control de acceso
11.1.2	Controles físicos de entrada	N6.1.2	Identificación de las personas
11.1.3	Seguridad de oficinas, despachos y recursos	N6.1.3	Clasificación de ubicaciones y niveles de seguridad de acceso
11.1.4	Protección contra las amenazas externas y ambientales	N6.3.1	Acondicionamiento de los locales
11.1.5	El trabajo en áreas seguras	N6.2.1	El trabajo en áreas seguras
11.1.6	Áreas de carga y descarga	N6.2.2	Áreas de carga y descarga
11.2.1	Emplazamiento y protección de equipos	N6.3.2	Emplazamiento y protección de equipos
11.2.2	Instalaciones de suministro	N6.3.3	Energía eléctrica
11.2.3	Seguridad del cableado	N6.3.4	Seguridad del cableado
11.2.4	Mantenimiento de los equipos	N6.2.4	Mantenimiento de los equipos

Control	ISO 27001	Código	Norma
11.2.5	Retirada de materiales propiedad de la empresa	N2.1.5	Retirada de materiales propiedad de la empresa
11.2.6	Seguridad de los equipos fuera de las instalaciones	N5.1.8	Seguridad de los equipos fuera de las instalaciones
11.2.7	Reutilización o eliminación segura de equipos	N5.1.6	Reutilización
11.2.8	Equipo de usuario desatendido	N5.2.1	Equipo de usuario desatendido
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	N5.2.2	Puesto de trabajo despejado
12.1.1	Documentación de procedimientos de las operaciones	N8.1.1	Documentación de procedimientos de las operaciones
12.1.2	Gestión de cambios	N8.1.5	Gestión de cambios
12.1.3	Gestión de capacidades	N8.1.6	Gestión de capacidades
12.1.4	Separación de los recursos de desarrollo, prueba y operación	N8.1.7	Separación de los recursos de desarrollo, prueba y operación
12.2.1	Controles contra el código malicioso	N8.2.1	Controles contra el código malicioso
12.3.1	Copias de seguridad de lainformación	N4.2.6	Copias de seguridad (backup)
12.4.1	Registro de eventos	N8.3.1	Registro de eventos
12.4.2	Protección de la información de registro	N8.3.3	Protección de la información de registro
12.4.3	Registros de administración y operación	N8.3.2	Registros de administración y operación
12.4.4	Sincronización del reloj	N8.3.4	Sincronización del reloj
12.5.1	Instalación del software en explotación	N8.2.2	Instalación del software en explotación
12.6.1	Gestión de las vulnerabilidades técnicas	N8.2.3	Gestión de las vulnerabilidades técnicas
12.6.2	Restricción en la instalación de software	N8.2.4	Restricción en la instalación de software
12.7.1	Controles de auditoría de sistemas de información	N8.3.7	Controles de auditoría de sistemas de información
13.1.1	Controles de red	N7.1.1	Controles de red
13.1.2	Seguridad de los servicios de red	N7.1.2	Seguridad de los servicios de red
13.1.3	Segregación en redes	N7.1.6	Segregación de redes
13.2.1	Políticas y procedimientos de intercambio de información	N4.3.1	Políticas y procedimientos de intercambio de información
13.2.2	Acuerdos de intercambio de información	N4.3.2	Acuerdos de intercambio de información
13.2.3	Mensajería electrónica	N4.3.3	Mensajería electrónica
13.2.4	Acuerdos de confidencialidad o no revelación	N4.3.4	Acuerdos de confidencialidad o no revelación

Control	ISO 27001	Código	Norma
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	N3.1.2	Análisis de requisitos y especificaciones de seguridad de la información
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	N3.2.1	Asegurar los servicios de aplicaciones en redes públicas
14.1.3	Protección de las transacciones de servicios de aplicaciones	N3.2.2	Protección de las transacciones de servicios de aplicaciones
14.2.1	Política de desarrollo seguro	N9.1.1	Política de desarrollo seguro
14.2.2	Procedimiento de control de cambios en sistemas	N9.3.1	Procedimiento de control de cambios en sistemas
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	N9.3.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
14.2.4	Restricciones a los cambios en los paquetes de software	N9.3.3	Restricciones a los cambios en los paquetes de software
14.2.5	Principios de ingeniería de sistemas seguros	N9.1.2	Principios de ingeniería de sistemas seguros
14.2.6	Entorno de desarrollo seguro	N9.1.3	Entorno de desarrollo seguro
14.2.7	Externalización del desarrollo de software	N9.1.4	Externalización del desarrollo de software
14.2.8	Pruebas funcionales de seguridad de sistemas	N9.1.5	Pruebas funcionales de seguridad de sistemas
14.2.9	Pruebas de aceptación de sistemas	N9.1.6	Pruebas de aceptación de sistemas
14.3.1	Protección de los datos de prueba	N9.1.7	Protección de los datos de prueba
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	N2.3.6	Política de seguridad de la información en las relaciones con los proveedores
15.1.2	Requisitos de seguridad en contratos con terceros	N2.3.7	Requisitos de seguridad en contratos con terceros
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	N2.3.8	Cadena de suministro de tecnología de la información y de las comunicaciones
15.2.1	Control y revisión de la provisión de servicios del proveedor	N2.3.2	Control y revisión de la provisión de servicios del proveedor
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	N2.3.4	Gestión de cambios en la provisión del servicio del proveedor
16.1.1	Responsabilidades y procedimientos	N10.1.1	Responsabilidades y procedimientos
16.1.2	Notificación de los eventos de seguridad de la información	N10.1.2	Notificación de los eventos de seguridad de la información

Control	ISO 27001	Código	Norma
16.1.3	Notificación de puntos débiles de la seguridad	N10.1.3	Notificación de puntos débiles de la seguridad
16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	N10.1.4	Evaluación y decisión sobre los eventos de seguridad de información
16.1.5	Respuesta a incidentes de seguridad de la información	N10.1.5	Respuesta a incidentes de seguridad de la información
16.1.6	Aprendizaje de los incidentes de seguridad de la información	N10.1.6	Aprendizaje de los incidentes de seguridad de la información
16.1.7	Recopilación de evidencias	N10.1.7	Recopilación de evidencias
17.1.1	Planificación de la continuidad de la seguridad de la información	N10.2.1	Planificación de la continuidad de la seguridad de la información
17.1.2	Implementar la continuidad de la seguridad de la información	N10.2.3	Implementar la continuidad de la seguridad de la información
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	N10.2.4	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
17.2.1	Disponibilidad de los recursos de tratamiento de la información	N10.2.5	Disponibilidad de los recursos de tratamiento de la información
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	N11.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
18.1.2	Derechos de propiedad intelectual (DPI)	N11.1.2	Derechos de propiedad intelectual (DPI)
18.1.3	Protección de los registros de la organización	N11.1.3	Protección de los registros de la organización
18.1.4	Protección y privacidad de la información de carácter personal	N11.1.4	Protección y privacidad de la información de carácter personal
18.1.5	Regulación de los controles criptográficos	N11.1.5	Regulación de los controles criptográficos
18.2.1	Revisión independiente de la seguridad de la información	N11.1.6	Revisión independiente de la seguridad de la información
18.2.2	Cumplimiento de las políticas y normas de seguridad	N11.1.7	Cumplimiento de las políticas y normas de seguridad
18.2.3	Comprobación del cumplimiento técnico	N11.1.8	Comprobación del cumplimiento técnico

Tabla 0-2. Anexo II.Relación entre las normas y los controles de la norma UNE-EN ISO/IEC 27001:2017

Anexo III. Listado de CMDB de proceso «O6 Gestión de la configuración»

Herramienta		Descripción
Plataforma Tecnológica	**Nombre**	
PT Documentación	ALFRESCO	Sistema de administración de contenidos, utilizado por AST para la gestión de su información documentada, según alcance del SIG.
PT. *Ticketing*	OTRS (*Open-source Ticket Request System*)	Sistema de solicitud de tiques de código abierto, utilizado para asignar identificadores únicos "*tickets*" a solicitudes de servicio o de información, a fin de facilitar el seguimiento y manejo de dichas solicitudes, así como cualquier otra interacción con sus clientes o usuarios.
PT.CMDB_PTD	GLPI-OCS	Contiene la CMDB de los Puestos de Trabajo Digital, tanto de hardware (PC fijos y portátiles), como del software instalado en los mismos
PT. CMDB Sistemas	Microsoft Excel, CMDB Sistemas	Contiene tanto la relación de los hosts físicos, como las máquinas virtuales que gestiona AST. Incluyen la información de su ubicación (incluido otros CPD del Gobierno de Aragón, como los de los hospitales). Si están monitorizados, sus características, etc.
PT. CMDB Electrónica de red	Microsoft Excel, Electrónica de red	Refleja todos los elementos de la electrónica de red que se gestionan desde AST. Incluye los SN, MAC, IP, ubicaciones y que interfaces están monitorizados
PT. CMDB Comunicaciones	Microsoft Visio, esquemas de red	Esquemas realizados con Microsoft Visio con la mayor parte de la infraestructura de red del Gobierno de Aragón. Incluye información de la topología física, y lógica. Tipo de cableado, interfaces de conexión, elementos monitorizados, identificadores de la electrónica de red, etc.
PT. CMDB. Aplicaciones	OTRS	Contiene todas las aplicaciones desarrolladas y gestionadas por AST.
PT. Monitorizacion	Nagios	Sistema de monitorización, basado en Nagios unificado que incluye: ■ Servidores físicos y virtuales ■ Estado de la electrónica de red y conectividad ■ Servicios (disponibilidad de páginas web y tiempos de respuesta)
PT. VoIP	CUCM	AST gestiona de forma interna más de 22.000 teléfonos, basados en tecnología de Voz IP, sobre Cisco Unified Communications Manager (CallManager). Para ello cuenta con una serie de servidores que dotan de disponibilidad y servicio en los principales edificios. La herramienta es tanto para la orquestación del servicio como herramienta CMDB. Incluimos en este epígrafe todos los servidores y tecnologías necesarios, incluyendo los sistemas de locuciones.
PT. IPAM	Infoblox	Administración de direcciones IP

Tabla 0-3. Listado de CMDB de proceso «O6 Gestión de la configuración»

La tabla de CMDB puede estar desactualizada, revise el proceso O6.

Anexo IV. PLA.O14 Clausula seguridad información AST Proveedor

El contenido de esta cláusula puede haberse modificado. Por favor, revise el modelo oficial, su inclusión aquí es a titulo meramente informativo.

En Zaragoza, a miércoles, 3 de julio de 2019

Reunidos

De una parte, _____, en nombre y representación de ARAGONESA DE SERVICIOS TELEMÁTICOS, con C.I.F. Q5000455E y domicilio a efectos del presente acuerdo en Parque Empresarial EXPO Zaragoza, Avda. Ranillas, nº 3 A, 3ª planta, oficina J, en adelante AST.

Del otro, _____ con D.N.I. número _____, en representación de AST _____, con CIF _____ y domicilio fiscal en _____, en adelante PROVEEDOR.

Exponen

Ambas partes acuerdan mutuamente, la capacidad legal necesaria para la suscripción del presente acuerdo y el cumplimiento y a dar cumplimiento a las siguientes Estipulaciones:

I. Que AST es una entidad de derecho público cuya misión es proporcionar servicios y soluciones de ALTO valor en el ámbito de las tecnologías y servicios de la información y telecomunicaciones a la Administración de la Comunidad Autónoma de Aragón y los organismos públicos de ella dependientes. Aragonesa de Servicios Telemáticos es también el operador de telecomunicaciones público para la Administración de la Comunidad Autónoma de Aragón, y como tal está registrado y habilitado para la prestación de servicios a entidades privadas por la CNMC. Por tanto, es responsable de la información generada y gestionada en su actividad.

II. Que PROVEEDOR es una organización de servicios y/o proyectos cuyo ámbito de relación con AST se inscribe dentro la realización del contrato denominado: _____ con número de expediente AST_____

Confidencialidad y de No Divulgación de Información

III. Que PROVEEDOR durante la prestación de sus servicios a AST puede recibir información confidencial de AST o disponer de acceso o de potencial acceso la misma. En este sentido se considera por información confidencial, toda la información relativa a: procesos de negocio, planes de marketing, planes estratégicos, clientes, proveedores know-how, métodos, análisis funcionales, código fuente, estudios de mercado, estadísticas, datos financieros, análisis de viabilidad, especificaciones técnicas, formulas, diseños, estudios, aquella afectada por LOPD, la GDPR y toda aquella información que AST no haya autorizado de modo explícito a PROVEEDOR su libre uso o difusión.

IV. 1. PROVEEDOR. únicamente utilizará la información facilitada por AST para el fin mencionado en la Estipulación I, comprometiéndose a mantener la más estricta confidencialidad respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a sus empleados, asociados, subcontratas y a cualquier persona que, por su relación con la PROVEEDOR, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del PROVEEDOR para con AST.

2. Las personas o entidades citadas en el párrafo anterior y que tengan acceso a información confidencial de AST en el marco de la prestación del servicio, no disponen de permiso para reproducir, modificar, publicar o difundir o comunicar a terceros dicha información sin previa autorización explícita de AST.

3. De igual forma, el PROVEEDOR. se compromete a aplicar, como mínimo, respecto de la información objeto de este acuerdo las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia organización. Procurando las medidas que eviten su pérdida, robo, difusión o sustracción. Así mismo, el PROVEEDOR asume la responsabilidad de aplicar todas las medidas exigibles por la legislación vigente.

V. Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

a) Cuando la información se encontrara en el dominio público en el momento de su suministro a PROVEEDOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.

b) Cuando la información ya estuviera en el conocimiento de PROVEEDOR. con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

c) Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso PROVEEDOR notificará a AST tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

d) En caso de que PROVEEDOR. pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con AST.

Calidad y Seguridad de la Información

VI. En este sentido el PROVEEDOR se compromete a:

a) Dar a conocer a sus empleados o personas a cargo la Política de Calidad y Seguridad de la Información de AST, para su correcto cumplimiento, así como los requisitos de seguridad exigidos. Así mismo el PROVEEDOR declara conocer la Política de Calidad y Seguridad de la Información de AST disponible en su página web.

b) Evaluar los posibles riesgos en calidad y seguridad de la información en la prestación del servicio. Es responsabilidad del PROVEEDOR establecer las medidas necesarias para la segura y correcta prestación del servicio. EL PROVEEDOR responderá frente a AST de los daños y perjuicios que le haya podido ocasionar como consecuencia del incumplimiento de este clausulado.

c) Destinar un uso profesional al uso de los programas y archivos informáticos puestos a disposición del PROVEEDOR para el servicio.

d) Tener adoptadas, en todos los equipos utilizados para la prestación del servicio y aquellos equipos a su cargo que por estar en la misma red puedan suponer un vector de ataque, las medidas de seguridad técnicas, tales como: cifrado de almacenamiento, sistemas de control de acceso, antivirus, etcétera. El PROVEEDOR se hace responsable de cualquier brecha de seguridad/ataque ocasionada desde su equipamiento a equipos del Gobierno de Aragón o de terceros.

e) Cumplir con las normas de uso aceptable de los activos establecidas por la AST en su gestión de la seguridad de la información.

f) Ubicará en emplazamientos securizados y protegidos con el fin de reducir los riesgos derivados de las amenazas externas.

g) Proteger la infraestructura tecnológica, que así lo necesite, contra fallos de provisión en el suministro eléctrico.

h) Devolver de forma íntegra todos los activos propiedad de AST y dispuesto al mismo para el desarrollo de su servicio. AST no será responsable de los retrasos, acciones contrarias a derecho, daños y perjuicios, averías e incidencias imputables al PROVEEDOR que puedan afectar al mantenimiento de la red o redes para la prestación del servicio.

i) Aplicar dentro de lo posible principios de ingeniería de sistemas seguros.

j) Garantizar el manejo de la información de acuerdo al criterio de clasificación establecido.

k) El PROVEEDOR ha de notificar a AST de cualquier punto débil – vulnerabilidad, riesgo, etc. – que observen o que sospechen que exista, en los sistemas o servicios; indistintamente de que PROVEEDOR opere o despliegue dichos sistemas o no.

Propiedad Intelectual e Industrial

VII. Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen a AST y el hecho de revelarla a LA PROVEEDOR para el fin mencionado en la Estipulación Primera no cambiará tal situación.

VIII. El PROVEEDOR garantiza y queda obligado a acreditar documentalmente ante AST, si fuere requerido, que dispone de las patentes, licencias, permisos, registros, autorizaciones y demás derechos de propiedad intelectual e industrial de los servicios a prestar. En cumplimiento de lo anterior el PROVEEDOR exime a AST de toda responsabilidad por las infracciones de la propiedad intelectual y/o industrial y por las infracciones de licencias y/o autorizaciones en que aquél pudiera incurrir, y se obliga a realizar cuanto sea necesario para dejar a la otra parte indemne, al margen y a salvo de las reclamaciones o demandas que por dichas infracciones pudieran exigirse contra él, directa o indirectamente, de tales reclamaciones o demandas.

Protección de datos

IX. De acuerdo al *Reglamento (UE) 2016/679 General de Protección de Datos 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* (RGPD) y a lo dispuesto en *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPD-GDD), ambas partes se informan respectivamente que los datos de carácter personal intercambiados en el marco de la relación contractual serán incluidos en los ficheros de los que cada una de ellas es titular, siendo la finalidad de estos tratamientos el soporte en el desarrollo de las tareas en el ámbito de la prestación del servicio. Dichos datos no serán cedidos a terceros. Adicionalmente, ambas partes se obligan a garantizar, el cumplimiento de ambas leyes. Asimismo, para ejercer los derechos de acceso, rectificación, cancelación y oposición cualquiera de las partes deberá dirigirse mediante comunicación formal a las direcciones recogidas al inicio de este acuerdo.

Duración y devolución

X. Toda la información en posesión del PROVEEDOR como resultado de la relación con AST e independientemente de su naturaleza, deberá de ser devuelta o destruida tras la finalización de la relación contractual o laboral, salvo que deban de ser conservados por requerimientos legales o normativos vigentes.

XI. Este acuerdo tendrá validez a partir del momento en que quede firmado por ambas partes, y se extenderá de forma indefinida, a pesar de que haya finalizado la relación contractual.

Estipulaciones penal y sanciones

XII. En caso de que la información resulte revelada o divulgada o utilizada por PROVEEDOR cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar a AST los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último.

XIII. El PROVEEDOR acepta que por parte de AST, o en nombre de ella otra organización debidamente acreditada, se le requieran, o auditen, las medidas de seguridad aplicadas según los párrafos IV y V. Si derivada de esta

acción AST indica como insuficientes las medidas adoptadas por el PROVEEDOR, este tendrá un plazo no superior a 3 MESES para subsanarlas. En caso contrario AST puede aplicar una penalización del 30% de la facturación. Si 5 meses después sin haberse adoptado medidas que mejoren la situación AST podrá rescindir el contrato con el PROVEEDOR sin ningún tipo de reclamación o indemnización por parte de este.

XIV. En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Juzgados y Tribunales de Zaragoza, con renuncia a su fuero propio, aplicándose la legislación española vigente.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por triplicado ejemplar y a un solo efecto en el lugar y fecha en el contrato indicados.

En nombre y representación de:

AST:	**PROVEEDOR**:

Anexo V. PLA.O14 Cláusula de seguridad de la información, para la utilización por parte de terceros de la infraestructura o servicios de AST

El contenido de esta cláusula puede haberse modificado. Por favor, revise el modelo oficial, su inclusión aquí es a titulo meramente informativo.

En Zaragoza, a miércoles, 3 de julio de 2019

Reunidos

De una parte, _____, en nombre y representación de ARAGONESA DE SERVICIOS TELEMÁTICOS, con C.I.F. Q5000455E y domicilio a efectos del presente acuerdo en Parque Empresarial EXPO Zaragoza, Avda. Ranillas, nº 3 A, 3ª planta, oficina J, en adelante **AST**.

De otra parte Del otro, Nombre Y Apellidos Del Representante Del Cliente con D.N.I. número Nº DNI, en representación de Elija un elemento. Denominación De La Organización, con CIF Nº CIF y domicilio fiscal en En Caso Que Procede Cumplimentar CIF Y Domicilio Fiscal, en adelante **CLIENTE**.

Y de la otra, Nombre Y Apellidos Del Representante Del Proveedor con D.N.I. número Nº DNI, en representación de AST Nombre De La EMPRESA, con CIF Nº CIF y domicilio fiscal en Domicilio Fiscal, en adelante **PROVEEDOR**.

Exponen

Todas las partes acuerdan mutuamente, la capacidad legal necesaria para la suscripción del presente acuerdo y el cumplimiento y a dar cumplimiento a las siguientes Estipulaciones:

I. Que AST es una entidad de derecho público cuya misión es proporcionar servicios y soluciones de ALTO valor en el ámbito de las tecnologías y servicios de la información y telecomunicaciones a la Administración de la Comunidad Autónoma de Aragón y los organismos públicos de ella dependientes. Aragonesa de Servicios Telemáticos es también el operador de telecomunicaciones público para la Administración de la Comunidad Autónoma de Aragón, y como tal está registrado y habilitado para la prestación de servicios a

entidades privadas por la CNMC. Por tanto, es responsable de la información generada y gestionada en su actividad.

II. Que el CLIENTE utiliza parte de la infraestructura y/o servicios gestionados por AST.

III. Que PROVEEDOR es una organización de servicios y/o proyectos cuyo ámbito de relación con CLIENTE se inscribe dentro la realización del contrato denominado: Cumplimentar Nombre Identificativo Del Contrato Entre El Proveedor Y El Cliente con número de expediente NUMERO DE EXPEDIENTE O IDENTIFICADOR ÚNICO DEL CONTRATO.

IV. Que derivado del contrato anterior el PROVEEDOR puede tener acceso a información de AST y/o utilizar parte de la infraestructura de AST.

Confidencialidad y de No Divulgación de Información

V. Que PROVEEDOR durante la prestación de sus servicios a CLIENTE puede recibir información confidencial tanto del CLIENTE como de AST, o disponer de acceso o de potencial acceso la misma. En este sentido se considera por información confidencial, toda la información relativa a: procesos de negocio, planes de marketing, planes estratégicos, clientes, proveedores know-how, métodos, análisis funcionales, código fuente, estudios de mercado, estadísticas, datos financieros, análisis de viabilidad, especificaciones técnicas, formulas, diseños, estudios, aquella afectada por LOPD, la GDPR y toda aquella información que AST no haya autorizado de modo explícito a PROVEEDOR su libre uso o difusión.

VI. 1. PROVEEDOR. únicamente utilizará la información facilitada, tanto por parte del CLIENTE como de AST, para el fin mencionado en la Estipulación III, comprometiéndose a mantener la más estricta confidencialidad respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a sus empleados, asociados, subcontratas y a cualquier persona que, por su relación con la PROVEEDOR, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del PROVEEDOR para con CLIENTE.

2. Las personas o entidades citadas en el párrafo anterior y que tengan acceso a información confidencial de AST en el marco de la prestación del servicio, no disponen de permiso para reproducir, modificar, publicar o difundir

o comunicar a terceros dicha información sin previa autorización explícita de AST.

3. De igual forma, el PROVEEDOR. se compromete a aplicar, como mínimo, respecto de la información objeto de este acuerdo las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia organización. Procurando las medidas que eviten su pérdida, robo, difusión o sustracción. Así mismo, el PROVEEDOR asume la responsabilidad de aplicar todas las medidas exigibles por la legislación vigente.

VII. Sin perjuicio de lo estipulado en el presente Acuerdo, las partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

e) Cuando la información se encontrara en el dominio público en el momento de su suministro a PROVEEDOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.

f) Cuando la información ya estuviera en el conocimiento de PROVEEDOR. con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

g) Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso PROVEEDOR notificará a AST tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

h) En caso de que PROVEEDOR. pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con AST.

Calidad y Seguridad de la Información

VIII. En este sentido el PROVEEDOR se compromete a:

l) Dar a conocer a sus empleados o personas a cargo la Política de Calidad y Seguridad de la Información de AST, para su correcto cumplimiento, así como los requisitos de seguridad exigidos. Así mismo el PROVEEDOR declara conocer la Política de Calidad y Seguridad de la Información de AST disponible en su página web.

m) Evaluar los posibles riesgos en calidad y seguridad de la información en la prestación del servicio. Es responsabilidad del PROVEEDOR establecer las medidas necesarias para la segura y correcta prestación del servicio. EL PROVEEDOR responderá frente a AST de los daños y perjuicios que le haya podido ocasionar como consecuencia del incumplimiento de este clausulado.

n) Destinar un uso profesional al uso de los programas y archivos informáticos puestos a disposición del PROVEEDOR para el servicio.

o) Tener adoptadas, en todos los equipos utilizados para la prestación del servicio y aquellos equipos a su cargo que por estar en la misma red o infraestructura puedan suponer un vector de ataque, las medidas de seguridad técnicas, tales como: cifrado de almacenamiento, sistemas de control de acceso, antivirus, etcétera. El PROVEEDOR se hace responsable de cualquier brecha de seguridad/ataque ocasionada desde su equipamiento a equipos del Gobierno de Aragón o de terceros.

p) Cumplir con las normas de uso aceptable de los activos establecidas por la AST en su gestión de la seguridad de la información.

q) Ubicará en emplazamientos securizados y protegidos con el fin de reducir los riesgos derivados de las amenazas externas.

r) Proteger la infraestructura tecnológica, que así lo necesite, contra fallos de provisión en el suministro eléctrico.

s) Devolver de forma íntegra todos los activos propiedad de AST y dispuesto al mismo para el desarrollo de su servicio. AST no será responsable de los retrasos, acciones contrarias a derecho, daños y perjuicios, averías e incidencias imputables al PROVEEDOR que puedan afectar al mantenimiento de la red o redes para la prestación del servicio.

t) Aplicar dentro de lo posible principios de ingeniería de sistemas seguros.

u) Garantizar el manejo de la información de acuerdo al criterio de clasificación establecido.

v) El PROVEEDOR ha de notificar a AST de cualquier punto débil – vulnerabilidad, riesgo, etc. – que observen o que sospechen que exista, en los

sistemas o servicios; indistintamente de que PROVEEDOR opere o despliegue dichos sistemas o no.

IX. El CLIENTE se compromete a:

a. Informar con la debida antelación a AST de la propuesta del servicio y/o proyecto a poner en marcha. Así como de cualquier modificación sustancial que se produzca en el mismo. Esta información incluirá toda la información técnica necesaria para que AST pueda hacer una evaluación de viabilidad.

b. Asumir todas las responsabilidades de seguridad y mantenimiento de cualquier servicio y/o plataforma tecnológica, desplegada dentro de la infraestructura de AST, indistintamente si la de la relación contractual entre el CLIENTE y el PROVEEDOR prosigue o ha finalizado. Esta cláusula no exime al PROVEEDOR de las obligaciones contractuales que tenga con el CLIENTE, entre las que se puede incluir la delegación de esta responsabilidad si el contrato entre ambos así lo especifica. El CLIENTE asume cualquier indemnización que se derive de cualquier brecha de seguridad/ataque ocasionada desde su equipamiento a equipos del Gobierno de Aragón o de terceros. En caso de que el CLIENTE carezca de la capacidad técnica para garantizar este punto, será responsabilidad del CLIENTE contratar a un soporte externo que pueda asumir dicha responsabilidad. Eximiendo en cualquier caso a AST de esta función, salvo que se genere un acuerdo expreso y por escrito en este sentido.

Notificación y permiso

X. AST ha de autorizar de forma expresa y por escrito, como por ejemplo mediante un informe de viabilidad antes de la puesta en marcha o de cualquier modificación sustancial, de cualquier servicio y/o proyecto que utilice la infraestructura que gestiona. Para lo cual ha de contar previamente con toda la documentación necesaria, y en cualquier caso solicitara información adicional si así lo considera necesario. En el informe de viabilidad ha de evidenciar la conformidad del servicio y/o proyecto con las instrucciones técnicas y normativas de seguridad de AST. En caso de un informe desfavorable, tanto el PROVEEDOR como el CLIENTE deberán acometer las modificaciones necesarias para ajustarse a las normativas de AST, y volver a enviar la propuesta a AST.

XI. AST no se responsabiliza de las consecuencias que pudiera ocasionar el retraso de la puesta en marcha, derivada de que el CLIENTE o el PROVEEDOR no hayan informado con suficiente antelación para la elaboración del informe de viabilidad. Así como de los retrasos u otras consecuencias, que puedan surgir como consecuencia de no recibir un informe favorable de viabilidad.

XII. Si derivado del servicio y/o proyecto, se produce algún coste a AST, tanto por adquisición de material como por carga de trabajo, consumo de recursos, o modificación física y/o lógica de la infraestructura gestionada por AST, este coste podrá ser repercutido al CLIENTE.

XIII. AST podrá aislar, apagar o interrumpir cualquier servicio o plataforma tecnológica del PROVEEDOR, o del CLIENTE, si detecta que esta es un riesgo para los servicios que presta la propia AST, para la infraestructura del Gobierno de Aragón o de terceros. En ese caso AST no se responsabiliza de las consecuencias que dicha actuación pueda producir sobre AST o el CLIENTE. Ni el CLIENTE, ni el PROVEEDOR podrán reclamar en este caso indemnización alguna a AST. Sin embargo no se excluye la posibilidad del que el CLIENTE reclame al PROVEEDOR si lo considera oportuno.

Propiedad Intelectual e Industrial

XIV. Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen a AST y el hecho de revelarla a LA PROVEEDOR para el fin mencionado en la Estipulación Primera no cambiará tal situación.

XV. El PROVEEDOR garantiza y queda obligado a acreditar documentalmente ante AST, si fuere requerido, que dispone de las patentes, licencias, permisos, registros, autorizaciones y demás derechos de propiedad intelectual e industrial de los servicios a prestar. En cumplimiento de lo anterior el PROVEEDOR exime a AST de toda responsabilidad por las infracciones de la propiedad intelectual y/o industrial y por las infracciones de licencias y/o autorizaciones en que aquél pudiera incurrir, y se obliga a realizar cuanto sea necesario para dejar a la otra parte indemne, al margen y a salvo de las reclamaciones o demandas que por dichas infracciones pudieran exigirse contra él, directa o indirectamente, de tales reclamaciones o demandas.

Protección de datos

XVI. De acuerdo al *Reglamento (UE) 2016/679 General de Protección de Datos 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* (RGPD) y a lo dispuesto en *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPD-GDD), las partes se informan respectivamente que los datos de carácter personal intercambiados en el marco de la relación contractual serán incluidos en los ficheros de los que cada una de ellas es titular, siendo la finalidad de estos tratamientos el soporte en el desarrollo de las tareas en el ámbito de la prestación del servicio. Dichos datos no serán cedidos a terceros. Adicionalmente, ambas partes se obligan a garantizar, el cumplimiento de ambas leyes. Asimismo, para ejercer los derechos de acceso, rectificación, cancelación y oposición cualquiera de las partes deberá dirigirse mediante comunicación formal a las direcciones recogidas al inicio de este acuerdo.

Duración y devolución

XVII. Toda la información en posesión del PROVEEDOR como resultado de la relación con el CLIENTE e independientemente de su naturaleza, deberá de ser devuelta o destruida tras la finalización de la relación contractual o laboral, salvo que deban de ser conservados por requerimientos legales o normativos vigentes.

XVIII. Este acuerdo tendrá validez a partir del momento en que quede firmado por ambas partes, y se extenderá de forma indefinida, a pesar de que haya finalizado la relación contractual.

Estipulaciones penal y sanciones

XIX. En caso de que la información resulte revelada o divulgada o utilizada por PROVEEDOR cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar a AST los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último.

XX. El PROVEEDOR acepta que por parte de AST, o en nombre de ella otra organización debidamente acreditada, se le requieran, o auditen, las medidas de seguridad aplicadas según los párrafos IV y V. Si derivada de esta

acción AST indica como insuficientes las medidas adoptadas por el PROVEEDOR, este tendrá un plazo no superior a 3 MESES para subsanarlas. En caso contrario AST, podrá rescindir el permiso de operación con el PROVEEDOR sin ningún tipo de reclamación o indemnización por parte de este o del CLIENTE.

XXI. Mientras dure la relación contractual entre el PROVEEDOR y el CLIENTE. En caso de que el proyecto y/o servicio, ya sea de forma dolosa o por mera negligencia, como por ejemplo por la falta de actualizaciones de las plataformas tecnológicas o por una mala configuración o cualquier otra causa, afecte negativamente a otros entornos y/o servicios de AST o de terceros. El PROVEEDOR habrá de indemnizar a AST los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último.

XXII. Cuando termine la relación contractual entre el PROVEEDOR y el CLIENTE, será este último que asuma las obligaciones del primero, derivadas de las clausulas XXI y XXII respecto a AST.

XXIII. En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Juzgados y Tribunales de Zaragoza, con renuncia a su fuero propio, aplicándose la legislación española vigente.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes a un solo efecto en el lugar y fecha en el contrato indicados.

En nombre y representación de		
AST:	**CLIENTE:**	**PROVEEDOR**:

Anexo VI. 02A Circular informativa RGPD y confidencialidad

El contenido de esta cláusula puede haberse modificado. Por favor, revise el modelo oficial, su inclusión aquí es a titulo meramente informativo.

CIRCULAR INFORMATIVA

En _____ a ____ de _____ de 20__

De acuerdo al Reglamento General de Protección de Datos 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 (RGPD) le informamos que:

Responsable del tratamiento: Sus datos forman parte de un fichero titularidad de Aragonesa de Servicios Telemáticos con domicilio social en Avenida de Ranillas, 3A planta 3º oficina j 50018 Zaragoza y CIF Q5000455E.

Finalidad: las finalidades del tratamiento de sus datos serán las siguientes:

Recursos Humanos: cumplir con todas aquellas obligaciones derivadas de la relación laboral, tales como la gestión del expediente personal, la formalización de nóminas, el cumplimiento de obligaciones sociales y tributarias, el cumplimiento de los deberes en materia de prevención de riesgos laborales, las actividades de formación, el control de asistencia al trabajo, así como la gestión de los canales de comunicación implementados por la entidad de conformidad, con los requisitos previstos en las normativas vigentes.

Derechos de imagen: utilización de su imagen para la elaboración de publicaciones internas, y para su utilización con finalidades de divulgación de conocimientos propios relacionados con la misión de la entidad en nuestra intranet, webs y blogs corporativos. En ningún caso estas imágenes e información de carácter personal serán cedidas a terceros, ni utilizadas para una finalidad distinta a la descrita.

Sus datos serán conservados el tiempo necesario para satisfacer la finalidad para la que fueron recabados y, en todo caso, durante los plazos mínimos exigidos para atender las obligaciones laborales y tributarias.

Legitimación: La legitimación para la recogida de sus datos se basa en el contrato laboral suscrito con Aragonesa de Servicios Telemáticos y en su caso, en la adscripción como personal del Gobierno de Aragón.

Destinarios: De igual modo, le informamos que para el cumplimiento de las obligaciones legales y laborales sus datos pueden ser comunicados a:

- Administraciones Públicas (Seguridad Social, Agencia Tributaria, Gobierno de Aragón, …).
- Mutuas de protección laboral y servicios de prevención de riesgos laborales o la preservación de la salud de los trabajadores.
- Entidades bancarias para pagos asociados a la relación laboral.
- Comités de empresa, sindicatos y delegados de prevención.

Aquellas entidades o clientes que exijan o ante las cuales sea necesario identificar a los empleados: aseguradoras, clientes, proveedores, entidades de formación, mensajería, renting, identificación de infracciones de tráfico, así como aquellas entidades o clientes que requieran datos identificativos y laborales del personal para llevar a cabo el servicio contratado y que acrediten la relación con AST.

Sus datos no serán cedidos para otras finalidades distintas a las anteriormente descritas.

Derechos: Puede ejercer sus derechos de acceso, rectificación, supresión y oposición, así como revocar su autorización para el uso de sus imágenes.

También podrá solicitar la limitación u oposición al tratamiento de sus datos cuando se den determinadas circunstancias, en cuyo caso únicamente serán conservados para el cumplimiento de las obligaciones legalmente previstas.

Para ejercer los derechos anteriormente descritos deberá dirigirse al Responsable del departamento de Recursos Humanos. De igual modo, le informamos de que la Agencia Española de Protección de Datos es el órgano competente destinado a la tutela de estos derechos.

Con la finalidad de mantener actualizados los datos, el empleado deberá comunicar, a la mayor brevedad posible, cualquier cambio que se produzca sobre los mismos.

Compromiso de confidencialidad: En atención a nuestro compromiso de cumplir con la legalidad vigente, le informamos que bajo ningún concepto usted debe utilizar ni incorporar a los sistemas informáticos y archivos documentales de esta Entidad la información de carácter personal o empresarial a la que haya tenido acceso durante el

desempeño de sus tareas o funciones en otras entidades, cuando ello pueda implicar la vulneración de las legislaciones anteriormente mencionadas.

En cumplimiento de la legislación anteriormente mencionada, usted asume el compromiso de confidencialidad y de guardar secreto profesional respecto de los datos personales, datos sobre los clientes, estrategias comerciales y organizativas e industriales, y cualquier otra información a la que tenga acceso con el motivo de las funciones asignadas. Dicha obligación de secreto profesional subsistirá aun después de finalizar la relación laboral.

De igual modo le informamos que, con la finalidad de garantizar el derecho a la intimidad y privacidad del trabajador por parte de Aragonesa de Servicios Telemáticos, bajo ningún concepto usted debe incorporar a los sistemas informáticos y archivos documentales de esta entidad, su información de carácter personal tales como fotos, videos o imágenes.

Asimismo, de conformidad con el artículo 32 del RGPD, el empleado se compromete a cumplir las normas internas de seguridad que afectan al desarrollo de sus funciones, así como al uso responsable de los equipos informáticos, correo electrónico y demás aplicaciones a las que va a tener acceso. De igual modo, el empleado, como parte necesaria y fundamental para conseguir el compromiso de responsabilidad corporativa y ética empresarial de esta Entidad, tiene la responsabilidad y el deber de realizar los programas formativos y aplicar los procedimientos y normas que se le comuniquen a tal efecto.

El empleado se compromete a aplicar y tener en consideración los protocolos y procedimientos que establezca la entidad en esta materia y que sean de aplicación en el ámbito de protección de datos de carácter personal en los términos previstos en este documento.

Ante cualquier duda, incidente, o imposibilidad de aplicación adecuada de los procedimientos y normas lo comunicará al responsable que se le designe en cada uno de los supuestos tal como quede establecido a tal efecto.

Anexo VII. Solicitudes de Autorizaciones activadas

Detalladas en https://ast.aragon.es/formularios/listado/todos

Tipo de Credencial	Tipo de Autorizaciones
Personal	Solicitud de Videoconferencia

Tipo de Credencial	Tipo de Autorizaciones
Personal	Alta de aplicación o portal web en servicio de Estadísticas
Personal	Alta en el Servicio de Estadísticas Web
Personal	Autorización empresas externas para usar servicios de atención a usuarios
Aplicación	Alta Aplicación en Plataforma VPN-SSL
Personal	Apertura de Puertos FW (Housing, RedSara, Internet)
Personal	Acceso VPN Remote
Personal	Acceso VPN LAN to LAN
Personal	Gestión de Grupos en Carpetas de Red Local
Personal	Usuario aplicaciones Oracle
Personal	Alta Base de Datos MYSQL
Personal	Aumento de Cuota a Usuario
Personal	Acceso a servicio FTP
Personal	Creación espacio SFTP
Personal	Transferencia de Ficheros con GTF
Personal	Envío masivo de Correo Electrónico
Personal	Gestión de usuarios de Datos MYSQL
Personal	Incremento de Cuota de cuenta de Correo
Personal	Solicitud de instalación de software adicional
Personal	Solicitud de recuperación de archivos
Personal	Solicitud de retirada de residuos electrónicos en Zaragoza
Aplicación	Soporte de integración al Servicio de Firma Electrónica
Sistemas	Solicitud de traspaso de datos entre servidores

Tabla 0-4.Anexo VII. Solicitudes de Autorizaciones activadas

Anexo VIII. Cláusulas de información de uso responsable en peticiones

Con el objetivo de:

Concienciar al peticionario de los riesgos que implican las peticiones de esta naturaleza.

Trasladar la responsabilidad del riesgo al usuario derivado de actuaciones negligentes. Indicar las restricciones o controles adicionales que puedan surgir.

Aplicar las medidas legales que permitir transferir o al menos compartir los riesgos que estas peticiones conllevan. Todas las solicitudes al CAU, mediante formulario, con afección a la seguridad perimetral del Gobierno de Aragón tendrán cláusulas de información de uso responsable que tendrán que han de ser aceptadas para poder tramitar la petición.

Solicitud para utilizar un acceso externo seguro a la red corporativa

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón.

Por ello, el usuario de la VPN acepta hacer un uso responsable de la misma.

a) Haber firmado un contrato de confidencialidad y uso responsable con el organismo dueño de los activos a los que se tenga acceso.
b) Admitiendo las mismas restricciones de navegación y uso, por motivos de seguridad, que si estuviera dentro de la red del Gobierno de Aragón.
c) Se tendrá especial cuidado de no navegar por paginas o servicios potencialmente peligrosos (P2P, páginas de streaming, etc).
d) No se usará la VPN desde ningún equipo cuyo software no este correctamente licenciado (riesgo elevado de malware), ni cuyo software antivirus y sistema operativo no es este correctamente actualizado.
e) El usuario se hace responsable de tomar las medidas de precaución adecuadas, así como de tener un comportamiento seguro y ético mientras se usan estas herramientas.

Informar que el uso de VPN esta monitorizado. Una actuación ilicitica, o que genere una brecha de seguridad, tendrá las consecuencias técnicas, administrativas y legales pertinentes.

Solicitud de acceso remoto al puesto de trabajo

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón.

Por ello, el usuario del acceso remoto al equipo acepta hacer un uso responsable de la misma.

a) Admitiendo las mismas restricciones de navegación y uso, por motivos de seguridad, que si estuviera dentro de la red del Gobierno de Aragón.
b) Se tendrá especial cuidado de no navegar por paginas o servicios potencialmente peligrosos (P2P, páginas de streaming, etc).
c) No se usará la VPN desde ningún equipo cuyo software no este correctamente licenciado (riesgo elevado de malware), ni cuyo software antivirus y sistema operativo no es este correctamente actualizado.

d) El usuario se hace responsable de tomar las medidas de precaución adecuadas, así como de tener un comportamiento seguro y ético mientras se usan estas herramientas.

Informar que el uso de VPN esta monitorizado. Una actuación ilicitica, o que genere una brecha de seguridad, tendrá las consecuencias técnicas, administrativas y legales pertinentes.

Entiende y acepta los términos anteriormente expuestos.

Creación de un acceso externo seguro (VPN)

Explicación: Petición de creación de una red privada virtual (VPN) para acceder de forma segura a la red corporativa desde el exterior de la misma. Una red privada virtual (VPN) permite una conexión individual desde el exterior de la red del Gobierno de Aragón a un conjunto de servicios ofrecidos únicamente desde la red de datos interna. Una vez creada la red privada virtual, se autoriza la lista de personas que pueden utilizarla.

Cuando se haya creado la red privada virtual (VPN) recibirá un correo en el que se le informará del identificador de la VPN. Este identificador será necesario para modificar la lista de personas autorizadas que pueden utilizarla o los servicios a los que se accede a través de ella.

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. La apertura de puertos e IP accesibles desde el exterior, incluso a través de una VPN, genera una brecha que puede convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Por ello, el usuario de la VPN acepta hacer un uso responsable de la misma.

a) Haber firmado un contrato de confidencialidad y uso responsable con el organismo dueño de los activos a los que se tenga acceso.
b) Admitiendo las mismas restricciones de navegación y uso, por motivos de seguridad, que si estuviera dentro de la red del Gobierno de Aragón.
c) Se tendrá especial cuidado de no navegar por paginas o servicios potencialmente peligrosos (P2P, páginas de streaming, etc).
d) No se usará la VPN desde ningún equipo cuyo software no este correctamente licenciado (riesgo elevado de malware), ni cuyo software antivirus y sistema operativo no es este correctamente actualizado.
e) El usuario se hace responsable de tomar las medidas de precaución adecuadas, así como de tener un comportamiento seguro y ético mientras se usan estas herramientas.

Informar que el uso de VPN esta monitorizado. Una actuación ilicitica, o que genere una brecha de seguridad, tendrá las consecuencias técnicas, administrativas y legales pertinentes.

Alta de aplicación en plataforma VPN SSL

Explicación: Solicitud para inscribir una aplicación en la plataforma SSL (Secure Socket Layer). Sirve para proporcionar acceso seguro a dicha aplicación a usuarios desde ubicaciones externas a la red del Gobierno de Aragón. El acceso se realiza a través del portal publicado en Internet https://accesoremoto.aragon.es, que permite el acceso seguro al portal del empleado, a aplicaciones específicas o a servicios web (WS) concretos de algunas aplicaciones, que previamente se han puesto accesibles mediante esta solicitud.

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. El acceso de aplicaciones accesibles desde el exterior, incluso a través de una VPN SSL, genera una brecha que puede convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Pida los accesos mínimos imprescindibles para el servicio requerido. Justifique la necesidad de los mismos.

Modificación de un acceso externo seguro (VPN)

Explicación: Petición de modificación de una red privada virtual (VPN) para acceder de forma segura a la red corporativa desde el exterior de la misma. La modificación se refiere a los servicios a los que se accede y/o usuarios autorizados para usar la red privada virtual.

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. La apertura de puertos e IP accesibles desde el exterior, incluso a través de una VPN, genera una brecha que puede convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Pida los accesos IP y puertos mínimos imprescindibles para el servicio requerido. Justifique la necesidad de los mismos.

Los usuarios de la VPN aceptan hacer un uso responsable de la misma.

a) Haber firmado un contrato de confidencialidad y uso responsable con el organismo dueño de los activos a los que se tenga acceso.
b) Admitiendo las mismas restricciones de navegación y uso, por motivos de seguridad, que si estuviera dentro de la red del Gobierno de Aragón.
c) Se tendrá especial cuidado de no navegar por paginas o servicios potencialmente peligrosos (P2P, páginas de streaming, etc).
d) No se usará la VPN desde ningún equipo cuyo software no este correctamente licenciado (riesgo elevado de malware), ni cuyo software antivirus y sistema operativo no es este correctamente actualizado.

e) El usuario se hace responsable de tomar las medidas de precaución adecuadas, así como de tener un comportamiento seguro y ético mientras se usan estas herramientas.

Informar que el uso de VPN esta monitorizado. Una actuación ilicitica, o que genere una brecha de seguridad, tendrá las consecuencias técnicas, administrativas y legales pertinentes.

Solicitud de apertura de puertos del FW para housing

Explicación: Petición para la apertura de puertos en el Firewall de servicios alojados en las infraestructuras de Aragonesa de Servicios Telemáticos

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. La apertura de puertos e IP accesibles desde el exterior genera una brecha que puede convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Pida los accesos IP y puertos mínimos imprescindibles para el servicio requerido. Justifique la necesidad de los mismos.

La apertura de puertos al exterior de un servicio, puede implicar revisar la actual arquitectura de red asociada a dicho servicio, con el fin de que se cumplen los parámetros de seguridad adecuados.

Solicitud de apertura de puertos del FW para red SARA

Explicación: Petición para la apertura de puertos del Firewall para el Sistema de Aplicaciones y Redes para las Administraciones, es decir, la red SARA.

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. La apertura de puertos e IP accesibles desde el exterior, incluso en la red SARA, genera una brecha que puede convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Pida los accesos IP y puertos mínimos imprescindibles para el servicio requerido. Justifique la necesidad de los mismos.

Solicitud de apertura de puertos del FW para servicios de internet

Explicación: Petición para la apertura de puertos en el Firewall para servicios ubicados en la DMZ (zona desmilitarizada).

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. La apertura de puertos e IP accesibles desde el exterior, incluso a través de una VPN, genera una brecha que puede

convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Pida los accesos IP y puertos mínimos imprescindibles para el servicio requerido. Justifique la necesidad de los mismos.

La apertura de puertos al exterior de un servicio, puede implicar revisar la actual arquitectura de red asociada a dicho servicio, con el fin de que se cumplen los parámetros de seguridad adecuados.

Solicitud de acceso seguro VPN LAN to LAN

Explicación: Petición de creación de un acceso seguro (VPN) LAN to LAN, es decir, una conexión bidireccional segura, como si se tratara de una red local, entre una ubicación externa, en la que puede haber diversos usuarios, y servicios de la red corporativa del Gobierno de Aragón. Este tipo de acceso se realiza para entidades o empresas que necesitan este acceso.

Texto de información de uso responsable

Su solicitud modifica la seguridad perimetral e implica riesgos para la infraestructura TIC del Gobierno de Aragón. La apertura de puertos e IP accesibles desde el exterior, incluso a través de una VPN, genera una brecha que puede convertirse en una brecha de seguridad que afecte a este y otros servicios. Pondere y valore los riesgos que asume, respecto al beneficio que le reporta.

Pida los accesos IP y puertos mínimos imprescindibles para el servicio requerido. Justifique la necesidad de los mismos.

La sede extrema de la VPN LAN to LAN, ha de cumplir:

a) Haber firmado un contrato de confidencialidad y uso responsable con el organismo dueño de los activos a los que se tenga acceso. se hace responsable de tomar las medidas de precaución adecuadas, así como de tener un comportamiento seguro y ético mientras se usan estas herramientas.
b) Contar con un sistema de gestión de seguridad de la información. Así como estar dotado de las necesarias medidas técnicas de seguridad (firewall, antivirus, etc).
c) Acepta que el Gobierno de Aragón y en su nombre AST pueda consultar o incluso auditar dicho sistema de gestión, así como verificar que cuenta con las medidas técnicas de seguridad apropiadas.
d) En caso de que se viera necesario, el Gobierno de Aragón podrá exigir una equivalencia en las mismas restricciones de navegación y uso, por motivos de seguridad, que si estuviera dentro de la red del Gobierno de Aragón. Se tendrá especial cuidado de no navegar por paginas o servicios potencialmente peligrosos (P2P, páginas de streaming, etc).
e) No se podrá tener en la sede remota ningún equipo cuyo software no este correctamente licenciado (riesgo elevado de malware), ni cuyo software antivirus y sistema operativo no es este correctamente actualizado.

Informar que el uso de VPN esta monitorizado. Una actuación ilicitica, o que genere una brecha de seguridad, tendrá las consecuencias técnicas, administrativas y legales pertinentes

Anexo IX. Glosario

- **Declaración de aplicabilidad** (*Statement of Applicability*, **SOA**): documento que relaciona los controles (de la ISO, ENS, etc.) que se utilizan en el sistema de gestión.
- **Gestión del Nivel de Servicio** (*Service Level Management*, **SLM**): Proceso operativo encargado de Negociar Acuerdos de Nivel de Servicio (SLA) con los clientes y diseñar servicios de acuerdo con los objetivos propuestos. La Gestión del Nivel de Servicio (SLM) también es responsable de asegurar que todos los Acuerdos de Nivel Operacional (OLA) y Contratos de Apoyo (UC) sean apropiados, y de monitorear e informar acerca de los niveles de servicio.
- **Requisitos de Nivel de Servicio** (*Service Level Requirements*, **SLR**): documento que contiene las requisiciones de servicio desde el punto de vista del cliente y define los niveles de servicio propuestos, las responsabilidades mutuas y otros requisitos específicos de los clientes o grupos de clientes.
- **Acuerdo de Nivel de Servicio** (*Service Level Agreement*, **SLA**): Es un acuerdo entre un proveedor de servicios de TI y un cliente. El SLA describe un servicio de TI, documenta los objetivos de nivel de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente. En un mismo SLA pueden incluirse varios servicios y clientes.
- **Acuerdo de Nivel Operacional** (*Operational Level Agreement*, **OLA**): Se trata de un acuerdo entre un proveedor de servicios de TI y otra parte de la misma organización. Un OLA brinda apoyo en la prestación de servicios al cliente por parte de proveedor de servicios de TI. El OLA define los bienes y servicios que se proveen y las responsabilidades de ambas partes
- **Contrato de Apoyo** (*Underpinning Contract*, **UC**): Es un acuerdo legal entre un proveedor de servicios de TI y una tercera parte. La tercera parte provee bienes o servicios que soportan la entrega de servicios para los clientes.
- **Solicitud de Cambio** (, **RFC**)

- **Planes de mejora del servicio** (*Service Improvement Plan*, **SIP**). Plan formal para implementar las mejoras a los servicios y procesos de TI. Se utiliza para gestionar y documentar las iniciativas de mejoramiento desencadenadas por el Perfeccionamiento Continuo del Servicio (CSI).
- **Tiempo objetivo de recuperación** (,**RTO**): es el tiempo definido dentro del nivel de servicio en el que un proceso de negocio debe ser recuperado después de un desastre o pérdida para así evitar consecuencias debido a la ruptura de continuidad de servicio.
- **Centros de Proceso de Datos** (**CPD**).
- ***Troubleshooting***. Proceso de eliminación o solución de problemas e incidentes.
- **Gestión de información y eventos de seguridad** (*security information and event management*, **SIEM**). Sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales.
- **INES** (Informe Nacional del Estado de Seguridad).
- **OWASP** (*Open Web Application Security Project*). proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro
- **SonarQube**. Herramienta de análisis de calidad de código.
- **Quiosco interactivo** (o kiosko interactivo) es una computadora situada en lugar público que permite a los usuarios realizar múltiples acciones. También se utiliza como herramienta de información y marketing para las empresas. Pudiendo tener interfaces de entrada como teclados pantallas táctiles.

Anexo X. Categorización de los sistemas

El Esquema Nacional de Seguridad, indica

« 1. La categoría de un sistema de información, en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

2. La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que afectará a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.

3. La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Artículo 43. Categorías **ENS**

En el anexo I de dicha ley se especifica:

«Categorías de los sistemas

1. Fundamentos para la determinación de la categoría de un sistema.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

La determinación de la categoría de un sistema se realizará de acuerdo con lo establecido en el presente real decreto, y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general.

2. Dimensiones de la seguridad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la

categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

a) Disponibilidad [D].

b) Autenticidad [A].

c) Integridad [I].

d) Confidencialidad [C].

e) Trazabilidad [T].

3. Determinación del nivel requerido en una dimensión de seguridad.

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

*a) **Nivel BAJO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.*

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño menor por los activos de la organización.

3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.

5.º Otros de naturaleza análoga.

*b) **Nivel MEDIO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.*

Se entenderá por perjuicio grave:

1.º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño significativo por los activos de la organización.

3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.

5.º Otros de naturaleza análoga.

*c) **Nivel ALTO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.*

Se entenderá por perjuicio muy grave:

1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3.º El incumplimiento grave de alguna ley o regulación.

4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5.º Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de un sistema de información.

1. Se definen tres categorías: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de un sistema sobre la base de lo indicado en el apartado anterior no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

5. Secuencia de actuaciones para determinar la categoría de un sistema:

1. Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3.

2. Determinación de la categoría del sistema, según lo establecido en el apartado 4.»

Anexo XI. Empresas asociadas a los servicios

El registro de los proveedores asociados a cada contrato o se encuentra en el *PRO_A3 Gestión de contratación*.

Anexo XII. Área Segura: Normativa de trabajos en CPD

Normativa básica

Los Centros de Proceso de Datos y Centros de Telecomunicaciones (Emisores), son *áreas de acceso restringido* donde se ubica equipamiento TIC muy sensible, a las que solamente deben entrar personas previamente autorizadas y únicamente a realizar la labor encomendada.

Disponen de una infraestructura eléctrica específica, por lo que se debe consultar AST antes de conectar móviles, portátiles, taladros, en cualquiera de las tomas eléctricas.

Son espacios climatizados para mantener la óptima refrigeración de los equipos TI y no con criterios de confort. Para su eficiente funcionamiento se debe evitar tener la puerta abierta.

El CPD tiene un sistema de detección y extinción automática de incendios (PCI). Los detectores son muy sensibles por lo que está prohibido hacer trabajos con llama, chispa o que generen polvo o humo. Todas estas operaciones: soldaduras, cortes, taladros… se deben realizar fuera del CPD. En el caso que no pueda realizarse en el exterior se debe solicitar autorización para hacerlo dentro, poniendo todas las medidas necesarias para minimizar la emisión de polvo y suciedad, esperando confirmación de desconexión del PCI por parte de AST e informando de la finalización del trabajo.

Tanto en el CPD como en Centros de Telecomunicaciones y otros espacios TIC se debe tener especial sensibilidad con el *orden y la limpieza*:

- Ensuciar y desordenar lo mínimo al realizar los trabajos.
- Dar un acabado pulcro y de calidad a los trabajos.
- Recoger y limpiar todo cuando se finalizan los trabajos.
- Los embalajes y las basuras se retirarán como mínimo al finalizar cada jornada.

- NO se podrá dejar NADA (documentación, CD-s, cables, conectores…) en las mesas o en los racks.
- El almacenaje temporal de material se hará en los espacios habilitados e indicados para ello, que en la medida de lo posible estarán ubicados fuera del CPD.
- Las conexiones eléctricas permitidas se realizarán hasta las PDUs (CPDs) o borneros (Centros) preparados por AST para nuevos servicios. No se permiten realizar ampliaciones de los suministros existentes. Dichas conexiones eléctricas se utilizará material adecuado según el Reglamento Electrotécnico para Baja Tensión. Las conexiones de red de datos se harán con cables y/o fibras debidamente certificados. En todos los casos, usando cableado de longitud adecuada. El nuevo cableado se ha de colocar de forma que no obstruya la manipulación de otros elementos del rack, colocándose por el costado de los mismos y evitando cruzar por delante – o detrás – de cualquier otro dispositivo existente en el armario. Se ha de informar de todos los cambios de conexión al equipo de Operaciones para que estos lo registren.

Es responsabilidad del trabajador traer las herramientas y EPIs necesarios para hacer su trabajo, guardar las medidas de seguridad y tener cumplimentado los requisitos de Coordinación de Actividades Empresariales exigidos por AST y por la leyes de prevención de riesgos laborales. Así mismo se han de seguir todas las directivas en materia de PRL, operaciones y seguridad que desde AST se emitan.

Acceso

La tarjeta, o llave, de acceso al CPD y a los Centros emisores es personal e intransferible. No se puede acceder acompañado de otras personas que no dispongan a su vez de tarjeta de acceso con los permisos de acceso a dichas salas, salvo que hayan sido previamente registradas y debidamente autorizadas.

Una vez dentro del CPD, se deben seguir las siguientes directrices:

- Queda *PROHIBIDO* manipular los sistemas de climatización, de incendios y cuadros eléctricos.
- Queda *PROHIBIDO* levantar las losetas, salvo permiso concedido expresamente para dicha visita o acceso. Si fuese preciso levantar, se señalizara debidamente.
- Así mismo queda *PROHIBIDO* enchufar o desenchufar equipos en los enchufes dispuestos bajo las losetas, salvo que se disponga de permiso expreso.
- Queda *PROHIBIDO* manipular cualquier otro equipo del que no sea titular.
- Queda *PROHIBIDO* beber y comer en las instalaciones.

Cualquier duda sobre estas normas o sobre cualquier necesidad que surja mientras se trabaja en el CPD deberá ser consultada con los operadores.

Se debe avisar de cualquier anormalidad observada a los técnicos de las salas de operación, o bien al servicio de seguridad. Ante cualquier duda consulte con su responsable de proyecto y/o servicio; o en su defecto al equipo de Operaciones.

Anexo XIII. Entidades Certificadoras reconocidas en AST

Entidades Certificadoras	Tipos de Certificado	Características
FNMT	Certificados de Servidor	de Confianza
Camerfirma	Certificados de Servidor;	de Confianza

Tabla 0-5. Anexo XII. Entidades Certificadoras reconocidas en AST

Área	Plataforma	Tipos de Certificado	característica
Área de Seguridad AST	PTS. Generación Certificados	Certificado de Servidor	Autofirmados

Anexo XIV. Documentación obsoleta que abarca total o parcialmente esta instrucción técnica

Documentación	Última revisión
NOR_GestionRiesgo	23/01/2018
NOR_GestionAutorizaciones	19/12/2017
NOR_GestionAutenticacion	19/12/2017
NOR_GestionProteccionConfidencialidad	19/12/2017
NOR_GestionProteccionIntegridad	19/12/2017
NOR_GestionTrazabilidad	19/12/2017
NOR_GestionCNSyCalidadNormativa	19/12/2017
NOR_GestionAuditoriasSeguridadInternas	19/12/2017
NOR_GestionCiberincidencias	19/12/2017
NOR_GestionSoportes	19/12/2017
NOR_GestionClavesAccesoSistemasyCifrado	19/12/2017
NOR_GestionProporcionalidadCoste	18/12/2017
NOR_GestionUsoSellodeTiempo	04/12/2017
NOR_GestionComunicacionesOperaciones	29/11/2017
NOR_GestionCuentasUsuario	29/11/2017
NOR_GestionLogsSistemasAplicaciones	29/11/2017
NOR_GestionVulnerabilidades	29/11/2017
NOR_GestionIntercambioSeguroInformacion	29/11/2017
NOR_UsoCorreoElectronico	29/11/2017
NOR_UsoRecursosyAccesosSistemasInformaciónAST	29/11/2017
NOR_GestionAccesoLogico	29/11/2017
NOR_GestionCertificadosSeguridad	29/11/2017
NOR_GestionActivos	29/11/2017
ASS - Abril16 - NOR_OrganizaciónSeguridadAST	09/10/2016
PROC_LogsAccesoCuentasAdministrador	01/07/2016

Documentación	Última revisión
NOR_RetencionDatosTelecomunicaciones	19/02/2015
NOR_AdquisiciónDesarrolloMantenimientoSistemasInformación	16/02/2015
NOR_DesarrolloSeguroSoftware	16/02/2015
NOR_AdquisicionDesarrolloMantenimientoSI	16/02/2015
NOR_ElaboracionMarcoNormativoSeguridad	12/11/2013
POL_GestionIncidencias	30/10/2013
NOR_GestionProteccionDisponibilidad	

Tabla 0-6. Documentos obsoletos

Anexo XV. Control de versiones

Debido a la extensión del documento, así como la obligación de revisarlo (ver norma *N1.1.3 Revisión del cuerpo normativo de seguridad*, página 25), con el fin de facilitar la legibilidad y estética del documento; se establece el control de versiones en el siguiente anexo.

Versión	Fecha	Autor	Descripción / Artículos modificados
0.1	07/02/2019	Ignacio Pérez [AST - Resp. Seguridad]	Creación del documento
1.0	03/07/2019		Primera versión del documento

Tabla 0-7. Anexo XIV. Control de versiones

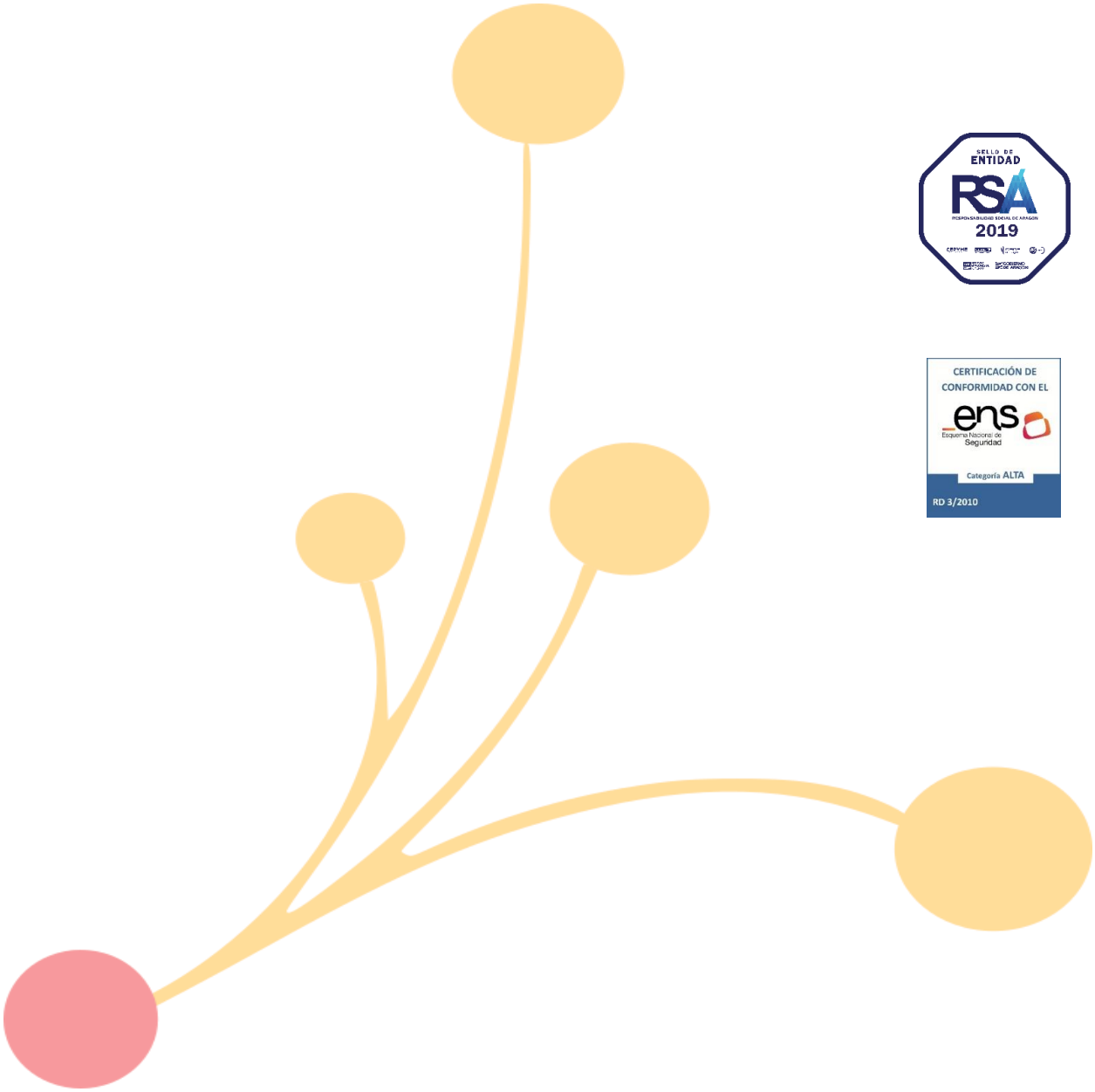
Anexo XVI. Índice de ilustraciones

No se encuentran elementos de tabla de ilustraciones.

Anexo XVII. Índice de tablas

Tabla 1-1. Roles y responsabilidades. 19
Tabla 2-1. Principios básicos y requisitos mínimos definidos en el ENS 22
Tabla 0-1. Anexo I. Relación entre las normas y las medidas de protección del Esquema Nacional de Seguridad 136
Tabla 0-2. Anexo II. Relación entre las normas y los controles de la norma UNE-EN ISO/IEC 27001:2017 140
Tabla 0-3. Listado de CMDB de proceso «O6 Gestión de la configuración» 141
Tabla 0-4.Anexo VII. Solicitudes de Autorizaciones activadas 159
Tabla 0-5. Anexo XII. Entidades Certificadoras reconocidas en AST 172
Tabla 0-6. Documentos obsoletos 173
Tabla 0-7. Anexo XIV. Control de versiones 173

■ Fin de documento.



ast
Aragonesa de Servicios Telemáticos

ast.aragon.es

ast@aragon.es

@tuitast

976 714 495

Avda. Ranillas 3A, 3º oficina J
50018 Zaragoza