POLÍTICA DE SEGURIDAD

Objeto:

- Misión y objetivos.
- Cumplimiento de los requisitos mínimos de seguridad.
- La seguridad como un proceso integral y mínimo privilegio.
- Vigilancia continua, reevaluación periódica e integridad, actualización del sistema y mejora continua del proceso de seguridad.
- Gestión de personal y profesionalidad.
- Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos.
- Incidentes de seguridad, prevención, detección, reacción y recuperación.
- Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados.
- Diferenciación de responsabilidades, organización e implantación del proceso de seguridad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Protección de la información almacenada y en tránsito y continuidad de la actividad.
- Registro de actividad y detección de código dañino.
- Modelo de gobernanza.
- Procedimientos de designación.
- Resolución de conflictos.
- Instrumentos de desarrollo.
- Terceras partes.
- Proceso de aprobación y revisión.
- Legislación.
- Registros.
- Manifiesto.

IDM Sistemas de Comunicación, S.L. – B96618129
Plaza Poeta Vicente Gaos, 4 bajo 46021 VALENCIA (Spain)
Tel.: 96 369 25 85 - E-mail: administracion@idmsistemas.com

NUEVO ENS

Articulado

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad.

Artículo 12. Política de seguridad y requisitos mínimos de seguridad.

3. Marco organizativo [ORG]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1. Política de seguridad [org. 1]

3.2. Normativa de seguridad [org. 2]

Requisitos.

Se dispondrá de una seria de documentos que describan:

[org.2.1.] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

[org.2.2.] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1 – Documentos específicos.

[org.2. r1.1.] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

3.3. Procedimientos de seguridad [org. 3]

Requisitos

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

- [org.3.1.] Cómo llevar a cabo las tareas habituales.
- [org.3.2.] Quién debe hacer cada tarea.
- [org.3.3.] Cómo identificar y reportar comportamientos anómalos.
- [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:
    a) Su control de acceso.
    b) Su almacenamiento.
    c) La realización de copias.
    d) El etiquetado de soportes.
    e) Su transmisión telemática.
    f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1 – Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

OBJETO:

CAPÍTULO III Política de seguridad y requisitos mínimos de seguridad. Artículo 12. Política de seguridad y requisitos mínimos de seguridad.

El objetivo de este documento es definir la política de seguridad en relación con el Esquema Nacional de Seguridad (ENS) de IDM SISTEMAS DE COMUNICACIÓN.

La Dirección de IDM SISTEMAS DE COMUNICACIÓN, consciente de la necesidad de promover, mantener y mejorar el enfoque hacia el cliente en todas sus actividades, ha implantado un Sistema de Gestión Integrado (SGI), basado en el ESQUEMA NACIONAL DE SEGURIDAD, conforme al estándar cuyo objetivo final es asegurar que entendemos y compartimos las necesidades y metas de nuestros clientes, intentando prestar servicios que cumplan sus expectativas trabajando en la mejora continua.

Manifiesta expresamente su compromiso de potenciar la Seguridad de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, a mantener alta nuestra competitividad en los servicios y productos

MISIÓN Y OBJETIVOS:

[org.1.1] Los objetivos o misión de la organización.

Fomentar la mejora continua de los servicios y soporte al cliente.

Continuar el posicionamiento de IDM SISTEMAS DE COMUNICACIÓN como referente en el sector.

Proporcionar soluciones de software para transformar los datos y la información para ayudar en la toma de decisiones de nuestros clientes.

Proporcionar a los clientes el equipo más profesional y disponer de forma inmediata y durante el tiempo necesario de técnicos altamente cualificados, expertos en las disciplinas requeridas y acostumbrados a trabajar en equipo.

Tener una prestación del servicio basada en nuestro compromiso con la mejora continua de nuestros sistemas, con la seguridad y ciberseguridad de la información como pilar central, y por defecto.

Nuestra misión y objetivos lo conseguiremos a través de:

- Un sistema de objetivos, métricas e indicadores de mejora continua, seguimiento, medición de nuestros procesos internos, así como de la satisfacción de nuestros clientes. Estableciendo y supervisando el cumplimiento de los requisitos contractuales para asegurar un servicio eficaz y seguro.
- Formando y concienciando continuamente a nuestro equipo para tener el mayor grado de profesionalidad y especialización posible, además teniendo nuestras infraestructuras en un estado adecuado y en concordancia con los requerimientos de nuestros clientes.
- Con un procedimiento seguro de gestión de adquisición de productos.
- Cumpliendo las exigencias de la legislación vigente, especialmente con el RGPD y el cumplimiento de nuestra Documentación de Seguridad.
- Introduciendo los procesos de mejora continua que permitan un avance permanente en nuestra gestión de Seguridad de la Información.
- Gestionando y elaborando planes para la gestión y tratamiento de los riesgos con una metodología de análisis y gestión de riesgos utilizada, basada en estándares.
- Gestionando las comunicaciones internas y externas e información almacenada y en tránsito.
- Asegurando la interconexión con otros sistemas de información.
- Gestionando y monitorizando la actividad con la gestión de logs.
- Con especial atención a la gestión de incidentes de seguridad.
- Asegurando la continuidad y disponibilidad del negocio y de los servicios.
- Asegurar que nuestros Activos y Servicios cumplen con las medidas del ENS de Nivel MEDIO para las dimensiones de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.

Así mismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- Física: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información.
- Lógica: Incluyendo los aspectos de protección de aplicaciones, redes, comunicación electrónica y sistemas informáticos.
- Político-corporativa: Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal. [org.1.2]

El objetivo último de la seguridad de la información es asegurar que una organización pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.

g) Diferenciación de responsabilidades

CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD *Artículo 12.*

IDM SISTEMAS DE COMUNICACIÓN, para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

LA SEGURIDAD COMO UN PROCESO INTEGRAL Y MÍNIMO PRIVILEGIO *Artículo 20.*

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a IDM SISTEMAS DE COMUNICACIÓN, estará presidida por este principio.

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

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

1. El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
2. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
3. En un sistema de explotación 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. [org.2.1]
4. 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.

VIGILANCIA CONTINUA, REEVALUACIÓN PERIÓDICA E INTEGRIDAD, ACTUALIZACIÓN DEL SISTEMA Y MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

Artículo 10. Vigilancia continua y reevaluación periódica.

La vigilancia continua por parte de IDM SISTEMAS DE COMUNICACIÓN, permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información

GESTIÓN DE PERSONAL Y PROFESIONALIDAD

Artículo 15. Gestión de personal. Artículo 16. Profesionalidad.

Todo el personal, propio o ajeno relacionado con los sistemas de información de IDM SISTEMAS DE COMUNICACIÓN, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

[org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados

GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS, ANÁLISIS Y GESTIÓN DE RIESGOS

Artículo 14. Análisis y gestión de los riesgos.

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II del Real Decreto 311/2022, de 3 de mayo, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

INCIDENTES DE SEGURIDAD, PREVENCIÓN, DETECCIÓN, REACCIÓN Y RECUPERACIÓN

El IDM SISTEMAS DE COMUNICACIÓN, dispondrá de procedimiento de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 del Real Decreto 311/2022, de 3 de mayo, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación de todos los activos.

EXISTENCIA DE LÍNEAS DE DEFENSA Y PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

IDM SISTEMAS DE COMUNICACIÓN, mantendrá actualizada una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa sea comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de la empresa se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

DIFERENCIACIÓN DE RESPONSABILIDADES, ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

Artículo 11. Diferenciación de responsabilidades.

IDM SISTEMAS DE COMUNICACIÓN, organizará su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas. *[org.1.3].*

AUTORIZACIÓN Y CONTROL DE LOS ACCESOS

Artículo 17

IDM SISTEMAS DE COMUNICACIÓN, implementará mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

PROTECCIÓN DE LAS INSTALACIONES

Artículo 18.

IDM SISTEMAS DE COMUNICACIÓN, implementará mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD
ARTÍCULO 19

Para la adquisición de productos o contratación de servicios de seguridad IDM SISTEMAS DE COMUNICACIÓN, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO Y CONTINUIDAD DE LA ACTIVIDAD

IDM SISTEMAS DE COMUNICACIÓN, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, 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.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

IDM SISTEMAS DE COMUNICACIÓN, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar

actividades indebidas o no autorizadas, permitiendo identificar en cada 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 la empresa, 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, el IDM SISTEMAS DE COMUNICACIÓN, 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.

INFRAESTRUCTURAS Y SERVICIOS COMUNES

IDM SISTEMAS DE COMUNICACIÓN, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de la empresa, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

PERFILES DE CUMPLIMIENTO ESPECÍFICOS Y ACREDITACIÓN DE ENTIDADES DE IMPLEMENTACIÓN DE CONFIGURACIONES SEGURAS

IDM SISTEMAS DE COMUNICACIÓN, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para empresas que sean de aplicación.

Revisión de la política

La revisión de la Política deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión IDM SISTEMAS DE COMUNICACIÓN, en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos.

En relación a las revisiones que puedan realizarse sobre la redacción del texto que constituye la Política, se distinguirán tres tipos de actividades:

- Revisiones periódicas, que se realizarán, al menos, con una periodicidad anual.
- Revisiones sistemáticas: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política. *[org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.*
- Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o que haya causado un impacto en la seguridad de la información IDM SISTEMAS DE COMUNICACIÓN.

MODELO DE GOBERNANZA

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en IDM SISTEMAS DE COMUNICACIÓN, designará roles de seguridad y constituirá un Comité de Seguridad de la información.

ROLES O PERFILES DE SEGURIDAD. *[org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.*

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable de Información: XXX
- Responsable de los Servicios: XXX
- Responsable de Seguridad: XXX
- Responsable del Sistema: XXX
- Responsable de contacto con proveedores: XXX.

RESPONSABILIDADES ASOCIADAS AL ESQUEMA NACIONAL DE SEGURIDAD

[org.3.1] Cómo llevar a cabo las tareas habituales.

[org.3.2] Quién debe hacer cada tarea.

[org.3.3] Cómo identificar y reportar comportamientos anómalos.

[org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS.

FUNCIONES DEL RESPONSABLE DE LA INFORMACIÓN

Proceso de autorización [org.4].

El responsable de la Información será designado por gerencia por un periodo de 2 años. A tal efecto:

1. Determinará los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que él es responsable.
2. Valorará, para cada información contemplada en el análisis de riesgos, las diferentes dimensiones de la seguridad.
3. Aceptará los riesgos residuales, calculados en el análisis de riesgos respecto de la información.

4. Realizará el seguimiento y control de los riesgos con la ayuda del responsable de Seguridad.

FUNCIONES DEL RESPONSABLE DEL SERVICIO

Proceso de autorización [org.4].

El responsable del Servicio será designado por gerencia por un periodo de 2 años. A tal efecto:

1. Realizará, junto a los responsables de la Información y el responsable de Seguridad, los preceptivos análisis de riesgos y seleccionarán las salvaguardas que se han de implantar.
2. Realizará el seguimiento y control de los riesgos, con la participación del responsable de Seguridad.
3. Suspenderá, de acuerdo con el responsable de la Información y el responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

FUNCIONES DEL RESPONSABLE DE SEGURIDAD

Proceso de autorización [org.4].

El responsable de Seguridad será designado por gerencia por un periodo de 2 años.

Tendrá las siguientes funciones:

1. Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
2. Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
3. Impulsar el cumplimiento normativo definido en, así como velar por el mantenimiento de la documentación de seguridad y la gestión de mecanismos de acceso a la misma.
4. Mantener un inventario actualizado de las normas de primer y segundo nivel detalladas, de los nombramientos derivados del procedimiento, así como de los informes de auditorías, autoevaluaciones y análisis de riesgos realizados y de las declaraciones y certificaciones de seguridad.
5. Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
6. Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.
7. Promover la mejora continua en la gestión de la seguridad de la información.
8. Impulsar la formación y concienciación en materia de seguridad de la información.
9. Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
10. Realizar los preceptivos análisis de riesgos y mantenerlos actualizados según la legislación vigente.

11. Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los responsables del Servicio y los responsables de la Información para que adopten las medidas correctoras adecuadas bajo su responsabilidad.

Cualesquiera otras funciones que el Real Decreto 311/2022, de 3 de mayo, asigne a los responsables de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán designarse «responsables de seguridad delegados», dependientes funcionalmente del responsable principal, que serán responsables de las actuaciones que se les deleguen.

FUNCIONES DEL RESPONSABLE DEL SISTEMA

Proceso de autorización [org.4].

El responsable del Sistema, será designado por gerencia por un periodo de 2 años. Será el titular del órgano con competencias en materia de sistemas y tecnologías de la información, y tiene las siguientes funciones:

1. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
2. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
3. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
4. Colaborar en la investigación y resolución de incidentes de seguridad.
5. Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el responsable de dicha información o servicio, según proceda, y con el responsable de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, el responsable del Sistema podrá designar «responsables de sistema delegados», dependientes funcionalmente del responsable principal, que se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. El responsable principal seguirá siendo el responsable final.

[org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

Comité de Seguridad de la Información está compuesto

CEO: Juan Carlos

Refuerzo R1- Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente

1. Responsable de Información: XXX
2. Responsable de los Servicios: XXX
3. Responsable de Seguridad: XXX
4. Responsable del Sistema: XXX
5. Responsable de contacto con proveedores: XXX. (*)

(*) En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

[org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

Informar regularmente del estado de la seguridad de la información al IDM SISTEMAS DE COMUNICACIÓN.

1. Promover la mejora continua del sistema de gestión de la seguridad de la información.
2. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.
3. Elaborar y revisar regularmente la Política y Organización de la Seguridad de la Información, para que sea aprobada por IDM SISTEMAS DE COMUNICACIÓN.
4. Proponer la aprobación de la normativa de seguridad de la información.
5. Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
6. Proponer planes de mejora de la seguridad de la información de la organización.

7. Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información, desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información, que sea requerida tras el cese en la utilización del mismo.
8. Divulgar la Política de Seguridad de la Información y normativas e instrucciones de seguridad de la información aprobadas.

El Comité de Seguridad de la Información de IDM SISTEMAS DE COMUNICACIÓN, se reunirá, con carácter ordinario, una vez al trimestre y podrá reunirse con carácter extraordinario en alguno de los siguientes supuestos:

a) A instancia del CEO.
b) Cuando aparezcan incidencias de seguridad graves o surjan nuevas necesidades de seguridad, que requieran la participación de los componentes del Comité.

PROCEDIMIENTOS DE DESIGNACIÓN

La constitución de los responsables identificados en esta Política y la designación de sus miembros será realizada por gerencia de IDM SISTEMAS DE COMUNICACIÓN, y comunicada a las partes afectadas.

La designación del Comité de Seguridad de la Información será llevada a cabo por el comité de dirección de IDM SISTEMAS DE COMUNICACIÓN, y comunicada a las partes afectadas.

Los roles de seguridad serán revisados cada dos años, en el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

RESOLUCIÓN DE CONFLICTOS

Si hubiera conflicto entre los responsables, será resuelto por el Comité de Seguridad de la Información.

Cuando un sistema al que afecte el Esquema Nacional de Seguridad maneje datos de carácter personal le será de aplicación lo dispuesto en el 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, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en lo que le afecte.

INSTRUMENTOS DE DESARROLLO

[org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

El cumplimiento de los objetivos marcados en esta Política se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se definirá una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

TERCERAS PARTES

Cuando IDM SISTEMAS DE COMUNICACIÓN, preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. IDM SISTEMAS DE COMUNICACIÓN, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que IDM SISTEMAS DE COMUNICACIÓN, lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando IDM SISTEMAS DE COMUNICACIÓN, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad 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. Dicho informe deberá

ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

PROCESO DE APROBACIÓN Y REVISIÓN

Esta Política de Seguridad de la Información ENS es aprobada por el CEO y revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando las circunstancias técnicas u organizativas lo requieran.

LEGISLACIÓN – *[ORG.1.2] EL MARCO LEGAL Y REGULATORIO EN EL QUE SE DESARROLLARÁN LAS ACTIVIDADES.*

La base reguladora que afecta al desarrollo de las actividades y competencias de IDM SISTEMAS DE COMUNICACIÓN, en relación con la prestación de servicios, y que implica la aplicación explícita de medios de seguridad en el sistema de información, está constituida por la legislación:

- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de octubre de 2016, la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Plan Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Oficina de Estado de Función Pública, mediante la cual se aprueba la Instrucción Técnica de Seguridad de auditoría de la seguridad de los sistemas de información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, mediante la cual se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito del Gobierno Electrónico.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico.
- Ley 37/2007, de 16 de noviembre, de reutilización de la información del sector público.

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las redes de comunicaciones electrónicas y comunicaciones públicas.
- Ley 56/2007, de 28 de diciembre, de medidas de promoción de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, de telecomunicaciones generales.
- Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, modificada por la Ley 11/1999, de 21 de abril.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Revisado de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto revisado de la Ley del Estatuto Básico de los Empleados Públicos.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Texto revisado de la Ley de Contratos del Sector Público, aprobada por el Real Decreto Legislativo 3/2011, de 14 de noviembre, y la normativa de desarrollo.
- Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto 203/2021

También forman parte del marco regulatorio las reglas restantes aplicables al gobierno electrónico de IDM SISTEMAS DE COMUNICACIÓN, derivadas de lo anterior y publicadas en la sede electrónica en el ámbito de aplicación de esta Política.

El mantenimiento del marco regulatorio será responsabilidad de IDM SISTEMAS DE COMUNICACIÓN, y permanecerá en un anexo a este documento.

Incluidas, las instrucciones técnicas de seguridad obligatoria, publicadas por resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta de la Comisión Sectorial de Gobierno Electrónico y a iniciativa del Centro Criptológico Nacional (CCN) tal y como establece el "Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad".

Del mismo modo, IDM SISTEMAS DE COMUNICACIÓN, también será responsable de identificar las guías de seguridad del CCN, a las que se hace referencia en el artículo antes mencionado, que serán aplicables para mejorar el cumplimiento de las disposiciones del Esquema de Seguridad Nacional.

Rpble. Información Rpble. Servicios Rpble. Seguridad Rpble. Sistema