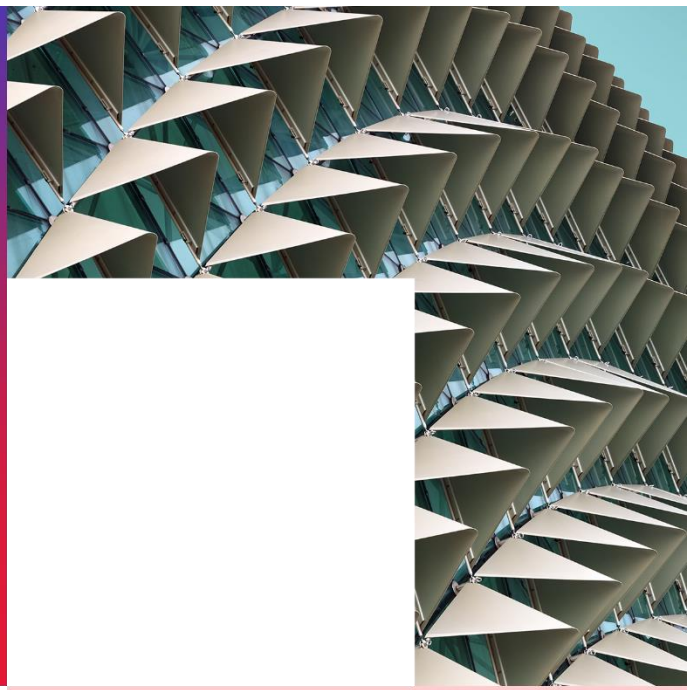


Política de Seguridad ENS

Tabla de contenidos

Control de versiones

Version	Autor	Descripcion	Fecha
1.0	José Tomás Vasco Morales	Versión Inicial	27/11/2023
1.1	José Tomás Vasco Morales	Revisión	08/01/2024
1.2	José Tomás Vasco Morales	Revisón NC	27/05/2024

1 Introducción

El objeto de este documento es definir el perímetro y límites del Sistema de Gestión de Seguridad de la Información.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

CGI establece como **objetivos de la seguridad** de la información los siguientes:

- Cumplir la legislación de seguridad y privacidad.
- Garantizar la calidad y protección de la información.
- Garantizar la prestación continuada de los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

Los sistemas TIC deben estar protegidos contra amenazas potenciales que puedan incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y valor de la información y los servicios. Para hacer frente a 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 se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos y la necesidad de realizar un seguimiento continuo que garantice la continuidad de los servicios prestados.

CGI debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos. Estableciendo así un Sistema integrado de Calidad y seguridad de la información en la manera de construir software y ofrecer servicios a las organizaciones con las que trabaja.

1.1. Prevención

CGI debe 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 se implementarán las medidas de seguridad determinadas por el ENS, RGPD y la LOPD, 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **CGI** debe:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en 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, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

1.3. Respuesta

- CGI Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **CGI** ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

2. Definición del alcance

Esta política de seguridad se aplica a todos los sistemas de información de CGI que den soporte a los siguientes servicios:

- Diseño, Desarrollo, mantenimiento y soporte de aplicaciones bajo especificaciones e infraestructura del cliente (este servicio incluye todo lo referente a toma de requerimientos, análisis, codificación, pruebas (en los entornos requeridos) y documentación de los trabajos solicitados en las modalidades de evolutivos y correctivos.
- Implantación, soporte y mantenimiento de sistemas en infraestructura del cliente (Este servicio incluye todos los trabajos necesarios para la puesta en marcha de una nueva plataforma y una vez en un entorno ya instalado y operativo se deberán realizar todas las tareas necesarias para mantener el entorno operativo (resolviendo cualquier incidencia que pueda aparecer), actualizado (tanto a nivel de versiones y parches y configurado (realizando los cambios en la configuración del sistema o datos de negocio o cualquier otro).

Quedan excluidos de este alcance los sistemas de información propiedad de la infraestructura de las propias administraciones públicas o de los clientes a los que se le presta alguno de los servicios incluidos en este alcance.

3. Misión y objetivos

CGI define esta política de seguridad de la información, de obligado cumplimiento para los empleados y empresas colaboradoras, marcando los objetivos fundamentales de garantizar la seguridad de la información y la prestación continua de los servicios que presta, las acciones preventivas, las actividades de seguimiento y la pronta reacción ante posibles eventos.

Esta política debe sentar las bases para que el acceso, uso, custodia y protección de los activos de información que CGI utiliza para el desempeño de sus funciones se realice de forma segura y garantice las medidas de seguridad dentro de las dimensiones indicadas en la adaptación al ENS:

- **Confidencialidad:** consecuencias de su revelación a personas no autorizadas o que no necesiten conocer la información.
- **Integridad:** consecuencia que tendría modificación por alguien no autorizado a modificar la información.
- **Disponibilidad:** tiempo de recuperación del objetivo (RTO) o tiempo de interrupción de referencia, que señala el tiempo máximo que el servicio puede estar interrumpido.
- **Autenticidad:** consecuencia que tendría que la información no fuese auténtica.
- **Trazabilidad:** consecuencia de no poder comprobar a posteriori quien ha accedido o modificado una cierta información.

Dentro de estas premisas, los objetivos específicos de CGI respecto a la seguridad de la información serán:

- Garantizar la seguridad de la información en los distintos aspectos mencionados anteriormente.
- Gestionar formalmente la seguridad de acuerdo con el proceso de análisis de riesgos.

- Elaborar, mantener y probar los planes de contingencia y planes de continuidad de negocio definidos para los diferentes servicios que presta la organización.
- Gestión adecuada de los incidentes que afecten a la seguridad de la información.
- Sensibilizar a todo el personal sobre los requisitos de seguridad y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar un nivel de seguridad acordado con terceros al compartir o transferir activos de información.
- Cumplir con las leyes y reglamentos vigentes.

Está Política de Seguridad:

- Deberá aprobarse formalmente por la organización.
- Se establece la necesidad de su revisión regularmente, con el objetivo que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite que se quede obsoleta.
- Se tiene que hacer extensible a todos los empleados y empresas externas qué trabajen con **CGI** dentro del alcance.

4. Marco normativo

CGI está sujeto a las leyes y reglamentos aplicables en materia de seguridad de la información, que es el siguiente:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- 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.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

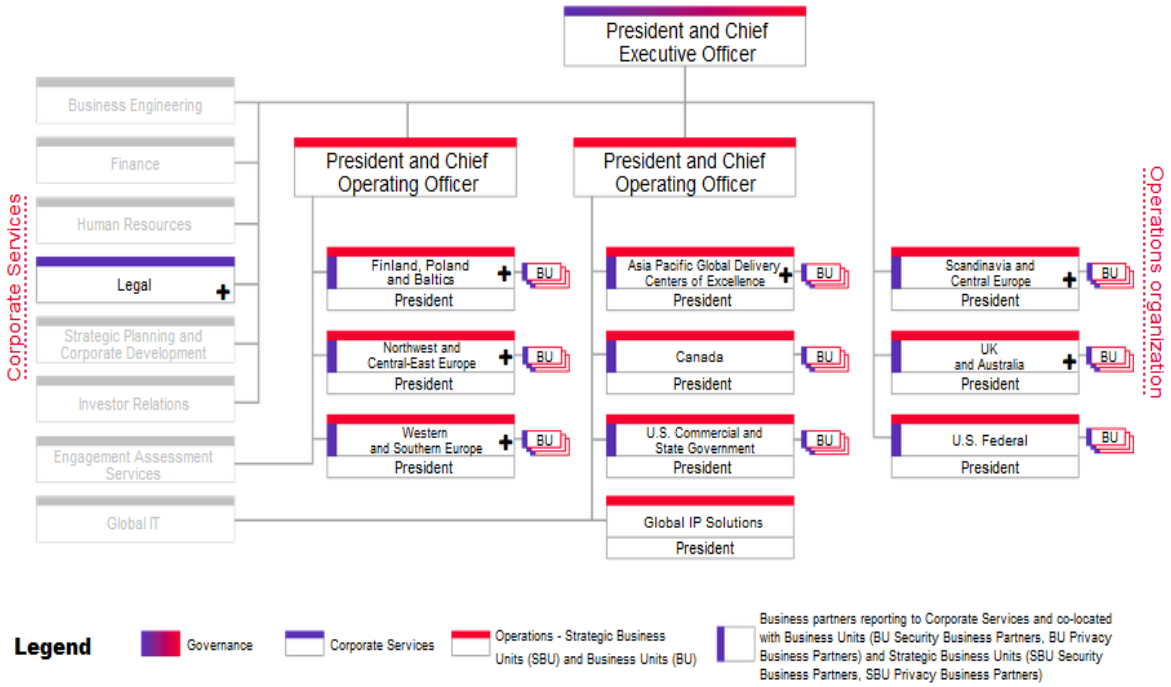
5. La organización

La seguridad y la privacidad de los datos son interdependientes.

La seguridad cubre la protección de los activos, incluidos los datos personales y los recursos que son vitales para las operaciones comerciales de CGI y para nuestros clientes, miembros y accionistas.

La privacidad de datos cubre el control del acceso y el uso de los datos personales del interesado (miembros de CGI, miembros de clientes y datos personales de los clientes). Las políticas de CGI están diseñadas para alinearse con las mejores prácticas de la industria, cumplir con nuestras obligaciones contractuales y cumplir o superar los requisitos de las leyes de privacidad de datos aplicables. Su organización es la siguiente:

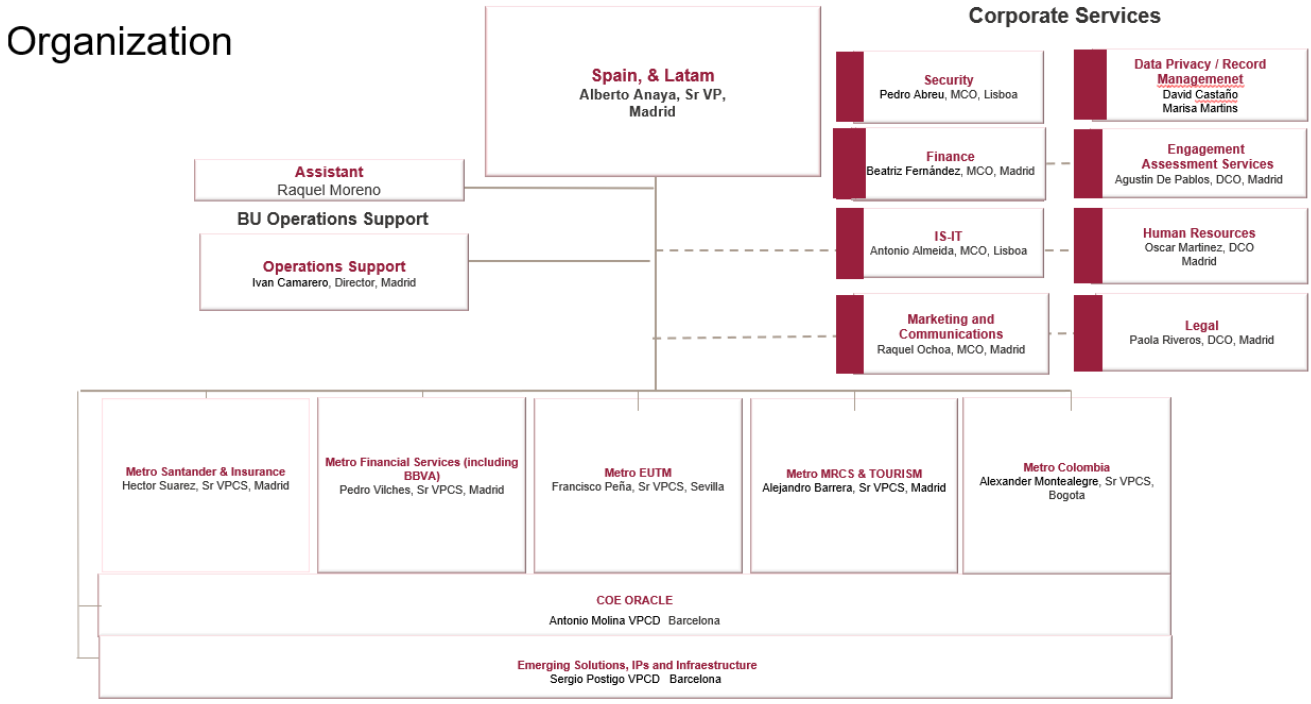
5.1. Organización global Seguridad y privacidad



5.2. Roles y Responsabilidades clave en Seguridad y Privacidad

Seguridad		Privacidad de datos	
Chief Security Officer (CSO)	La función de seguridad reporta al Vicepresidente Ejecutivo de Asuntos Legales y Económicos y al Secretario Corporativo, y proporciona la dirección y estrategias para supervisar el programa de seguridad de CGI.	**Chief Privacy Officer (CPO)**	Función de privacidad de datos que informa al Vicepresidente Ejecutivo de Asuntos Legales y Económicos, y al Secretario Corporativo, y proporciona la dirección y estrategias para supervisar el programa de privacidad de datos de CGI.
Security Centers of Expertise (COE)	Función corporativa que gestiona el programa, políticas, procesos de gobernanza y marco de gestión con el fin de administrar la seguridad a nivel global en CGI.	**Data Privacy Centers of Expertise (COE)**	Función corporativa que gestiona el programa, políticas y procesos de gobernanza con el fin de administrar la privacidad a nivel global en CGI.
Security Shared Services (SSS)	Su principal responsabilidad es proporcionar servicios de seguridad compartidos que satisfagan las necesidades y estándares comunes de seguridad de todas las Unidades Estratégicas de Negocio/Unidades de Negocio en la organización.	**Data Privacy Shared Services**	Función que proporciona servicios compartidos de privacidad de datos para respaldar las funciones corporativas de CGI junto con los sistemas y procesos asociados de CGI
Strategic Business Unit Security Business Partners (SBU SBP)	Punto central de contacto para la gobernanza y supervisión de la seguridad de CGI dentro de la Unidad Estratégica de Negocio, y apoyo a los contratos con clientes.	**Strategic Business Unit Privacy Business Partners***	Punto central de contacto para la gobernanza y supervisión de la privacidad de datos de CGI dentro de la Unidad Estratégica de Negocio, y apoyo a los contratos con clientes y al ecosistema de CGI.
Business Unit Security Business Partners (BU SBP)	Punto central de contacto para todas las implementaciones de seguridad dentro de la Unidad de Negocio.	**Business Unit Privacy Partners***	Custodios de la confidencialidad que promueven una mentalidad de respeto a la privacidad y trabajan para aplicar el programa de protección de datos.

5.3. Organización Funcional



6. Organización e implantación del proceso de seguridad

A nivel local, se implementa un plan de actividades regulares de manera mensual, que incluye programación de evaluaciones de brechas, análisis de riesgos, revisiones con la alta dirección, entre otras iniciativas. La frecuencia de las reuniones de los comités actuales es anual para la revisión de seguridad con la alta dirección y mensual para el comité local. Este enfoque estructurado garantiza una supervisión continua y eficiente de las medidas de seguridad, asegurando la alineación con los objetivos estratégicos y la capacidad de respuesta ágil ante cualquier cambio en el entorno operativo.

6.1. Comité: funciones y responsabilidades

Se han creado comités a nivel estratégico, táctico y operativo para garantizar el gobierno y la mejora continua de la seguridad dentro CGI. A nivel local, se ha creado un Comité de Gobernanza de la Seguridad. Se pueden agregar otros comités según sea necesario.

- Comité de revisión de seguridad de la alta dirección:

Presidido por el Líder de BU España, Italia y Latam o su representante, el Comité de Revisión de Seguridad de la Alta Dirección vela por la gestión táctica de las actuaciones realizadas por el equipo de seguridad.

Los objetivos del Comité son:

- Definir los objetivos del SGSI para cada año;
- Informar al Líder de BU y VP de los sitios certificados sobre las Evaluaciones de Seguridad; KPI de seguridad; Incidentes de Seguridad; Resultados de la auditoría de seguridad.
- Dar a las distintas partes interesadas la visibilidad necesaria sobre las acciones operativas.

Sus principales miembros son:

- El líder de la BU o su representante.
- Vicepresidentes de los sitios ISO27001 certificados.
- Quality Business Partner.
- Security business Partner (Gerente SGSI).
- Privacy Business Partner.

Ocasionalmente, si su contribución es necesaria, se invita a miembros de otros servicios de apoyo.

Este comité se reúne una vez al año, dos veces si es necesario. Las actas de estas reuniones se documentan y distribuyen.

- Comité SGSI:

Presidido por el Gerente de SGSI, el Comité de SGSI asegura la gestión de las acciones realizadas por el equipo de SGSI.

Los objetivos / funciones del comité son:

- Informar a la BU SBP de las opciones y decisiones estratégicas que pueden afectar la seguridad de los diferentes sites de CGI.
- Asegurar la coordinación, concertación, coherencia e integración de las acciones relacionadas con la seguridad.
- Dar a las distintas partes interesadas la visibilidad necesaria sobre las acciones operativas.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de **CGI** en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la organización.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de los responsables de área, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por **CGI** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de **CGI.** En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

Sus principales miembros son:

- Security Business Partner (Gerente SGSI).
- Privacy Business Partner.
- Local Risk Owner.
- Quality Business Partner.
- Operations Support (O.S.).
- IS / IT.
- GTO.

Ocasionalmente, se invita a miembros de otros servicios de apoyo si su contribución es necesaria.

La agenda de este comité puede incluir, pero no se limita a :

- Monitoreo de incidentes de seguridad del sitio.
- Seguimiento de indicadores – e-learning & workstations.
- Seguimiento de controles.

- Concientización y Comunicación.
- Seguimiento de acciones correctivas o de mejora.
- Despliegue de estándares y políticas de seguridad CGI en proyectos y a nivel de sitio.
- Monitoreo de Seguridad Física.

Este comité se reúne una vez al mes. Las actas de estas reuniones se documentan y distribuyen.

- Comité SGSI-ENS (marco ENS):

Para adaptarse al real decreto 311/2022 del 3 de Mayo por el que se regula el esquema nacional de seguridad, se acuerda la integración del comité ENS dentro del comité SGSI para el seguimiento de la seguridad de la información en el marco del ENS.

La integración implica la adaptación de los roles preexistentes a las responsabilidades definidas por el ENS. Así, los participantes del Comité SGSI ajustarán sus funciones a los roles específicos del ENS, abordando aspectos clave como la gestión de la información, el sistema, la seguridad y el servicio. Cabe destacar que las funciones y el alcance del servicio, así como las correspondientes figuras, ya están contemplados en el ámbito del Comité SGSI. Por lo tanto, estas responsabilidades se integran de manera coherente en el Comité ENS, asegurando una alineación efectiva con los requisitos y estándares del Esquema Nacional de Seguridad.

En el contexto de la integración del Comité ENS en el Comité SGSI, los roles específicos que asumen los participantes son los siguientes:

- **Responsable de Seguridad (RSEG)**: Security Business Partner.
- **Responsable del Servicio (RSERV)**: Director de Operations Support (O.S.).
- **Responsable de la Información (RSINFO):** Privacy Business Partner.
- **Responsable del Sistema (RSIS):** Manager del área de IS/IT.

La coordinación del comité estará a cargo del **Local Risk Owner.**

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Establecer y promover la estrategia y planificación de seguridad de la información, proponiendo asignaciones presupuestarias y recursos necesarios para su implementación.
- Analizar la Política de Seguridad de la Información y las responsabilidades principales, y presentar una propuesta para su aprobación al Órgano de Gobierno.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.

- Supervisión y seguimiento de aspectos tales como:
  - Elaboración y actualización de planes de continuidad.
  - Principales incidencias en la Seguridad de la información.
  - Cumplimiento y difusión de las Políticas de Seguridad.

6.2. Roles: funciones y responsabilidades

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

Responsable de Seguridad

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.
- Además, ver Tareas.

Responsable del Sistema

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.

- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Además, ver tareas.

6.3. Tareas

RINFO - Responsable de la Información.

RSERV - Responsable del Servicio.

RSEG - Responsable de la Seguridad

RSIS - Responsable del Sistema

Tarea	RINFO	RSERV	RSEG	RSIS	COMIT.SEG.	Organización
Hacer un registro de los tratamientos	responsable					
Garantizar el cumplimiento de los deberes de secreto y seguridad.	responsable					
Garantizar derechos LOPD/RGPD	responsable					
Determinación de los niveles de seguridad requeridos por la información	elabora		responsable		aprueba	
Determinación de los niveles de seguridad requeridos por el servicio		elabora	responsable		aprueba	
Determinación de la categoría del sistema	elabora	elabora	responsable			
Análisis de riesgos			elabora			aprueba
Declaración de aplicabilidad			elabora / Responsable			
Medidas de seguridad adicionales			elabora			
Configuración de seguridad			elabora	responsable		
Implantación de las medidas de seguridad			responsable			
Aceptación del riesgo residual			responsable			aprueba
Documentación de seguridad del sistema			elabora			
Política de seguridad					elabora	aprueba
Normativa de seguridad					elabora /aprueba	
Procedimientos operativos de seguridad			elabora			
Estado de la seguridad del sistema			valida		aprueba	
Planes de mejora de la seguridad			elabora	elabora	aprueba	
Planes de concienciación y formación			elabora		aprueba	
Planes de continuidad			valida	elabora	aprueba	
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios			valida	aprueba		

7. Procedimiento de designación

La asignación de responsabilidades conforme a la Política de Seguridad del ENS está a cargo de la Dirección.

Los roles clave incluyen el Responsable de Seguridad, el Responsable del Sistema, el Responsable del Servicio y el Responsable de la Información, todos reportando al Comité de Seguridad.

La Dirección ajustará estas asignaciones en caso de cambios organizativos, asegurando la coherencia con las responsabilidades establecidas en la política de seguridad.

8. Política de seguridad de la información

En CGI, la seguridad es un requisito obligatorio que es esencial para generar confianza con nuestros clientes, cumplir con nuestros requisitos contractuales y cumplir con las leyes, los reglamentos y las mejores prácticas comerciales en todas las jurisdicciones en las que operamos.

La seguridad está integrada en las operaciones diarias de CGI como parte de todo lo que hacemos y entregamos.

CGI protege los datos y sistemas de clientes, socios y sus empleados (“Miembros”) con el debido cuidado y diligencia, asegurando que la información y los sistemas estén protegidos contra amenazas, uso indebido o acceso no autorizado en todo momento.

CGI aprovecha un marco de gestión de seguridad empresarial (ESMF) basado en estándares industriales reconocidos (ISO 27001, NIST, COBIT, CIS, etc.) que se utiliza en toda la organización global para proteger CGI y los activos de información, tecnologías e instalaciones del cliente, así como Miembros y Accionistas de CGI. El ESMF está respaldado por las políticas, estándares y controles de seguridad de CGI (que comprenden su línea base de seguridad) y se implementa a través de nuestros procesos, prácticas, servicios y soluciones. Los requisitos ESMF son aplicables a terceros que trabajan en nombre de CGI. En virtud del ESMF, las medidas técnicas y organizativas se definen con un enfoque basado en el riesgo, en particular para tener en cuenta situaciones en las que CGI tiene la responsabilidad del procesamiento de datos personales.

La línea de base de seguridad de CGI es el estándar predeterminado que deben aplicar y acordar tanto CGI como los clientes. No obstante, en algunos casos, los clientes pueden acordar reforzar el nivel de seguridad para tener en cuenta requisitos específicos (riesgos, regulatorios, etc.) definiendo medidas de seguridad adicionales dentro de los servicios contratados de CGI.

Las secciones a continuación brindan información específica sobre cómo CGI organiza y opera su programa de seguridad para garantizar que los activos de información estén protegidos continuamente contra amenazas en evolución.

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

- CGI policies and standards
- SMSI SBU
- Information Security
- PIMS

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.

8.1. Datos de Carácter personal

La Ley Orgánica de Protección de Datos (LOPD) y el Reglamento General de Protección de Datos (RGPD) tienen como objetivo garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas en relación con el tratamiento de sus datos personales, especialmente su honor, intimidad y privacidad personal y familiar. Estas normativas son aplicables a los datos de carácter personal registrados tanto de forma informática como en soporte papel. Para asegurar el cumplimiento con estas normativas, se emplea un "Documento de Seguridad de la LOPD/RGPD", que detalla los tratamientos de datos personales realizados.

La evaluación continua de riesgos se centra en garantizar la privacidad en todas las interacciones y compromisos con los clientes, desde la gestión de proyectos hasta la prestación de servicios internos. Además, se evalúa la privacidad en las relaciones con terceros que colaboran. Estos procesos, complementados con una auditoría anual, permiten establecer con claridad la postura general frente a los riesgos de privacidad.

Además, se evalúan individualmente los riesgos que pudieran generarse de cada nuevo tratamiento de datos, utilizando el formulario "Data Privacy and Security Checklist" (DPSC) registrado en una herramienta propia. Esta evaluación ayuda a identificar riesgos y definir acciones para mitigarlos, asegurando así el cumplimiento con las regulaciones de protección de datos y la mejora continua de las prácticas de privacidad y seguridad.

8.2. Gestión de Riesgos

Todos los sistemas de información impactados por a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.

- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información que 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.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

El Responsable de Seguridad (RSEG) será responsable de la determinación de los riesgos residuales asociados a la información y servicios, incluyendo la aplicación de medidas de seguridad especificadas en el Anexo II del ENS.

Una vez identificados, los niveles de riesgo residual esperados serán presentados a la dirección para su validación y aprobación, asegurando así la conformidad con las decisiones estratégicas y la aceptación de los riesgos residuales asociados a la implementación de medidas de seguridad.

8.3. Desarrollo de la política de seguridad de la información

La Política de Seguridad de la Información será revisada, a propuesta del Comité de Seguridad de la Información.

Al menos una vez al año, el Comité de Seguridad de la Información incluirá entre los temas a discutir la revisión, actualización y propuestas de modificaciones de la Política de Seguridad.

La estructuración de la documentación del sistema, su gestión y acceso se encuentran detalladas en el procedimiento general ‘Quality System Management Process’.

8.4. Gestión de personal

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones, servicios e información.

Se requerirá la firma de un documento de seguridad por parte de todos los empleados en el que se establecen los principios básicos y obligaciones con respecto al tratamiento de información personal y al uso adecuado de los recursos de la compañía para prevenir la divulgación de información confidencial. Este documento también aborda temas como el intercambio seguro de información sensible, las prácticas de protección de datos personales, las medidas de seguridad física, los procedimientos para reportar incidentes de seguridad y la importancia de salvaguardar la información confidencial de la empresa.

Todos los empleados de CGI y los subcontratistas deben participar en el programa de formación obligatoria en materia de Conciencia de Seguridad. Este programa se realiza de forma continua con el propósito de asegurar que los empleados comprendan plenamente sus responsabilidades en materia de seguridad.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

8.5. Profesionalidad

La seguridad de los sistemas es gestionada y revisada por personal de CGI cualificado y personal externo especializado, asegurándose de recibir y mantener la formación necesaria para garantizar la seguridad de la información en todas las etapas del ciclo de vida de los sistemas de información: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento. CGI establece en todo caso los requisitos de cualificación (formación y experiencia) para asegurar la idoneidad del personal.

8.6. Autorización y control de los accesos

Se han definido políticas y estándares en materia de acceso a la información, redes y servicios. El control de acceso a los sistemas y la información se basa en los principios de “necesidad de conocer” y “mínimo privilegio”.

El acceso a los recursos de CGI está vinculado a las responsabilidades laborales y se revisa regularmente para detectar cualquier cambio y garantizar que los accesos estén alineados con las funciones asignadas a cada empleado.

8.7. Protección de las instalaciones

Los sistemas de CGI y su infraestructura de comunicaciones están alojados en áreas debidamente protegidas, equipadas con medidas de seguridad física, redundancia, continuidad y ambientales. Se implementa un estricto procedimiento de control de acceso físico.

8.8. Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos, CGI tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, 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.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional determinará los siguientes aspectos:

- Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- Otras certificaciones de seguridad adicionales que se requieran normativamente.
- Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el punto 8.5.

8.9. Mínimo privilegio

En CGI los sistemas se diseñan y configuran siempre pensando en la Seguridad por Defecto. El sistema proporciona la mínima funcionalidad requerida para que las funciones de operación, administración y registro de actividad sean las mínimas necesarias y se asegura que sólo son accesibles por las personas, y desde emplazamientos o equipos autorizados. Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario. Para ello, se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

8.10. Integridad y actualización del sistema

En CGI los sistemas se evalúan de manera periódica para conocer en todo momento su estado de seguridad, tomando en consideración las especificaciones de los fabricantes, las vulnerabilidades, las deficiencias de su configuración, las actualizaciones que procedan y la detección temprana de incidentes, gestionando de esta manera la integridad de los mismos. Todos los elementos de los sistemas requieren autorización previa a su instalación.

8.11. Protección de la información almacenada y en tránsito

La información se clasifica de acuerdo con la sensibilidad requerida en su tratamiento y según los niveles de seguridad y protección exigibles, según lo detallado en las Políticas y Normas de CGI.

Los requisitos de encriptación de CGI se basan en la sensibilidad de la información y en la exposición potencial al riesgo.

Para garantizar la seguridad de la información en todos los aspectos de su procesamiento y transmisión, CGI aplica diversas medidas de encriptación, incluyendo:

- Encriptación de discos completos en todos los dispositivos portátiles.
- Encriptación de medios portátiles en todos los equipos de escritorio.
- Encriptación de todos los dispositivos móviles.
- Encriptación de conexiones de acceso remoto utilizando SSL o IPsec.
- Encriptación SSL para acceso a aplicaciones.
- Establecimiento de interconexiones comerciales con terceros a través de redes encriptadas.
- Encriptación de todas las redes Wi-Fi de CGI con WPA2 y AES.
- Encriptación de correos electrónicos intercambiados con clientes y socios a nivel de servidor utilizando TLS.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

8.12. Prevención ante otros sistemas de información interconectados

CGI protege el perímetro de su sistema de información, especialmente en conexiones a redes públicas, reforzando la prevención, detección y respuesta a incidentes de seguridad. Se analizan y controlan los riesgos de interconexión con otros sistemas para garantizar un nivel de seguridad adecuado. Las zonas de red están definidas con reglas que aseguran controles de acceso, autenticación y encriptación, y la segregación del tráfico mantiene la confidencialidad, integridad y autenticidad de la información según los estándares de la industria.

Las redes de clientes están aisladas de la red de CGI y de otras redes de clientes. Los accesos administrativos a las redes de clientes se realizan a través de pasarelas seguras con encriptación y autenticación de dos factores. Las interconexiones con terceros se establecen a través de redes privadas o encriptadas usando IPsec, y los datos sensibles transmitidos por redes no confiables están encriptados.

Todos los sistemas de acceso remoto utilizan encriptación (SSL o IPsec), requieren autenticación de dos factores y limitan el acceso a individuos autorizados. Las redes Wi-Fi de CGI están encriptadas por defecto (WPA2 con encriptación AES) y requieren autenticación adecuada. Las redes de CGI son monitoreadas para detectar ciberamenazas mediante tecnologías avanzadas como detección y prevención de intrusiones, análisis de comportamiento y detección de amenazas avanzadas, supervisadas por el Centro de Operaciones de Seguridad Global de CGI.

Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

.

8.13. Registro de la actividad y prevención de código dañino

CGI ha habilitado registros de la actividad del usuario al retener la información estrictamente necesaria para monitorear, analizar, investigar y documentar actividades inadecuadas o no autorizadas, permitiendo identificar en todo momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, se podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

9. Obligaciones del personal

Todos los miembros de **CGI** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **CGI** recibirán concienciación en materia de seguridad 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.

10. Terceras partes

Cuando **CGI** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad 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 partícipe 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.

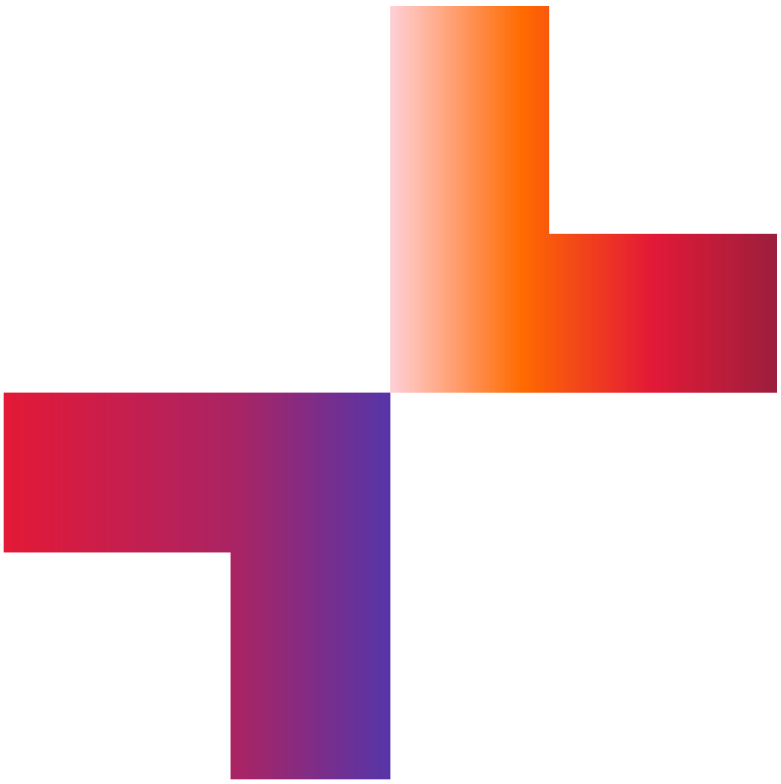
Documento: Política de Seguridad ENS

Estado: Aprobado

Firmado: Fdo. Alberto Anaya Reig (Spain BU Lider)

02876505X
ALBERTO ANAYA
(R: A81154197)

Firmado digitalmente por
02876505X ALBERTO
ANAYA (R: A81154197)
Fecha: 2024.05.30
17:50:10 +02'00'



cgi.com

CGI