Política de Seguridad Corporativa de ICM

DIRECCIÓN DE SEGURIDAD CORPORATIVA

Agencia de Informática y Comunicaciones de la Comunidad de Madrid

VICEPRESIDENCIA, CONSEJERÍA DE CULTURA Y DEPORTE Y PORTAVOCÍA DEL GOBIERNO
Comunidad de Madrid

DATOS GENERALES DEL DOCUMENTO

Tipo: Política
Código: GN-SEGR-02
Versión: 0.8
Título: Política de Seguridad Corporativa de ICM
Origen: Cuerpo Normativo de Seguridad Corporativa ICM

OBJETO

La Política de Seguridad Corporativa de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid (ICM) tiene como objeto establecer el marco de seguridad necesario para garantizar la capacidad de ICM para atender eficazmente con sus obligaciones corrientes con la Comunidad de Madrid, a través de sus servicios y sistemas.

Será aplicada por ICM para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios automatizados o manuales que gestione ICM en el ejercicio de sus competencias, alcanzando al *personal*; a *la información*; a todas *las instalaciones, recursos y procesos* utilizados para la prestación de servicios.

El presente documento de política persigue el cumplimiento de las siguientes directrices de seguridad:

- Establecer los requisitos de seguridad de obligado cumplimiento para el personal interno y externo a ICM, así como los activos de su propiedad o custodiados por ICM.
- Estructurar un marco de gestión y organización de la seguridad, donde se asignen responsabilidades y tareas relacionadas con la seguridad.
- Establecer el alcance de los controles que se precisan para cumplir con las necesidades de seguridad a nivel corporativo.
- Impulsar el establecimiento sistemas de gestión de seguridad de la información para los procesos de ICM.

ALCANCE

El alcance de esta Política de Seguridad comprende a todo *el personal* de ICM así como a contratistas y terceros con acceso a los activos propiedad de ICM o bajo su responsabilidad; a *la información* tratada, almacenada y custodiada desde ICM; a todas *las instalaciones, recursos y procesos* utilizados para la prestación de servicios a la Comunidad de Madrid, sean estos internos o vinculados con terceros a través de acuerdos o contratos.

CONTENIDO

PRINCIPIOS BÁSICOS

Los principios básicos de la seguridad corporativa de ICM son:

a) Seguridad integral.

b) Gestión de riesgos.

c) Prevención, reacción y recuperación.

d) Líneas de defensa.

e) Reevaluación periódica.

La seguridad como proceso integral. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

La aplicación de esta política estará presidida por este principio, que incluye contemplar la seguridad como un proceso y no como un hito o incidente en el ciclo de vida de los servicios y sistemas.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la falta de organización, de coordinación o concienciación, sean fuentes de riesgo para la seguridad.

Gestión de la seguridad basada en los riesgos. El análisis y gestión de riesgos será considerado como parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de protección, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de protección.

Prevención, reacción y recuperación. La seguridad se estructurará de forma que impida que se produzcan acontecimientos o incidentes con consecuencias negativas para la misma, mediante la aplicación de planteamientos preventivos, desarrollo de mecanismos de reacción e implantación de sistemas de recuperación.

La prevención se basará en medidas de disuasión de potenciales atacantes u otras que impidan que el incidente llegue a tener lugar o impidan su éxito.

Se establecerán mecanismos que detecten los incidentes que no hayan podido evitarse, de modo que se pueda reaccionar de forma rápida y eficaz ante los mismos.

Se han de tener previstas medidas que permitan la restauración de la información y los servicios para el caso que un incidente de seguridad inhabilite los medios habituales.

Los sistemas garantizarán la conservación de los datos, informaciones y servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos fiables que

generen objetos digitales auténticos y estables, y sean la base que posibilite la preservación del patrimonio digital.

Líneas de defensa. Los sistemas han de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Evaluación periódica. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

ROLES Y FUNCIONES EN EL CICLO DE VIDA DE SERVICIOS Y SISTEMAS

ICM ha organizado su modelo productivo en procesos TI, dentro de los cuales la seguridad es parte inseparable e imprescindible.

Por ello, las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas (diseño, instalación, mantenimiento, operación y explotación, gestión de incidencias y desmantelamiento), acompañadas de los correspondientes procedimientos de control.

ICM, a través de la Dirección competente en materia de Seguridad Corporativa, *establecerá los requisitos de seguridad* que deban cumplir los servicios y sistemas, y establecerá los mecanismos de control para garantizar de forma real y efectiva el cumplimiento.

ICM, a través de las Direcciones de ICM responsables de los procesos productivos de ICM que garantizan el ciclo de vida de los servicios y sistemas, *implementará y velará por la efectiva aplicación* de esta Política, de los controles de seguridad técnica y organizativa derivados de ésta, de los Planes de Seguridad de ICM y de la Normativa de Seguridad.

Se habilita a la *Subdirección General de Secretaría General* para establecer el flujo de autorizaciones para la aprobación de la normativa y procedimientos que por su naturaleza o singularidad se haga necesario, por motivo de urgencia o necesidad, a fin de establecer un marco de seguridad que garantice la capacidad de ICM para atender eficazmente sus obligaciones corrientes con la Comunidad de Madrid, a través de sus servicios y sistemas.

ORGANIZACIÓN DE LA SEGURIDAD CORPORATIVA DE ICM

ICM ha definido y establecido una organización de seguridad con la misión de definir, implementar, gestionar, mantener y garantizar la seguridad corporativa de sus activos (información, personas y patrimonio).

Esta organización constará de las siguientes figuras:

Consejero-Delegado de ICM. Es el propietario de la presente Política de Seguridad Corporativa.

e impulsor de su cumplimiento. Para facilitar y asegurar la correcta implantación de la política de seguridad, facilitará los medios técnicos y humanos bajo los criterios de eficiencia y racionalización, y aprobará la Política y Normativa de Seguridad de ICM.

Secretaría General. Es la Subdirección General de ICM que tiene atribuidas las funciones de vigilancia y control del cumplimiento normativo u organizativo de la seguridad en ICM, y a cuyo fin depende *orgánicamente* la Dirección de Seguridad Corporativa y *funcionalmente* las distintas unidades organizativas de ICM responsables de los procesos productivos de ésta, en lo que afecta a la seguridad.

Dirección de Seguridad Corporativa de ICM. Es la Dirección de ICM que se configura como responsable funcional del proceso de seguridad corporativa de ICM, que tiene encomendadas las funciones de *elaboración y propuesta de políticas y normativas de seguridad, definición de los planes de acción y requisitos para su implantación, la medición de su efectividad y la planificación de acciones de mejora* respecto de la seguridad técnica y organizativa de la información que sea propiedad o custodiada por ICM, del personal interno y externo de ICM, sus instalaciones, y de los recursos de procesamiento de dicha información.

Comité de Gestión de la Seguridad Corporativa. El Comité de Gestión de Seguridad Corporativa se establecerá como máximo órgano consultivo y de apoyo a la gestión en materia de seguridad corporativa en ICM.

La Presidencia del Comité será ocupada por el titular de la unidad organizativa con responsabilidad en materia de Secretaría General de ICM, y como Secretario el titular de la unidad organizativa con responsabilidad en materia de Seguridad Corporativa. Ambos cargos serán designados por resolución del Consejero-Delegado de ICM.

En particular, se responsabilizará de *implementar y velar por la efectividad de la normativa de seguridad corporativa de ICM, de aprobar los procedimientos y guías o instrucciones técnicas de seguridad elaboradas y propuestas por cada Dirección gestora, planificar anualmente el Programa de Actuación de Seguridad y priorizar sus planes de acción y los requisitos para su implantación, así como proponer los medios de gestión materiales y humanos adecuados para su buen fin*.

Lo conformarán de modo permanente los titulares de las Direcciones de Coordinación, así como de las Direcciones competentes en materia de seguridad corporativa, de relaciones laborales, de infraestructuras y comunicaciones, desarrollo y mantenimiento de aplicaciones, sistemas y servicios en red, de sistemas de información corporativos, régimen jurídico y de contratación administrativa.

Podrán participar a criterio de este Comité cualesquiera otras Direcciones de modo no permanente cuando proceda tratar asuntos de competencia o responsabilidad, y especialmente, los titulares de las Direcciones de Servicio de ICM ante la Comunidad de Madrid.

Direcciones de Servicio de ICM ante la Comunidad de Madrid. Los titulares de las Direcciones de Servicio a continuación relacionadas, representarán a ICM ante la Comunidad de Madrid, recibiendo el soporte y coordinación interna necesaria de la Dirección competente en materia de Seguridad Corporativa:

a) En materia de Servicios a la Consejería con competencias en la gestión de los fondos de

ayuda a política agraria común.

b) En materia de Servicios a la Consejería con competencia en la determinación de los Criterios generales de seguridad en los sistemas de información procesales al servicio de la Administración de Justicia.

c) En materia de Servicios a la Consejería con competencia en Administración Electrónica.

d) En materia de Servicios a la Consejería con competencia en sistemas de información para el Ámbito Sanitario.

CONTROLES DE SEGURIDAD

Seguidamente se establece las medidas y controles de seguridad que ICM deberá implementar para gestionar las necesidades de seguridad de la información propiedad o custodiada por ICM, del personal interno y externo de ICM, las instalaciones de ICM y de los recursos de procesamiento de dicha información.

Política de seguridad. ICM ha elaborado la presente Política de Seguridad Corporativa en cuyo contenido se proporciona las directrices para gestionar y soportar la seguridad del personal, los activos y la información bajo la responsabilidad de ICM. Para su desarrollo, se definirá la "Normativa" que contendrá el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido, y la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias, así como los "Procedimientos y Guías Técnicas" para contemplar el cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

Organización de la seguridad. ICM establecerá una organización de seguridad que permita gestionar la seguridad de la información dentro de la organización y mantenga la seguridad de la información y de los recursos de procesado de la información que son tratados o gestionados por terceros. A tal fin, se ha definido una estructura organizativa de la función de la seguridad de ICM.

Gestión de los recursos humanos. ICM establecerá medidas de seguridad ligadas con el personal propio en las etapas correspondientes al antes, durante y después del cese del empleo o cambio de puesto de trabajo. Estas medidas también se extrapolarán a los contratistas que participan en los servicios prestados por ICM.

Gestión de terceros. ICM establecerá medidas de seguridad destinadas a mitigar el riesgo que suponen los accesos por parte de terceros a información, sistemas o instalaciones propiedad de ICM o bajo su responsabilidad.

Gestión de activos y clasificación de sus riesgos. ICM definirá e implantará las medidas y procesos necesarios para mantener un análisis y gestión de riesgos de seguridad en el diseño de sus sistemas y activos, asignándole a cada uno de ellos un administrador o gestor para establecer y mantener una protección adecuada de los mismos.

Seguridad patrimonial y de personas. ICM establecerá e implementará en las instalaciones donde almacena, custodia o procesa información, las medidas de seguridad patrimonial necesarias para prevenir los accesos no autorizados, daños e interferencia a las instalaciones y a

la información, robos, daños o circunstancias que pongan en peligro a las personas o los activos o provoquen la interrupción de las actividades o el servicio.

Continuidad, recuperación y respaldo. *P*ara asegurar la disponibilidad de los servicios y sistemas de información, ICM diseñará e implantará Planes de Continuidad de Servicio que eviten las interrupciones de las actividades de la organización y garanticen ante una contingencia la reanudación de los servicios y sistemas de información en un nivel y tiempo preestablecido.

Criptografía. ICM definirá e implantará las medidas y procesos necesarios para el uso de controles criptográficos en los sistemas y aplicaciones bajo su responsabilidad.

Internet y correo. ICM desarrollará e implementará las medidas y procesos necesarios en materia de seguridad para proteger sus comunicaciones a través de correo electrónico y la conexión de sus sistemas a Internet.

Protección frente a software dañino. ICM desarrollará e implementará las medidas y procesos necesarios en materia de seguridad para proteger sus sistemas de información ante cualquier tipo de software que pudiera realizar actividades maliciosas en los mismos y poner en riesgo la confidencialidad, integridad y disponibilidad de la información o servicios provistos por dichos sistemas.

Adquisición, desarrollo y mantenimiento de sistemas de información. ICM definirá y aplicará los aspectos y requisitos de seguridad necesarios para el tratamiento correcto de las aplicaciones durante las etapas de desarrollo y mantenimiento. Se definirán e implantarán medidas para: garantizar que la seguridad se integra en los sistemas de información; evitar errores, perdidas o usos indebidos durante el tratamiento de la información; garantizar la seguridad de los archivos del sistema, mantener la seguridad del software y de la información de las aplicaciones, y reducir los riesgos de al explotación de vulnerabilidades técnicas publicadas.

Control de acceso lógico. ICM desarrollará e implementará las medidas y procesos necesarios en materia de seguridad para: controlar el acceso a la información, asegurar el acceso de los usuarios autorizados y prevenir el acceso no autorizado a los servicios en red y a los sistemas operativos.

Cumplimiento y auditoría. ICM definirá e implantará las medidas y procesos necesarios para garantizar el cumplimiento de las obligaciones legales, reglamentarias o contractuales. En la misma línea, se implementarán controles que aseguren que se cumplan las políticas y normas de seguridad de la organización y medidas para que los procesos de auditoría de los sistemas de información se consigan con la máxima eficacia y con las mínimas interrupciones.

Gestión de incidencias. ICM definirá e implantará procedimientos de gestión de incidencias que aseguren el que se notifican los eventos y debilidades de seguridad de la información de manera que sea factible emprender las acciones correctoras oportunas, y garantizar que se aplica con eficacia una gestión de incidencias de seguridad de la información.

Seguridad perimetral y de las comunicaciones. ICM aplicará aspectos de seguridad en las medidas y procesos requeridos para la gestión de comunicaciones y operaciones de los sistemas de información de su responsabilidad; de este modo se consigue: garantizar el funcionamiento correcto y seguro de los recursos de procesamiento de la información, mantener en nivel apropiado en la gestión de servicios por terceros, minimizar el riesgo de fallos de los sistemas, proteger la información contra código malicioso, mantener la integridad y disponibilidad de la

información, asegurar la protección de la información en redes y evitar las actividades de procesamiento de la información no autorizadas.

REQUISTOS DE SEGURIDAD DE OBLIGADO CUMPLIMIENTO

Para la correcta implementación y cumplimiento de la presente política de seguridad, es necesario aplicar los siguientes requisitos de seguridad de obligado cumplimiento.

- Para su correcta aplicación, esta Política de Seguridad Corporativa es aprobada por el Consejero-Delegado de ICM y posteriormente divulgada y comunicada entre todo el personal de ICM y personal externo afectado.
- Todo el personal de ICM, entidades u organizaciones externas y terceros que accedan, usen, gestionen, operen, desarrollen o mantengan activos o información propiedad o custodiada por ICM están sujetos al obligado cumplimiento con las directrices y normas de esta política de seguridad.
- Todos los sistemas de información explotados desde ICM son de su propiedad y por tanto su uso es profesional y restringido. Queda totalmente prohibido el tratamiento de dichos sistemas con otros fines diferentes a su uso oficial.
- La información deberá ser clasificada y tipificada, así como os sistemas de información o infraestructuras tecnológicas que procesen, almacenen o transmitan información, o las instalaciones que los contengan, debiendo ser categorizados en función a la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para atender eficazmente con sus obligaciones corrientes.
- Los servicios y sistemas deben ser evaluados desde el punto de vista de seguridad en el momento de su diseño o adquisición, así como antes de su paso al entorno de explotación o comienzo de su uso efectivo.
- Los proveedores de servicios con los que ICM mantenga relación contractual o convencional deberán conocer y aplicar la normativa de seguridad corporativa de ICM, estando sujetos a las directrices y revisiones de su aplicación que por parte de la Dirección de Seguridad Corporativa se determine.

REVISIÓN Y APROBACIÓN DE LA POLÍTICA Y NORMATIVA DE SEGURIDAD CORPORATIVA DE ICM.

La Dirección de Seguridad Corporativa de ICM revisará esta Política de Seguridad Corporativa y la Normativa de Seguridad de ICM a intervalos planificados o siempre que se produzca un cambio significativo en la organización, funciones o recursos de procesamiento de ICM, obteniéndose como resultado nuevas versiones del presente documento y de los relativos a la Normativa, siendo elevados al Consejero-Delegado para aprobación, previa revisión de la Secretaría General.

GLOSARIO DE TÉRMINOS Y DEFINICIONES

La relación de términos y definiciones que se utilicen en este documento se describen en el documento *GRAL-ICM-02 Glosario de términos y definiciones*.

DOCUMENTOS DE REFERENCIA

ISO/IEC 27002:2005 Código de prácticas para la gestión de seguridad de la información