Fundación Diagrama

Política de Seguridad de la Información

Fundación Diagrama

Revisión: 1ª
Fecha de aprobación: 9 de enero de 2023

Revisión 2ª
Fecha de aprobación: 30 enero de 2024

Revisión 3ª
Fecha de aprobación: 23 abril de 2024

Política de Seguridad

Fundación Diagrama

Contenido

1. INTRODUCCIÓN

1.1. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundación Diagrama depende 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, confidencialidad, trazabilidad o autenticidad de la información tratada o los servicios prestados.

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, como prestadores de servicio para la administración pública, Fundación Diagrama debe 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 de los sistema de información, seguir y analizar las vulnerabilidades reportadas, y ofrecer una respuesta efectiva a los incidentes de seguridad que puedan producirse, para garantizar la continuidad de los servicios prestados.

La Fundación debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad, de acuerdo con los Artículos 33 y 34 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS).

1.2. ALCANCE

Esta política de seguridad será de obligado cumplimiento para todo el personal que, de manera permanente o eventual, se encuentre vinculado a Fundación Diagrama, siendo aplicable a todos los activos empleados por la misma para la prestación de sus servicios.

2. POLÍTICA DE SEGURIDAD

La Fundación define la presente Política de Seguridad de la Información teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes de seguridad que puedan ocurrir.

Esta Política sienta las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve la organización para desarrollar sus funciones, se realicen bajo garantías de seguridad en sus distintas dimensiones:

- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- Integridad: propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- Confidencialidad: propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- Autenticidad: propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas, los objetivos específicos de la Seguridad de la Información serán:

- Velar por la seguridad de la información como un proceso integral.
- Gestionar formalmente la seguridad sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y aprobar los planes de contingencias y continuidad de la actividad que se definan.
- Realizar una adecuada gestión de incidentes que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes, cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Esta Política de Seguridad:

- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todo el personal y empresas externas que trabajen con los sistemas de información de la Fundación.
- Está escrita a un nivel amplio, por lo que se complementará con documentos más precisos: Normativas de seguridad, ya sean generales o específicas, procedimientos de seguridad y si se considera necesario, también podrán detallarse en instrucciones técnicas tareas específicas.

3. MARCO NORMATIVO

El marco legal en materia de seguridad de la información aplicable a Fundación Diagrama viene establecido por la siguiente legislación:

- Las entidades de derecho privado deberán aplicar el Esquema Nacional de Seguridad en virtud de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público que, en su Disposición Adicional vigésima quinta, establece la condición de encargado del tratamiento a la entidad que contrate con la Administración Pública cuando la contratación implique el acceso del contratista a datos de carácter personal por cuenta de aquella. En consecuencia, cuando la entidad pública contratante esté obligada a aplicar las medidas del Esquema Nacional de Seguridad a los datos de los que fuese responsable, deberá exigir al contratista que vaya a tratar dichos datos la adopción de las correspondientes medidas de seguridad, estableciéndolas como obligación en el correspondiente contrato.
- El Real Decreto 311/2022 de 3 de mayo, por el que se regula el 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,
- 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 (en adelante RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio. De Servicios de Sociedad de la Información y de comercio electrónico.

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, que deroga la Ley 59/2003 de 19 de diciembre, de firma electrónica.
- Reglamento (UE) nº 910/2014: relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 199/93/CE.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- • Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Esado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

La identificación y actualización de la Normativa de seguridad de la información aplicable está desarrollada en el procedimiento de Gestión de la legislación aplicable.

4. PRINCIPIOS BÁSICOS

4.1. SEGURIDAD COMO UN PROCESO INTEGRAL

La Fundación se asegura que la seguridad de la información 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 están identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

4.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

El análisis y la gestión de riesgos están establecidos como elementos esenciales del proceso de seguridad, siendo una actividad continua y permanentemente actualizada.

La gestión de riesgos permite mantener los riesgos identificados dentro de unos niveles aceptables mediante la aplicación de medidas de seguridad, que son proporcionales a la naturaleza de la información, los servicios prestados y los riesgos a los que se exponen.

4.3. PREVENCIÓN

La Fundación evita, o al menos previene en lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello ha implementado 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, están claramente definidos y documentados.

4.4. DETECCIÓN

Dado que los sistemas de información se pueden degradar rápidamente debido a incidentes de seguridad, que van desde una simple desaceleración hasta su detención, la operación está monitorizada de manera continua. De esta forma se pueden detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en el Artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecen mecanismos de detección, análisis y reporte que llegan a las personas responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.5. RESPUESTA

La Fundación:

- Establece mecanismos para responder eficazmente ante incidentes de seguridad, capaces de restaurar la información y servicios que pudieran haberse visto afectados.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes de seguridad detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

4.6. CONSERVACIÓN

Sin perjuicio de los principios establecidos por la Fundación, el Sistema de Información garantiza la conservación de los datos e información en soporte electrónico.

4.7. LÍNEAS DE DEFENSA

La Fundación establece líneas de defensa organizativas, físicas y lógicas que, en caso de incidente de seguridad y alguna de ellas falle, le permiten desarrollar una reacción adecuada y reducir el impacto global, evitando que el sistema de información se vea comprometido en su conjunto.

4.8. VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA

La Fundación vigila de forma continua si se producen comportamientos anómalos, detectando vulnerabilidades o deficiencias de configuración.

Se procede con una reevaluación periódica del estado de seguridad, para revisar la eficacia de las medidas de protección aplicadas y la evolución de los riesgos a los que se encuentran expuestos los activos.

4.9. DIFERENCIACIÓN DE RESPONSABILIDADES

En la presente Política se determinan las funciones y responsabilidades en los sistemas de información de la Fundación conforme a los criterios definidos por el ENS, estableciendo las específicas de cada rol requerido, así como los mecanismos de coordinación y resolución de conflictos, en caso de producirse.

5. REQUISITOS MÍNIMOS

La política de seguridad de Fundación Diagrama se desarrolla aplicando los siguientes requisitos mínimos:

5.1. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

La seguridad compromete a todas las personas que forman parte de la organización, es compromiso y debe ser conocida por todos y todas. Están definidos las personas responsables que velan por dicho cumplimiento.

5.2. ANÁLISIS Y GESTIÓN DE RIESGOS

El análisis de riesgos es un proceso que comprende la identificación de activos, las vulnerabilidades y amenazas a las que se encuentran expuestos así como, su probabilidad de ocurrencia y el impacto de las mismas.

Fundación Diagrama realiza un análisis de riesgos a todos los sistemas sujetos a esta Política evaluando las vulnerabilidades y amenazas a los que están expuestos.

Para llevar a cabo esta acción, Fundación Diagrama sigue la metodología Magerit, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

El proceso de análisis de riesgos está definido en el procedimiento de Análisis de riesgos y sigue básicamente el siguiente esquema:

1. Definición del Alcance
2. Identificación de activos
3. Identificación de amenazas
4. Identificación de salvaguardas
5. Evaluar el riesgos
6. Plan de tratamiento de riesgos.

Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información gestionada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

5.3. GESTIÓN DE PERSONAL

Los diferentes roles de Seguridad de la información vienen representados en el siguiente esquema:

Todo el personal de la organización tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a todas las personas afectadas.

Se establecerá un programa de formación y concienciación continua para atender a todo el personal, en particular a los de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas reciben 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 que intervenga en los procesos de la organización, constituyendo su incumplimiento la correspondiente infracción laboral sancionable en virtud a lo dispuesto en el régimen sancionador del convenio colectivo que resulta de aplicación. Del mismo modo, la presente Política de Seguridad Política de Seguridad será de obligado cumplimiento para todo personal externo que pueda intervenir en los procesos de organización, constituyendo su incumplimiento una infracción grave que facultará a esta entidad para resolver la relación contractual que le une.

5.4. PROFESIONALIDAD

La seguridad de la información es gestionada por personal cualificado y con unos niveles idóneos de gestión y madurez en los servicios prestados.de vacante.

5.5. AUTORIZACIÓN Y CONTROL DE ACCESOS

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación del ENS está limitado a las personas usuarias de los sistemas de información, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

5.6. PROTECCIÓN DE LAS INSTALACIONES

Los sistemas de información y su infraestructura de comunicaciones asociada se encuentra en áreas controladas y dispone de mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

5.7. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación del ENS, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, siempre que sea posible y, en caso contrario, se adoptarán las medidas compensatorias necesarias para asegurar el cumplimiento con el ENS.

5.8. MÍNIMO PRIVILEGIO

Los sistemas de información de Fundación Diagrama están diseñados y configurados otrorgando los mínimos privilegios necesarios para su correcto desempeño.

5.9. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

La inclusión o modificación de cualquier elemento físico o lógico en el inventario de activos del sistema, requerirá autorización formal previa conforme al procedimiento de autorizaciones y se llevará a cabo conforme al procedimiento de paso a producción.

Los sistemas de información serán monitorizados y evaluados de forma permanente con el fin de detectar errores de configuración, vulnerabilidades o la detección temprana de incidentes, que serán tratados conforme a los procedimientos de Mantenimiento de HW/SW, gestión de incidentes de seguridad y gestión de cambios.

5.10. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Se presta especial atención a la información almacenada o en tránsito a través cualquier tipo de soporte o red de comunicación, que se protegerá mediante los procedimientos que le sean de aplicación, en especial aquellos que traten la gestión de soportes y el cifrado de las comunicaciones.

Se garantizará la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información mediante la aplicación de procedimiento de gestión de copias de seguridad.

Toda información en soporte no electrónico se protegerá con el mismo grado de seguridad que la información en soporte electrónico. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas y procedimientos que resulten de aplicación.

5.11. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas,

reforzándose las tareas de prevención, detección y respuesta ante 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 los procedimientos correspondientes, que incluirán, entre otros, la gestión de autorizaciones, el control de acceso, el cifrado de las comunicaciones, la gestión de cambios o los pasos a producción según sea de aplicación.

5.12. REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

En Fundación Diagrama cada persona usuaria de los sistemas de información está identificada de forma única, de modo que se sabe en todo momento quien recibe derechos de acceso, de qué tipo y quien ha realizado una determinada actividad.

Se registran las actividades de las personas usuarias de los sistemas de información, 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.

Se analizarán las comunicaciones entrantes o salientes 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 ataques de denegación de servicio, evitar la distribución malintencionada de código dañino, así como otros daños derivados de un acceso no controlado.

5.13. INCIDENTES DE SEGURIDAD

Se deberá evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

Fundación Diagrama dispone de procedimientos de gestión de incidentes de seguridad que garantizan una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

Se dispone de mecanismos adecuados de detección, criterios de clasificación, procedimientos de análisis y resolución, así como cauces de comunicación a las partes interesadas y registro de las actuaciones.

El registro de incidentes se empleará para la mejora continua de la seguridad del sistema.

5.14. CONTINUIDAD DE LA ACTIVIDAD

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

5.15 MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

El sistema de gestión de seguridad de la información implantado es actualizado y mejorado siguiendo el Ciclo de mejora Continua "Plan- Do - Check - Act".

Para la mejora continua del proceso de seguridad se tienen en cuenta las conclusiones de informes de auditoría periódicos, los análisis periódicos de métricas e indicadores, No conformidades, incidentes de seguridad, etc.

De forma periódica el Responsable de seguridad y el Responsable del Sistema analizan toda la información para elaborar planes de mejora que serán aprobados en el comité de Seguridad.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. ROLES, FUNCIONES Y RESPONSABILIDADES

6.1.1. RESPONSABLE DE LA INFORMACIÓN

- Determinar los niveles de seguridad en cada dimensión y establecer 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.
- Ser el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad, de integridad, trazabilidad o autenticidad.
- Velar por el buen uso uso que se haga de una cierta información y, por tanto, de su protección.
- Aceptar, junto al Responsable del Servicio, los riesgos residuales calculados en el análisis de riesgos. Esta tarea podrá delegarla, de acuerdo con la persona Responsable del Servicio, en la persona Responsable de Seguridad de la Información y la persona Responsable del Sistema.
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los tratamientos de 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.

6.1.2. RESPONSABLE DEL SERVICIO

- Determinar los niveles de seguridad en cada dimensión del servicio.
- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Velar por el buen uso de determinados servicios de los Sistemas de Información y, por tanto, de su protección.
- Es el/la responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios de los Sistemas de Información.
- Aceptar, junto a la persona Responsable de la Información, los riesgos residuales calculados en el análisis de riesgos. Esta tarea podrá delegarla, de acuerdo con la persona Responsable de la Información, en la persona Responsable de Seguridad de la Información y la persona Responsable del Sistema.

6.1.3. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de Seguridad de la Información (en adelante, "SGSI") cumple con los requisitos del Esquema Nacional de Seguridad.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los/las Responsables de la Información y los Servicios, conforme a lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas, así como otras medidas de seguridad adicionales.
- Promover las actividades de formación y concienciación en materia de seguridad de la información.
- Elaborar, junto con la persona Responsable del Sistema, los planes de mejora de Seguridad de la información.
- Coordinación y seguimiento de la implantación de los proyectos de adecuación al ENS, en colaboración con la persona Responsable del Sistema.

- Realizar, en colaboración con el/la Responsable del Sistema, los preceptivos análisis de riesgos, seleccionar las salvaguardas a implantar y revisar el proceso de gestión del riesgo. A instancias de la persona Responsable de la Información y los Servicios, podrá ser consultado sobre los niveles de riesgos residuales a aceptar, calculados en el análisis de riesgos.
- Aprobar los procedimientos operativos e instrucciones técnicas de Seguridad de la Información.
- Promover la realización de auditorías periódicas de seguridad, 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 la persona Responsable del Sistema, al Responsable de la Información y los Servicios, para que adopten las medidas correctoras adecuadas.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema, conforme estipulado en Art, 28 y Anexo II del ENS.
- Elaborar informes periódicos de seguridad, que incluyan los incidentes de seguridad más relevantes en cada periodo, en colaboración con el/la Responsable del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse, de acuerdo con el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la Información y los Servicios
- Colaborar estrechamente con el/la Delegado/a de Protección de Datos, en relación a las obligaciones y disposiciones del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD GDD).
- Participar en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información y la Normativa de seguridad.

Como Secretario/a del Comité de Seguridad de la Información le corresponde:

- 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.
- Es responsable de la ejecución directa o delegado de las decisiones del Comité.

6.1.4. RESPONSABLE DEL SISTEMA

- 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 tipología 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.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Hacer seguimiento del ciclo de vida de los Sistemas: especificación, arquitectura, desarrollo, operación, cambios, etc.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con la persona Responsable de Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- 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/la Responsable de dicha Información o servicio, y con el/la Responsable de Seguridad de la Información.

- Elaborar, en colaboración con la persona Responsable de Seguridad de la Información, la documentación de seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente, o ante incidentes de seguridad relevantes, a la persona Responsable de Seguridad de la Información junto a los responsables de la información y el servicio.
- Elaborar los Planes de Continuidad del Sistema, para que sean validados por el/la Responsable de Seguridad de la Información y coordinados y aprobados por el Comité de Seguridad de la Información.
- Elaborar, junto con el/la Responsable de Seguridad planes de mejora de Seguridad.
- En caso de Incidentes de Seguridad de la información:
  - Planificará la implantación de las salvaguardas en el sistema.
  - Ejecutará el plan de seguridad aprobado.
- Este rol no podrá coincidir con el de Responsable de la Información, Responsable del Servicio, ni con el de Responsable de Seguridad de la Información.

6.1.5. ADMINISTRADOR/A DE LA SEGURIDAD DEL SISTEMA

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a las personas usuarias del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar, junto con el/la Responsable del Sistema, el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a las personas Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Se ha creado el Comité de Seguridad de la Información que está compuesto por los siguientes miembros:

PRESIDENCIA: Presidente del Consejo de Dirección de la Fundación Diagrama.

SECRETARIO/A: Responsable de Seguridad de la Información.

VOCALES:

- Responsable del Servicio
- Responsable de la Información
- Delegada/o de Protección de Datos
- Responsable del Sistema

(se incorporarán durante el proceso de implantación)

- Dirección del área de Gestión de Personas
- Responsable de Seguridad Física de las Instalaciones
- Coordinación del área Económica y Financiera

Podrán acudir a requerimiento del Comité cualesquiera otros responsables de recursos o áreas y responsables cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por el RGPD.

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

- Atender las inquietudes del Patronato y de los diferentes recursos de la Organización.
- Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de la Entidad 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 el Patronato.
- Aprobar la normativa de seguridad de la información.
- Elaborar y acordar los requisitos de formación y cualificación del personal de los sistemas de información y personal trabajador desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Entidad 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 la Entidad. 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.
- Impulsar el cumplimiento y difusión de la Política de Seguridad de la Información, promoviendo las actividades de formación y concienciación en materia de seguridad para el personal de la organización.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes personas 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 acerca 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.

En caso de ocurrencia de incidentes de seguridad de la información:

- Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente.

- La toma de decisiones en materia de seguridad se realiza en el seno del Comité de Seguridad, elevando al Consejo de Dirección aquellos asuntos en los que exista conflicto o éste no tenga suficiente autoridad para decidir.

6.3. JERARQUÍA EN EL PROCESO DE DECISIONES Y RESOLUCIÓN DE CONFLICTOS

Los diferentes roles de Seguridad de la información vienen representados en el siguiente esquema:

6.4. PROCEDIMIENTOS DE DESIGNACIÓN DE PERSONAS

La creación del Comité de Seguridad, así como la designación de sus miembros y de la estructura de Seguridad de la información, es designada y aprobada por el Consejo de Dirección en reunión ordinaria.

El Consejo de Dirección nombrará, por tanto:

- Al Responsable de la Información; pudiendo ser éste un cargo unipersonal o un órgano colegiado.
- Al Responsable del Servicio; pudiendo ser el mismo que el Responsable de la Información; del mismo modo podrá ser un cargo unipersonal o un órgano colegiado.
- Al Responsable de la Seguridad.
- Al Responsable del Sistema,
- Al Administrador de Seguridad del Sistema a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

Estos nombramientos se revisarán cada 2 años o cada vez que alguno de los puestos quede vacante.

7. DATOS DE CARÁCTER PERSONAL

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y las correspondientes personas responsables y encargadas del tratamiento,

así como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos. Todos los sistemas de información 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 Registro de Actividades del Tratamiento.

7.1. FIGURAS VINCULADAS A PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

7.1.1. DELEGADO/A DE PROTECCIÓN DE DATOS

Fundación Diagrama cuenta con una Delegada de Protección de Datos, debidamente inscrita en la Agencia Española de Protección de Datos, que llevará a cabo las tareas establecidas en el artículo 39 del Reglamento (UE) 679/2016 y los artículos 36 y 37 de la Ley Orgánica 3/2018, así como las que se deriven de la normativa de aplicación en materia de privacidad y protección de datos de carácter personal y de los documentos de buenas prácticas que se adopten por la propia AEPD, en su condición de autoridad de control, o por el Comité Europeo de Protección de Datos.

La delegada de protección de datos desempeñará su labor prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento y, como mínimo, tendrá las siguientes funciones:

a. informar y asesorar a la persona responsable o encargada del tratamiento y a las personas empleadas que se ocupen del tratamiento de datos de las obligaciones que les incumben en materia de protección de datos personales;

b. supervisar el cumplimiento de la legislación aplicable y de las políticas de la persona responsable o encargada del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c. ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;

d. mantener el contacto con las personas interesadas;

e. mantener las relaciones con las autoridades de supervisión y control y, más concretamente, actuar como punto de contacto con la Agencia Española de Protección de Datos en las cuestiones relativas al tratamiento, realizar las consultas preceptivas y cooperar con ella en todo lo necesario.

Además de estas funciones genéricas, la DPD efectuará las tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
2. Identificación de las bases jurídicas de los tratamientos.
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
4. Definición de los plazos de conservación para los datos y existencia de procedimientos correctos para su destrucción cuando corresponda.
5. Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
6. Diseño e implantación de medidas de información a las personas afectadas por los tratamientos de datos.
7. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los/as interesados/as.
8. Valoración de las solicitudes de ejercicio de derechos por parte de las personas interesadas.
9. Contratación de encargados/as de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado/a.

10. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
11. Diseño e implantación de políticas de protección de datos.
12. Revisión de los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección.
13. Establecimiento y gestión de los registros de actividades de tratamiento.
14. Revisar y validar los análisis de riesgos de los tratamientos realizados.
15. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
16. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
17. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
18. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los/a afectados/as y los procedimientos de notificación a las autoridades de supervisión y a las personas afectadas, cuando se requiera.
19. Implantación de programas de formación, concienciación y sensibilización de personas usuarias del personal en materia de protección de datos.
20. Reportar periódicamente al Comité de Seguridad de la Información sobre el estado de cumplimiento en la materia y las acciones que haya que acometer, así como reportar ante incidencias y circunstancias relevantes.

7.1.2. PERSONAL CON ACCESO A DATOS

Todo el personal de la entidad está sujeto a funciones y obligaciones en materia de protección de datos de carácter personal adoptando para ello las medidas técnicas y organizativas que sean necesarias para garantizar su seguridad. Todo el personal de la entidad que disponga de acceso a los datos de carácter personal debe cumplir lo previsto en la presente política, así como en las normas y procedimientos que la desarrollen. Asimismo:

- Se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión del deber de la persona trabajadora.
- Se responsabilizará de seguir las normas de seguridad descritas en el documento "Normas de Seguridad de la Información".

7.1.3. RESPONSABLE DEL TRATAMIENTO

El/la Responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

Las funciones de la persona Responsable del tratamiento son:

- 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.
- Deberá cesar en la utilización o cesión ilícita de los datos cuando así lo requiera la persona interesada.
- Deberá informar a los/las titulares de los datos los derechos que les asisten y en los términos en los que pueden ejercerlos.

- Obligación de hacer efectivos los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición al tratamiento de las personas interesadas en el plazo máximo de 1 mes.
- Notificar las rectificaciones o cancelaciones efectuadas en los datos personales a quien se haya comunicado dichos datos, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

7.1.4. ENCARGADO/A DEL TRATAMIENTO

El/la Encargado/a de Tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta de la persona responsable del tratamiento.

Las personas encargadas del tratamiento tienen como misión realizar las tareas ordinarias para el desarrollo efectivo de las funciones para las que ha sido creado el tratamiento por cuenta de la persona Responsable del tratamiento y deberá aplicar 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.

Igualmente deberá implementar las medidas de seguridad a que se refiere el párrafo anterior y que aparecerán estipuladas en el contrato de encargo suscrito con la persona Responsable del Tratamiento.

En concreto, sus funciones son las de:

- Tratar los datos del tratamiento.
- Realizar el control de tratamiento, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a las adiciones y cancelaciones.
- Controlar los soportes de seguridad.
- Control y acceso de contraseñas.
- Mantenimiento del registro de incidencias.
- Crear una lista para las situaciones en la que una persona afectada no desee que sus datos personales se almacenen en el tratamiento.
- Dar traslado a la persona responsable del tratamiento de aquellas solicitudes de ejercicio de derecho que se reciban por parte de los/las interesados/as.

7.2. CONDICIÓN DE FUNDACIÓN DIAGRAMA COMO ENTIDAD RESPONSABLE / ENCARGADA DEL TRATAMIENTO

Fundación Diagrama podrá actuar como entidad Responsable o Encargada del Tratamiento en función de la condición por la cual desarrolla los servicios prestados, es decir, dependiendo de si realiza el servicio en nombre propio (siendo considerada Responsable) o por cuenta de otra entidad -pública o privada- (siendo considerada en este caso Encargada).

En los casos en que se atribuya a Fundación Diagrama la condición de Responsable de Tratamiento de los datos de carácter personal, que obran en sus sistemas de información, y que derivan de la prestación de los servicios que realiza, cabe decir que la consideración de Responsable de Tratamiento no debe ser asociada a persona física representante de la Fundación, en calidad del cargo o puesto (como, por ejemplo, el Vicepresidente o Secretario).

A estos efectos, Fundación Diagrama deberá llevar a cabo un registro actualizado donde se identificarán:

- Cuando actúa como entidad Responsable: Los/las encargados/as de tratamiento que están prestando servicios en la Entidad, así como la indicación de la formalización del pertinente contrato con estos/as prestadores/as de servicios con acceso a datos.
- Cuando actúa como entidad Encargada: Los/las responsables de tratamiento con los que tiene suscrito el correspondiente contrato, convenio o acuerdo.

8. RIESGOS QUE DERIVAN DEL TRATAMIENTO DE DATOS PERSONALES

Dentro de la responsabilidad proactiva de Fundación Diagrama, se encuentra la gestión y el análisis de los riesgos para los derechos y libertades de los interesados aplicable a cualquier tratamiento de datos de carácter personal, así como la realización de las correspondientes Evaluaciones de Impacto cuando sean necesarias para una adecuada protección de los datos de categorías especiales en tratamientos de alto riesgo.

El procedimiento general para llevarlo a cabo se desarrolla en la Política de Protección de Datos de Fundación Diagrama y se concreta en cada uno de los informes que se pueden generar para cada tratamiento.

9. TERCERAS PARTES

Cuando se presten servicios o se gestione información de otras organizaciones, 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 para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

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

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe de la persona responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por parte de las personas responsables de la información y los servicios afectados antes de seguir adelante.

10. DESARROLLO, REVISIÓN Y APROBACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

La gestión de la documentación de Seguridad de la información se realiza siguiendo el procedimiento PSCA-01 Control de la Información Documentada.

En este procedimiento se establecen la sistemática y responsabilidades para la elaboración, identificación, control, distribución, revisión, actualización y aprobación de los soportes que constituyen la estructura documental de Fundación Diagrama en general, donde se incluye la documentación de seguridad de la información.

Esta estructura documental es piramidal, situándose en el extremo superior las Políticas de Fundación Diagrama.

En el caso concreto de seguridad de la información, encontramos la Política de Seguridad de la Información que se cumplimentará con documentos más precisos que ayudan a llevar a cabo lo propuesto. Para ello se utilizarán

- Normas de seguridad.
- Procedimientos de seguridad.
- Instrucciones de Seguridad.

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de las personas usuarias. Son de carácter obligatorio.

Los procedimientos de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las instrucciones son descripciones muy detalladas de tareas concretas de un procedimiento.

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.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el Patronato de la Fundación, de acuerdo con el artículo 12 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11. GLOSARIO DE TÉRMINOS

Activo

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Administrador de la seguridad del sistema (ASS)

Administrador de la seguridad del sistema (ASS): Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad.

Amenaza

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Autenticidad

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. ENS.

Categoría de un sistema

Categoría de un sistema: Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Confidencialidad

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Control (Controles)

Mecanismo o procedimiento que evita, previene, o detecta un riesgo.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables.

Declaración de Aplicabilidad

Es el documento, en el ámbito del ENS, en el que se formaliza la relación de medidas de seguridad que resultan de aplicación al sistema de información de que se trate, conforme a su categoría.

Disponibilidad

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Dimensiones de seguridad

Cada una de las magnitudes que se tendrán en cuenta para establecer la categoría de seguridad de un sistema de información. En el marco del ENS se establecen las siguientes dimensiones de seguridad: Confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad.

Gestión de incidentes

Actuaciones realizadas para atender y resolver un incidente de seguridad. En la gestión de incidentes, se establecerán, además, medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Integridad

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada

Medidas de Seguridad

Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Minimo privilegio

Principio según el cual los sujetos deben acceder exclusivamente a aquellos objetos que precisen inexcusablemente para ejecutar sus trabajos o procesos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de Seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Persona encargada de velar por la seguridad de la información de la organización. Su labor consiste en estar al día de la evolución tecnológica en la medida en que afecta a la seguridad de la infor-

mación, estableciendo puentes entre el responsable de seguridad corporativa y los responsables de tecnología.

Responsable de Servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del Sistema

Persona que tiene la potestad de establecer los re-
Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar,

Trazabilidad

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Vulnerabilidad

Una debilidad que puede ser aprovechada por una amenaza.

www.fundaciondiagrama.es