**SOLICITUD DE CERTIFICACIÓN ENS (ESQUEMA NACIONAL DE SEGURIDAD) SEGÚN R.D. 3/2010 y R.D. 311/2022.**

**1. VERSIÓN ENS A CERTIFICAR**

RD 3/2010[[1]](#footnote-1)

RD 311/2022 [[2]](#footnote-2)

**2. CATEGORÍA DE SUS SISTEMAS DE INFORMACIÓN**

BASICA

MEDIA

ALTA

**3. ALCANCE DE LA CERTIFICACIÓN**

* 1. **Propuesta de Alcance**

Escribir en este espacio las actividades / procesos aplicables al alcance ENS

*“Los sistemas de información utilizados para prestar los servicios de…….”*

**4. IDENTIFICACIÓN DE LA ENTIDAD SOLICITANTE:**

CIF:

Razón Social:

Domicilio social:

Código Postal:       Población:       Provincia:

Teléfono:       e-mail:       http//www.

Nombre Comercial:

* 1. **Representantes (nombres):**

Representante legal

Nombre:

Título de representación:

Persona de contacto que habitualmente mantendrá las relaciones con el IVAC

Nombre:

Cargo:

* 1. **Datos de los centros de trabajo que van a formar parte del proceso de certificación**

*(Añádanse los centros de trabajo necesarios si procede).*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CENTRO PRINCIPAL** | Actividad | Turnos | Cod. CNAE | Departamento | Personal subcontratado  (% jornada) | Nº TRABAJADORES | |
| Jornada parcial  (% jornada) | Jornada completa |
| *Razón social / Dirección, C.P., población, provincia, teléfono, email)* |  |  |  | Alta Dirección |  |  |  |
| Responsables de área |  |  |  |
| Administradores de Sistemas |  |  |  |
| Responsables Seguridad S.I. |  |  |  |
| Otro (especifique) |  |  |  |
| **OTROS CENTROS** | Actividad | Turnos | Cod. CNAE | Departamento | Personal subcontratado  (% jornada) | Nº TRABAJADORES | |
| Jornada parcial  (% jornada) | Jornada completa |
| *Razón social / Dirección, C.P., población, provincia, teléfono, email)* |  |  |  | Alta Dirección |  |  |  |
| Responsables de área |  |  |  |
| Administradores de Sistemas |  |  |  |
| Responsables Seguridad S.I. |  |  |  |
| Otro (especifique) |  |  |  |
| **OTROS CENTROS** | Actividad | Turnos | Cod. CNAE | Departamento | Personal subcontratado  (% jornada) | Nº TRABAJADORES | |
| Jornada parcial  (% jornada) | Jornada completa |
| *Razón social / Dirección, C.P., población, provincia, teléfono, email)* |  |  |  | Alta Dirección |  |  |  |
| Responsables de área |  |  |  |
| Administradores de Sistemas |  |  |  |
| Responsables Seguridad S.I. |  |  |  |
| Otro (especifique) |  |  |  |

¿Los sistemas de información a certificar ofrecen Servicios en la Nube? En caso afirmativo indicar Ubicación (ciudad, región y país) de los CPD en los que soporta dichos servicios

* 1. **Trabajadores con más de un idioma** ¿Tiene personal que hable en más de un idioma que exija intérprete o que impida que los auditores trabajen independientemente?  Sí  No En caso informativo indique número de personas y sus puestos

**4. CERTIFICADO DEL IVAC**

Indique en qué idiomas quiere que se emita el certificado y el anexo técnico:

**5. FECHAS EN LAS QUE DESEARÍA HACER LA AUDITORÍA**

**6. ASESORAMIENTO EXTERNO**

¿Ha tenido asesoramiento externo para implantar el sistema que desea certificar?       En caso afirmativo indicar el asesor externo (empresa de consultoría y persona física que lo ha realizado).

**7. INFORMACIÓN GENERAL**

**7.1. Subcontrataciones**. ¿Subcontrata alguna actividad incluida en el alcance de la certificación?  En caso afirmativo, indique que parte del proceso,       y número de trabajadores adscritos a cada proceso subcontratado

**7.2. Proveedores**. Indique los proveedores críticos con influencia en el alcance de la certificación (Comunicaciones, desarrollo de software, Cloud, Hosting, etc).

**7. Grupo Kiwa** ¿Tiene o ha tenido relación con Kiwa o alguna empresa del Grupo Kiwa? En caso afirmativo, indique el tipo de relación que ha tenido, qué tipo de servicio ha recibido por parte de Kiwa.       y la entidad dentro del grupo Kiwa

**8. [[3]](#footnote-3)INFORMACIÓN ADICIONAL QUE CONSIDERE DE INTERÉS APORTAR**

|  |
| --- |
| **INFORMACIÓN PARA CERTIFICACIÓN ENS** |

ANÁLISIS DE RIESGOS

|  |  |
| --- | --- |
| ¿Ha realizado un análisis de riesgos? | Elija un elemento. |
| Especificar la metodología empleada o aquella que piensa utilizar: | Magerit.  ISO 31000.  NIST SP 800-30.  Otras: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ¿Tiene identificado los activos que sustentan sus sistemas de información? *(en caso afirmativo, envíenos su inventario).* | Elija un elemento. |

CUMPLIMIENTO LEGAL

|  |  |
| --- | --- |
| ¿Cumple el reglamento de protección de datos según la normativa vigente? | Elija un elemento.  Ha sido auditado (interna o externamente). |
| ¿Ha incluido los riesgos derivados del tratamiento de datos personales? | Elija un elemento. |
| ¿Está obligada su empresa a tener un delegado de protección de datos? | Elija un elemento. |

NIVEL DE MADUREZ DE LOS PROCESOS

|  |  |
| --- | --- |
| De acuerdo con la CCN-STIC-824 ¿su nivel de implantación de las medidas de seguridad es igual o superior al nivel L3 (mínimo nivel para categoría Media)? | SI  NO  Especificar: |

MECANISMOS DE AUTENTICACIÓN

|  |  |
| --- | --- |
| ¿Cuáles de los siguientes mecanismos de autenticación utiliza? | Credenciales mediante identificador y la contraseña.  Tarjetas inteligentes.  Otros métodos: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Autenticación biométrica: |
| Huella.  Reconocimiento facial.  Patrones oculares.  Voz. |

INFRAESTRUCTURA TÉCNICA

|  |  |
| --- | --- |
| Modelo de gestión: | Los equipos se gestionan de forma individual (Grupo de trabajo, etc.).  Gestión de equipos centralizada (Dominio, etc.).  Otro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ¿Tipo de Infraestructura de servidores? | Infraestructura física (modelo tradicional).  Infraestructura virtualizada. |
| En caso emplear virtualización: |
| Nº de equipos host: \_\_\_\_\_  Nº de máquinas virtuales: \_\_\_\_\_ |
| ¿Qué soluciones de virtualización está utilizando? |
| VMware ESX.  Microsoft Hyper-V.  Otro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ¿Dispone de servicios que sustenten sus operativas de negocio en la nube? | Elija un elemento.  ¿Cuáles?: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ¿Utiliza mecanismos de acceso remoto? | Elija un elemento. |
| ¿Con que finalidad? |
| Administración de sistemas.  Teletrabajo.  Otro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ¿Qué herramientas o mecanismo emplea?: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ¿Dispone de un mapa de red (representación visual de su red de computadoras y telecomunicaciones)?  (en caso afirmativo, envíenos su diagrama). | Elija un elemento. |

ACTIVOS CRÍTICOS

|  |  |  |
| --- | --- | --- |
| Número de servidores (físicos): | | Nº: \_\_\_\_ |
| Tipos /características de sus servidores | Descripción | Localización |
| Servidor controlador de dominio. |  |  |
| Servidor de correo Exchange o equivalente. |  |  |
| Servidor web. |  |  |
| Servidor de base de datos. |  |  |
| Otros servidor dedicados como: | | |
| Servidor: |  |  |
| Servidor: |  |  |
| Servidor: |  |  |
| Familia de sistemas operativos de sus servidores: | Microsoft Windows.  Linux.  Otros: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| ¿Dónde se sitúan sus activos más críticos  (servidores, electrónica de red, etc.)? | Elija un elemento. | |
| Armario rack informático.  Sala dedicada como CPD.  Infraestructura en Housing.  Otros: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Otro hardware/Software crítico de procesamiento interno o externo. | Firewalls.  Routers  Switches  Sistemas de detección de intrusiones (IDS)  Otros: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

PLANES DE RESPALDO Y RECUPERACIÓN

|  |  |
| --- | --- |
| ¿Dispone de una Plan de Continuidad de Negocio? | Elija un elemento. |
| ¿Incluye en sus copias de seguridad? | Datos.  Aplicaciones y programas.  Imágenes completas de los sistemas operativos de los equipos.  Máquinas virtuales. |
| Tipos de soportes que utiliza en los backup: | Discos duros.  Cabina o NAS.  Almacenamiento en la nube (servidores de terceros).  Otros:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Tipos de copias de respaldo que realiza: | Completa.  Incremental.  Diferencial. |
| Identificar las herramientas software de generación de copias de respaldo que utiliza: | |
|  | |

PROTECCIÓN ANTE CÓDIGO DAÑINO/MALWARE

|  |  |
| --- | --- |
| Especificar las distintas herramientas de análisis y detección de malware de su organización: | |
|  | |
| ¿Están centralizadas? | Elija un elemento. |

OTRAS CUESTIONES:

|  |  |
| --- | --- |
| ¿Dispone de certificación en vigor en ISO 27001? | SI  NO  En caso afirmativo, adjunte copia de su certificado. |
| ¿Se ha realizado pruebas o test de intrusión? | SI  NO  En caso afirmativo, indicar la metodología empleada:  Y la fecha de realización: |
| ¿Existe alguna información que, por indicación del Responsable del Sistema, del Servicio o del de Seguridad, no estará accesible al equipo auditor? | SI  NO  En caso afirmativo, indicar qué información:  El Auditor Jefe evaluará si ésta es una limitación para realizar la auditoría. Si es así y se decide continuar con el proceso de auditoría, esta limitación se reflejará en el informe de auditoría. |
| ¿Dispone de sistemas de información instalados en modo local que originalmente hubieran sido desplegados como soluciones en la nube en su modalidad Software as a Service (SaaS)? | SI  NO  En caso afirmativo, marca si dispone también de:  Guía de Instalación y Configuración Segura del Sistema destinada a administradores  Guía de Uso Seguro del Sistema destinada a usuarios finales  Guía de Recomendaciones para la gestión de la relación entre proveedor y cliente contratante  Cualquier otro documento que pudiera haber sido contemplado como requisito de seguridad adicional para dichos sistemas. Especificar: |

|  |
| --- |
| DOCUMENTACIÓN O INFORMACIÓN QUE SE DEBE ADJUNTAR UNA VEZ SE ACEPTE EL PRESUPUESTO |

A continuación, se indica la documentación mínima que se debe adjuntar a la presente solicitud y a fin de poder dimensionar adecuadamente la propuesta de la auditoría del cumplimiento del ENS

* Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.
* Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares). Así como listado de documentación que lo sustancia.
* Categoría del sistema según el Anexo I del ENS, incluyendo los criterios de identificación y valor de los niveles de las dimensiones de seguridad que serán de aplicación al sistema.
* La Política de Seguridad.
* La Normativa de Seguridad.
* La Declaración de Aplicabilidad.
* En caso de contar con certificado anterior por otra entidad de certificación acreditada, el informe de la anterior auditoría.
* Cualquier otra documentación, información que se considere de interés para poder concretar el alcance de la auditoría.

Para una adecuada planificación y preparación de la auditoría, y una vez aceptada la propuesta económica, se le solicitará también la siguiente documentación mínima, que se remitirá al auditor jefe con una antelación suficiente:

* Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.
* Identificación de los responsables: de la información, de los servicios, de la seguridad y del sistema.
* Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares).
* La Política de Firma Electrónica y Certificados (si se emplean estas tecnologías).
* Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.
* Informes con el desarrollo y resultado de la apreciación del riesgo, incluyendo la identificación de escenarios de riesgo, su análisis y evaluación.
* Informe y o plan de tratamiento del riesgo.
* Relación de las medidas de seguridad implantadas por requisitos legales o como resultado de la apreciación del riesgo.
* Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas y estado de implantación.
* Informe de la auditoría bienal de protección de datos de carácter personal (si se dispone, ya no es requisito con el RGPD) e informes de auditorías previas con el mismo objetivo y alcance que la auditoría de certificación.
* Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad, y relacionadas con el sistema a auditar.
* Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.
* Sistemas de métricas con referencia a las guías CCN-STIC-815 “Sistema de Métricas e Indicadores”, CCN-STIC -824 “Informe Nacional del Estado de la Seguridad, teniendo en consideración lo indicado en la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad”.

|  |
| --- |
| CONDICIONES DE LA CERTIFICACIÓN ENS EN IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. |

**Este apartado no puede ser modificado, puesto que forma parte del sistema de certificación del IVAC. En todo caso, las condiciones para la certificación en el Esquema Nacional de Seguridad que se considerarán válidas a todos los efectos son las que constan en la página.** [**https://www.kiwa.com/es/es/acerca-de-kiwa/documentos-publicos/**](https://www.kiwa.com/es/es/acerca-de-kiwa/documentos-publicos/)**. Éstas estarán disponibles para cualquier persona interesada.**

Manifiesto que he leído y acepto las condiciones de certificación ENS.

**CONDICIONES GENERALES ECONÓMICAS DE LA CONTRATACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN**

1. El pago de los servicios de certificación se efectuará a través de las siguientes modalidades:

a. Mediante cheque o pagaré nominativo a IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. a 10 días fecha factura.

b. Mediante transferencia bancaria a la cuenta que le indique IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. en la factura a 10 días fecha factura.

c. Mediante giros domiciliados a 30 días fecha factura en la cuenta que se le indique al IVAC-INSTITUTO DE CERTIFICACIÓN.

2. En el caso de certificación: se anticipará el 50% del importe total de los servicios de certificación a la aceptación del presupuesto, debiendo ser abonado antes de la realización de la auditoría.

3. En todo caso, IVAC-INSTITUTO DE CERTIFICACIÓN, S.L. no entregará los documentos de certificación hasta no haberse realizado el pago de la totalidad de los servicios de certificación.

Don/Doña      , representante legal de la entidad solicitante con capacidad suficiente para suscribir este contrato de servicios de certificación, declara que los datos consignados en la solicitud son ciertos y que en base a los mismos solicita presupuesto de certificación para formalizar, previa aceptación del mismo, el contrato de servicios de certificación, conociendo, entendiendo y aceptando las condiciones generales de la certificación. Igualmente manifiesta su conformidad con la presencia, si fuera necesario, de personal técnico del IVAC, de ENAC o del CCN para evaluar al equipo auditor designado, sin que ello represente ningún coste adicional para el solicitante.

Lugar, fecha, firma del representante legal y sello de la entidad solicitante

**CLAUSULAS SOBRE PROTECCIÓN DE DATOS**

Los datos de carácter personal son necesarios para poder prestar los servicios de certificación solicitados para mantener los contactos con los interlocutores designados por la entidad; se guardan en una base de datos denominada “clientes” y en una base de datos denominada “auditorías” consideradas en nuestro registro de tratamientos de datos de carácter personal que se conservan durante todo el tiempo que dure la relación comercial y hasta tres años después de la cancelación de la certificación. Su oposición al tratamiento dificultaría las comunicaciones necesarias para la prestación del servicio solicitado.

Son comunicados a los auditores a los efectos de identificación de los interlocutores de la empresa para la realización de la auditoría y eventualmente a ENAC o al CNN en caso de que evalúe la certificación emitida, así como en los casos previstos por la legislación fiscal y mercantil. No son objeto ni de transferencia internacional ni a terceros países fuera del EEE ni a organizaciones internacionales. Todo el personal de IVAC, así como los auditores de IVAC y los auditores de ENAC o del CCN tienen suscrito compromiso de confidencialidad.

Puede ejercer los derechos de acceso, rectificación, limitación, oposición, cancelación y portabilidad por cualquier medio escrito dirigido a nuestro delegado de protección de datos a nuestra dirección postal (calle Catedrático Agustín Escardino Benlloch, nº 9 – 46980 Paterna) o dirección de correo electrónico ([legal@ivac.es](mailto:legal@ivac.es)). Puede además presentar cualquier denuncia ante la AEPD

Si presta su consentimiento serán utilizados para informarle de los servicios de evaluación de la conformidad de IVAC y especialmente cualquier novedad relacionada con el campo de la certificación solicitada.

Acepto recibir información de Kiwa IVAC

No acepto recibir información de Kiwa IVAC

Lugar, fecha, firma de las personas cuyos datos personales se cumplimentan en la solicitud

1. *A partir del 05/05/2024, dejarán de tener la condición de acreditados los certificados emitidos frente al RD 3/2010.* [↑](#footnote-ref-1)
2. *No se podrán emitir certificados con el RD 311/2022 hasta el 01/12/2022* [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)