POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 11 de febrero de 2021 por la dirección de Coordinadora de Gestión de Ingresos.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

En Coordinadora de Gestión de Ingresos, S.A. (en adelante CGI) somos expertos especialistas en colaboración tributaria y recaudatoria para la Administración Local española. Desde 1998 optimizamos la gestión de tributos e incrementamos la recaudación de las entidades locales con una fórmula de proximidad: colaboramos estrechamente con los funcionarios y técnicos sobre el terreno, mediante equipos altamente especializados, y aplicando tecnología y metodologías contrastadas en multitud de proyectos.

La proximidad, calidad de servicio y orientación a resultados son nuestras señas de identidad, por lo que, conscientes de la trascendencia de la seguridad de la información, y en consonancia del camino que marca nuestra propia identidad, desde CGI se ha impulsado el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo a los requisitos de la norma ISO/IEC 27001:2013 con el fin de identificar, evaluar y minimizar los riesgos a los que se expone su información y la de sus clientes así como garantizar el cumplimiento de los objetivos establecidos y los requisitos del Esquema Nacional de Seguridad (ENS).

La **información** es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Este activo debe ser adecuadamente protegido, mediante las medidas de seguridad necesarias, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas o personas que intervengan en su conocimiento, procesado o tratamiento.

La **seguridad de la información** es la protección de este activo, con la finalidad de asegurar la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio. Es un proceso que requiere medios técnicos, humanos, una adecuada gestión y definición de los procedimientos. Es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

CGI depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados.

- Preservando la **confidencialidad** de la información y evitando su divulgación y el acceso por personas no autorizadas.
- Manteniendo la **integridad** de la información procurando su exactitud y evitando su deterioro.
- Asegurando la **disponibilidad** de la información en todos los soportes y siempre que sea necesaria.
- Protegiendo la **autenticidad** de los accesos de los usuarios.
- Garantizando la **trazabilidad** de las acciones que se realizan durante el tratamiento de los datos.

La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad y confidencialidad de su información y aún más la de sus clientes. Así, se compromete a desarrollar, implantar, mantener y mejorar continuamente su Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de la mejora continua en la forma en que prestamos nuestros servicios y en la forma en que tratamos la información de nuestros clientes, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Por ello, es política de CGI que:

- Se establezcan anualmente objetivos con relación a la Seguridad de la Información.
- Se cumpla con los requisitos legales, contractuales y del negocio.
- Se realicen actividades de formación y concienciación en materia de los procesos de Seguridad de la Información para todo el personal.
- Se desarrolle un proceso de análisis, gestión y tratamiento del riesgo sobre los activos de información y se clasifiquen de acuerdo con los niveles establecidos por el ENS.
- Se establezcan los objetivos de control y los controles correspondientes para mitigar los riesgos detectados.
- Se establezca la responsabilidad de los empleados en relación a:

    - Reportar las violaciones a la seguridad
    - Preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información en cumplimiento de la presente política
    - Cumplir las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información y ENS.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad e identidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizarla continuidad de los servicios prestados.
Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación de los servicios a llevar a cabo.
Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. PREVENCIÓN

Los trabajadores deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los responsables de área deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.
Para garantizar el cumplimiento de la política, los responsables de área deben:

1- Autorizar los sistemas antes de entrar en operación.
2- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
3- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en

los niveles de prestación de los servicios y actuaren consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

El responsable de seguridad debe:

1- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
2- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
3- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias o soporte externo especializado.

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, el responsable de seguridad y los responsables de los servicios, deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de CGI y a todos los miembros de la organización, sin excepciones. CGI ha establecido el siguiente alcance:

“Sistema de información relacionado con los procesos de implantación, mantenimiento y soporte técnico de infraestructuras tecnológicas y alojamiento en centro de datos propiedad de CGI (o centro de datos certificados de igual categoría), para las actividades de colaboración en la Aplicación Integral de Tributos, Inspección Tributaria, Recaudación Ejecutiva, Tramitación de Denuncias y Sanciones, así como en la Atención Telefónica y Telemática, en

modalidad de servicio en la nube, desplegado en modo privado como Software-as-a-Service (SaaS)."

4. MISIÓN

Preservar la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad (identidad) de toda la información y servicios vinculados a la actividad de CGI, en concreto:

- Servicio de aplicación Integral de Tributos, Inspección Tributaria, Recaudación Ejecutiva, así como la Tramitación de Denuncias y Sanciones, así como en la Atención Telefónica y Telemática relacionado con lo anterior.

- Gestión de la relación y colaboración entre las personas que forman CGI.

5. MARCO NORMATIVO

- Real Decreto 1993/1995 de 7 de diciembre (Entidad colaboradora con la Seguridad Social)
- Real Decreto 625/2014, de 18 de julio (Incapacidad).
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 3/2010, de 8 de enero, Esquema Nacional de Seguridad (como entidad de Derecho Público).
- Real Decreto 951/2015, de 23 de octubre (que modifica el anterior)
- Ley Orgánica 03/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016. (a partir del 25 de Mayo de 2018).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.
- Ley 35/2014, de 26 de diciembre (Mutuas de accidentes de trabajo y enfermedades profesionales).

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TIC está formado por:

- Director de la Organización
- Responsable de Seguridad
- Responsable de la Información
- Responsable de los servicios
- Responsable RRHH y Jurídica

El Comité de Seguridad TIC reportará al Comité de Dirección.
El Comité de Seguridad TIC tendrá las funciones descritas en el documento "Comité de Seguridad TIC".
El comité es el órgano de resolución de conflictos entre los distintos actores del ENS.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

La alta dirección asigna responsabilidad y autoridad para los roles relevantes de la seguridad de la información y la comunica debidamente. Esta asignación de responsabilidad y autoridad se define para garantizar que el SGSI cumple con los requisitos de la norma ISO/IEC 27001:2013 y para informar sobre el rendimiento general del SGSI a la dirección.

Los roles, su responsabilidad y autoridad, definidos para el SGSI de la empresa son:

- **Responsable de Seguridad**
  - ❖ Redactar, mantener y comunicar de forma adecuada las políticas, procesos y procedimientos de seguridad.
  - ❖ Capacidad de delegar responsabilidad sobre la redacción de procedimientos técnicos.
  - ❖ Integrar el comité de seguridad
  - ❖ Dimensionar los recursos necesarios para la eficacia del SGSI.
  - ❖ Apoyar el proceso de revisión del SGSI por la dirección aportando información ejecutiva sobre su eficacia para la toma de decisiones.
  - ❖ Aportar información operativa del SGSI para reuniones del comité de seguridad.

- Realización de análisis de riesgos del SGSI.
- Apoyar el proceso de auditorías internas y de certificación del SGSI.
- Planificar la implantación y mejora del SGSI.
- Recolección y protección de registros de cumplimiento.
- Establecer los requisitos del servicio en materia de seguridad

- **Responsable del servicio (ENS)**

  - Redactar, mantener y comunicar de forma adecuada las políticas, procesos y procedimientos del servicio.
  - Capacidad de delegar responsabilidad sobre la redacción de procedimientos.
  - Integrar el comité de seguridad
  - Dimensionar los recursos necesarios para la eficacia del servicio.
  - Apoyar el proceso de revisión del servicio por la dirección aportando información ejecutiva sobre su eficacia para la toma de decisiones.
  - Aportar información operativa del servicio para reuniones del comité de seguridad.
  - Realización de análisis de riesgos del ENS.
  - Apoyar el proceso de auditorías internas y de certificación del ENS
  - Planificar la implantación y mejora del servicio.
  - Recolección y protección de registros de cumplimiento.
  - Establecer los requisitos del servicio en materia de seguridad

- **Responsable de sistemas (informático de sistemas)**

  - Implantar las medidas técnicas sobre las infraestructuras y sistemas de información de la empresa.
  - Redactar procedimientos técnicos de las medidas implantadas.
  - Monitorizar las infraestructuras y sistemas de información.
  - Informar periódicamente al comité de seguridad sobre el desempeño de las implantaciones efectuadas.
  - Aportar información técnica y económica para la definición de mejoras sobre la implantación.

- **Responsable de la información**

  - Se encarga básicamente de que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados.

- Se encarga de mejorar los procesos de tecnologías de la información de la organización.
- Gestionar el riesgo y la continuidad de negocio.
- Controlar el coste en infraestructura de tecnologías de la información.
- Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos.
- Establecer mejoras e innovaciones de soluciones y productos.

- **Responsable de Recursos Humanos**

  - Definir, aplicar y registrar procedimientos de selección, contratación y despido de personal.
  - Comunicar al comité de seguridad sobre contrataciones y despidos.
  - Planificar la formación y concienciación en seguridad del personal.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El **responsable de la Información** es nombrado por la Dirección de CGI a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante. El **responsable de seguridad** es el director/a del área D_Sistemas y **responsable del Servicio** es el director/a del área D_Tec_Col_Trib

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección de CGI y difundida para que la conozcan todas las partes afectadas. (intranet y WebCGI)

7. DATOS DE CARÁCTER PERSONAL

CGI trata datos de carácter personal. El documento de seguridad y/o el Registro de actividades de tratamiento, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y/o actividades de tratamiento y los responsables correspondientes. Todos los sistemas de información de CGI se ajustarán a los niveles de seguridad requeridos por la normativa para la

naturaleza y finalidad de los datos de carácter personal recogidos en los mencionados Documentos.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

1- Regularmente, al menos una vez al año.
2- Cuando cambie la información manejada.
3- Cuando cambien los servicios prestados.
4- Cuando ocurra un incidente grave de seguridad.
5- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de CGI en diferentes materias:

- Política de Privacidad (para RGPD)
- Política del SIG (Calidad, Medio Ambiente, Salud y Seguridad en el Trabajo)

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.
La normativa de seguridad estará disponible en la página web de CGI .

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de CGI tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de CGI atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de CGI, en particular a los de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Cuando CGI preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando CGI utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12. REQUISITOS BÁSICOS

12.1. REQUISITOS MÍNIMOS DE SEGURIDAD

Esta política de seguridad se establece de acuerdo con los principios básicos indicados y se desarrolla aplicando los siguientes requisitos mínimos:

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

Todos estos requisitos mínimos de han definido en proporción a los riesgos identificados en cada sistema.

12.2. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

La seguridad compromete a todos los miembros de la organización. La política de seguridad identifica unos claros responsables de velar por su cumplimiento y es conocida por todos los miembros de la organización.

12.3. ANÁLISIS Y GESTIÓN DE LOS RIESGOS

CGI realiza su propia gestión de riesgos. Esta gestión se realiza por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Para ello se emplea una metodología reconocida internacionalmente (Magerit), con herramientas propias de gestión.
Las medidas adoptadas para mitigar o suprimir los riesgos se apoyan en las definidas por el propio esquema nacional y la ISO 27001:2013 y, existe una proporcionalidad entre ellas y los riesgos.

12.4. GESTIÓN DE PERSONAL

Todo el personal relacionado con la información y los sistemas ha sido formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones son supervisadas para verificar que se siguen los procedimientos establecidos.

El personal relacionado con la información y los sistemas, ejercita y aplica los principios de seguridad en el desempeño de su cometido.

El significado y alcance del uso seguro del sistema se concreta y plasma en unas normas de seguridad específicas relacionadas en el documento de "funciones y obligaciones del personal".

Para corregir, o exigir responsabilidades en su caso, cada usuario que accede a la información del sistema está identificado de forma única, de modo que se conoce, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

12.5. PROFESIONALIDAD

La seguridad de los sistemas está atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento, por el departamento de sistemas y seguridad, así como por empresas y consultoras contratadas para prestar servicios a tales efectos si no se dispone del conocimiento necesario en la organización.

El personal de la organización recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la misma.

La organización exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

12.6. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS

El acceso al sistema de información es controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

12.7. PROTECCIÓN DE LAS INSTALACIONES

Los sistemas están instalados en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas están cerradas y disponen de un control de llaves.

12.8. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por CGI y las Administraciones Públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

La certificación indicada en el apartado anterior está de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

Para la contratación de servicios de seguridad se ha tenido en cuenta lo dispuesto en los apartados anteriores.

12.9. SEGURIDAD POR DEFECTO

Los sistemas se han diseñado y configurado de forma que garantizan la seguridad por defecto:

a) El sistema proporciona la mínima funcionalidad requerida para que la organización alcance sus objetivos.
b) Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y se asegurar que sólo son accesibles por las personas, o desde

emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
c) En el sistema de explotación se eliminan o desactivan, mediante el control de la configuración, las funciones que no son de interés, innecesarias e, incluso, aquellas que son inadecuadas al fin que se persigue.
D) El uso ordinario del sistema es sencillo y seguro, de forma que una utilización insegura requiere de un acto consciente por parte del usuario.

12.10. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Todo elemento físico o lógico requiere autorización formal previa a su instalación en el sistema, y requiere de la intervención de SAU de CGI.
Se conoce en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. (Gestión de parches centralizada, notificaciones de fabricantes, inscripción en foros, etc …).

12.11. PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO

En la estructura y organización de la seguridad del sistema, se ha prestado especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tienen la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos por la organización en el ámbito de sus competencias.

Toda información en soporte no electrónico, que ha sido causa o consecuencia directa de la información electrónica, está protegida con el mismo grado de seguridad que ésta. Para ello se aplican las medidas que corresponden a la naturaleza del soporte en que se encuentran, de conformidad con las normas de aplicación a la seguridad de estos.

12.12. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

El sistema protege el perímetro, en particular, existe una segmentación clara con las redes públicas. Se entiende por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente,

para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. En todo caso se han analizado los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controla su punto de unión. (Por ejemplo: Conexión VPN).

12.13. REGISTRO DE ACTIVIDAD

Con la finalidad exclusiva de lograr el cumplimiento del objeto del propio ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

12.14. INCIDENTES DE SEGURIDAD

Se establecido un sistema de detección y reacción frente a código dañino, basado en un sistema de detección e IDS en los dispositivos de seguridad perimetral, una consola distribuida para la gestión del antivirus en estaciones de trabajo y servidores y un sistema de protección contra Ransomware.

La organización dispone de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se emplea para la mejora continua de la seguridad del sistema

12.15. CONTINUIDAD DE LA ACTIVIDAD

Los sistemas disponen de copias de seguridad y se ha establecido los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

12.16. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

El proceso integral de seguridad implantado es actualizado y mejorado de forma continua. Para ello, se aplican los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información y los estándares marcados por el sistema de gestión de la ISO 27001 implantada en la organización.

12.17. CUMPLIMIENTO DE REQUISITOS MÍNIMOS

Para dar cumplimiento a los requisitos mínimos establecidos en el ENS, la organización aplica las medidas de seguridad indicadas en el Anexo II del Real Decreto de referencia, considerando:

a) Los activos que constituyen el sistema.
b) La categoría del sistema, según lo previsto en el artículo 43.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 03/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad. (y a partir del 25 de Mayo de 2018 lo establecido por el RGPD vigente)
Las medidas a las que se refieren los apartados a y b tienen la condición de mínimos exigibles, y pueden ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

La relación de medidas seleccionadas del Anexo II del Real Decreto de referencia se ha formalizado en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.

Las medidas de seguridad referenciadas en el Anexo II del Real Decreto de referencia pueden ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indica de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad.

12.18. INFRAESTRUCTURAS Y SERVICIOS COMUNES

La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas no es de aplicación a CGI por su naturaleza jurídica de relación con las AAPP.

12.19. INSTRUCCIONES TÉCNICAS Y GUÍAS DE SEGURIDAD

Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, ha elaborado y difundido algunas de las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.

El Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Para la redacción y mantenimiento de las instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas a nivel europeo que resulten de aplicación.

12.20. SISTEMAS DE INFORMACIÓN NO AFECTADOS

CGI podrá determinar aquellos sistemas de información a los que no les sea de aplicación lo dispuesto en el presente de real decreto por tratarse de sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de junio.

37650474A
RAMON SOLE
(R: A81982225)

Firmado digitalmente por 37650474A RAMON SOLE (R: A81982225)
Nombre de reconocimiento (DN): 2.5.4.13=Ref:AEAT/AEAT0125/PUESTO 1/43991/28032019132616, serialNumber=IDCES-37650474A, givenName=RAMON, sn=SOLE VILANOVA, cn=37650474A RAMON SOLE (R: A81982225), 2.5.4.97=VATES-A81982225, o=COORDINADORA DE GESTION DE INGRESOS SA, c=ES
Fecha: 2021.02.12 13:35:25 +01'00'

Firmado: Ramón Solé Vilanova
Director General