Política de Seguridad Corporativa

OMC ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA | CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

Aprobado por la Comisión Permanente el 19/07/2018

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Histórico de cambios

Versión	Fecha	Descripción acción	Páginas
1.0	25/09/2012	Creación del documento	*Todas*
1.1	17/05/2017	Actualización documentos	*Todas*
2.0	24/05/2018	Adaptación al ENS	*Todas*

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

ÍNDICE

Plaza de las Cortes,11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

1 INTRODUCCIÓN

1.1 JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Consejo General de Colegios Oficiales de Médicos de España (en adelante CGCOM) concibe la información como un activo estratégico y la seguridad de esta información como un valor prioritario. Las dependencias de CGCOM con respecto de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, requieren que los sistemas de información deban ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada y de los servicios prestados.

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.

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 las diferentes áreas de CGCOM deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS, en adelante) y por estándares de seguridad de la información como ISO 27001, 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 garantizar la continuidad de los servicios prestados.

Todas las áreas 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 de sistemas y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en las propuestas de licitación para proyectos de TIC. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

Plaza de las Cortes,11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Por este motivo, la Dirección de CGCOM ha decidido desarrollar y adoptar una Política de Seguridad de la Información que sea el principal instrumento sobre el que vertebrar la seguridad, incluyendo una serie de medidas para proteger la información de la Organización, en las que la seguridad no se contempla como un estado, sino como un proceso.

1.2 MISIÓN Y SERVICIOS PRESTADOS

CGCOM, como órgano que agrupa, coordina y representa a todos los Colegios Oficiales de Médicos a nivel estatal, tiene la condición de Corporación de Derecho Público con personalidad jurídica propia y plena capacidad en el cumplimiento de sus fines. La presentación completa de CGCOM, de su estructura, funcionamiento y servicios se encuentra en el Portal web www.cgcom.es.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa CGCOM a través de medios electrónicos, y en particular a los trámites y servicios identificados en dicho Portal web corporativo.

2 OBJETIVOS

El objetivo principal de esta Política es establecer las directrices y principios establecidos por CGCOM para garantizar la protección de la información y los recursos de tratamiento de la misma, así como el cumplimiento del resto de los objetivos de seguridad definidos, los cuales se indican a continuación:

- Considerar la seguridad como un medio fundamental para la consecución de los objetivos estratégicos de la Organización.
- Involucrarse en la decisión de los aspectos estratégicos de la seguridad de manera que estén alineados con los objetivos de negocio.
- Proporcionar los medios y recursos necesarios para la consecución de los objetivos de seguridad establecidos.
- Promover la adecuación de la Organización a los requerimientos legales, reglamentarios y contractuales que resulten aplicables.
- Impulsar la definición, desarrollo e implantación de los controles técnicos y organizativos que resulten necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por CGCOM.

Plaza de las Cortes,11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

- Crear una "cultura de seguridad", formando adecuadamente a todo el personal de CGCOM e implicando a los clientes, proveedores y colaboradores.

- Considerar la seguridad de la información como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más avanzados.

3 MARCO NORMATIVO

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades de CGCOM en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el cual fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de información.

- Real Decreto 951/2015, de 23 de octubre, de modificación del Esquema Nacional de Seguridad.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, en lo que se refiere a las medidas de seguridad técnicas y organizativas a implantar.

- Ley 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (LOPD en adelante), la cual tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

- 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).

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Además, se han tenido en consideración los requisitos en materia de seguridad de:

- Norma ISO 27001 para la Gestión de la Seguridad de la Información.
- Estándar ISO 27002 de buenas prácticas para la Gestión de Seguridad de la Información.
- Norma ISO 22301 para la Gestión de la Continuidad de Negocio.

4 ÁMBITO DE APLICACIÓN

Esta política es de obligado cumplimiento a todo empleado, colaborador o proveedor que disponga de acceso a información del CGCOM en cualquier soporte o formato.

5 ORGANIZACIÓN DE LA SEGURIDAD

Tal como indica el artículo 12 del ENS, La seguridad deberá comprometer a todos los miembros de la organización. La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. Se establecen por tanto los siguientes roles en la organización relacionados con la Seguridad de la Información.

5.1 ROLES Y RESPONSABILIDADES

A continuación, CGCOM ha definido los siguientes roles:

- Responsable de la Información
- Responsable de Servicio
- Responsable de Seguridad de la Información
- Responsable del Sistema

5.1.1 Responsable de la Información

El Responsable de la Información es habitualmente una persona u Órgano que ocupa un alto cargo en la dirección de la organización. Corresponde al nivel de

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Alta Dirección, que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde que éstos se alcancen. Sus funciones pueden ser asignadas a personas individuales, o bien ser asumidas por un Comité.

En línea con lo establecido en el punto anterior, se propone que esta condición recaiga en la Comisión de Coordinación de CGCOM.

Al responsable de la Información le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

- Responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

5.1.2 Responsable de Servicio

Puede corresponder al nivel de un órgano de gobierno de máximo nivel, al igual que el Responsable de la Información, o bien al de una Dirección Ejecutiva, que entiende qué hace cada departamento, y cómo los Departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.

Se propone que esta condición recaiga en cada uno de los Responsables de los Servicios afectados por el Esquema Nacional de Seguridad.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Sus funciones podrán ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información. La tabla a continuación define los Responsables por cada Servicio objeto de alcance:

Servicio	Responsable del Servicio
Gestión Electrónica Fundación para la Protección Social	Fundación para la Protección Social de la OMC
Registro de Médicos Colegiados	Secretaría General
Registro de Médicos Colegiados del CACM	Comisión Coordinación
Directorio de Médicos en Ejercicio Privado	Vocalía de Médicos de Ejercicio Privado
Gestor de Firma	Comisión de Coordinación
Certificados Electrónicos Administrativos	- Internacional - Área Profesional - Fundación para la Formación de la OMC
Certificados Electrónicos Médicos	Comisión de Coordinación
Receta Médica Papel	Comisión de Coordinación
Receta Dentistas	Comisión de Coordinación
Receta Podólogos	Comisión de Coordinación
Registro E/S	- Secretaría General - Área Profesional - Fundación para la Formación de la OMC - Fundación para la Cooperación Internacional de la OMC - Fundación para la Protección Social de la OMC
Ventanilla Única	- Secretaría General - Asesoría Jurídica
eColegio	- Comisión de Coordinación
Observatorio Pseudociencias	Responsable del Observatorio
Custodia de Certificados de Defunción en soporte papel	Comisión de Coordinación
Portal CGCOM	Comisión de Coordinación
Plataforma VPC	Área Profesional
Plataforma VPC-R	Área Profesional

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

Campus Virtual de Aprendizaje	Fundación para la Formación de la OMC
Registro de Cooperantes	Fundación para la Cooperación Internacional de la OMC
Acreditación de Páginas Web	Área Profesional
Acreditación de Actividades Formativas	Área Profesional
Diario Médicos y Pacientes	Comunicación
Portales Web Institucionales	Comunicación

Las funciones del Responsable de Servicio son las siguientes:

- En cuanto a la legislación en materia de protección de datos personales y privacidad, el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su Departamento en concreto, y en particular en lo relacionado con el soporte papel.

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información para sus servicios dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.

- Responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.

- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como en su caso otros como accesibilidad, interoperabilidad, etc.

5.1.3 Responsable de Seguridad de la Información

Corresponde al nivel de una Dirección en Tecnologías de la Información. Se nombrará formalmente como Responsable de Seguridad de la Información, por parte del órgano de gobierno, a una única persona en la organización. El rol no podrá ser desarrollado por un órgano colegiado, ni podrá haber más de una

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

persona asumiendo el rol en la organización, aunque pueda delegar parte de sus funciones en otras personas.

En este sentido, se propone designar como Responsable de Seguridad de la Información al Director del Departamento Tecnológico.

Al Responsable de Seguridad le corresponden las siguientes funciones:

- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la presente Política de Seguridad.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
- Realizará el Análisis de Riesgos de Tecnologías de la Información.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por Dirección.
- Aprobará los procedimientos y normativas relativos a la seguridad de la información.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo al que está expuesto el sistema).

- Elaborará, junto al Responsable del Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.

- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.

- Validará los Planes de Continuidad y Planes de Contingencias, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable del Sistema.

- Aprobará las directrices propuestas por el Responsable del Sistema para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

5.1.4 Responsable del Sistema

El Responsable del Sistema es la persona que se encarga de la explotación del sistema de información. Corresponde al nivel de una Dirección Operativa. Se debe nombrar formalmente como tal a una única persona. El rol no podrá ser desarrollado por un órgano colegiado, aunque pueda delegar parte de sus funciones en otras personas.

En este sentido, se propone designar como Responsable del Sistema al Encargado de Administración de Sistemas.

Al Responsable del Sistema le corresponden las siguientes funciones:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.

- Aplicar los procedimientos operativos y las normativas de seguridad.

- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

- Elaborar los Planes de Continuidad y Planes de Contingencias para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.

- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

5.2 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Es el órgano que coordina la Seguridad de la Información a nivel de organización. Las funciones del Comité de Seguridad se llevarán a cabo por parte de la **Comisión de Coordinación de CGCOM**.

Siempre que sea posible deberá asumir las siguientes funciones:

- Responsabilidades derivadas del tratamiento de datos de carácter personal.

- Asunción de la figura de Responsable de Servicio para los servicios prestados en el marco del ENS.

- Asunción de la figura de Responsable de la Información para todas las informaciones manejadas por los servicios prestados en el marco del ENS.

A requerimiento del Comité se convocará cualesquiera otros Jefes de Departamento y responsables, cuya intervención sea precisa por ser afectados

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

por el Esquema Nacional de Seguridad y por la legislación vigente en materia de protección de datos.

Corresponde al Secretario/a del Comité de Seguridad de la Información:

- Convocar las reuniones del Comité de Seguridad de la información
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

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

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de CGCOM en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas 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 Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

- Monitorizar los principales riesgos residuales asumidos por CGCOM y recomendar posibles actuaciones respecto de ellos.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad 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 CGCOM. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

- Velar para que 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 y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- Recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.

- Se asesorará de los temas que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

  - Grupos de trabajo especializados internos, externos o mixtos.
  - Asesoría interna y/o externa.
  - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

- Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente, en caso de ocurrencia de incidentes de seguridad de la información.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

5.3 JERARQUÍA EN EL PROCESO DE DECISIONES Y MECANISMOS DE COORDINACIÓN

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la presente Política.

El Responsable del Sistema:

1. Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

2. Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

3. Da cuenta al Responsable de la Seguridad:

    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
    - Resumen consolidado de los incidentes de seguridad.
    - Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad:

1. Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

2. Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

3. Da cuenta al Comité de Seguridad de la Información, como secretario:

    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

6 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en su Artículo 6.

6.1 CRITERIOS DE EVALUACIÓN DE RIESGOS DE TI

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios detallados de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, aquellos riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

6.2 DIRECTRICES DE TRATAMIENTO

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

6.3 PROCESO DE ACEPTACIÓN DEL RIESGO RESIDUAL

Los niveles de riesgo residual serán determinados por el Responsable de Seguridad de la Información, y presentados por éste al Comité de Seguridad de la Información, para que proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

6.4 NECESIDAD DE REALIZAR O ACTUALIZAR LAS EVALUACIONES DE RIESGOS

El análisis de los riesgos y su tratamiento posterior deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

7 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para garantizar la consecución de los objetivos de seguridad establecidos, se han desarrollado normativas y procedimientos de seguridad, en los que se detallan las medidas técnicas, organizativas y de gestión necesarias para garantizar el cumplimiento de las directrices establecidas en la presente Política.

Estas normativas y procedimientos deberán mantenerse actualizados y se revisarán de forma periódica, para garantizar su adecuación a las necesidades específicas de CGCOM.

8 OBLIGACIONES DEL PERSONAL

Los miembros de CGCOM tienen la obligación de conocer y cumplir las Políticas de seguridad de la información, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los interesados.

Los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a los miembros de la organización, en particular a los de nueva incorporación.

Plaza de las Cortes,11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

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.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

9 TERCERAS PARTES

Cuando CGCOM 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 de la Información y se establecerán procedimientos de actuación conjuntos para la reacción ante incidentes de seguridad.

Cuando CGCOM utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad de la Información 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 esta Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se solicitará un informe del Responsable de Seguridad que concrete los riesgos en que se incurre y la forma de tratarlos. Será necesaria la aprobación de este informe por parte de los responsables de la información y los servicios afectados, previamente al uso de los servicios de terceros o cesión de información a los mismos.

10 REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.