POLITICA DE SEGURIDAD DE REDES Y SISTEMAS DE INFORMACIÓN SERVICIO DE ENTREGA ELECTRÓNICA CERTIIFICADA

2025-11-22

Índice

1 Objeto y ámbito de aplicación 3

2 Referencias normativas 4

3 Relación de Políticas 5

4 Definiciones 5

5 Desarrollo 6

5.1 Normativa general de seguridad 6

5.2 Política y Estándares de seguridad 6

5.3 Definición 7

6 Seguimiento, aprobación, publicación y revisión 7

7 Documentación de referencia 7

Control de cambios

Versión	Descripción/Historial de cambios	Revisado y aprobado por	Fecha de aprobación
V.3.0	Adaptación a la Norma	Armando Rodríguez	07/11/2023
V.4.0	Revisión Anual	Armando Rodríguez	11/10/2024
V. 4.1	Revisión de mantenimiento anual del Servicio de Entrega Electrónica Certificada de acuerdo con la siguiente normativa: Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014. Estándar ETSI EN 319401 V3.1.1. Directiva (UE) 2022/2555 (Directiva NIS II) y su Reglamento de Ejecución de 17/10/2024.	Security Business Partner Spain	11/11/2024
V.5.0	Revisión en el marco del proceso de recertificación del Servicio de Entrega Electrónica Certificada	Armando Rodríguez	29/10/2025

1 Objeto y ámbito de aplicación

El objeto del presente documento es definir las políticas de seguridad de redes y sistema de información a aplicar dentro del servicio de entrega electrónica certificada, en adelante “Servicio de ERDS (Electronic Registered Delivery Service”).

CGI se compromete a desarrollar las máximas capacidades en materia de seguridad (incluyendo la ciberseguridad), reduciendo así las amenazas para los sistemas de red y de información utilizados por la entidad en el marco del Servicio ERDS conforme a la normativa europea de ciberseguridad.

En este sentido, CGI, en su condición de Prestador Cualificado de Servicio de Confianza, se considera entidad esencial de la infraestructura digital europea de conformidad con la Directiva (UE) 2022/25551 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, denominada comúnmente como “Directiva NIS 2”, lo que conlleva su condición de sujeto obligado.

Es por eso por lo que, la presente Política se integra en la estrategia de seguridad que persigue CGI, con la finalidad de que el uso de las redes y sistemas de información responda al respecto del derecho de las partes interesadas y a la salvaguarda de los más altos estándares de ciberseguridad, teniendo en cuenta las actividades y estructura de CGI.

Por tanto, CGI pasará a ser responsable del cumplimiento de las obligaciones exigidas por esta normativa.

Misión y objetivos:

Entre los objetivos que persigue la política de seguridad de CGI se encuentran los siguientes:

- Facilitar los recursos adecuados necesarios para aplicar la presente Política, incluidos el personal, los recursos financieros, los procesos, las herramientas y las tecnologías necesarias.
- Impulsar y promocionar una cultura de ciberseguridad entre todos sus profesionales y sujetos obligados por esta Política, ya sea internamente, o entre sus clientes y proveedores.
- Integrar dentro del sistema de métricas del SGSI indicadores vinculados al nivel de implantación y de madurez de las medidas de seguridad.
- Gestionar diariamente medidas encaminadas a la protección y seguridad de las redes y sistemas de información, diseñando medidas de seguridad robustas, alineadas con las necesidades de las diferentes partes interesadas, así como con la normativa vigente aplicable en la materia, para lo cual, CGI aprueba las políticas y/o procedimientos específicos que desarrollan los principios y requisitos básicos de seguridad de las redes y sistemas de información establecidos en la presente Política. El objetivo es identificar los riesgos y corregir las vulnerabilidades detectadas, ciberamenazas e incidentes de ciberseguridad, a fin de evitar la materialización de incidentes que comprometan la continuidad de negocio de CGI.
- Establecer, implantar y aplicar procedimientos y/o políticas de seguridad de la cadena de suministro que rijan las relaciones con los proveedores directos y prestadores de servicios y establezca las medidas y controles oportunos con el fin de mitigar los riesgos detectados derivados de estos terceros para la seguridad de las redes y los sistemas de información de CGI.

Las directrices expresadas en este documento serán tomadas como base para la realización de los documentos específicos de este servicio en caso de que sean necesarios. Por tanto, para todo lo no desarrollado en la presente Política, se atenderá a las políticas, procedimientos y prácticas específicas del servicio.

[1] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un nivel elevado común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva 2016/1148.

La política de seguridad de CGI esta publicada en la intranet corporativa “Security and Data Privacy | Management Foundation”

2 Referencias normativas

- ISO/IEC 27001:2022 Information technology – Security techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002:2022 Information technology – Security techniques – Code of practice for information security management.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018 de protección de datos de carácter personal y garantía de derechos digitales.
- REGLAMENTO (UE) No 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 la que se deroga la Directiva 1999/93/CE modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2) y su Reglamento de Ejecución de 17 de octubre de 2024 por el que se establecen normas para la aplicación de la Directiva (UE) 2022/2555 en materia técnica y requisitos metodológicos de las medidas de gestión de riesgos de ciberseguridad.
- Reglamento de Ejecución (UE) 2025/1944 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas de referencia de los procesos de envío y recepción de datos en los servicios cualificados de entrega electrónica certificada y en lo que respecta a la interoperabilidad de tales servicios.

Adicionalmente, para el servicio de Entrega Electrónica Certificada, en base a la naturaleza del propio servicio prestado, se han seguido las disposiciones establecidas en las normas ETSI 319 401 y ETSI 319 521 para Proveedores de Servicios de Entrega Electrónica Certificada, las cuales contienen preceptos específicos para la prestación de este tipo de servicio.

CGI cuenta con una Declaración de Prácticas de Certificación (DPC) del Servicio de Entrega Electrónica Certificada que recoge las normas y condiciones generales que presta CGI en relación con el Servicio de Entrega Electrónica Certificada.

3 Relación de Políticas

Por razones de privacidad, no es posible incluir mayor detalle específico acerca de la política de seguridad estándar de CGI en este documento y otras políticas corporativas, por lo que proporcionamos los siguientes enlaces de referencia para obtener más información:

- CGI policies and standards
- SMSI SBU
- Information Security
- PIMS
- ESMF and ISO (cgi.com)
- Third Party Management Framework | Management Foundation (cgi.com)
- Quality System | Management Foundation (cgi.com)
- Client Partnership Management Framework | Management Foundation (cgi.com)
- Client Satisfaction Assessment Program (CSAP) | Management Foundation (cgi.com)
- Human resources | Management Foundation (cgi.com)

En lo que respecta a normas de seguridad, CGI a nivel global tiene elaborado el siguiente bloque de políticas relacionadas con distintos ámbitos de seguridad:

- Security and Acceptable Use Policy
- Information Security Policy
- Information Classification Policy
- Business Continuity Policy
- Safety Policy
- Facilities and Physical Security Policy

En el marco del Servicio de ERDS, las políticas y documentos de referencia son los siguientes:

- Declaración de Prácticas del Servicio Electrónico de confianza de Entrega Electrónica Certificada.
- Términos y condiciones del servicio
- Plan de Cese

En virtud de nuestra política de seguridad, algunos detalles específicos no pueden ser divulgados públicamente debido a la naturaleza confidencial de la información interna. Sin embargo, para proveedores y clientes interesados en detalles adicionales, estamos comprometidos a facilitar reuniones de divulgación seguras, donde se explicarán en profundidad nuestras prácticas de seguridad. Este proceso garantiza la confidencialidad de la información compartida y refuerza nuestro compromiso con la transparencia y la construcción de relaciones sólidas basadas en la confianza.

4 Definiciones

Consultar Manuales de Seguridad de CGI.

5 Desarrollo

Las líneas Políticas y Estándares de seguridad de CGI están divididos en dos grandes grupos

5.1 Normativa general de seguridad

Las políticas de seguridad de CGI establecen las directivas para una gestión coherente de los riesgos de seguridad y la gestión de documentos así como un compromiso con la seguridad y comunicación de los comportamientos esperados de los miembros, de empleados, de terceros (por ejemplo, subcontratistas o proveedores de servicios) y clientes, para garantizar la protección de la información y los activos para los cuales CGI es responsable.

CGI ha establecido procedimientos para notificar los cambios importantes en el marco de la prestación del Servicio de confianza a las partes interesadas teniendo en cuenta los requisitos empresariales y la normativa aplicable. Además, como Prestador de Servicios de Confianza cualificado, informará al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza al menos un mes antes de llevar a cabo el cambio y con una antelación de al menos tres meses en caso de que tenga intención de cesar la actividad.

- En el marco de la gestión del cambio, estas serán las actividades principales a seguir por CGI: Se identificarán y registrarán los cambios significativos del servicio.
- Se procederá a planificar y a verificar los cambios.
- Se valorarán los impactos potenciales, incluyendo impactos de seguridad de la información, debido a cambios.
- Se deberá documentar las aprobaciones formales de los cambios propuestos.
- Se verificará que los requisitos de seguridad de la información son conocidos.
- Se comunicará todos los detalles del cambio a todas las partes relevantes del servicio.
- Se establecerán procedimientos de marcha atrás, incluyendo procedimientos y responsabilidades para abortar, y recuperarse de un cambio no satisfactorio.

CGI revisa periódicamente todos sus sistemas y aplicaciones implicados en la gestión del Servicio con una periodicidad anual y, en todo caso, cuando se produzca cualquier cambio relevante que provoque un incidente de seguridad que afecte a los mismos.

Asimismo, revisará la Política de Seguridad y el inventario de los activos a intervalos planificados, como mínimo anualmente y, en todo caso, si se produjesen cambios significativos en la organización con el objetivo de mantener la idoneidad, adecuación y eficacia de los mismos. Cualquier cambio que afecte al nivel de seguridad deberá ser aprobado por la Dirección de CGI.

5.2 Política y Estándares de seguridad

Los estándares de seguridad CGI contienen reglas que promueven la implementación de políticas de seguridad de la empresa. Especifican las acciones o respuesta a un riesgo identificado y delimitan los controles para garantizar la protección de CGI y los activos de los clientes. Están alineados con el código de práctica ISO 27002 y Certificación ISO 27001.

Toda la documentación de ciberseguridad que se desarrolle en ejecución de los requisitos establecidos en este punto se gestiona, estructura y conserva conforme a los procedimientos documentados que CGI ha desarrollado teniendo en cuenta los estándares y normas técnicas nacionales e internacionales que apliquen en cada caso.

Se ha establecido un plazo mínimo de conservación del marco normativo y de las evidencias que sustentan el cumplimiento del mismo en materia de ciberseguridad de [3] años. Los criterios establecidos para la conservación de la documentación son los siguientes:

- Documentación relativa al marco de seguridad de la información del SGSI se conservará durante un periodo de “3” años.
- Documentación relativa al Servicio electrónico de Confianza de Entrega Electrónica Certificada se conservará durante un periodo de 15 años desde la finalización del servicio.

5.3 Definición

El detalle de estas políticas esta descrita en el siguiente documento.
https://intranet.ent.cgi.com/browse/sec/global/Documents/GS/CGI_GS_Security_Policies_and_Standards.pdf

6 Seguimiento, aprobación, publicación y revisión

El Comité de Seguridad debe aprobar las Políticas de Seguridad de la entidad, publicarlas y distribuirlas a todos sus empleados, así como a terceras partes que puedan verse involucrados en la implementación de los sistemas de información.

El responsable del SGSI y el responsable del Servicio correspondiente en lo que respecta a las políticas específicas de cada servicio, se encargarán de hacerla pública, manteniéndola siempre en los sistemas de CGI.

Las Políticas para la Seguridad de la Información y las políticas específicas de cada servicio deben revisarse a intervalos planificados, como mínimo anualmente y siempre que se produzcan cambios significativos en la organización, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

7 Documentación de referencia

- CGI policies and standards
- SMSI SBU
- Information Security
- PIMS
- ESMF and ISO (cgi.com)
- Third Party Management Framework | Management Foundation (cgi.com)
- Quality System | Management Foundation (cgi.com)
- Client Partnership Management Framework | Management Foundation (cgi.com)
- Client Satisfaction Assessment Program (CSAP) | Management Foundation (cgi.com)
- Human resources | Management Foundation (cgi.com)
- Security and Acceptable Use Policy
- Information Security Policy
- Information Classification Policy
- Business Continuity Policy
- Safety Policy
- Facilities and Physical Security Policy
- Declaración de Prácticas del Servicio Electrónico de confianza de Entrega Electrónica Certificada.

02876505X ALBERTO ANAYA (R: A81154197)

Digitally signed by 02876505X ALBERTO ANAYA (R: A81154197)
Date: 2025.11.26 10:47:30 +01'00'