Revisión: 0
Fecha publicación: 18.11.2022

POLÍTICA DE SEGURIDAD ESQUEMA NACIONAL DE SEGURIDAD (ENS)

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 1 de septiembre de 2021 por la Dirección.

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

2.INTRODUCCIÓN

CIUDAD DE LAS ARTES Y LAS CIENCIAS, en adelante CAC, depende entre otros, de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o 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 de forma rápida y eficiente frente a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes Direcciones y 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 y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación y en la solicitud de ofertas.

CAC debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1 PREVENCIÓN

CAC 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 debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y

responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, los departamentos del Área de Sistemas deben:

- 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.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple degradación hasta su detención, los servicios deben 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 regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los distintos departamentos del Área de Sistemas deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, el Área de Sistemas debe desarrollar planes de continuidad de los sistemas TIC como parte del plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de y a todo el personal de CAC, sin excepciones.

4. MISIÓN Y VISIÓN

Misión: Ofrecer a la sociedad unos contenidos culturales y de entretenimiento, innovadores y de calidad para su enriquecimiento intelectual y disfrute, en un conjunto arquitectónico vanguardista único en el mundo. Todo ello, buscando siempre satisfacer las necesidades y

expectativas de todos sus grupos de interés en general, y en particular de los valencianos.

Visión: En la Ciutat de les Arts i las Ciències perseguimos ser un referente a nivel internacional de:

- Divulgación cultural,
- Sostenibilidad y
- Turismo de Calidad

Y ser el espacio público de encuentro y ocio de los valencianos, todo ello, mediante una gestión excelente que se anticipe y adapte al cambio, basada en el aprendizaje y la innovación permanente.

Valores:

- ÉTICA en todas nuestras actuaciones. Integridad. Transparencia. Igualdad. Respeto mutuo.
- CONCIENCIA DE SERVICIO HACIA LA SOCIEDAD. El norte que guía nuestras actuaciones es la creación de valor con repercusión en la sociedad, en particular la valenciana, y en las empresas e instituciones vinculadas o afectadas por nuestra actividad, dado nuestro carácter de empresa pública.
- RIGOR CIENTÍFICO. Precisión en el desarrollo y divulgación de los contenidos de la Ciutat de les Arts i les Ciències.
- ORIENTACIÓN A NUESTROS VISITANTES. Conseguir la plena satisfacción de nuestros visitantes, tanto a nivel empresarial e institucional como a nivel individual.
- COMPROMISO SOCIAL Y MEDIOAMBIENTAL. Contribuimos al desarrollo sostenible en todas las actuaciones de la Ciutat de les Arts i les Ciències.
- INTERÉS POR LAS PERSONAS QUE INTEGRAN EL EQUIPO. Promovemos un clima de trabajo en equipo, integrado por personas comprometidas, y nos preocupamos por la igualdad, reconocimiento, crecimiento y desarrollo profesional.
- INNOVACIÓN Y MEJORA CONTINUA. El personal de La Ciutat de les Arts i les Ciències tiene que ser emprendedor, adoptando una actitud activa, dinámica e innovadora para la mejora continua y la creación de valor añadido. Se le pide implicación, trabajo en equipo y respeto a los valores de la organización.

5. MARCO NORMATIVO

CIUDAD DE LAS ARTES Y LAS CIENCIAS se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- El convenio colectivo aplicable, correspondiente a “Oficinas y Despachos”.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

- RD-ley 13/2012 de 30 de marzo, ley de cookies.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

El marco de referencia que da cobertura legal a este documento se establece en las siguientes secciones del Real Decreto 3/2010 de 8 de enero, modificado por el RD 951/2015 , por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS):

- ENS. Artículo 12. Organización e implantación del proceso de seguridad

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la empresa.

- ENS. Anexo II. Medidas de Seguridad Marco organizativo [org] Política de seguridad [org.1]

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Gestión de la Seguridad de la Información estará formado por la Coordinadora del Sistema Integrado de Gestión, el Director de Seguridad de la Información, el Responsable Técnico de seguridad de la información, y el personal del Área de Sistemas.

El Comité tiene las siguientes funciones:

- Revisar periódicamente la política de seguridad teniendo en cuenta los cambios en el entorno y en la infraestructura TIC de CAC y proponer al Responsable del Sistema de Gestión las modificaciones pertinentes en la misma.
- Mantener actualizadas las normativas de obligado cumplimiento en CAC
- Establecer planes de formación e información que garanticen que el personal de CAC conoce los riesgos en esta materia y sabe cómo minimizarlos.
- Organizar, de forma periódica las auditorías técnicas de seguridad para verificar el cumplimiento de las normativas. Definir el plan de vigilancia de las mismas actuando incluso con técnicas de ingeniería social para comprobar su cumplimiento.
- Velar por la eficacia y eficiencia de los controles y salvaguardas implantadas.
- Marcar las hipótesis de partida y el alcance para el desarrollo de auditorías técnicas de seguridad internas o externas en materia de seguridad (incluidas las auditorías bienales del Reglamento de Medidas de Seguridad de la LOPD)
- Analizar las incidencias de seguridad y escalar, si se considera oportuno, al Responsable del Sistema de Gestión o al responsable de área correspondiente, los incidentes que requieran actuaciones de índole interno ya sea en aspectos disciplinarios o de comunicación interna o externa.
- Revisar el análisis de riegos y comunicar los riesgos residuales para su aprobación y traslado al Responsable del Sistema de Gestión.
- Proponer al Responsable del Sistema de Gestión proyectos e iniciativas diseñados para minimizar el nivel de riesgo identificado.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en los procedimientos del sistema de gestión de documentación de calidad “Qdoc”, documentos:

MO-SI-01 MANUAL DE FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN
MO-SGP-01 MANUAL DE ROLES Y RESPONSABILIDADES RGPD

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Director de Seguridad de la Información será nombrado por la Dirección General de la empresa, a propuesta del Comité de Gestión de la Seguridad de la Información. El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Gestión de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el mismo comité y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

CIUDAD DE LAS ARTES Y LAS CIENCIAS trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de CIUDAD DE LAS ARTES Y LAS CIENCIAS se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política formarán parte de 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 valoración del análisis de riesgos, el Comité de Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Gestión de la 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.

9. GESTIÓN DOCUMENTAL

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el procedimiento PC-PLC-01 CONTROL DE LA DOCUMENTACIÓN.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de CIUDAD DE LAS ARTES Y LAS CIENCIAS en diferentes materias:

- PSI-SI-01 AUDITORÍA TECNOLÓGICA DE SEGURIDAD DE LA INFORMACIÓN. Define el procedimiento a aplicar para la ejecución y tratamiento de los resultados de auditorías internas de seguridad tecnológica, tanto planificadas como extraordinarias, dentro de CAC, de forma que se garantice permanentemente la integridad, disponibilidad y confidencialidad de los recursos corporativos y la mejora continua de los sistemas de gestión implantados.
- PSI-SI-02 CONTROL DE SISTEMAS EN OPERACIÓN. Describe los mecanismos de control de los sistemas de información en CAC, para garantizar los niveles de calidad y seguridad en su operación diaria adecuados a las necesidades de la organización.
- PSI-SI-03 CALIBRACIÓN. Define de los mecanismos de calibración del sistema de gestión de eventos de CAC, emas, para garantizar su correcto funcionamiento en el entorno de trabajo de la organización.
- PSI-SI-04 CONTROL DE CAMBIOS. Determina de las tareas a realizar para garantizar el control adecuado de los cambios operacionales sobre los activos relacionados con la seguridad de los sistemas de información de CAC; ya que un control incorrecto de dichos cambios es causa habitual de fallos de seguridad o del sistema.
- PSI-SI-05 GESTIÓN DE SOPORTES DE COPIAS DE SEGURIDAD. Define de los mecanismos de gestión de soportes que contienen datos resultantes de realizar las copias de seguridad de los servidores gestionados por el Área de Sistemas.
- PSI-SI-06 GESTIÓN DE INCIDENTES DE SISTEMAS DE INFORMACIÓN. Define de la gestión de incidentes de los sistemas de información, incluidos los específicos de seguridad, que afecten a la información de CAC o a los sistemas que la tratan.
- PSI-SI-07 COPIAS DE RESPALDO Y RECUPERACIÓN. Describe de la metodología a seguir para la realización de copias de respaldo y la restauración de las mismas.
- PSI-SI-08 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS. Describe la metodología a seguir para llevar a cabo la identificación y la autenticación de los usuarios en el entorno de trabajo de CAC.
- PSI-SI-09 CONTROL DE ACCESO LÓGICO. Define de las normativas y líneas de trabajo aplicables para llevar a cabo de forma satisfactoria el control de accesos a los recursos de información corporativos de CAC.
- PSI-SI-11 CONTROL DEL DISEÑO DE APLICACIONES. Especifica las medidas de control asociadas al diseño y desarrollo de aplicaciones orientadas a Internet desarrolladas internamente, así como a las modificaciones posteriores para garantizar que se cumple con todos los requisitos de seguridad.
- PSI-SI-13 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN. Define de los mecanismos necesarios para reaccionar ante interrupciones severas de los sistemas informáticos y de comunicaciones que afecten al negocio de Ciudad de las Artes y las Ciencias con el fin de proteger sus sistemas de información y cualesquiera otros activos frente a grandes fallos o desastres, así como de la prueba, mantenimiento y evaluación de tales mecanismos.

- PSI-SI-14 GESTIÓN DE ÁREAS SEGURAS. Establece la sistemática para la gestión de la seguridad física en los espacios de la Ciudad de las Artes y las Ciencias en los que están ubicados activos pertenecientes al dominio protegible.
- PSI-SI-15 ANÁLISIS DE RIESGOS. Define el procedimiento a aplicar para la realización del Análisis de Riesgos de Seguridad en CAC. Este análisis tiene por objeto la identificación y valoración de amenazas, impactos y riesgos que afectan a los activos del dominio protegible de la organización.
- PSI-SI-16 CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN. Describe la clasificación y el tratamiento de la información corporativa dentro de Ciudad de las Artes y las Ciencias, para garantizar los niveles de seguridad apropiados durante su operación, almacenamiento y tránsito.
- PSI-SI-17 INTERCAMBIO DE INFORMACIÓN. Define los modelos de intercambio de información en CAC, para evitar la degradación de los subestados de seguridad de la información en este proceso.
- PSI-SI-18 GESTIÓN DE ACTIVOS. Describe los mecanismos de operación necesarios para garantizar la seguridad en la entrada y salida de activos de las áreas protegidas de CAC.
- PSI-SI-19 GESTIÓN Y CONTROL DE CAMBIOS DEL SISTEMA DE TICKETING. Define la sistemática a seguir para la gestión y el control de los cambios que conllevan nuevas funcionalidades del sistema de Ticketing, o del software utilizado para el proceso de ventas en la Ciudad de las Artes y las Ciencias.
- PSI-SI-20 GESTIÓN DE MEDIOS EXTRAÍBLES. Define de los mecanismos de gestión de los medios extraíbles para evitar daños a los activos y la interrupción de las actividades de CAC.

La normativa de seguridad estará a disposición de todos los miembros de la empresa, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intraweb de la empresa que se encuentra a disposición de todo el personal de la empresa: http://intraweb.cac.es/politica_ens.pdf

11. OBLIGACIONES DEL PERSONAL

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

Todos los trabajadores de la CIUDAD DE LAS ARTES Y LAS CIENCIAS asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal de la CIUDAD DE LAS ARTES Y LAS CIENCIAS, 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.

12. TERCERAS PARTES

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

Cuando CIUDAD DE LAS ARTES Y LAS CIENCIAS utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad relacionada con 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.

Dirección General

Ciudad de las Artes y las Ciencias